

TOWARDS AN INTEROPERABILITY FRAMEWORK FOR BLOCKCHAIN IN THE BANKING SECTOR

by

Senate Sylvia Mafike
12180352

Submitted in fulfilment of the requirements for the degree
Doctor of Philosophy (Information Technology)

in the

**FACULTY OF ENGINEERING, BUILT ENVIRONMENT AND INFORMATION
TECHNOLOGY**

at the

UNIVERSITY OF PRETORIA

Supervisor:
(Professor Tendani Mawela)

Date of submission
(28 March 2024)

Declaration regarding Plagiarism

The Department of Informatics emphasises integrity and ethical behaviour with regard to the preparation of all written assignments.

Although the lecturer will provide you with information regarding reference techniques, as well as ways to avoid plagiarism, you also have a responsibility to fulfil in this regard. Should you at any time feel unsure about the requirements, you must consult the lecturer concerned before submitting an assignment.

You are guilty of plagiarism when you extract information from a book, article, web page or any other information source without acknowledging the source and pretending that it is your own work. This doesn't only apply to cases where you quote verbatim, but also when you present someone else's work in a somewhat amended (paraphrased) format or when you use someone else's arguments or ideas without the necessary acknowledgement. You are also guilty of plagiarism if you copy and paste information directly from an electronic source (e.g., a website, e-mail message, electronic journal article, or CD-ROM), even if you acknowledge the source.

You are not allowed to submit another student's previous work as your own. You are furthermore not allowed to let anyone copy or use your work with the intention of presenting it as his/her own.

Students who are guilty of plagiarism will forfeit all credits for the work concerned. In addition, the matter is referred to the Committee for Discipline (Students) for a ruling. Plagiarism is considered a serious violation of the University's regulations and may lead to your suspension from the University. The University's policy regarding plagiarism is available on the Internet at <http://upetd.up.ac.za/authors/create/plagiarism/students.htm>.

I (full names and surname):	SENATE SYLVIA MAFIKE
Student number:	12180352

Declare the following:

1. I understand what plagiarism entails and am aware of the university's policy in this regard.
2. I declare that this assignment is my own, original work. Where someone else's work was used (whether from a printed source, the internet or any other source) due acknowledgement was given and reference was made according to departmental requirements.
3. I did not copy and paste any information directly from an electronic source (e.g., a web page, electronic journal article or CD-ROM) into this document.
4. I did not make use of another student's previous work and submitted it as my own.
5. I did not allow and will not allow anyone to copy my work with the intention of presenting it as his/her own work.



28 March 2024

Signature

Date

TOWARDS AN INTEROPERABILITY FRAMEWORK FOR BLOCKCHAIN IN THE BANKING SECTOR

ABSTRACT

Banking enterprises globally are considering the adoption and leveraging of the benefits of blockchain technology to enhance their processes. Most of these organisations seek ways to integrate blockchain into incumbent technologies to augment and support such systems. However, incompatibilities between different blockchain systems and extant banking systems mean that these systems cannot communicate as required. This lack of interoperability between heterogeneous blockchain systems and between blockchain systems and other non-blockchain systems is referred to as a lack of blockchain interoperability. An absence of blockchain interoperability is one of the obstacles to the mass adoption of the technology and, consequently, an obstacle to organisations wishing to leverage the technology to provide better, cost-effective and more efficient processes. Therefore, it is crucial for organisations to address blockchain interoperability. However, organisations do not currently have the appropriate tools, methods or frameworks to guide the complex process of implementing blockchain interoperability.

This study is underpinned by the pragmatist philosophical paradigm and employs a design science research approach to address the blockchain interoperability challenge by developing and evaluating a blockchain interoperability framework. This qualitative study solicited data through systematic literature reviews, interviews with blockchain experts and industry webinars. The data were used to formulate an artefact, i.e., the blockchain interoperability framework intended to guide banking organisations during the process of implementing blockchain interoperability. The framework components were conceptualised and organised through a general system theory lens.

Following the design science process, the proposed framework was evaluated through a summative, artificial and *ex-post* evaluation process, which included demonstrating the applicability of the framework and evaluating its utility and relevance. The applicability of the framework to the banking sector is demonstrated through an illustrative scenario. The

scenario was derived from real projects focusing on the integration of real-time gross settlement systems and a blockchain system. Moreover, to evaluate the framework, the study conducted additional interviews with blockchain experts. These interviews were guided by a set of questions based on predefined artefact evaluation criteria.

The main output of the study is the proposed blockchain interoperability framework. The framework includes a high-level architectural component framework, a process flow and a set of guidelines and considerations for organisations. Practitioners and researchers can use the framework components as a reference point to understand and guide the process of implementing blockchain interoperability. The key findings represented in the framework are organised according to general systems theory elements. The findings indicated that the following aspects should be considered to implement blockchain interoperability in the banking sector: legal and regulatory requirements for interoperability, a clear blockchain-focused use case or business case, an understanding of the goal of blockchain in the organisation, a determination of the systems involved, and determining the type of interoperability required for the selected use case. In addition, the organisation needs to consider the data to be shared. This involves identifying the type of data to be shared (normal business data, cryptocurrency or tokenised assets); the data formats, representations and standards, and identifying any inconsistencies in how the data are represented across the systems. Furthermore, the findings show that banking organisations should ensure the selected approach fulfils the required interoperability and enables the exchange of the necessary data while satisfying essential regulatory, security, privacy, and performance requirements.

The study makes several contributions. From a theoretical perspective, the study offers an extended conceptualisation of blockchain interoperability for the banking sector. The study has expanded on the currently limited research on blockchain interoperability and contributes to opening opportunities for further academic research on the topic. Methodologically, the study offers insights on how Peffers' (2007) design science research methodology and the general systems theory could be utilised to interrogate blockchain interoperability as a nascent topic and support the development of a blockchain interoperability framework. Practically, practitioners and banking organisations with an

interest in enabling blockchain interoperability in their operations can use the developed framework, process flow and guidelines as a point of reference.

Keywords: blockchain, banking, blockchain interoperability, design science research

DEDICATION

To my son:

Tshele Molati

Mosia, always remember to go for your dreams!

ACKNOWLEDGEMENTS

I would like to extend my sincere gratitude to everyone who supported me throughout this journey. I am particularly grateful to The Almighty God for His divine mercies, provisions and grace that carried me this far.

To my wonderful supervisor, Professor Tendani Mawela, words cannot express how grateful I am for your continued support, patience, motivation, guidance and insights. Without your mentorship and guidance, this study would not have been possible.

To my mum, Motseoa Rosina 'Masenate Mafike. Thank you, Letebele, for being my pillar of strength, my sounding board and my voice of reason. Your unwavering support and wisdom kept me going through this journey.

To my family and friends, thank you for your continued support and prayers.

Thank you to the University of Pretoria and the Department of Informatics for awarding me with a Postgraduate Bursary, which allowed me to complete my studies.

Lastly, to all the respondents, thank you for sharing your experiences and knowledge. Your contributions were invaluable in making this study a success.

TABLE OF CONTENTS

CHAPTER 1	1
1 INTRODUCTION	1
1.1 BACKGROUND INFORMATION	1
1.2 CONTEXT OF THE STUDY	3
1.3 PROBLEM STATEMENT	4
1.4 PURPOSE OF THE STUDY	6
1.4.1 Aim	7
1.4.2 Objectives:	7
1.5 RESEARCH QUESTIONS	7
1.6 DELIMITATIONS	8
1.7 STUDY CONTRIBUTION	8
1.8 BRIEF CHAPTER OVERVIEW	10
CHAPTER 2	13
2 LITERATURE REVIEW	13
2.1 INTRODUCTION	13
2.2 BLOCKCHAIN OVERVIEW	14
2.2.1 Blockchain technology	14
2.2.2 Characteristics of Blockchain	15
2.2.3 Types of Blockchain	17
2.2.4 Consensus mechanisms	19
2.3 INTEROPERABILITY OF INFORMATION SYSTEMS	21
2.3.1 Types of interoperability	21
2.4 BLOCKCHAIN INTEROPERABILITY	23
2.4.1 Types of blockchain interoperability	25
2.4.2 Blockchain Interoperability Goals	26
2.5 BLOCKCHAIN USE CASES AND APPLICATIONS	29
2.5.1 Real Industry Use Cases of Blockchain	29
2.5.2 Blockchain Use Cases in Finance and Banking	30
2.6 CONTEXTUALISING BLOCKCHAIN INTEROPERABILITY IN BANKING	32
2.6.1 Interoperability in the Banking Sector	32
2.6.2 Blockchain Interoperability in the Banking Sector	33
2.6.3 Blockchain Interoperability Studies	34
2.7 SUMMARY	41
CHAPTER 3	43
3 METHODOLOGY	43

3.1	INTRODUCTION	43
3.2	RESEARCH PHILOSOPHY.....	44
3.3	PHILOSOPHICAL PARADIGMS	45
3.3.1	Positivism	45
3.3.2	Interpretivism.....	46
3.3.3	Pragmatism	47
3.3.4	Critique of Pragmatism.....	49
3.4	RESEARCH STRATEGY: DESIGN SCIENCE RESEARCH (DSR)	52
3.4.1	An Overview of Design Science	52
3.4.2	Design Science Research Contribution.....	53
3.4.3	The DSR process and its application in this study	55
3.5	RESEARCH APPROACH.....	60
3.5.1	Overview of the Cognitive Process in Research	60
3.5.2	The Cognitive Process for this Study	62
3.6	METHODOLOGICAL CHOICE: QUALITATIVE METHODS.....	62
3.7	TIME FRAME.....	64
3.8	DATA COLLECTION TECHNIQUES.....	64
3.8.1	Systematic Literature Review	65
3.8.2	Interviews	66
3.8.3	Webinars	68
3.9	SAMPLING TECHNIQUES.....	69
3.9.1	Target Population	69
3.9.2	Sampling Method	69
3.9.3	Summary of the Data Collection.....	70
3.9.1	Sample Size	71
3.10	DATA ANALYSIS TECHNIQUES	71
3.10.1	Analysis of the Systematic Literature Review Data	72
3.10.2	Analysis of the Interview Data	72
3.10.3	Analysis of Webinar Data	73
3.11	RESEARCH RELIABILITY AND VALIDITY	73
3.11.1	Internal Validity.....	74
3.11.2	External Validity	75
3.11.3	Reliability.....	75
3.12	ETHICS CONSIDERATIONS	75
3.12.1	Ethical Clearance	76
3.12.2	Informed Consent.....	76
3.12.3	Anonymity, Confidentiality and Protection from Harm	76
3.13	SUMMARY	77
CHAPTER 4.....		78
4	THEORETICAL FRAMEWORK.....	78

4.1	INTRODUCTION	78
4.2	THE ROLE OF THEORY IN IS RESEARCH	79
4.2.1	Types of Theories in IS Research	80
4.3	ORGANISATIONAL ADOPTION OF TECHNOLOGY INNOVATION	81
4.3.1	Diffusion of Innovation Theory.....	82
4.3.2	Technology, Organisation and Environment Framework	84
4.4	INTEROPERABILITY FRAMEWORKS	87
4.4.1	ATHENA Interoperability Framework	88
4.4.2	Enterprise Interoperability Framework	90
4.4.3	European Interoperability Framework	91
4.4.4	European interoperability framework application.....	94
4.5	INTRODUCTION TO THE GENERAL SYSTEMS THEORY APPLIED IN THIS STUDY	94
4.5.1	Open and Closed Systems.....	95
4.5.2	General Concepts in Systems Theory.....	97
4.5.3	The Rationale for Selecting Systems Theory	99
4.5.4	Systems Theory Application.....	101
4.5.5	Criticism of Systems Theory.....	101
4.5.6	Overview of Selected Theories and Models	102
4.6	SUMMARY	102
CHAPTER 5.....		104
5	PROBLEM AWARENESS (A SYSTEMATIC LITERATURE REVIEW)	104
5.1	INTRODUCTION	104
5.2	SYSTEMATIC LITERATURE REVIEW	105
5.2.1	Planning: Identification and need for review	106
5.2.2	Planning: Development of a Review Protocol	107
5.2.3	Conducting the Review: Identification of Research	107
5.2.4	Selection of primary studies	109
5.2.5	Study Quality Assessment	111
5.2.6	Data Extraction and Synthesis	113
5.2.7	Data Synthesis (Results).....	113
5.3	SUMMARY	121
CHAPTER 6.....		123
6	OBJECTIVES OF A SOLUTION (A SYSTEMATIC LITERATURE REVIEW).....	123
6.1	INTRODUCTION	123
6.2	SYSTEMATIC LITERATURE REVIEW	124
6.2.1	Planning: Identification and Need for Review	124
6.2.2	Conducting the Review: Identification of Research	125
6.2.3	Selection of Primary Studies	126
6.2.4	Data Extraction.....	127
6.2.5	Data Synthesis	128

6.2.6	Technical and Semantic Interoperability Requirements (TSR).....	129
6.2.7	Organisational Interoperability Requirements (OR).....	133
6.2.8	Legal Interoperability Requirements (LR).....	136
6.3	SUMMARY	138
CHAPTER 7.....		139
7	OBJECTIVES OF A SOLUTION (EXPERT INTERVIEWS).....	139
7.1	INTRODUCTION	139
7.2	BLOCKCHAIN EXPERT INTERVIEWS.....	140
7.2.1	Interview Process Overview	140
7.2.2	Participant No.....	141
7.3	INTERVIEW RESULTS	142
7.3.1	Theme 1: Branch of blockchain Interoperability	142
7.3.2	Theme 2: Business Perspective (Case)	148
7.3.3	Theme 3: Legal and Regulatory Compliance	150
7.3.4	Theme 4: Interoperability Techniques	156
7.3.5	Theme 5: Interoperability Mechanism Properties	159
7.3.6	Theme 6: Data	161
7.3.7	Theme 7: Interoperability Through Standardisation	164
7.4	SUMMARY	166
CHAPTER 8.....		167
8	DESIGN AND DEVELOPMENT	167
8.1	INTRODUCTION	167
8.1.1	Overview of General Systems Theory and Its Concepts.....	168
8.1.2	Application of Systems Theory Concepts to Develop the Interoperability Framework.....	170
8.2	CYCLE 1: FRAMEWORK DEVELOPMENT	183
8.3	CYCLE 2: FRAMEWORK DESIGN AND DEVELOPMENT BASED ON WEBINAR DATA.....	187
8.3.1	Overview of Webinars	187
8.4	WEBINAR ANALYSIS RESULTS	192
8.4.1	Theme 1: Branch of blockchain interoperability.....	192
8.4.2	Theme 2: Business perspective (business case)	196
8.4.3	Theme 3: Legal and regulatory compliance	198
8.4.4	Theme 4: Interoperability techniques	200
8.4.5	Theme 5: Properties of Interoperability Techniques.....	202
8.4.6	Theme 6: Data	204
8.4.7	Interoperability through standardisation	206
8.5	INSIGHTS FROM WEBINAR DATA.....	208
8.6	EXPLANATION OF FRAMEWORK.....	213
8.6.1	Framework Components.....	213

8.7	SUMMARY	215
CHAPTER 9.....		216
9	DEMONSTRATION AND EVALUATION	216
9.1	INTRODUCTION	216
9.2	ARTEFACT EVALUATION IN DESIGN SCIENCE RESEARCH	216
9.2.1	The Evaluation Approach in This Study	219
9.3	DEMONSTRATION OF THE EBI FRAMEWORK USING AN ILLUSTRATIVE SCENARIO	222
9.3.1	Overview of Project Khoka	222
9.3.2	Overview of Project Meridian	224
9.3.3	Overview of the industry RTGS to DLT integration project by Accenture, R3 and SAP	225
9.3.4	Application of EBI Framework to Assist the Skybank in Its Case for Enabling Blockchain to RTSG Interoperability (Scenario 1)	229
9.4	EVALUATION OF THE EBI FRAMEWORK USING EXPERT INTERVIEWS.....	243
9.4.1	Interview Process	243
9.4.2	Evaluation results from the analysis of expert interviews	245
9.5	SUMMARY	250
CHAPTER 10.....		251
10	CONCLUSION AND EVALUATION OF THE RESEARCH STUDY.....	251
10.1	INTRODUCTION.....	251
10.2	ADDRESSING RESEARCH QUESTIONS.....	252
10.3	EVALUATING THE RESEARCH CONTRIBUTION.....	257
10.3.1	Practical Contribution	257
10.3.2	Theoretical Contribution	258
10.3.3	Methodological Contribution.....	258
10.4	LIMITATIONS OF THE STUDY.....	259
10.5	DIRECTIONS FOR FUTURE RESEARCH	260
10.6	CONCLUDING SUMMARY	261
11	REFERENCES	263

APPENDICES

APPENDIX A: ETHICS APPROVALS	5
APPENDIX B: CONSENT FORMS AND INTERVIEW GUIDES.....	7
APPENDIX C: SAMPLE TRANSCRIPT	7

LIST OF FIGURES

Figure 1-1 Thesis chapter outline	10
Figure 2-1 Levels of Interoperability adapted from (Van Der Veer & Wiles, 2008).....	23
Figure 2-2: Simplified atomic swap process (adapted from Emugro Academy, 2022).....	27
Figure 3-1 The three relationships between knowledge and action in pragmatism (Goldkuhl, 2008)	48
Figure 3-2 DSR knowledge contribution matrix (adapted from Gregor & Hevner 2013)	53
Figure 3-3 DSR process model (adapted from Peffers et al., 2007)	55
Figure 3-4 An overview of the DSRM process followed in this study (adapted from Peffers et al., 2007)	59
Figure 3-5 Inductive research process (adopted from DeCarlo 2018)	60
Figure 3-6 Deductive research process (adopted from DeCarlo,2018).....	61
Figure 3-7 A summary of the data collection phases of the study.....	65
Figure 4-1 Innovation adoption curve (Rogers, 1995).....	83
Figure 4-2 Diffusion of innovation at the organisational level (Rogers, 1995).....	83
Figure 4-3 The three contexts of the technology, organisation and environment framework (Tornatzky et al., 1990)	85
Figure 4-4 ATHENA Interoperability Reference Architecture (Berre et al., 2007)	89
Figure 4-5 The enterprise interoperability framework (Chen & Daclin, 2006)	90
Figure 4-6 Principles of the European interoperability framework (European Commission, 2017).....	92
Figure 4-7 The four levels of interoperability (European Commission, 2017)	93
Figure 4-8 Open systems model (Katz & Kahn, 1978).....	96
Figure 5-1 PRISMA 2020 chart of the selection strategy (Adapted from Page et al., 2021)	111
Figure 6-1 PRISMA 2020 chart representing the search process. (Adapted from Page et al., 2021).....	127
Figure 8-1 Pictorial representation of systems theory elements	169
Figure 8-2 Overview of systems theory concepts	170
Figure 8-3 Overview of systems involved for blockchain interoperability in banking.....	172
Figure 8-4 Business related aspects and guidelines.....	174
Figure 8-5 Environmental aspects of blockchain interoperability	177
Figure 8-6 Data elements for blockchain interoperability	180
Figure 8-7 Conceptualisation of the Transformational Component.....	181
Figure 8-8 Overview of Proposed Enterprise Blockchain Interoperability (EBI) framework	184
Figure 8-9 Enterprise Blockchain Interoperability Process Flow	185
Figure 8-10 EBI Framework guidelines and considerations.....	186

Figure 8-11 The EBI architectural component framework revised from webinar data.....212

Figure 8-12 Revised guidelines and considerations per webinar data212

Figure 9-1 Evaluation method selection framework (adapted from Venable et al., 2012) 218

Figure 9-2 Summary of evaluation methods used to evaluate the EBI Framework in this study220

Figure 9-3 Hierarchy of criteria of IS artefact evaluation (adapted from Prat et al.,2014) 221

Figure 9-4 Overview of the RTGS payment process for the SAMOS systems (adapted from South African Reserve Bank, 2018).....223

Figure 9-5 Illustrative real-life example showing the integration of RTGS with blockchain (adapted from Bank of England, 2023)224

Figure 9-6 Example Illustration of a real-life project scenario for RTGS to blockchain integration(adapted from R3, 2021)225

Figure 9-7 Banking scenario: Enabling RTGS to blockchain interoperability.....226

Figure 9-8 Technical specification example for the RTGS227

Figure 9-9 Technical specification example for *Corda*228

Figure 9-10 Flow diagram representing the EBI framework application to the RTGS-to-Blockchain scenario for Skybank242

Figure 9-11 Simplified EBI framework249

LIST OF TABLES

Table 3-1 Summary of the comparison between the positivism, interpretivism and pragmatism paradigms	51
Table 3-2 A list of publications forming part of this study	59
Table 3-3 Overview of the methodological choices of the study	77
Table 4-1 A list of studies that used systems theory	100
Table 5-1 Databases used and respective search strings	108
Table 5-2 Search keys for identifying financial institutions involved in blockchain experimentation	109
Table 5-3 Banks experimenting with blockchain	109
Table 5-4 Assessment criteria to evaluate academic studies (adapted from Dyba & Dingsøyr, 2008)	112
Table 5-5 Assessment criteria to evaluate grey literature (adapted from Garousi et al.,2019).....	112
Table 6-1 Search strings used to identify the literature.....	126
Table 6-2 The Inclusion and Exclusion criteria	126
Table 6-3 Security, Privacy and Data Confidentiality	130
Table 6-4 Distiguishability requirements for blockchains	131
Table 6-5 Cross-chain protocol requirements	132
Table 6-6 Data standardisation requirements	133
Table 6-7 Business model requirements.....	134
Table 6-8 Trust requirements.....	135
Table 6-9 Governance requirements	135
Table 6-10 Identification requirements.....	137
Table 6-11 Jurisdictional requirements	137
Table 6-12 Smart contract requirements.....	138
Table 7-1 The profiles of the interview participants.....	141
Table 8-1 Conceptualisation of system and their goals	173
Table 8-2 Conceptualisation of the environment.....	176
Table 8-3 Conceptualisation of data (input/output)	178
Table 8-4 Conceptualisation of interoperability	182
Table 8-5 Inclusion and exclusion criteria for webinars.....	189
Table 8-6 List of webinars included for analysis	190
Table 8-7 Comparison of key findings of interviews and webinars for Theme 1	196
Table 8-8 Comparison of key findings of interviews and webinars for Theme 3	200
Table 8-9 Comparison of key findings of interviews and webinars for Theme 4	202

Table 8-10 Comparison of key findings of interviews and webinars for Theme 5	204
Table 8-11 Comparison of key findings of interviews and webinars for Theme 6	206
Table 8-12 Comparison of key findings of interviews and webinars for Theme 7	208
Table 8-13 Additional elements obtained from the webinars	210
Table 9-1 Possible types of interoperability in banking organisations	231
Table 9-2 Overview of blockchain systems used by the banking sector	233
Table 9-3 Example assessment of interoperability approaches based on the type of data they support	237
Table 9-4 Simple example of security and performance assessment of the interoperability approaches	239
Table 9-5 Comparative assessment of cross-chain approaches (adapted from Mao et al., 2023)	240
Table 9-6 Regulations that impact interoperability in the banking sector in the South African context	240
Table 9-7 Description of participating experts	244

TABLE OF ACRONYMS

DSRM	Design Science Research Methodology
DSR	Design Science Research
SARB	South African Reserve Bank
CBDC	Central Bank Digital Currency
PoW	Proof of Work
PoS	Proof of Stake
DLT	Distributed Ledger Technology
ICT	Information and Communication Technology
IS	Information Systems
BFT	Byzantine Fault Tolerance
PBFT	Practical Byzantine Fault Tolerance
dAPPs	Distributed Applications
AML	Anti-Money Laundering
KYC	Know-Your-Customer
API	Application Programming Interface
SLR	Systematic Literature Review
RTGS	Real-Time Gross Settlement
HTLC	Hash-Time Lock Contracts

CHAPTER 1

1 INTRODUCTION

1.1 BACKGROUND INFORMATION

The importance of information and communications technology (ICT) in organisations is an undeniable and well-documented fact (Ekwonwune et al., 2016; Yunis et al., 2018; Das, 2019). For decades, ICT has transformed industries and organisations into becoming more productive and efficient in their operations. ICT enables businesses to provide new innovative products and services cost-effectively and efficiently and creates a robust competitive market. The advent of the COVID-19 pandemic has further emphasised the importance of ICT in organisations and the need for organisations to be responsive and adaptive to new ways of living and, consequently, new technologies. For instance, due to the COVID-19 pandemic, work-from-home, e-commerce, and cashless payments have become the norm (Wisniewski et al., 2021). Organisations had to find alternative ways of conducting business, which drove interest and investment towards improving existing technologies and adopting alternative technologies such as blockchain.

Blockchain is a decentralised, immutable, and transparent distributed ledger, which allows peer-to-peer transactions (De Filippi, 2016). The primary use case of this technology resides in the banking/financial sector, where it operates as the foundational technology for *Bitcoin*, a cryptographic currency. However, its applications span various other industries, such as supply chains, energy, health, and education. Blockchain technology is developing rapidly and has attracted much attention and interest from industries and academics alike. Consequently, there has been an increase in the number of blockchain platforms and decentralised applications from various spheres of society. For example, the financial sector has put forward significant experimentation efforts and investments geared towards blockchain. Central banks globally, in collaboration with commercial and retail banks, have embarked on projects to investigate ways in which they can adopt the technology in their operations (Chapman et al., 2017; South African Reserve Bank, 2018). These efforts have yielded promising results in the development of central bank digital currencies and in

improving the inefficiencies of current payment systems. Despite these efforts, the adoption of this technology in the sector has been sluggish, and there are very few blockchain-driven banking products in the market (Albrecht et al., 2018; Renduchintala et al., 2022). The available literature has attributed this slow adoption to challenges associated with current blockchains, such as scalability, lack of regulation and lack of appropriate governance (Qasse et al., 2019; Zachariadis et al., 2019). Furthermore, Qasse et al. (2019) and Belchior et al. (2021b) identify the lack of appropriate interoperability standards, protocols and tools as another obstacle in the adoption of blockchain.

Current efforts in developing blockchain applications happen in silos, using various blockchain platforms. Consequently, the blockchain landscape is heavily fragmented (Schulte et al., 2019b; Wang et al., 2023), leading to the development of incompatible blockchain applications and networks, which, in turn, complicates data- and asset-sharing between these blockchain applications (Ghaemi et al., 2021). Furthermore, integrating blockchain, a decentralised technology, into currently centralised legacy systems exacerbates the challenge of adopting the technology. The interoperability between different blockchain applications and with existing technology is pertinent to the full-scale adoption of the technology (Liu et al., 2019; Al-Rakhami & Al-Mashari, 2022).

For organisations to reap the benefits of blockchain fully, existing and new blockchain solutions must communicate with each other and existing technologies within incumbent organisations. This necessity is particularly apt in the financial sector, which constitutes a large network of participants and relies heavily on legacy technology. Hughes et al. (2019) state that the lack of a common architecture across the financial industry and the challenge of integrating blockchain into current transactional systems hinder the migration of the sector towards blockchain. Moreover, existing interoperability protocols and tools are not appropriate for blockchain applications, and new tools have been proposed. However, these new protocols, models, tools and frameworks are still immature and “fall short of building robust integration between blockchains” (Hughes et al., 2019, p. 122) and thus, warrant further development (Belchior et al., 2021b).

1.2 CONTEXT OF THE STUDY

This study focuses on the banking industry in South Africa. It is essential to understand the context to facilitate a better understanding of the adoption of blockchain in the South African banking system. Therefore, this section provides a brief background on South Africa and its banking sector.

South Africa, or the Republic of South Africa (RSA), as it is officially known, is a country located at the southern tip of Africa. The country is diverse both geographically and in terms of its heterogeneous population. According to the mid-year report by Statistics South Africa (2020), the country's population was 59.62 million people in July 2020. This population is distributed through ten provinces, with Gauteng province accounting for the largest population size at approximately 26.0%. The majority of the population (80.8%) is of Black African descent, followed by Coloured (8.8%), White (7.8%) and Indian and Asian (2.6 %).

South Africa's political system is based on democratic principles and is governed predicated on a constitution established in 1996. The country has robust and sound political, justice, legal, regulatory, and economic systems. It is rated among the top largest economies in Africa with a gross domestic product valued at 369.9 billion USD, with the mining, agriculture, services industries (finance, real estate and business) and government services the most significant contributing sectors (Santander Trade Markets, 2020). The country has a well-developed and well-regulated financial sector (Mishi et al., 2016), with one of the leading stock exchanges in the world and various banks, investment and insurance companies offering a range of services.

The South African banking sector consists of commercial and mutual banks operating under the oversight of the South African Reserve Bank (SARB). The Reserve Bank is responsible for managing the country's monetary policy, the production, wholesale and distribution of the Rand (local currency) and the settlement of interbank claims (South African Reserve Bank, 2020). The Reserve Bank also registers any banks wishing to operate in the country. The amalgamation of registered banks includes locally run banks, foreign banks, foreign bank branches and some cooperation and mutual banks (South African Reserve Bank, 2020). According to BusinessTech (2020), there are four major banks: Standard Bank, First

National Bank, Absa and Nedbank. The banks are ranked according to their market share and contribute to over 84% of the total share.

Similar to other global banks, the South African banking sector has shown much interest in adopting blockchain in various banking operations. For instance, the SARB initiated two proof-of-concept projects in collaboration with local banks. The project called Project Khoka (South African Reserve Bank, 2018) focused on developing a blockchain-based real-time inter-bank settlement system. Recently, the SARB embarked on another blockchain project to develop a blockchain-based digital currency. These two projects demonstrate that there indeed exists an appetite and intention within the sector to adopt the technology.

1.3 PROBLEM STATEMENT

Blockchain technology offers substantial potential benefits to the banking industry. The technology can enable banks to reduce transactional and onboarding costs, improve payment and remittance processing efficiency, help address the fraud and money laundering problem and, ultimately, open up opportunities for the enhancement of financial inclusion efforts (Benos et al., 2019; Soni & Duggal, 2014). In addition, inherent properties of blockchain, such as decentralisation, immutability, transparency and other associated blockchain-related technologies, such as smart contracts, can assist organisations in enhancing existing business models (Morabito, 2017) and also create new business models (Lakhani & Iansiti, 2017). Despite the benefits of blockchain technology for organisations, particularly financial institutions, the adoption of the technology is still slow due to scalability, regulatory, governance and interoperability issues associated with current blockchain systems. As a result, the sector cannot realise the full value of the technology.

Interoperability is critical to many organisations relying on ICT in their operations. Interoperability refers to the ability of heterogeneous information systems to communicate and share information seamlessly. Without interoperability tools and protocols, ICT systems cannot communicate, and business processes can be highly inefficient. Similarly, blockchain interoperability is a critical functionality to facilitate communication between heterogeneous blockchains (Liu et al., 2019), for example, in blockchain-based cross-border payments. In the absence of tools facilitating effective inter-blockchain communication and

communication between blockchains and legacy systems, blockchain cannot satisfy the needs of modern organisations (Bhatia, 2020). Therefore, it is critical to ensure that disparate blockchains interoperate with each other and other non-blockchain systems to realise the full value of the technology (Abebe et al., 2019a). Furthermore, addressing blockchain interoperability issues can, in turn, alleviate the scalability constraint associated with the technology (Qasse et al., 2019). Improving the scalability of blockchain limits its applicability to a few functions only (Tan et al., 2022). Simplifying how data are shared between heterogeneous systems enables such systems to accommodate future growth and demands (Besançon et al., 2019).

Blockchain interoperability, particularly in the context of blockchain-to-blockchain, has gained traction from practitioners and scholars in recent years. This is because traditional interoperability standards, tools and methods do not accommodate emerging forms of data and digital assets used on the blockchain sufficiently (Abebe et al., 2019a). The existing literature on blockchain-to-blockchain interoperability proposes various interoperability mechanisms to address this issue. However, because blockchain technology is still in its infancy, the proposed tools are still immature (Hughes et al., 2019), specific solutions have not yet been developed (Al-Jaroodi & Mohamed, 2019), and existing solutions are inherently not interoperable (Abebe et al., 2019a). Further, current literature, particularly peer-reviewed academic literature, on the interoperability of blockchain and non-blockchain systems is generally scarce. The literature primarily originates from industry, and emphasises the critical challenges organisations face concerning the integration of new blockchain-based systems into current enterprise systems (Nazarov et al., 2020). Extant literature in this domain primarily focuses on the integration of blockchain in healthcare (Biswas et al., 2020; Reegu et al., 2023); none, to this researcher's knowledge, addresses the issue of the interoperability of blockchain in the banking sector.

Current blockchain adoption initiatives indicate that organisations, including financial institutions, do not intend to replace existing systems with blockchain but rather to leverage the technology for specific business areas (Prewett et al., 2020; Javaid et al., 2022). This implies the need for such new blockchain systems to integrate and interoperate with existing systems. The dilemma remains that blockchain interoperability is a complex process (Bhatia, 2020; Hardjono et al., 2019), and no appropriate standards, tools and frameworks currently

exist to guide blockchain interoperability implementation (Belchior et al., 2021b). Existing interoperability protocols, models, tools and frameworks were historically designed for traditional systems and thus are incompatible with blockchain (Abebe et al., 2019a; Koens & Poll, 2019). The aforementioned lack of tools and frameworks hinders the ability of organisations interested in the technology to realise the technology's full benefits.

This shortage is a particular challenge for the financial sector, which relies heavily on legacy technology. Currently, legacy payment systems rely on a centralised mechanism. Incorporating blockchain, a decentralised technology, also introduces significant interoperability complexity, especially when decentralised systems are expected to rely on the existing central mechanism (Chapman et al., 2017). Furthermore, the financial markets ecosystem is highly regulated and traditionally involves many global participants using different technologies and data formats. Introducing blockchain into such already complex systems leads to further interoperability challenges concerning how data can be transferred and interpreted between different blockchain systems (South African Reserve Bank, 2018). This problem is exacerbated by existing solutions and studies mainly focusing on addressing interoperability from a technical and semantic perspective. However, to achieve true interoperability, legal and business-related aspects must be considered (Ndlovu et al., 2021). Given the aforementioned challenges, this study aims to contribute to the body of knowledge on blockchain adoption by addressing the challenges organisations, particularly banking organisations, face when implementing interoperability between blockchains and between blockchains and legacy systems.

1.4 PURPOSE OF THE STUDY

This study mainly intends to interrogate blockchain interoperability in the context of the banking sector and to develop a framework to guide and assist practitioners and researchers towards a better understanding of the nuances of blockchain interoperability implementation regarding inter-blockchain and blockchain to non-blockchain communication.

1.4.1 Aim

This study primarily aims to develop a blockchain interoperability framework to guide the implementation of blockchain interoperability in the banking sector.

1.4.2 Objectives:

- To identify the use cases, challenges, and considerations for blockchain implementation in the banking sector
- To identify the requirements for enabling blockchain interoperability
- To identify critical elements required to formulate a blockchain interoperability framework.
- To develop a blockchain interoperability framework.
- To evaluate the framework

1.5 RESEARCH QUESTIONS

This study intends to address the challenges mentioned above by answering the following overarching question:

- *How can a blockchain interoperability framework be conceptualised to guide the process of implementing blockchain interoperability in the banking sector?*

The following sub-questions support the question above:

- What are the use cases, challenges, and considerations for blockchain implementation in the banking sector?
- What are the requirements for interoperable blockchain systems?
- What are the critical elements required to formulate a blockchain interoperability framework?
- How can a blockchain interoperability framework be developed?
- How can the developed framework be evaluated?

1.6 DELIMITATIONS

Delimitations represent the boundaries and scope of a study. The following delimitations apply to this study:

- The study mainly focuses on addressing blockchain interoperability issues in the banking context.
- The study aims to develop a conceptual framework to provide guidance on how banking organisations can implement blockchain interoperability. However, the study does not offer a technical framework. Furthermore, the study assumes that organisations have already made the decision to implement blockchain for a specific use case; therefore, this study does not provide any guidance pertaining to the selection of the type of blockchain platform.

1.7 STUDY CONTRIBUTION

This study made the following contributions, as discussed below:

- **Practical contribution:** The study formulated a blockchain interoperability framework offering insights and guidance concerning the process of integrating blockchain systems within the banking sector. The proposed framework provides organisations and practitioners interested in deploying blockchain-based systems with a reference and departure point from which to determine appropriate approaches for integrating blockchain systems into their incumbent systems.
- **Theoretical Contribution:** Blockchain interoperability is still a relatively new research area; thus, the development of the proposed framework contributes towards the building of new knowledge and cultivates a better understanding of this research area. The present study expands on the currently limited research on blockchain, specifically on blockchain interoperability, and contributes to opening opportunities for further academic research on the topic. This will, in turn, contribute to and enrich the literature on the topic of blockchain interoperability in general.

- **Methodological contribution:** The study followed a qualitative approach which leveraged methodological triangulation in which data were collected through traditional methods like interviews and uncommon data collection methods like webinars. The application of webinars in this study revealed that webinars could be an effective supplementary data collection method that could enable researchers to collect data from subjects who might not be accessible through traditional methods and for new research areas which might have a limited number of experienced participants. Therefore, other researchers can explore the use of webinars to complement traditional methods of collecting data, particularly when investigating emerging topics with constrained populations. In addition, the study can act as a reference for other DSR researchers on how to apply the DSRM to develop and evaluate an artefact such as the EBI framework proposed in this study.

1.8 BRIEF CHAPTER OVERVIEW

This thesis is organised as illustrated below

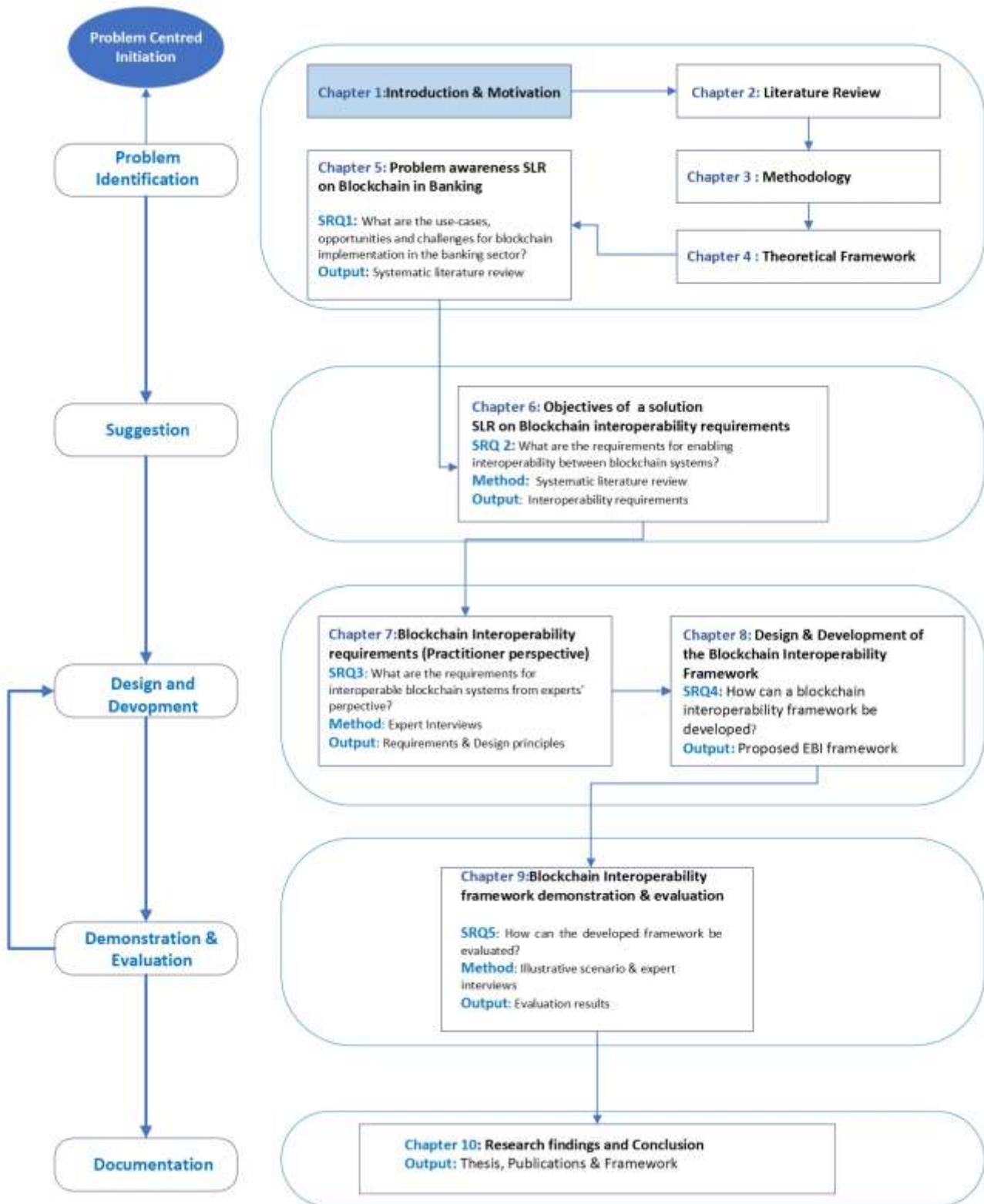


Figure 1-1 Thesis chapter outline

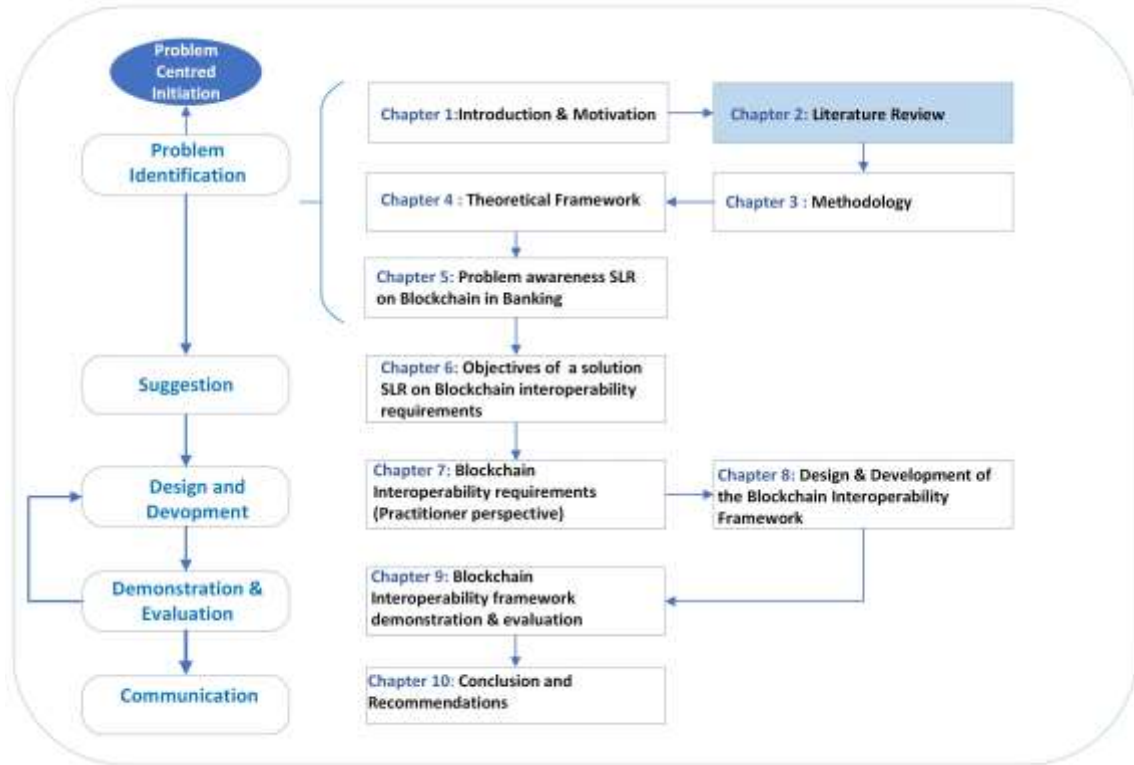
- **Chapter 1:** Introduced the background and objectives of the study. The chapter also highlighted the problem being addressed, the motivation for the study, and the research questions the study intends to address. It further outlines the research assumptions on which the study is based, its scope and limitations, and the intended contribution.
- **Chapter 2:** Explains key concepts relating to blockchain technology and blockchain interoperability. The chapter also provides a brief contextualisation of blockchain and blockchain interoperability in the banking sector. Chapter 2 contains a discussion on existing interoperability frameworks in addition to the existing literature on blockchain interoperability.
- **Chapter 3:** Deliberates on the research methodology and the associated philosophical grounding of the current study. It articulates the rationale for selecting the research methodology and research paradigm. Chapter 3 further elucidates how the selected design science methodology is applied in the study, as well as the different data collection methods applied. The chapter also discusses issues of reliability, validity and ethics.
- **Chapter 4:** Explicates the theoretical grounding for this study, specifically by explaining the different theories used at different phases of the DSRM process and how they were applied in this study.
- **Chapter 5:** Presents the findings of a systematic literature review conducted as part of the problem awareness phase of this dissertation. The chapter explains the systematic literature review process and its associated findings.
- **Chapter 6:** Describes the process of the systematic literature review study, which forms part of the phase identifying the objectives of the solution. The chapter also presents the various interoperability requirements identified through the review.
- **Chapter 7:** Constitutes the second cycle of the phase identifying the objectives of the solution. The chapter presents the findings from the analysis of expert interviews, which were used to identify the requirements and elements needed to construct a blockchain interoperability framework.
- **Chapter 8:** Explicates how the proposed framework was conceptualised using the findings from systematic literature reviews and interviews. The chapter also

discusses the second cycle of development in which data from webinars were used to refine the framework.

- **Chapter 9:** Presents the details on how the proposed framework was evaluated.
- **Chapter 10:** Concludes this study by outlining how the research questions were addressed and presents the key contributions of the study. The chapter also presents recommendations for future research.

CHAPTER 2

2 LITERATURE REVIEW



2.1 INTRODUCTION

This chapter provides a comprehensive review of the existing literature on blockchain technology, focusing particularly on blockchain interoperability. Primarily, the chapter elucidates the current state of the art on enterprise blockchain interoperability to understand the intricacies of interoperating and integrating blockchain within organisational settings globally and in South Africa. The discussion includes clarifying the relationship between blockchain adoption and blockchain interoperability, and identifying the key barriers and goals for interoperating blockchain.

The chapter first introduces blockchain and its associated concepts. Thereafter, follows an evaluation of the existing literature on enterprise interoperability, highlighting key concepts and findings. The discussion on information systems interoperability is followed by a discussion on blockchain interoperability, covering the various definitions of blockchain

interoperability presented in the literature, how enabling interoperability between blockchains differs from interoperating other ICTs, and barriers to achieving interoperability of blockchains. Chapter 2 further presents an evaluation of the literature on the existing solutions and approaches for enabling blockchain interoperability. The chapter concludes with a review of existing interoperability frameworks.

2.2 BLOCKCHAIN OVERVIEW

2.2.1 Blockchain technology

Existing research defines blockchain or the distributed transaction ledger (DTL) in many ways, with each definition characterising it from a different perspective. Some define blockchain in terms of its purpose. Underwood (2016) defines blockchain as an open, global distributed ledger and consensus-based technology that enables businesses and individuals to transact without a middleman. Larios-Hernández (2017) states that blockchain is a distributed ledger system used as the foundational technology for cryptocurrencies. Others define it based on its characteristics. Hughes et al. (2019) define it as a distributed peer-to-peer ledger consisting of a set of interlinked blocks of data. According to Nakamoto (2009), the developer of blockchain, it is an “electronic payment system based on cryptography and not of trust”. Nakamoto (2009) further specifies that blockchain offers a decentralised peer-to-peer payment mechanism for the transfer of value by eliminating the need for third-party entities such as clearing agents, governments, or banks (Frizzo-Barker et al., 2020; Larios-Hernández, 2017; Parino et al., 2018). This design means that transactions on the blockchain are not verified by a single entity but can be verified by any set of nodes (computers) within the blockchain network. The technology was developed to create the digital currency *Bitcoin* and to address the Byzantine Generals' Problem and the Double Spend Problem of traditional currency systems, which necessitated a third party (Aras & Kulkarni, 2017).

Blockchain comprises five main features: a shared transaction database, a consensus mechanism for updating the database, unique cryptographic signatures for time-stamping records, tamper-proof records and cryptographic hash linking a block to the preceding block (Swan, 2017). Each block contains a list of completed time-stamped transactions.

Cryptographic algorithms encrypt the blocks for anonymity and to ensure immutability. However, Hughes et al. (2019) explain that portions of the transaction called the transaction headers are publicly available and, thus, can be accessed by any node or computer on the blockchain network. A consensus mechanism adds a new transaction record onto a block; it enables all parties in the blockchain to reach an agreement regarding the contents and legitimacy of a transaction prior to that transaction is added to the block (Beck et al., 2018). The above-mentioned features ensure that all transactions occurring within a blockchain are secure, immutable, transparent and stored in a decentralised manner. These attributes make blockchain "powerful in modern internet architecture" (Hughes et al., 2019, p. 276). The following is a discussion of these essential characteristics of blockchain technology.

2.2.2 Characteristics of Blockchain

Decentralised

A blockchain system consists of a set of nodes. These nodes can transact directly with each other in a peer-to-peer fashion without the need for an intermediary entity. All nodes in the network keep a copy of the transaction database and participate in the consensus mechanism to validate and authenticate transactions. The data or information stored on the blockchain is not controlled by any one node or party (Tapscott & Tapscott, 2017). This is contrary to conventional transaction systems whereby a central authentication and verifications agency is required to validate transactions. The use of a central agent leads to high transactional costs and performance bottlenecks on the server (Wang et al., 2019). The disintermediation provided by blockchain technology can benefit industries, such as the financial industry, which rely on intermediary clearing houses for payment settlements.

Immutability

One of the key attributes of blockchain is its immutable design, which ensures that once a transaction has been recorded on the blockchain, it cannot be altered. Blockchain ensures that blocks and records are immutable by linking old blocks to new blocks such that the new block contains a hash of the previous block (Nakamoto, 2009). Consequently, it is

computationally infeasible to alter because changing one block would require changing subsequent blocks. Furthermore, a new block is added to the chain approximately every ten minutes, and this rate of expansion of the chain renders alterations to the blockchain linearly impossible (Böhme et al., 2015). In addition, every node in the network keeps a copy of the blockchain database, which adds to the difficulty of forging transactions (Clohessy et al., 2019). The immutability of the transaction on the blockchain can enhance trust and is suited for environments where transactional fraud is a challenge. However, immutability is cited as a disadvantage by dint of not accommodating refunds or transaction corrections where a mistake has occurred (Surujnath, 2017).

Transparency

As mentioned above, all nodes in the blockchain community have a replica of the transaction ledger and every transaction and its value is visible to all nodes within the network. This feature implies that all transactions occurring within the blockchain network occur under complete transparency (Lakhani & Iansiti, 2017). Transparency plays a critical role in public cryptocurrency blockchains because it gives the assurance that the transactions have indeed occurred and are valid. However, though transparency is a desirable feature for public cryptocurrency blockchains, it presents a challenge for organisations. For most business applications, disclosing private and sensitive business data is often undesirable and conflicts with data privacy policies and regulations (Sedlmeir et al., 2022).

Pseudo-Anonymity

Nodes or users on the blockchain networks are uniquely identified using an alphanumeric address (Lakhani & Iansiti, 2017). The address is generated through a cryptographic hash function performed on the user's public key and some additional information (Yaga et al., 2019b). These addresses are then used as source and destination addresses during transactions.

2.2.3 Types of Blockchain

Blockchains are typically classified as permissioned, permissionless or hybrid and differ based on how participants are selected and access control restrictions for validators/miners. The section below discusses principal variations between permissioned, permissionless, and hybrid blockchain networks.

Permissionless Blockchain

Permissionless blockchain networks are blockchain platforms open for all to use. A permissionless blockchain does not restrict who can access and validate transactions on the blockchain. Any user on the network can access, read and write the ledger (Yaga et al., 2019b). Further, any user on the permissionless network can post transactions, mine, and participate in the consensus. Permissionless blockchains are also categorised as public blockchains because of their open-access policy. However, it is possible to have private permissionless blockchain networks in which access to private data is restricted through cryptographic primitives (Wüst & Gervais, 2018).

Permissionless blockchain networks do not rely on a central party to manage membership or ban malicious participants, rather incentive mechanisms are employed to encourage participation (Wüst & Gervais, 2018). Consensus mechanisms (see Section 2.2.4) are typically used to prevent malicious users from publishing blocks by ensuring that users expend some resources when adding blocks and rewarding non-malicious users with cryptocurrency (Yaga et al., 2019b).

Permissioned Blockchain

Permissioned blockchains are closed networks with more restrictive access controls to limit who can participate in accessing, writing and validating transactions. Contrary to permissionless blockchains, permissioned blockchains offer an additional authorisation and authentication layer to determine who can participate in the network (De Angelis et al., 2018). Thus, only the nodes granted permission by the network can join, access and validate transactions. Each member is assigned a role associated with specific access-control authorisations. In addition, nodes in the network are required to be identifiable to other

members in the network to discourage malicious behaviour (Li et al., 2020). Accordingly, different members can be assigned different rights to read, write or validate transactions. Owing to the variations in access rights that can be attributed to members, permissioned blockchains can be centralised or partially decentralised. Furthermore, due to the access-control restrictions in these types of blockchains, they are well suited for private enterprises where governance is centralised, and data security and privacy are critical requirements (Monrat et al., 2020). Because permissioned blockchains operate in more centralised and trusted environments than their permissionless counterparts, they do not rely on incentive-based consensus mechanisms and hash procedures (De Angelis et al., 2018). Instead, the consensus mechanisms in permissioned blockchains are message-based (De Angelis et al., 2018). For example, Byzantine Fault-Tolerant (BFT) consensus algorithms such as the Practical Byzantine Fault Tolerance Algorithm (PBFT) are normally applied in permissioned blockchain networks. Generally, blockchain networks in this category can be private or consortium; however, some public blockchains can also be permissioned if the validation of transactions is controlled. Both the private and consortium networks may include some features of the public blockchain, such as the consensus mechanism (Sheth & Dattani, 2019).

Private blockchains

Private blockchains are centralised to one organisation, and only that organisation has the right to write on the ledger (Li et al., 2018; Aras & Kulkarni, 2017). Participation in the private blockchain is by invitation and only authorised entities are allowed to join (Rajasekaran et al., 2022). Private networks are more secure than their permissionless counterparts because only authorised and trusted entities can participate in the network (Bhutta et al., 2021). As a result, they are suitable for applications where privacy and confidentiality are essential.

Consortium blockchains

In contrast, consortium blockchains are owned by a group of organisations collaborating to maintain the network. Unlike private blockchains governed by one entity, consortium blockchains are governed by all the participating organisations (Dib et al., 2018). This means that, in a consortium blockchain, a selected group of members can validate and approve

transactions (Li et al., 2018). They offer customisable access control, which enables members to control what data is accessed, when, and how it is accessed. Therefore, consortium blockchains are useful when multiple organisations want to collaborate and share a blockchain infrastructure without relying on a single central authority. As such, they are suitable for applications in industries such as finance and supply chain management where confidentiality and strategic collaboration are critical.

Hybrid blockchains

Hybrid blockchains integrate elements of permissionless (public) and permissioned (private) blockchains in the same network to provide a more flexible approach to blockchain technology (Rajasekaran et al., 2022). Typically, they include public elements to ensure transparency and decentralisation, and private elements to provide controlled access to sensitive data (Andoni et al., 2019). Therefore, hybrid blockchains enable organisations to select which data to share publicly and which to keep private. Thus they provide organisations with the benefit of maintaining autonomy and control over their data while benefiting from the collaborative nature of public blockchains.

2.2.4 Consensus mechanisms

Consensus mechanisms are protocols used on blockchains to achieve distributed agreement regarding the state of the distributed ledger. They are responsible for verifying and validating transactions and adding new blocks to the blockchain (Bhutta et al., 2021). Consensus mechanisms are utilised in public and private networks to ensure the blockchain data is consistent and incorruptible (Xie et al., 2019). The following discussion presents some major consensus protocols applied in both public and private blockchains.

Proof-of-Work (PoW)

PoW is the original consensus mechanism used in the *Bitcoin* blockchain network. In this mechanism, nodes solve a computationally intensive cryptographic puzzle to gain the right to add a block to the blockchain. The produced solution is the proof of work, and the node

that first solves the puzzle is then rewarded. PoW consensus mechanisms have been criticised for being highly energy efficient due to their high consumption power required to perform the computationally intensive cryptographic puzzle (Xiao et al., 2020).

Proof of stake (PoS)

The Proof-of-Stake consensus mechanism was developed to address the energy inefficiencies of the PoW mechanism. PoS consensus mechanisms use ownership stakes to determine which miner can append a block to the blockchain (Aras & Kulkarni, 2017). Ownership stake refers to the number of tokens that a node or participant owns. The more stake a miner has, the higher the likelihood of being selected to append the block onto the chain (Nguyen & Kim, 2018). Though this approach is more efficient than PoW, it has the disadvantage of favouring participants with a large number of tokens, which implies that these participants can have an unfair advantage of dominating the network (Zheng et al., 2018). The challenges with PoS mentioned above, are addressed by a variation of PoS referred to as Delegate Proof-of-Stake (DPoS). Similar to PoS, in DPoS, participants or miners are selected to verify transactions based on their ownership stake. However, in DPoS, the participants delegate and select miners to verify transactions resulting in fewer nodes verifying transactions (Zheng et al., 2018). As a such, DPoS' process of verifying blockchain data is much quicker than in PoS.

Byzantine Fault Tolerance Consensus (BFT)

BFT consensus mechanisms refer to consensus protocols that ensure consensus even when some validation nodes fail to validate or provide incorrect information. A typical form of a BFT consensus algorithm is the Practical Byzantine Fault Tolerance (PBFT) mechanism. PBFT uses a replication algorithm to tolerate byzantine faults. In PBFT, a consensus is reached as long as the number of faulty or malicious validation nodes is less than one-third of the total nodes in the blockchain (Guo & Yu, 2022). Due to its security, PBFT is mostly used in the consortium blockchain with a fixed number of nodes but is not applicable in a public blockchain with a large number of nodes because of its poor scalability (Yang et al., 2019).

2.3 INTEROPERABILITY OF INFORMATION SYSTEMS

Interoperability has been a continuous and long-term concern for organisations globally. The rapid development of new technologies and increasing global competition are compelling organisations to adopt new technologies continuously and collaborate. Organisations, whether private companies, public companies or government institutions, cannot operate in isolation anymore. Adopting new technologies is a business imperative for most organisations to maintain a competitive edge and improve service delivery. However, introducing these new technologies into existing organisational systems poses a challenge relating to how these technologies can be incorporated to work seamlessly with the existing systems. The ability of different systems to work seamlessly is broadly referred to as interoperability. More formally, interoperability is defined as the “ability of two or more systems or components to exchange information and to use the information that has been exchanged” (IEEE Computer Society, 1991, p. 114). Interoperability can also be viewed as the “capability to communicate, execute problem, or transfer data among various functional units in a manner that requires the user to have little knowledge of the characteristics of those units” (ISO/IEC International Standard, 2011). In information systems (IS) and information technology (IT) studies, interoperability has been used to refer to the ability of heterogeneous and autonomous systems to exchange and use information and services to achieve a particular goal (Banouar & Raghay, 2016; Soares & Amaral, 2014).

2.3.1 Types of interoperability

The interoperability of heterogeneous systems can be viewed from different perspectives. The nature of the heterogeneity between such systems determines the form or level of interoperability required (Sheth, 1999). According to Sheth (1999), technological differences in IS systems can lead to four types of interoperability: syntactic, semantic, system and structural. Semantic interoperability focuses on the interpretation of the data exchanged between systems. The purpose of semantic interoperability is to ensure that the data shared can be interpreted unambiguously by both systems involved in the data exchange. Hence, the meaning of the exchanged data must be consistent between the communication systems (Davies et al., 2020). Syntactic interoperability regards how the data to be exchanged is formatted and transmitted; it enables data exchange between systems but does not

guarantee that the shared information is interpreted in the same way by the communicating systems (Ide & Pustejovsky, 2010). According to Sheth (1999), structural interoperability relates to the schematic representation of the data, whereby system interoperability is defined in terms of interoperability between hardware systems platforms and between different larger information systems, such as database management systems.

Other scholars classify interoperability into four levels: technical, syntactic, semantic and organisational (business/enterprise) interoperability (see Figure 2-1) (Lehne et al., 2019; Rezaei, Chiew, Lee, et al., 2014; Scholl et al., 2011; Van Der Veer & Wiles, 2008, 2018). The syntactic and semantic forms of interoperability are similar to those discussed in the previous paragraph. However, the technical interoperability aspect refers to when two communication systems or machines can exchange information or services effectively between them and their users (Rezaei, Chiew, Lee, et al., 2014). It relates to how communication between hardware/software components, platforms and systems enables machine-to-machine communication (Van Der Veer & Wiles, 2008). Organisational interoperability denotes the effective and meaningful transfer of data/information between distinct organisations using different information systems or between organisation units within a single distributed organisation (Van Der Veer & Wiles, 2008). Organisational interoperability is considered the highest form of interoperability as it enables the integration of business processes beyond the scope of a single organisation (Funmi et al., 2013) and between organisations that may be in different geographical locations (Van Der Veer & Wiles, 2008). Moreover, the goal of organisational interoperability is to ensure that user-centric services are easily identifiable, accessible, and available to the user community (Vernadat, 2010). Achieving organisational interoperability requires both collaboration between the concerned organisations and the willingness to share business processes and work towards a common goal (Funmi et al., 2013; Tsagkani, 2005; Whitman & Panetto, 2006). Furthermore, organisational interoperability relies on the successful implementation of the other three forms of interoperability: semantic, technical and syntactical (Van Der Veer & Wiles, 2008).

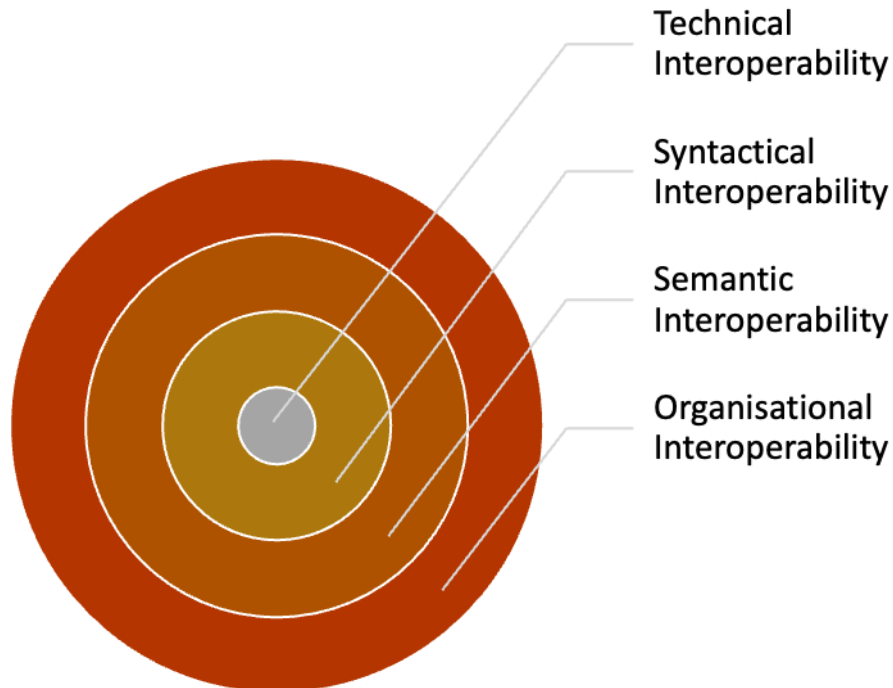


Figure 2-1 Levels of Interoperability adapted from (Van Der Veer & Wiles, 2008)

2.4 BLOCKCHAIN INTEROPERABILITY

Blockchain technology has evolved over the years from being the technology underlying cryptocurrencies to the recent blockchain 4.0, which is driving real-life applications of blockchain in various industries. Through blockchain 4.0, many industries, such as supply chains, finance, education, and health, have developed blockchain applications within their operations and for varying purposes, causing the emergence of multiple, heterogeneous blockchain systems differing in technologies, consensus mechanisms and architectures (Mohanty et al., 2022). The heterogeneity of these systems hinders interactions and communication between the systems, thus leading to interoperability difficulties, which prevent users on one blockchain from sending or receiving information or services directly from another blockchain. However, it is critical for disparate blockchains to communicate for organisations to realise the benefits of the technology fully and facilitate mass adoption of the technology. The ability of two heterogeneous blockchains to communicate is termed blockchain interoperability.

Though interoperability is a widely researched area in IS, the concept of blockchain interoperability is relatively new. The literature defines interoperability in the context of

blockchains from varying viewpoints. The National Institute of Standards and Technology (NIST) of the United State of America, describes the interoperability of blockchains by defining an interoperable blockchain architecture as: “distinguishable blockchain systems, each representing a unique distributed data ledger, where atomic transaction execution may span multiple heterogeneous blockchain systems, and where data recorded in one blockchain are reachable, verifiable, and referable by another possibly foreign transaction in a semantically compatible manner” (Yaga et al., 2019a, p. 50). Similarly, Lohachab et al. (2021, p. 135:134) define an interoperable blockchain infrastructure as a “composition of autonomous blockchain networks where each network is depicted as a distributed ledger of data, in which data can be operated among heterogeneous unconnected blockchain networks and data ledger can be accessed by validated foreign data”. Monika and Bhatia (2020a) explain blockchain interoperability as how different blockchains can reference and verify each other’s data or use the computational capabilities of another blockchain network, whereas Lipton and Hardjono (2022) state that blockchain interoperability is the exchange of assets created on the same blockchain which supports smart contracts. Blockchain interoperability can also be viewed as connecting multiple blockchains to enable information access and act on the information by changing the state of another blockchain or its own (Scheid et al., 2019). This study defines blockchain interoperability as the exchange of data and digital assets between blockchains or between a blockchain and non-blockchain systems, in a manner that enables the verification and validation of the state of a blockchain.

The definitions above, though diverse, highlight crucial attributes that distinguish interoperability in the context of blockchain from the interoperability of other IS or ICT systems. First, the definitions provided by (Yaga et al., 2019b) highlight heterogeneity in blockchain networks as one of the key factors driving the need for interoperability. Heterogeneity in blockchain networks refers to addressing incompatibilities in the underlying architecture of different blockchain platforms, differences in consensus algorithms, smart contracts, and governance protocols (Haugum et al., 2022b; Qasse et al., 2019). The definitions provided by (Lohachab et al., 2021; Scheid et al., 2019) indicate a critical element of blockchain interoperability relates to state changes and validations. State changes refer to the data append and validation processes utilised to add data onto a block in the blockchain (Pillai et al., 2020). State changes are governed by the underlying consensus mechanisms of individual blockchains. When information is sent from one blockchain to

another, the receiving blockchain is expected to be able to validate the correctness/validity of the received information and update its state based on the information (Pillai et al., 2020). This means the receiving blockchain should be able to verify that a particular state transition has occurred on the source blockchain (Johnson et al., 2019) to confirm that the information received from another blockchain was reached through consensus on that blockchain. An additional element unique to blockchain interoperability pertains to the nature of the information stored and shared between blockchains. In contrast to other IS systems and databases that store arbitrary data, blockchains store both arbitrary data and value (digital assets) (Haugum et al., 2022b; Pillai et al., 2020); therefore, blockchain interoperability does not only focus on sharing of data but should also facilitate a seamless transfer of value.

2.4.1 Types of blockchain interoperability

Blockchain interoperability can present in a variety of ways to serve varying purposes. Koens and Poll (2019) identified three main types of blockchain interoperability:

- *Interoperability between different blockchain platforms*
- *Interoperability between a blockchain and a legacy system*
- *Interoperability between smart contracts within the same blockchain network*

Interoperability between different blockchain platforms is required when two or more distinct and heterogeneous blockchains interact. In that case, the distinct blockchains could be a pair of permissioned blockchains (e.g., *Quorum* and *Hyperledger*) or permissionless blockchains (e.g., *Bitcoin* and *Ethereum*), and could also be between a combination of permissioned blockchain and a permissionless blockchain (e.g., *Bitcoin* and *Corda*).

Conversely, interoperability between a blockchain and a legacy system concerns interactions between any type of blockchain and a system that is not blockchain-based. Connecting a blockchain to a legacy system might be required to enable the blockchain to access off-chain data (real-world data) from other data resources or access off-chain computation capabilities which cannot be executed on the blockchain (Pasdar et al., 2023). For instance, on-chain storage and the calculation of big datasets like electronic health records and banking records are very costly; consequently, connecting blockchain to a legacy system for storage and calculation might require optimising the on-chain computation requirements (Sonkamble et al., 2021). However, achieving this form of interoperability is

still an open practical challenge concerning how real-life data can be transferred to and from blockchains (Pasdar et al., 2023).

The last type of interoperability defined by (Koens & Poll, 2019) concerns interactions between smart contracts. Smart contracts are computer programs that execute automated agreements/contractual clauses on the blockchain to enable trusted transactions between parties (Ren et al., 2021). They can be written using different programming languages such as *Solidity* (Solidity, 2022) and other traditional programming languages like *C++*, *Java*, *et cetera*. Furthermore, they are used to support the development of decentralised applications (dAPPs) across industries. Disparate dAPPs are incompatible due to the heterogeneity of the languages used to develop smart contracts. Therefore, smart contract interoperability enables communication between disparate, heterogeneous smart contracts within the same blockchain network or across networks (Koens & Poll, 2019). However, it should be noted that inasmuch as heterogeneities in smart contracts hinder interoperability, smart contracts can also enhance blockchain interoperability. In particular, homogenous smart contracts (i.e., smart contracts developed using the same language) enable information exchanges between heterogeneous blockchains and homogeneous blockchains (Khan et al., 2021). For instance, Dagher et al. (2017) demonstrate the use of smart contracts in aiding access to and exchanging patient health data across private and public blockchain networks.

2.4.2 Blockchain Interoperability Goals

Generally, the overarching goal of interoperability is to support communication between different systems and applications (Novakouski & Lewis, 2012). In the blockchain context, achieving interoperability serves the following goals: 1) asset exchange (atomic swaps), 2) asset transfers, and 3) data migration and transfer.

- 1) *Asset exchanges/cross-chain atomic swaps*: As stated in the previous sections, blockchains store value in the form of digital assets (cryptocurrencies, tokens or digital representations of real-life assets). Similar to real-life tradeable assets, owners of digital assets may also wish to exchange these assets. The process of exchanging digital assets on the blockchain is called a cross-chain atomic swap. A cross-chain atomic swap is essentially a coordinated decentralised process through which users

on different blockchains can exchange assets (Herlihy, 2018). Atomic swaps do not involve the actual transfer of assets across blockchains but rather can be viewed as a form of change-of-ownership of the assets on their native blockchains (Mohanty et al., 2022). To enable atomic swaps, parties lock their respective funds for a predetermined time and allow the other party to withdraw them in exchange for a secret (Nadahalli et al., 2022). The locked funds remain on the original blockchain, but the user address changes. This process requires both users to have addresses (wallets) on both blockchains. Figure 2-2 illustrates a simplified example of an atomic swap in which user A on a Bitcoin network wishes to trade their Bitcoins with user B's Ether coins on an *Ethereum* blockchain.

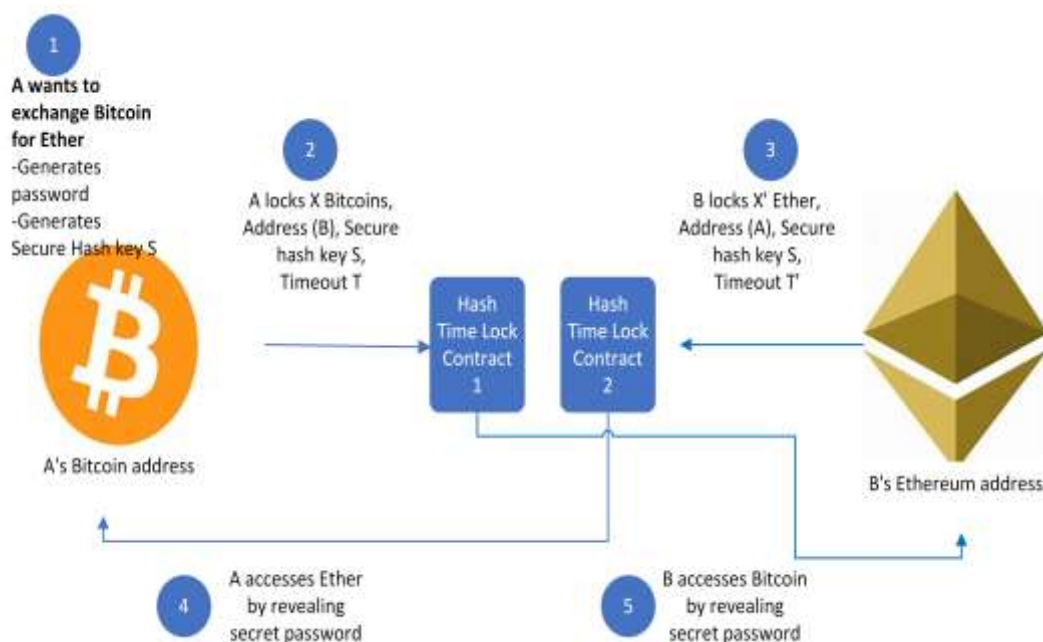


Figure 2-2: Simplified atomic swap process (adapted from Emugro Academy, 2022)

2) *Asset transfers*: Blockchain interoperability also contributes towards enabling the exchange of assets between users on different blockchains. Contrary to the atomic swap process described above, asset exchange involves the actual transfer of assets from one blockchain to another. Several approaches have been proposed to enable interoperability for asset transfers. For example, (Belchior, Vasconcelos, et al., 2022; Borkowski et al., 2019; Marten Sigwart et al., 2021; Sober et al., 2022) propose different procedures for enabling the transfer of assets. Some approaches employ a type of integration mechanism to connect disparate blockchains. However, these

approaches rely on an integration middleware and often have security constraints (Pillai et al., 2021). Other authors recommend a more decentralised burn-to-claim approach in which assets are first destroyed on the source blockchain, and then the equivalent amount is recreated on the destination blockchain (Pillai et al., 2021; Marten Sigwart et al., 2021).

- 3) *Cross-chain data migration and data transfer*: Enabling interoperability between blockchains can expand the nature of interactions between blockchains beyond the capability to exchange and transfer assets. In addition, interoperability can support data migration between blockchains and the transfer of data between a blockchain and an external source. The migration of data between blockchains could be necessitated for several reasons. For instance, businesses might opt to migrate data from one blockchain to a newer one with enhanced features in response to the evolving economic and regulatory landscape to remain competitive (Bandara et al., 2020). In some cases, migrations might be driven by the need to separate or consolidate data in response to hardware changes (Bandara et al., 2020) or due to disk space exhaustion (M. Zhang et al., 2021).

Furthermore, enabling interoperability is paramount to supporting the transfer of real-life data in blockchain applications that have to interact with other external systems. As stated previously, the programmability of blockchains through smart contracts has promoted the development of various industry-based blockchain applications. These applications may require access from outside the blockchain. Smart contracts need to obtain external (off-chain) data concerning real-world events (Al-Breiki et al., 2020). However, this is a challenge to achieve because blockchains are intrinsically not designed to access or store different types of data. Rather, they are designed to store transactions that may include other forms of data. For example, a transaction can include a reference to cloud storage, where the actual data are stored (Karaarslan & Konacaklı, 2020).

Therefore, overcoming this limitation requires an interoperability mechanism enabling some types of data feeds to bring external data into the blockchain system. Typically, this is achieved through data feeds referred to as oracles. Blockchain oracles are

trusted middleware of which the purpose is to collect off-chain data (external data) and feed it to the blockchain (Lu et al., 2023). Some research has demonstrated the application of oracles for data migrations and transfers. An example is a paper by Gao et al. (2020) in which the authors demonstrate interoperability between two heterogeneous blockchains by using a unidirectional data migration oracle. Their oracle approach not only establishes a communication channel between a source and destination blockchain but also enables access to external data. Similarly, Lu et al. (2023) demonstrate the need for data migration between consortium blockchains. Their study applies a bi-directional oracle to facilitate the interoperability process that enables data migration from one consortium blockchain to the next.

2.5 BLOCKCHAIN USE CASES AND APPLICATIONS

This section reviews actual and potential use cases of blockchain as explored by various scholars. The section discusses use cases from the perspectives of non-financial industries and the finance industry.

2.5.1 Real Industry Use Cases of Blockchain

Blockchain has been applied in several countries and different industries to achieve transparency and reduce fraud and transaction costs. Globally, particularly in developed countries, technology has been employed in real, practical applications within various business spheres. IBM has developed several blockchain-based technological solutions, such as the IBM Food Trust, identity protection, and global sales solutions (IBM, 2019). The IBM Food Trust uses a permissioned blockchain to connect participants in the food supply chain transparently, while Alibaba developed a blockchain system for shipment consignment tracking (Ledger Insights, 2020). Accenture, in partnership with Akshay Patra, has also developed a reputation management system for a school feeding system based on blockchain. The Midday Meal Program Management project, based in India, uses a permissioned blockchain to gather feedback in real-time from schools without using an intermediary agent (Aras & Kulkarni, 2017). In South Africa, the Centre for Affordable Housing Finance in Africa, a consultancy firm 71point4, and blockchain developer Seso Global piloted a blockchain-based property registration platform for social housing (Ledger

Insights, 2019). The South African Reserve Bank developed a proof of concept for its Project Khoka, a blockchain-based wholesale payment system (The South African Reserve Bank, 2018).

2.5.2 Blockchain Use Cases in Finance and Banking

The financial sector has been at the forefront of blockchain adoption and the exploration of potential applications. This can be attributed to blockchain first being introduced to the world as a foundational technology for the cryptocurrency, Bitcoin. However, the technology holds many other attractive properties for the financial sector, offering vast opportunities for application beyond cryptocurrency. Blockchain can solve the majority of challenges experienced by the financial sector (Guo & Liang, 2016). Below is a discussion of some of the applications of blockchain in the financial sector.

Anti-money laundering and the Know-Your-Customer process: Anti-money laundering (AML) and Know-Your-Customer (KYC) compliance are also cited as key areas where blockchain can play a critical role in reducing costs. Money laundering is an attempt to legitimise funds obtained as proceeds from illegal trade by passing the money through legitimate businesses and organisations such as banks. Globally, banks must comply with AML and KYC regulations to minimise the risk of money laundering by knowing their customers. However, AML and KYC compliance is a very laborious and costly exercise for banking institutions and clients. According to Shbair et al. (2018), this is because each bank has to conduct checks for every client during onboarding, and a client has to undergo the process with every bank they wish to transact with. Blockchain, especially the *Bitcoin* blockchain, has been criticised by some as an enabler of money laundering (Campbell-Verduyn, 2018; Juels et al., 2016). However, the technology can also be used to curb money laundering and reduce KYC compliance costs if applied formally in financial institutions such as banks (Morabito, 2017).

Moyano and Ross (2017) propose a KYC verification system based on distributed ledger technology to reduce the high cost associated with the KYC process in banks and also improve customer satisfaction. The authors posit that the system enhances the KYC process and customer experience by enabling the KYC process to be performed once per customer instead of the customer having to undergo the same process at every institution. Shbair et

al. (2018) implemented an *Ethereum* blockchain-based KYC proof of concept system that uses smart contracts. The proof of concept demonstrated how banks could configure and implement the technology to manage the KYC process despite some challenges with scaling and performance degradation when the number of nodes increased.

Payment clearing and settlements: The contemporary manner of clearing and settling payment transactions is plagued by high inefficiencies and exorbitant costs, particularly for cross-border payments (Rella, 2019). Currently, the payment settlement process includes several participants, such as brokers, intermediary agents and clearing agents; each of these parties maintains a copy of the same transaction record and reconciling these copies is a costly and inefficient process (Morabito, 2017). In cross-border payments, money is sent between parties in different countries with divergent currencies and regulations and relies on intermediary banks in each country to facilitate the transaction. This process makes cross-border payments very complex; however, transacting parties still demand and expect these transactions to be "cost-effective, timely, predictable, and traceable" (Caron, 2018, p. 58). Guo and Liang (2016) suggest blockchain is a better alternative than current methods to address payments involving multiple parties, whereby each party has the right to modify the transaction record as in cross-border payments.

Several industry reports and academic literature have highlighted the importance of blockchain in addressing challenges in payments and settlements. McKay (2014) demonstrated how *BitPesa*, a Kenyan-based remittance system developed using blockchain, facilitates the affordable transfer of funds between Kenya and the United Kingdom. Similarly, in a case study on *Ripple*, a blockchain-based instant money transfer platform enabling users to transfer money from anywhere in the world, Rosner and Kang (2015) found that the platform's distributed settlements surpass traditional money transfer methods. Peters and Panayi (2016) argue that using consortium blockchains can reduce payment clearance time significantly and propose possible ways to apply such blockchains. For instance, the authors suggest clearing agents set up a distributed clearinghouse to enable bilateral clearing.

In addition, blockchain proof of concept projects conducted by global central banks have grown. The South African Reserve Bank also demonstrates the potential use of blockchain

in the payment space through its Project Khoka. The Khoka project aimed to integrate the existing South African multiple-option settlement system with blockchain (The South African Reserve Bank, 2018). According to The South African Reserve Bank (2018), the system reduced transaction processing times from approximately two hours to seconds.

Central Bank Digital Currencies: Another banking application of blockchain that has amassed significant attention from researchers relates to Central Bank Digital Currencies (CBDCs). CBDCs are essentially blockchain-based digital currency versions of national currencies (Elsayed & Nasir, 2022). As the name suggests, CBDCs are issued by central banks in various countries. Many central banks globally are considering issuing or have implemented a CBDC version of their currencies. Interest in the technology is driven by the potential benefits offered by CBDCs.

The literature highlights several advantages of issuing CBDCs and indicates that CBDCs offer a more efficient and cost-effective alternative to physical cash (Kshetri, 2021). Furthermore, CBDCs can complement existing digital services to improve financial inclusion by extending access to digital payments for specific groups of consumers (Panetta, 2018) if barriers such as the high cost of digital devices are addressed. Moreover, the adoption of CBDCs can decrease settlement risks (Ozili, 2022) and “digitalize the economy and achieve innovation across the payments and monetary systems” (Foster et al., 2021).

2.6 CONTEXTUALISING BLOCKCHAIN INTEROPERABILITY IN BANKING

2.6.1 Interoperability in the Banking Sector

As stated previously, interoperability concerns enabling seamless interactions between systems despite differences in their underlying technologies and data models. However, in the banking context, interoperability generally relates to payment systems. Payment systems are complex systems that do not only consist of technological components but include other elements, such as scheme rules and applications (World Bank Group, 2021) and “law and regulation, communication and settlement infrastructure, platforms, standards and institutions” (Berg, 2022). Therefore, interoperability in banking can be achieved by enabling interoperability of the different elements of the payment systems. An example is

the interoperability of payment schemes, in which multiple banks (and, consequently, their clients) can agree to join a scheme that allows seamless payments between users of the banks in the scheme. Essentially, interoperability allows customers operating on different platforms and infrastructures to clear and settle financial transactions across systems without participating in multiple systems (World Bank Group, 2021).

2.6.2 Blockchain Interoperability in the Banking Sector

Blockchain interoperability in the banking context further relates to how emerging payment systems such as CBDCs and other blockchain-based payments would interoperate with each other and existing legacy platforms and infrastructures. Regarding CBDCs, blockchain interoperability becomes a concern when blockchain-based CBDCs are used for cross-border payments where each country has its own CBDC. In such a case, enabling blockchain interoperability capabilities is required to enable CBDCs in different countries to be convertible or exchangeable with each other or with fiat currency (Herrada & Lawson, 2022). This notion of blockchain interoperability is demonstrated in Project mBridge by the Bank for International Settlements (BIS) (Chen et al., 2022). The project demonstrates interoperability between multiple CBDCs by enabling central banks to exchange their respective CBDCs.

When CBDCs are used domestically, interoperability concerns how the CBDCs can communicate with other established domestic payment systems to allow for the seamless transfer of funds across the systems (Chen et al., 2022). Allowing established, popular payment platforms (such as e-money solutions) to be interoperable with CBDCs is critical in driving the adoption of CBDCs by the public already using those platforms (Brunnermeier et al., 2019). Furthermore, it will help reduce the risk of fragmentation and closed-loop systems, which disadvantage users with high risk and high costs (Committee on Payments and Market Infrastructures, 2018).

In addition to the need for emergent blockchain systems to be interoperable with payment systems, blockchains must become interoperable with each other and existing legacy technologies (Berg, 2022). The banking sector is traditionally a collaborative ecosystem involving multiple players from within the sector and other industries and government enterprises. The literature indicates many enterprises within these industries and

government institutions are adopting blockchain (Bellavista et al., 2021) to address inefficiencies in some of their operations. As a result, new blockchain ecosystems of permissioned blockchains (private and consortium blockchains) are emerging.

The use of private and consortium blockchains in many industrial scenarios raises complex questions. The first question pertains to how to establish interoperability between these emerging blockchains and the existing IT systems that have been the backbone of many industries. The concern is that many banks and enterprises depend heavily on centralised core mainframes and other IT systems for their transaction processing, which reduces the likelihood of these technologies being replaced by blockchain. This implies that, for most organisations, it is impractical to overhaul their existing systems to accommodate blockchain; therefore, blockchain systems have to coexist with established systems (Herold et al., 2022). Thus, introducing blockchain into industries and organisations requires new approaches to integrating and interoperating the technology with established IT systems to address new privacy and cybersecurity challenges (Wiatt, 2019). The second question relates to how these blockchains would communicate and interact to sustain existing collaborative relationships (Lu et al., 2023). The current trend in industries is creating permissioned blockchain networks (consortium networks) as “minimum viable ecosystems” (Abebe et al., 2019b, p. 29), which involve only a few participants. This trend caused the emergence of multiple heterogeneous permissioned blockchain networks unable to communicate and, therefore, hinder collaboration. Schaffers (2018) argues that to maintain collaborative relationships and a viable ecosystem, “interoperability and standards across different blockchain platforms and applications are required” (Schaffers, 2018). This study aims to address interoperability issues from this perspective by focusing on blockchain-to-blockchain interactions instead of the interoperability between blockchain and specific payment systems.

2.6.3 Blockchain Interoperability Studies

Several studies are exploring issues and possible solutions to address challenges hindering blockchains from sharing information. The existing scientific literature mainly focuses on technical approaches for addressing interoperability between blockchains. Several surveys (Al-Rakhami & Al-Mashari, 2022; Belchior et al., 2021b; Monika & Bhatia, 2020b; Qasse et al., 2019; Ren et al., 2023) provide differing classifications of existing cross-chain

approaches used to address blockchain interoperability issues. Generally, these surveys provide a foundation for understanding the operations and mechanics of the different approaches.

A survey by Qasse et al. (2019) classified the existing cross-chain solutions into four categories: sidechains solutions, blockchain routers, smart contracts and industrial solutions. Their study elucidates some key limitations with these solutions, such as a single point of failure relating to industry solutions and the limited scope of applications in the case of sidechains, which apply to cryptocurrencies and homogeneous blockchains and cannot address the complexities of interoperating heterogeneous blockchains. Monika and Bhatia (2020b) surveyed interoperability solutions from industry and the academic community and presented a classification containing similar categories to those classified by (Qasse et al., 2019), but also including an additional solution they term bridging solutions. Similarly, they presented the limitations of the respective solutions; however, their survey has been criticised for possibly miscategorising some of the solutions “due to very little information about the solutions in the literature” (Kotey et al., 2023, p. 893). A similar survey was presented by (Belchior et al., 2021b), with public connectors, hybrid connectors and blockchains of blockchains as categories. Their study also proposes a decision framework for selecting interoperability approaches in relation to specific use cases. (Al-Rakhami & Al-Mashari, 2022) discuss existing blockchain interoperability solutions within a supply chain context. A more recent survey provides a performance evaluation of current blockchain interoperability solutions (Ren et al., 2023). Their study also classifies existing solutions into five main categories (sidechains, relays, notary schemes, hash time lock contracts and blockchain agnostic protocols). In addition, they provide additional sub-classes under each category to distinguish between solutions for atomic swaps and those for asset exchange. The following discussion highlights some of the common approaches identified in the surveys.

Notary Schemes

Notary schemes are the simplest method for enabling blockchain interoperability (Haugum et al., 2022a). They utilise a trusted third party to provide cross-blockchain communication and manage transactions between separate blockchains. The third party can be a single

node or a group of nodes. The third-party notary establishes a connection between two separate networks by providing guarantees of the validity of transactions and events on each blockchain. The notary's role is monitoring and recording events on multiple blockchains and providing assurance to the receiving blockchain that an event has indeed occurred on the sending blockchain (Lin et al., 2021). To achieve this, the notary scheme provides "infrastructure (e.g., miner nodes) and service (e.g., event monitoring) to facilitate asset transfer and data exchange" (Ren et al., 2023, p. 7). They do not require changes to the underlying blockchain; however, notaries should be trusted as any malicious activity from them can compromise the integrity of the interoperation process. Therefore, the success of the notary-based interoperability schemes depends entirely on the reliability and honesty of the selected notaries.

A notary scheme can be a single signatory, multi signatory or distributed (Lin et al., 2021). A single signatory scheme uses a single node to verify transactions between the communicating blockchains, whereas the multi-signature scheme employs multiple notaries for data collection and confirming transactions. In this scheme, a transaction is successfully verified and confirmed only if it is confirmed by the majority of the notaries. Though single signatory notary and multi-notary schemes are the simplest to implement and offer high-speed transactions, their centralised nature contradicts the decentralised nature of blockchain technology and makes them susceptible to single-point-of-failure challenges. In the distributed notary mechanism, multiple notaries are randomly allocated fragments of a cryptographic key, and these notaries collectively verify and confirm transactions. For a transaction to be confirmed and verified successfully, it must be confirmed by a predetermined number of the nodes allocated the key fragment and must include a signature/certificate of each of the verifying nodes (Lin et al., 2021). The use of the distributed key enhances the "security and decentralisation of the system" (Zhang & Hou, 2021, p. 326).

Notary schemes have several advantages and drawbacks. A key advantage of using notaries is that they are simple to implement as they do not require the underlying blockchain to be changed. In addition, for the aforementioned reason, notary schemes also offer interoperability capabilities for different blockchains (Wang et al., 2023). However, notary schemes (particularly single notary schemes) suffer from single-point-of-failure challenges

and may also be malicious. These limitations are often minimised by employing a multi-signatory approach.

Sidechains/Relays

Sidechains are scalable mechanisms that offer cross-chain communication. They are side blockchains connected to a main blockchain through a two-way peg. The key role of the sidechain is to support and reduce the workload of the main chain by processing some transactions on behalf of the main chain (M. Sigwart et al., 2021). Sidechains are independent of and separate from the main chain and thus can have features, such as a consensus mechanism and miner nodes, that are different from those of the main chain (Ren et al., 2023). These mechanisms were initially designed to offer interoperability for asset transfer (Buterin, 2016); however, they can also enable interoperability between disparate blockchains. Sidechains enable interoperability between separate blockchains by reading, verifying and confirming transaction data between blockchains wishing to exchange data and assets (Sun et al., 2022). Such verification occurs via a message exchange protocol known as *simplified payment verification* (SPV) (Zhang & Hou, 2021). Some industry blockchain interoperability solutions, such as *PolkaDot*, employ sidechain mechanisms. For instance, *PolkaDot* utilises a sidechain mechanism consisting of a main relay chain and sidechains called parachains. The main relay chain manages and distributes transactions to the parachains, the role of which is to process transactions (Nissl et al., 2021).

Currently, there are three ways of implementing sidechains: 1) centralised two-way peg, 2) federated two-way peg, and 3) *simplified payment verification* (SPV). In the centralised two-way peg approach, a central third party is utilised to lock and unlock the funds between the sidechain and the main chain (Wang et al., 2023). Alternatively, the federated two-way peg or multi-signature design employs multiple nodes or notaries to lock and unlock funds instead of one centralised party. In this case, funds are transferred only when a certain number of nodes have signed the transaction. The federated two-way peg approach was developed to address the drawback relating to the centralised two-way mechanism. Sidechains can also be implemented by pegging a sidechain to a main chain using SPV proofs. An SPV is a lightweight client that verifies the inclusion of a transaction on a

blockchain. SPV works by downloading only the headers of a block instead of the whole blockchain, which makes the process efficient. Furthermore, SPV clients request proof (Merkle Proofs) to verify the inclusion of a transaction in a valid block of the blockchain (Singh et al., 2020).

Using sidechains, especially centralised two-way peg sidechains, is beneficial because of their simple design, which simplifies how they are implemented and managed. In addition, employing two-way pegged sidechains allows for fast processing speeds because the sidechain does not have to include complex locking mechanisms (Singh et al., 2020). Federated sidechain solutions have the advantage of enhancing the decentralisation of multi-blockchain systems (Wang et al., 2023), while SPV sidechains eliminate the need for third parties when enabling interoperability for asset transfer between blockchains. However, similar to notaries, the sidechain approach is prone to single-point-of-failure risks and malicious behaviour (Ren et al., 2023). Moreover, the SPV approach has some limitations relating to the duration for transactions to be confirmed and for users to gain access to their funds (Singh et al., 2020).

Hash Locks

Hash time lock contracts are smart contract-based payment agreements for cross-chain atomic swaps. They use hash and time locks to aid interoperability between two blockchains. Hash locks and time locks are used to secure the transaction and reduce counterparty risk (Bhatia, 2020). Hash time lock contracts achieve fair atomic swaps by locking assets and binding the transacting parties to issue a cryptographic hash as proof of payment before a set period elapses (Haugum et al., 2022a; Lin et al., 2021). Hash time lock mechanisms do not rely on a third party and involve very little data exchange between the transacting party to enable interoperability (Koens & Poll, 2019). However, their functionality is only limited to asset swaps and does not allow complete asset transfer between blockchains (Wang et al., 2023).

Blockchain Oracles

Blockchain oracles are third-party systems or agents connecting blockchains with the real world. They collect information from different external data sources (e.g., cloud, the IoT, weather, financial, *et cetera*) and send it to blockchain smart contracts as transaction data and *vice versa* (Ezzat et al., 2022). Blockchains and smart contracts are not designed to access external data. However, for many industrial and enterprise applications, information must be shared between blockchains and non-blockchain systems. Oracles act as a link between blockchain ecosystems and existing data sources, legacy systems, and complex computations that cannot be executed on the blockchain.

Oracles can be classified in different ways depending on the nature of the data source (software, hardware or human), the direction in which the information flows (inbound or outbound), the underlying trust model (centralised or decentralised) (Beniiche, 2020) or based on the design pattern used (Al-Breiki et al., 2020). Although oracles can connect blockchain to external systems and are easy to implement, they are limited in terms of the trust and reliability of the data they transfer. This is because oracles connect trusted and untrustworthy external systems, and thus, the validity or correctness of the information they source from external sources cannot be guaranteed (Caldarelli, 2020). Furthermore, oracles introduce a central, single point of failure, which goes against the purpose of decentralising blockchain systems (Berger et al., 2020).

Applications Programming Interface (API) Gateway

An API gateway is a single point of entry through which all API messages/calls for an application are exchanged. API gateways are already in use in most enterprises to connect disparate ICT systems and facilitate real-time data transfer. APIs are rules and protocols often used to build and integrate new software applications into existing systems or architecture. They enable applications to communicate without the need to know the internal workings of each application. API gateways can be integrated with blockchains to enable interoperability between heterogeneous blockchains and blockchains with non-blockchain data. Through APIs, external applications can send message calls to the blockchain and *vice versa*. For instance, events triggered on a smart contract can be captured by the

blockchain API layer and used to send messages to the external non-blockchain system; alternatively, the blockchain can invoke an API exposed by the non-blockchain application to source data from the external applications (Wipro, 2023). Interoperability between heterogeneous blockchains can also be implemented through API integration. In this case, each blockchain can expose its API, and the blockchain can communicate using its exposed APIs (Hitarshi, 2020). In addition, API gateways can also provide security by verifying and validating API requests (Niya et al., 2021).

In addition to the surveys above, other studies have proposed interoperability frameworks for blockchain systems. Pillai et al. (2023) propose a design decision framework for designing cross-chain integration systems. Integration systems or mechanisms enable interoperability by creating a physical link or connection between a network and other networks outside its boundaries and, as a result, enable the exchange of information across network boundaries. Their framework proposes five steps to guide developers in the selection of the appropriate integration solution: identifying an application's value type (data to be shared), identifying integration goals, selecting an approach (centralised or distributed), selecting an integration mode (third-party, bridge, connector or other), and selecting the integration protocol. Furthermore, Pillai et al. (2023) discuss some security assumptions concerning each of the possible integration modes. Another study by Nodehi et al. (2022) presents an enterprise blockchain design framework that includes architectural elements for designing enterprise blockchain systems. The framework includes an interoperation layer to support connectivity between the blockchain and external systems. The authors argue that the interoperation layer enables external data sources to be connected to the blockchain; however, details regarding how this interoperation is achieved are not included or discussed in that study.

Belchior, Riley, et al. (2022) propose a decision framework to support the selection of an interoperability solution or mechanism. The authors first proposed a potential assessment criterion to evaluate the interoperation capabilities of a solution. In addition, the study presented a framework to determine if an interoperability solution is required or not based on infrastructural choices as well as the functionality that the solution should provide. In the study, the infrastructural choices relate to the infrastructure on which the solution is hosted, which could be a DLT node, DLT proxy or DLT gateway. The authors defined the

functionality of the solution based on two elements: what is being connected (homogenous network and subnetworks or heterogeneous networks) and the level of interoperability desired (semantic, organisational and either or both legal). However, their framework is limited because it ignores other important considerations that should be factored in when selecting interoperability solutions. For instance, their solution considers the availability of the solution as a consideration in selecting a solution, but other critical considerations, such as security and privacy, are not included. Furthermore, this framework does not address aspects relating to the types of blockchains being connected. In the current study, we argue that knowing which types of blockchains being connected is essential to selecting the correct interoperability solutions. This is necessary because the requirements the solution should meet vary based on the nature of the blockchain systems being connected. For example, connecting a private blockchain to a public blockchain has different security requirements than those required when two public blockchains are connected.

The studies discussed above provide some invaluable insights regarding the different considerations and design choices for enabling interoperability between blockchains and other systems; nevertheless, they are not comprehensive. Most of the studies focus on semantic and technical interoperability solutions and overlook key considerations for enabling other forms of interoperability, such as legal and organisational interoperability. In addition, pertinent requirements interoperability solutions should fulfil are ignored in the studies. Moreover, the studies focus primarily on public (permissionless) blockchains while mostly ignoring interoperability issues relating to connecting permissioned (private/consortium) networks in enterprise settings. Therefore, the present study proposes to address these deficiencies by developing a comprehensive blockchain interoperability framework to address enterprise challenges relating to interoperating blockchain systems.

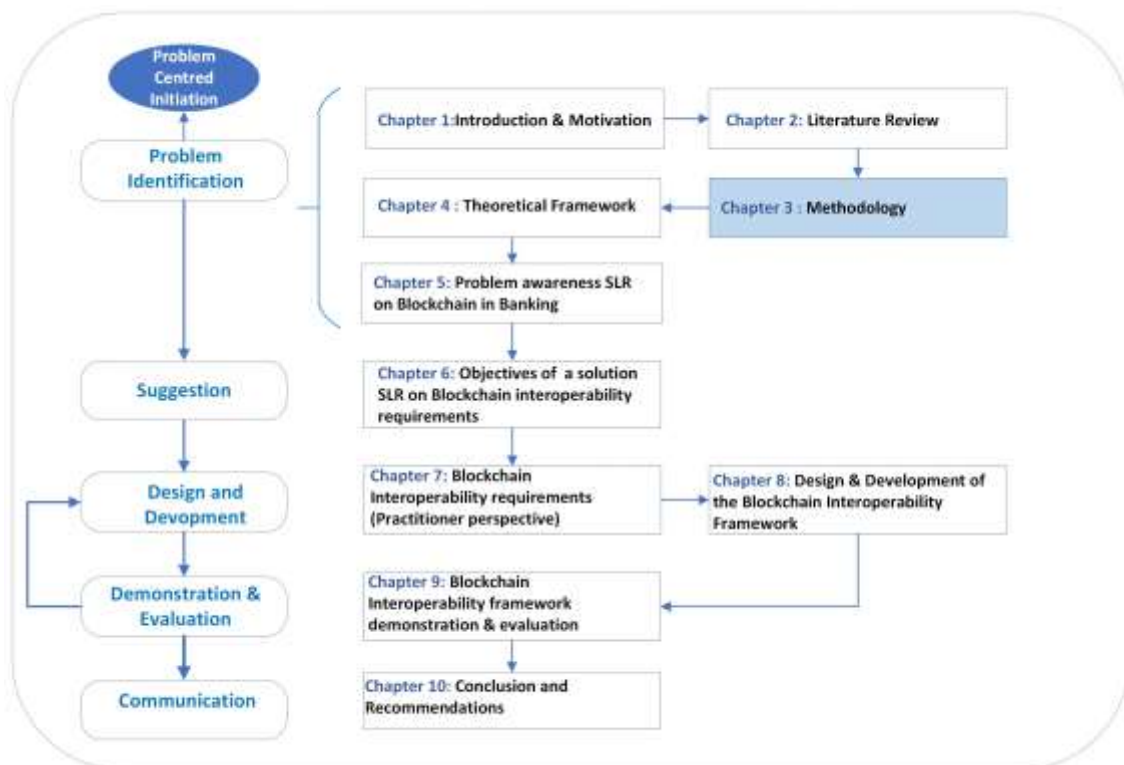
2.7 SUMMARY

This chapter presented the literature relating to blockchain technology and interoperability. First, the chapter discussed concepts related to blockchain technology as a foundation for the rest of the chapter. This discussion proceeded to discuss interoperability in information systems briefly. Thereafter, the study introduced and elucidated the concept of blockchain interoperability, followed by a discussion in which blockchain interoperability was

contextualised for the banking sector, highlighting some important banking use cases that necessitate interoperability between blockchain systems. Lastly, the chapter presented a review of the current literature focusing on addressing interoperability obstacles relating to blockchain technology and, from these studies, identified deficiencies. The next chapter elaborates on the study methodology for the current research.

CHAPTER 3

3 METHODOLOGY



3.1 INTRODUCTION

This chapter discusses the research methodology employed to answer the research questions stipulated in this study. A research methodology is a logical and systematic process that a researcher follows to address the research problem (Kothari, 2004). The methodology includes the philosophical beliefs and assumptions of the researcher about reality and knowledge (Melnikovas, 2018). The researcher's beliefs about reality, knowledge and how that knowledge can be acquired constitute the research philosophy or philosophical paradigm of the research. Further, these beliefs influence how the researcher conducts the research or methodology. According to Saunders et al. (2015), the research philosophy is the starting point of a methodology. The research approach, strategy and techniques, and procedure for data collection and analysis follow subsequently.

The upcoming sections highlight the study's methodology of following the research onion by (Saunders et al., 2015). The first section discusses the research philosophy underpinning this study, followed by the research design. The research design guides how, from whom, and when to collect data (Kothari, 2004). As such, the research strategies, data collection, and analysis techniques are discussed collectively under the research design section.

3.2 RESEARCH PHILOSOPHY

A research philosophy is a set of beliefs and assumptions about the development of knowledge (Saunders et al., 2015). The purpose of research is to create knowledge in a particular field of study, and often, the researcher undertaking the study brings along specific beliefs and views of the world and knowledge creation. These views may influence the research process; thus, the researcher should be aware of and reflect on these assumptions and views in their study (Cresswell, 2014).

A study's philosophical assumptions provide the basis for a philosophical paradigm. Guba and Lincoln (1994) describe a paradigm or worldview as a broad philosophical stance about how reality is perceived and knowledge is gained (Žukauskas et al., 2018). A paradigm defines an underlying belief system guiding a research investigation (Guba & Lincoln, 1994). It consists of shared assumptions about reality and knowledge and how knowledge can be acquired. These assumptions can be adopted by an individual or shared by a group of scholars (Hirschheim & Klein, 1989). These assumptions constitute ontology, epistemology, and axiology (methodology) (Cresswell, 2014).

Ontology refers to an assumption about the nature of reality and may also refer to the objectivity or subjectivity of reality (Boman et al., 2017). Ontological assumptions determine how a researcher views the object under study (Cresswell, 2014). Epistemology denotes how we understand the world, how knowledge is perceived and acquired, and the nature of truth (Boman et al., 2017). Epistemology also determines the nature of the relationship between a researcher, the subjects and the object being researched (Aliyu et al., 2015; Guba & Lincoln, 1994). Epistemological assumptions are influenced and determined by ontological assumptions (Denzin & Lincoln, 2018). On the other hand, axiology represents the values, beliefs and ethical considerations a researcher brings to the research

(Melnikovas, 2018). The axiology determines how the researcher conducts the research, i.e., "how the inquirer (would-be knower) goes about finding out whatever he or she believes can be known" (Guba & Lincoln, 1994, p. 108). A paradigm and its assumptions guide the research approach during its execution (Boman et al., 2017).

3.3 PHILOSOPHICAL PARADIGMS

Several research paradigms can be used within information systems research, of which the most commonly used are positivism, pragmatism and interpretivism (see summary in Table 3-1). According to (Cresswell, 2014), these paradigms differ depending on their ontological, epistemological and axiological elements.

3.3.1 Positivism

Positivism is a philosophical research paradigm which views the world from the perspective of a natural scientist (Saunders et al., 2015). It is based on the assumption of measurable relationships between the variables of a phenomenon (Orlikowski & Baroudi, 1991). Such relationships are often measured by applying natural scientific methods of measurement, such as experimentation, to study and understand the social world (Crotty, 1998). Thus, within positivist research, knowledge is acquired through observation and experimentation, independent of context, view, opinions and culture (Cibangu, 2010).

The positivist ontological assumption is that there is a single objective reality independent of the individual observer, and reality is only that which is observable and measurable (Park et al., 2020). The positivist epistemology involves an objective researcher who is separate from the research object. The researcher acts as an observer of the phenomenon and does not influence the outcome of the study. Positivist studies primarily aim to test theories to predict and understand a specific phenomenon (Orlikowski & Baroudi, 1991). Such a theory is tested by proposing hypotheses which test cause and effect relationships between variables, making inferences and often generalising results to a specific population (Cibangu, 2010; Orlikowski & Baroudi, 1991).

The positivist paradigm has been criticised for providing deterministic explanations of a phenomenon without considering the context and complex dynamics of the social world.

This study intends to understand the phenomenon of blockchain interoperability within the specific enterprise context of a bank. Therefore, positivism cannot be applied in this case. Furthermore, positivism has been criticised for not being "conducive to the discovery and understanding of non-deterministic and reciprocal relationships" (Orlikowski & Baroudi, 1991, p. 13), which may exist in a complex social context such as a bank. In addition, this study intends to provide an in-depth understanding of the phenomenon rather than make predictions; as such, the study did not follow the positivism paradigm, which focuses on theory testing and can be generalised and used to predict future occurrences.

3.3.2 Interpretivism

The interpretivist paradigm is based on the subjective ontological assumption that reality is socially constructed and dynamic (Melnikovas, 2018) and holds that there are multiple realities which are individually and socially constructed (Schwartz-Shea & Yanow, 2012). Interpretivism aims to understand social phenomena in their contexts and the interpretations of individuals regarding their interactions with a specific phenomenon (Rehman & Alharthi, 2016). It can also create new meanings and understandings of the social world (Saunders et al., 2015). Interpretivist research regards the researcher and the object of the research as intertwined and inseparable (Žukauskas et al., 2018). The researcher participates actively in the research by interacting directly with the respondents and may apply their worldview to guide the research (Pather & Remenyi, 2005).

In addition, the interpretivist paradigm aims to understand a phenomenon from the individual participants' perspectives and from within the context of the phenomenon (Rehman & Alharthi, 2016). Interpretivist researchers do not collect quantitative data as in positivist studies to understand the meanings individuals attribute to a specific phenomenon; instead, the researcher collects data describing feelings, opinions and perceptions, among others (Pather & Remenyi, 2005). The collected data are often analysed inductively to identify patterns and themes and build theory (Gioia & Pitre, 1990). Interpretive studies do not seek to generalise findings from one context to a population, as with positivist studies; however, the studies seek to understand a phenomenon in depth, and their findings can be extended to other settings (Orlikowski & Baroudi, 1991). Pather and Remenyi (2005) explain that interpretivism seeks to understand a phenomenon rather than predict it and to build a theory

that provides a detailed description, insights and explanations of the phenomenon under study (Gioia & Pitre, 1990).

The interpretive paradigm has been criticised for several reasons. Critics of the paradigm argue that because the paradigm allows for direct involvement of the researcher with the participants, the researcher may influence the participants' views and responses, which may, in turn, lead to a lack of objectivity and bias. However, proponents of interpretivism argue that this criticism can be addressed by collecting data from multiple sources and applying triangulation (Pather & Remenyi, 2005). Schwartz-Shea and Yanow (2012) further note criticism by critical theorists who claim interpretive research relates more to establishing meanings while ignoring what critical theorists regard as pertinent issues, like the institutional aspect of power and domination. The paradigm also receives criticism for its lack of generalisability (Schwartz-Shea & Yanow, 2012), namely that using qualitative data, which are not measurable, limits the generalisability of interpretive research findings to a larger population; consequently, such studies are deemed ineffective in addressing the validity of the results. Given the above-mentioned arguments and this study's intention to construct a framework, we concluded that the interpretive approach would not suffice.

3.3.3 Pragmatism

Pragmatism does not support the traditional worldview of the dualism of objectivity and subjectivity as two mutually exclusive concepts (Biesta, 2010). Rather, a pragmatist views the world by juxtaposing the two concepts. Ontologically, pragmatists acknowledge the objective existence of the physical world apart from human experiences (Kaushik & Walsh, 2019), yet believe that the social world is a construction of individual human actions and differs according to the individual's experiences, beliefs and actions (Goldkuhl, 2008; Kaushik & Walsh, 2019; Morgan, 2014). A pragmatic researcher can select a reality based on how that choice results in achieving the desired outcome within a specific context (Biesta, 2010). In a study grounded in pragmatism, the researcher becomes an active participant in and interpreter of the study, and their prior experiences and beliefs inform the researcher's choices concerning the types of research questions, methodology, and research tools (Morgan, 2007). Thus, the researcher does not separate themselves from the object of the study and instead becomes an active participant by interacting with the information systems artefact being developed and the organisation using the artefact. The researcher selects the

research questions intentionally, choosing the methodology and tools they believe can best answer the research question.

Pragmatism makes the epistemological assumption that valid knowledge is a consequence of belief, action and experience. Pragmatists believe that knowledge comprises inferences and assertions derived from the consequences of taking action and the experience applied during an enquiry (Morgan, 2014). Hence, from the pragmatist perspective valid knowledge is only that which results from some action or by interacting with the environment. Goldkuhl (2008) identifies three forms of pragmatism: functional, referential and methodological, which demonstrate different relationships between knowledge and action. Functional pragmatism asserts that knowledge should be useful and applied through actions. Within IS, functional pragmatism involves using and applying models and frameworks to guide practice (Goldkuhl, 2008). Referential pragmatism involves describing the world based on actions taken by using theories, whereas methodological pragmatism refers to knowledge about the world acquired through actions. Figure 3-1 demonstrates these three types.

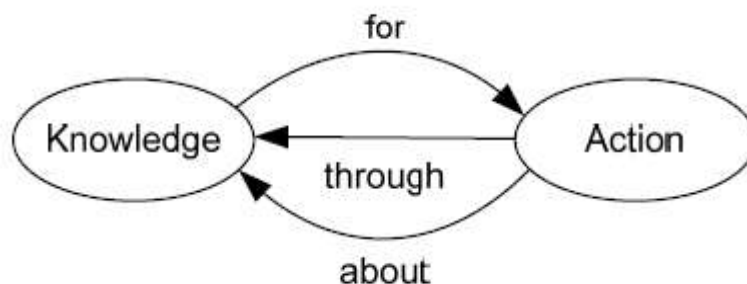


Figure 3-1 The three relationships between knowledge and action in pragmatism (Goldkuhl, 2008)

Figure 3-1 demonstrates that pragmatists regard valid knowledge only as that which results from actions. Pragmatists believe that knowledge is a social construct and is always based on human experiences of interacting with the world and that these experiences differ between persons (Kaushik & Walsh, 2019). This belief implies that knowledge is not universally constant but varies between individuals, depending on their experience and practices. Furthermore, other pragmatists view valid knowledge as provisional and context-dependent (Vo, 2012). Goldkuhl (2011) suggests that pragmatism is well-suited to design science research approaches which involve artefact development and are used to build

theories. Hevner (2007) and Hovorka (2009) support this view of design science research as the support for a pragmatic paradigm.

Considering this study aims to construct an artefact in the form of a blockchain interoperability framework to provide a better understanding of blockchain interoperability, the study adopted the pragmatic paradigm. Pragmatism is deemed an appropriate paradigm for this study for several reasons: Pragmatic research advocates for the pursuit of knowledge through experience and action (Goldkuhl, 2008), and pragmatism promotes the idea that research should use experience and actions that work to produce actionable that solves existing problems (Yvonne Feilzer, 2010). This study intended to design a framework for addressing the current challenges organisations (particularly banks) experience concerning interoperating blockchain with other blockchains and existing systems. The construction of the framework requires both experiences and actions; as such, approaching it from a pragmatic perspective is appropriate. In addition, pragmatism allows for multiple perspectives from which to interpret the world (Kelemen & Rumens, 2012) and a pluralist application of methods (Goles & Hirschheim, 2000). Accordingly, a pragmatic researcher can select and apply research methods best suited to solving the problem under study (Tashakkori et al., 1998). Therefore, a researcher can mix methods and leverage from either the interpretivist or positivist perspectives, which enables the researcher not only to gain an in-depth understanding of a phenomenon but also to appreciate the complexities of the specific context in which the phenomenon occurs (Creswell, 2013).

3.3.4 Critique of Pragmatism

Several criticisms have been levelled at pragmatism in research, of which one is its relaxed view of the truth. Critics argue that the pragmatic stance that truth is not constant and that it changes with circumstances could lead to moral degradation in society. According to Bertrand Russell's essay on the definition of truth cited in (Vocal Philosopher, 2018), the pragmatic view of the truth that holds any belief true as long as it works has undesirable moral consequences because it implies that if any group of people agree on an idea (good or bad), that idea can be deemed correct. Another argument against pragmatism is that its focus on "what works" removes pragmatism from its important philosophical grounding (Hesse-Biber, 2015). The author further criticises pragmatism for not providing a clear logic to guide researchers in determining what works and deciding what legitimate, useful

knowledge is. In addition, Denzin (2010) argues against the pragmatic focus on the practical. He argues that this focus encourages researchers to adopt a soft approach that avoids the significance of having a clear epistemological distinction between qualitative and quantitative research. Thompson (1996) contends that the problem-centred nature of pragmatism inhibits how researchers identify and analyse structural social problems. A further criticism is that pragmatism favours the research question over the method or philosophy underpinning it (Doyle et al., 2009).

The researcher acknowledges the above-mentioned criticism and limitations of pragmatism yet believes that the problem-centred nature of the pragmatist paradigm is well-suited to achieving the main objective of this study, which is to address the blockchain interoperability problem. Furthermore, pragmatism is regarded as a more suitable approach than other prominent paradigms in probing the “inner world of organisational processes due to its emphasis on knowledge generated through experience and action” (Kelly & Cordeiro, 2020, p. 4). These aspects make a pragmatism lens suitable for this study, which intends to develop a blockchain interoperability framework to guide and assist organisations (particularly banks) to understand and achieve blockchain interoperability. Developing the framework requires the researcher to draw knowledge from the experiences of participants from the banking sector and generate knowledge by constructing the framework.

Table 3-1 Summary of the comparison between the positivism, interpretivism and pragmatism paradigms

	Positivism	Interpretivism	Pragmatism
Ontology (nature of reality)	<ul style="list-style-type: none"> • A single objective reality, independent of the individual observer 	<ul style="list-style-type: none"> • Reality is socially constructed and dynamic 	<ul style="list-style-type: none"> • Dualism of reality is natural and socially constructed
Epistemology (nature of knowledge)	<ul style="list-style-type: none"> • Believes that knowledge is only that which can be tested through experiments and proofs 	<ul style="list-style-type: none"> • Understands the phenomenon from the perspective of individual participants and from within the context of the phenomenon 	<ul style="list-style-type: none"> • Valid knowledge is a consequence of belief, action and experience
Methodology	<ul style="list-style-type: none"> • Seeks to test theories • Favours quantitative research methods (surveys, experiments, statistical analysis) for precise measurement and comparison. 	<ul style="list-style-type: none"> Seeks to understand meanings individuals attribute to a specific phenomenon, Qualitative Emphasises qualitative methods (interviews, case studies and observations) 	<ul style="list-style-type: none"> Combines both qualitative and quantitative methods to provide an in-depth understanding of a phenomenon
Axiology Role of researcher	<ul style="list-style-type: none"> • An objective researcher who is separate from the object of research 	<ul style="list-style-type: none"> • Subjective researcher and the object of the research are intertwined and inseparable 	<ul style="list-style-type: none"> • The researcher's values play a large role in interpreting results, • The researcher adopts both objective and subjective perspectives
Limitations	<ul style="list-style-type: none"> • Over-simplifies reality by disregarding contextual conditions 	<ul style="list-style-type: none"> • The subjective role of researcher introduces bias 	<ul style="list-style-type: none"> • Problem-centred nature inhibits how researchers can identify and analyse structural social problems

3.4 RESEARCH STRATEGY: DESIGN SCIENCE RESEARCH (DSR)

The study adopted the design science research (DSR) approach to answer the research questions stipulated in Chapter 1 of this study. Design science research is grounded in the pragmatist research paradigm and supports the creation of artefacts to solve real-life problems (Hevner et al., 2004). DSR originated as a research paradigm in the architecture and engineering disciplines; however, through the work of researchers such as (Hevner et al., 2004; Peffers et al., 2007), DSR has found popularity within information systems (IS) and information technology (IT) fields. DSR manifests in information systems literature in two forms: either as a paradigm (Baskerville et al., 2018; Gregor & Hevner, 2013) or as an approach (Weber, 2010). This study follows the latter view of DSR as an approach grounded in the pragmatism paradigm and promotes the creation of IS artefacts.

3.4.1 An Overview of Design Science

DSR is a problem-solving approach to conducting research (vom Brocke et al., 2020), which advocates for the construction of artefacts to solve real-life problems (Gerber et al., 2015). Kuechler and Vaishnavi (2012) define DSR in IS as research that facilitates learning by constructing IS artefacts to generate new knowledge related to a specific problem. Similarly, Adomavicius et al. (2008) define DSR within IT contexts as the creation and evaluation of IT artefacts through which organisational IT problems can be solved. DSR can be applied to create new innovative solutions to problems or drive improvements or change within a particular context (Kuechler & Vaishnavi, 2012). The core of DSR encompasses the development of sociotechnical artefacts that solve a specific problem and are useful within a particular context (Gregor & Hevner, 2013). In DSR, researchers can contribute to the body of knowledge (design knowledge) by creating an innovative artefact to address a real-life organisational problem (vom Brocke et al., 2020). In essence, the crux of DSR is to generate knowledge to support the creation of artefacts as opposed to emphasising the act of creation itself.

3.4.2 Design Science Research Contribution

Every research discipline strives to contribute to the body of knowledge (Straub et al., 1994). However, the nature of this contribution has been questioned and debated in DSR, resulting in opposing views, with some researchers arguing for design theories as the only contribution and others for the artefact as the only contribution. Gregor and Hevner (2013) instead argue that these perspectives are complementary and that both theory and the artefact can be viewed as contributions to the body of knowledge.

The primary form of knowledge contribution in DSR is design knowledge (Baskerville et al., 2018). Design knowledge is inherently prescriptive and provides prescriptions for design and actions (Gregor & Hevner, 2013). Gregor and Hevner (2013) argue that the generation of this knowledge and the level of knowledge contribution depends on several factors, such as the maturity of the problem (problem maturity) and the maturity of the available solutions (solutions maturity). Figure 3-2 depicts the knowledge contribution matrix proposed by (Gregor & Hevner, 2013).

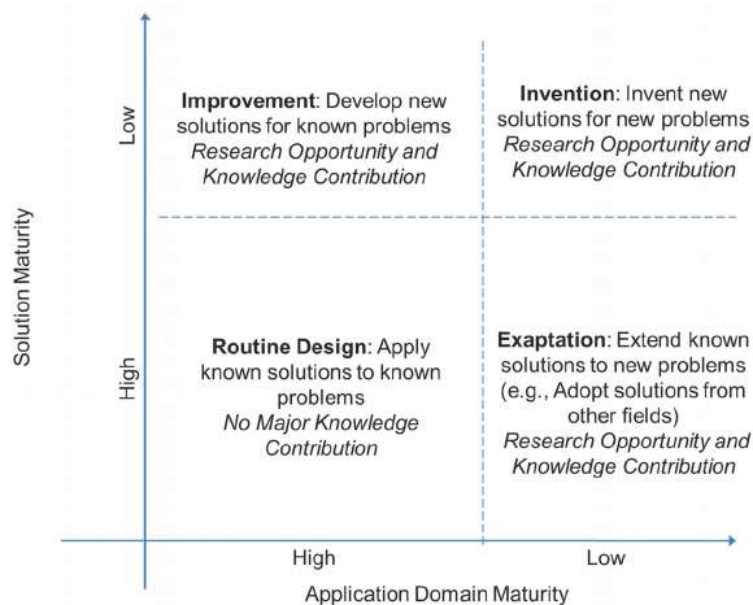


Figure 3-2 DSR knowledge contribution matrix (adapted from Gregor & Hevner 2013)

Gregor and Hevner (2013) matrix categorises DSR contributions according to four types of projects: routine design, exaptation, improvement and invention. They define routine design projects as ventures focusing on a very well-understood problem domain addressed using existing artefacts in a routine. They argue that routine projects do not contribute research knowledge because solving the problem in such projects does not require any research methods. Exaptation involves the application of an existing known solution to new problems. In this case, the knowledge contribution can be either or both in the form of an artefact and a design theory. Improvement projects relate to projects in which the researcher focuses on improving an inadequate artefact or creating an entirely new artefact to solve a contextual problem. With improvement projects, the contribution is the artefact itself as well as a nascent design theory resulting from gaining a better understanding of the problem and solution domain. Knowledge contributions in the form of an artefact and a well-developed theory can manifest through invention projects in which a novel solution to a new problem is provided. Essentially, the knowledge contribution matrix provides for the contribution of a DSR project to be either or both an artefact and a design theory. The design theory prescribes how artefacts can be constructed and evaluated (Baskerville et al., 2018) and should explain why the artefact works in a specific context (March & Smith, 1995).

In DSR, an artefact refers to artificial or man-made objects created to solve a practical problem (Weigand et al., 2021), in contrast to naturally occurring objects. Hevner et al. (2004); (March & Smith, 1995) identified the following categories of DSR artefacts:

- Constructs: vocabulary and symbols
- Methods: abstractions and representations
- Models: algorithms and practices
- Instantiations: implementations and prototypes

This study's contribution resides in the contribution types described under the invention projects shown in Figure 3-2. The study explored a novel solution to a new problem. Though the interoperability of information systems is a well-researched area in IS, the blockchain interoperability problem is still very new and unique to the field. As indicated in the literature, the novelty of blockchain technology means that existing interoperability tools, models and frameworks cannot address interoperability issues in blockchain systems. Therefore, this

study contributes a new solution in the form of a blockchain interoperability framework designed to guide banking enterprises through the process of implementing blockchain interoperability. In addition, the study contributes to the advancement of knowledge on blockchain interoperability.

3.4.3 The DSR process and its application in this study

The process of knowledge generation in DSR can follow various approaches, as suggested by the models proposed by (March & Smith, 1995; Peffers et al., 2007; Vaishnavi & Kuechler, 2004). Despite some variations in the DSR process among the proposed models, some key overarching activities can be identified. The first activity stems from the nature of DSR as a problem-centred approach to research, which is to identify a practically relevant problem to solve. Second, the solution to the identified problem should be an artefact. Thus, the second common activity is the development and evaluation of an artefact to address the identified problem. The third key activity comes about as a consequence of the development and evaluation of the artefact, namely the generation of new knowledge (theory) (Baskerville et al., 2018). This study adopted the design science research methodology (DSRM) by (Peffers et al., 2007) (see Figure 3-3), as discussed below.

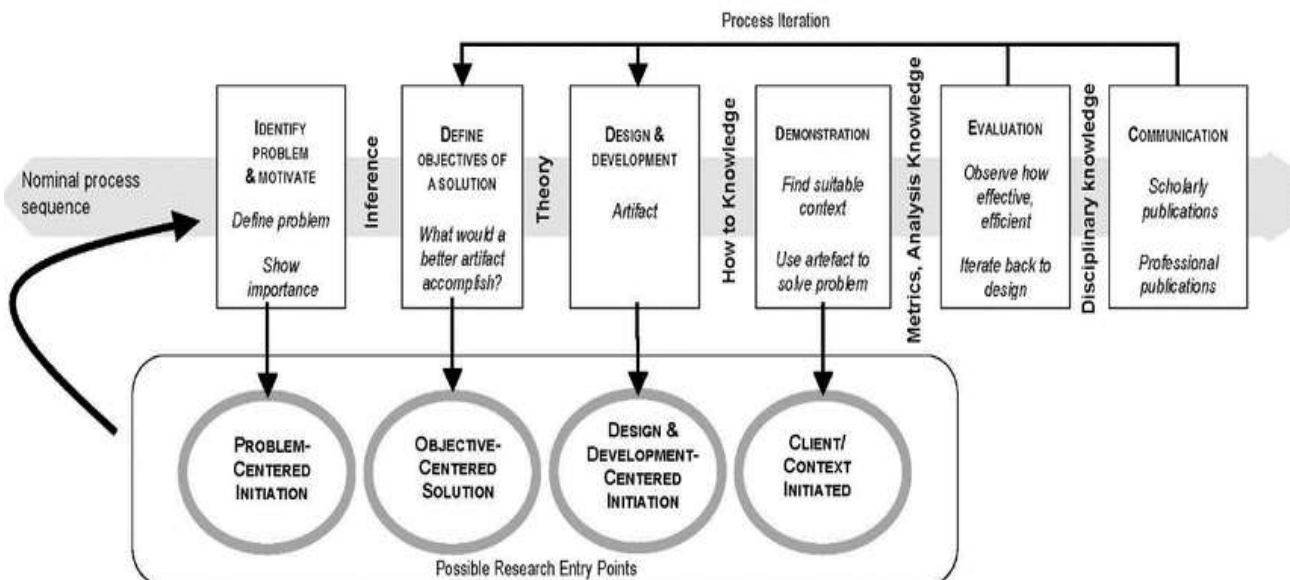


Figure 3-3 DSR process model (adapted from Peffers et al., 2007)

According to the model depicted above, the DSR process follows an iterative process through six nominal steps described below. The DSR process can start at different entry points, depending on the nature of the project. The project can be initiated from a problem-centred, objective-centred, design and development or context perspective. Below is an overview of the nominal steps and how they are applied in this study (as summarised in Figure 3-4).

Step 1: Problem Identification

According to the model, a DSR project starts with problem identification. In this step, Peffers et al. (2007) suggest identifying a specific research problem and providing a rationale to justify the need for the solution. Such identification requires the researcher to comprehend the state of the problem and the benefit of solving the problem. The problem can be identified from an organisational or business need or an opportunity resulting from an emerging technology (Offermann et al., 2009). However, the problem should be relevant to the specific context (Hevner et al., 2004).

This study identified an existing problem from the literature. A systematic literature review (Chapter 5) was performed to explore the nuances of the problem from various literature sources, which included peer reviews, academic articles and industry reports. The findings from the systematic literature review indicated a lack of interoperability of blockchain systems as one of the key challenges in many organisations, including the banking sector. In particular, the literature indicated that enabling the interoperability of blockchain systems is a complex undertaking for many organisations due to the novelty and peculiarities of blockchain technology that make traditional approaches to interoperability unsuitable. Chapters 1 and 5 of this study describe the motivation to address this problem.

Step 2: Define Objectives of a Solution

This step requires the researcher to infer the objective of the solution from the problem definition and knowledge of what is feasible and possible. These objectives can be viewed as the requirements the solution should meet to solve the identified problem and can be

expressed qualitatively or quantitatively. The step further requires the researcher to understand existing solutions and their limitations. The researcher may utilise available knowledge such as tools, technologies, methods or theories to determine the feasibility of the intended solution and also identify the required capabilities for the solutions (Geerts, 2011).

This study identified the objectives of the solution through a systematic literature review, as explained in Chapter 6. The purpose of the systematic literature review was to identify the various interoperability requirements for blockchain interoperability in organisational contexts. Specifically, the systematic literature review sought to understand the fundamental elements and considerations (from technological, organisational, semantic and legal perspectives) to consider when addressing blockchain interoperability in organisational contexts.

Step 3: Design and Develop

This step involves constructing the artefact. The artefact can fall under any of the broad categories defined by (Hevner et al., 2004) and should include knowledge contribution as part of the design.

In this step, an enterprise blockchain interoperability (EBI) framework was constructed. The construction of the framework was guided by the requirements collected using the systematic literature review in Chapter 6, as well as the requirements collected through an interview process involving blockchain experts and analysing webinars, as explained in Chapters 7 and 8.

Step 4: Demonstration

This step requires the researcher to demonstrate the use of the developed artefact to solve one or more instances of the problem. This could be accomplished through an experiment, simulation, case study, proof or another relevant approach.

The demonstration of the proposed framework was operationalised through an illustrative scenario derived from three real-life projects from the banking sector. The purpose of the demonstration was to showcase the applicability of the proposed framework. Chapter 9

explains the evaluation process followed and the rationale for the selected demonstration approach.

Step 5: Evaluation

In this step, the developed artefact is evaluated to measure how well it solves the problem. This activity requires a comparison of the objective of the solution to the actual results obtained from the demonstration artefact. The choice of evaluation approach depends on the nature of the problem and the solution produced.

The evaluation process in this study followed an ex-post, summative, expert evaluation approach. In this process, a sample of blockchain experts evaluated the proposed framework through one-on-one interview sessions. The evaluation was guided by a set of questions based on selected evaluation criteria proposed by (Prat et al., 2014), as explicated in Chapter 9.

Step 6: Communication

The communication step involves articulating the identified problem and its relevance, the developed artefact and its novelty and use, the rigour of its design, and its effectiveness to the relevant audience. The communication process includes this dissertation and other scholarly conference and journal publications published as part of this study. Table 3-2 below outlines the publications.

Table 3-2 A list of publications forming part of this study

DSRM step	Publication
Problem awareness	Mafike, S.S., & Mawela, T. (2022). "Blockchain design and implementation techniques, considerations and challenges in the banking sector: A systematic literature review", <i>Acta Informatica Pragensia</i> , Prague University of Economics and Business, vol. 2022(3), pages 396–422.
Objectives of a solution	Mafike, S.S., & Mawela, T. (2023). Requirements for interoperable blockchain systems: a systematic literature review. In: M.Younas, M., Awan, I., Benbernou, S. & D. Petcu (Eds.), <i>The 4th Joint International Conference on Deep Learning, Big Data and Blockchain (DBB 2023). Deep-BDB 2023. Lecture notes in networks and systems</i> , vol 768. Springer, Cham. https://doi.org/10.1007/978-3-031-42317-8_4
Objectives of a solution and Preliminary framework Design	Mafike, S.S., & Mawela, T. (2023). Towards a blockchain interoperability framework. Presented at BLOCKCHAIN'23: 5th International Congress on Blockchain and Applications University of Minho Guimarães, Portugal, July 12–14, 2023.

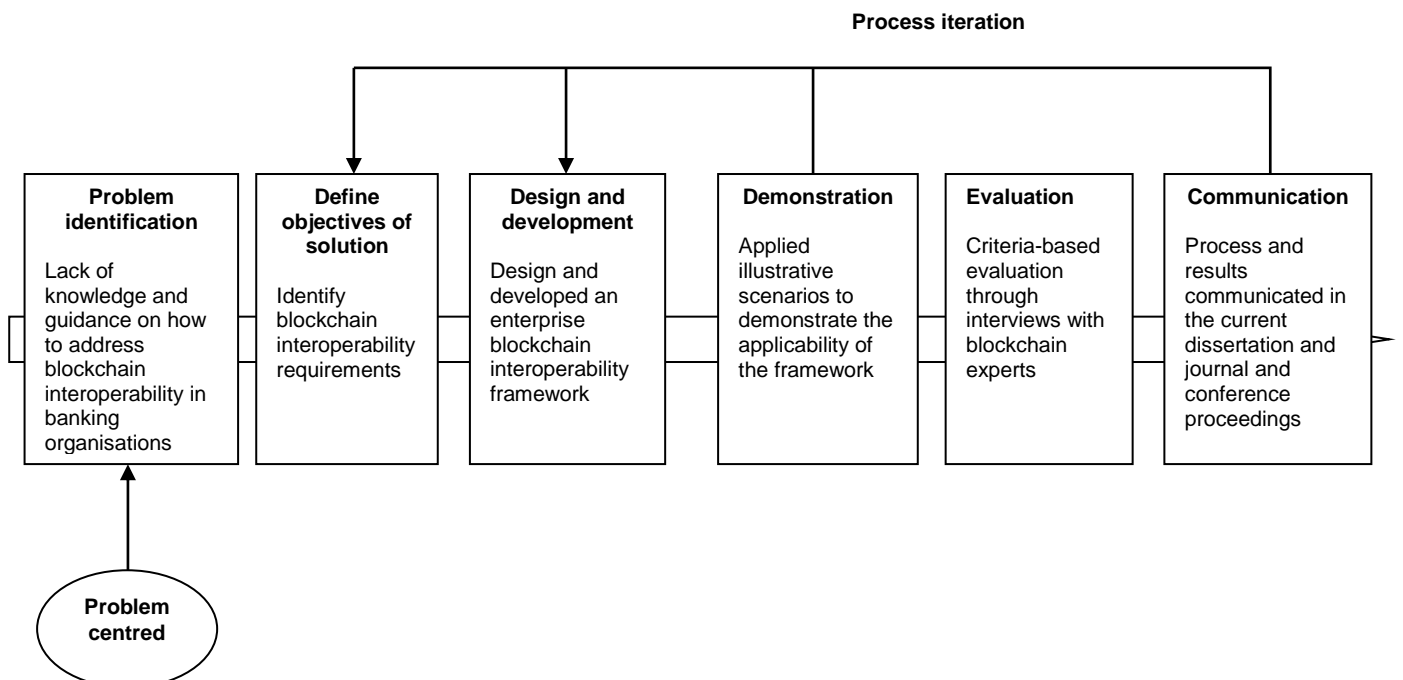


Figure 3-4 An overview of the DSRM process followed in this study (adapted from Peffers et al., 2007)

3.5 RESEARCH APPROACH

3.5.1 Overview of the Cognitive Process in Research

The process of developing theory in research follows three main cognitive processes or approaches, namely inductive, deductive and abductive reasoning. Inductive reasoning is an approach to constructing and evaluating inductive arguments based on a specific observation (Gregory & Muntermann, 2011). It concerns making “predictions about novel situations based on existing knowledge” (Hayes et al., 2010, p. 278). Thus, new information can be added to refine existing knowledge through inductive reasoning. In inductive reasoning, a researcher investigates specific cases and then makes conclusions about a premise based on the observed cases or facts (Hyoung Seok, 2019), thereby allowing for generalised assumptions to be made from the specific premises. To achieve this, a researcher commences by collecting data relevant to the topic under study and then proceeds to analyse the data to identify patterns and build a theory that explains the identified patterns, as shown in Figure 3-5.



Figure 3-5 Inductive research process (adopted from DeCarlo 2018)

Conversely, deductive reasoning is a theory-testing process which begins with an existing theory or generalisation and seeks to test the theory's applicability to specific cases (Hyde, 2000). It is often referred to as a form of reasoning which moves from the general to the specifics by drawing conclusions from general premises (Miller & Brewer, 2003). The general premise or rule is used as a theoretical base along with the cause to make predictions for a specific case (Upmeier zu Belzen et al., 2021) by assuming that if the premise is true, then it is “impossible” for the conclusion to be false (Hurley, 2000, p. 33) cited in (Walton, 2013). The deductive process (see Figure3-6) entails commencing with a theory, using the theory to derive hypotheses, collecting and analysing data to test the

hypotheses, and revising the theory (Woiceshyn & Daellenbach, 2018). Because deductive reasoning only focuses on testing hypotheses, it does not generate any new theory (Fischer, 2001).

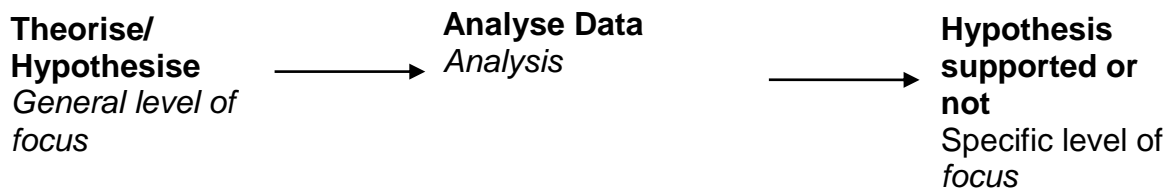


Figure 3-6 Deductive research process (adopted from DeCarlo,2018)

Abductive reasoning is the third common form of reasoning used in research. It is a form of reasoning that moves from factual premises to explanatory conclusions and is defined as a process of adopting or formulating an “explanatory hypothesis” (Peirce, 1974, p. 106). This logical inference relates to generating theory by studying facts. The resulting original theory is generated through an iterative process involving data collection, conjecture and hypothesis refinement (Janiszewski & van Osselaer, 2022). Furthermore, in abductive reasoning, the most probable hypothesis is adopted as an explanation for observed facts. The explanations are theoretically informed and often related to new, surprising empirical observations (Lukka & Modell, 2010), thus making it beneficial when the researcher intends to discover new concepts, variables and relationships (Dubois & Gadde, 2002). It is based on the principle that there are “no prior hypothesis, no presuppositions and no advanced theorising” (Levin-Rozalis, 2004, p. 3). However, this does not mean that abductive reasoning overlooks the role of prior theory.

Instead, in abductive reasoning, existing theoretical knowledge is used to aid the process of identifying the most probable explanation for the empirical observations (Lukka & Modell, 2010). Furthermore, unlike inductive and deductive forms of reasoning, which focus solely on either theory generation or testing hypothesis, abduction consists of both the generation and testing of hypotheses and theories (Haig, 2008); thus, it is often viewed as a combination of both the inductive and deductive forms of reasoning.

3.5.2 The Cognitive Process for this Study

This study adopted the design science strategy to develop the proposed interoperability framework. Design science research follows an iterative process that may involve various data collection and analysis points. Hence, DSR can involve different forms of reasoning for the different DSR steps (Vaishnavi & Kuechler, 2008).

The overall data analysis for this study followed both inductive and deductive cognitive approaches for analysing collected during the different phases and cycles of the DSRM. The deductive approach was applied in the Problem Awareness and Identifying the Objectives of the Solution phases of the DSRM process. The study applied the deductive approach for analysing the collected data as part of the systematic literature reviews presented in Chapters 5 and 6. Furthermore, deductive reasoning informed the process of conceptualising and constructing the proposed framework and evaluating the proposed framework. General systems theory elements informed the process of constructing the framework. In addition, the evaluation was guided by existing evaluation criteria proposed by (Prat et al., 2014), which were tested to determine the utility and efficacy of the framework within a selected problem domain. In addition, this study employed inductive reasoning to analyse the interview data. The inductive approach involved identifying themes from the interview data without relying on an existing theory to guide the process.

3.6 METHODOLOGICAL CHOICE: QUALITATIVE METHODS

In information systems, research can be undertaken by following two broad methodological approaches: quantitative and qualitative (Kothari, 2004). A quantitative research approach explains a phenomenon in a measurable and quantifiable manner (Kothari, 2004). It involves collecting numerical data and thus applies methods that enable such numerical data to be collected. The researcher may use mathematical and statistical models to analyse the data. This approach is often used to test hypotheses and theories by investigating the relationship between variables (Cresswell, 2014). Generally, quantitative research examines causal relationships between variables to make predictions and generalisations about the

phenomenon (Antwi & Hamza, 2015). A quantitative researcher sets a hypothesis and uses empirical data to test this hypothesis (Antwi & Hamza, 2015). Quantitative research is often associated with a positivist paradigm, whereby a researcher takes an objective stance and is separate and independent from the participants (Park et al., 2020). This approach is critiqued for attempting to apply natural scientific methods to study the complex social world and is accused of lacking the depth to represent the complex dynamics of human and social behaviour.

The qualitative approach intends “exploring and understanding the meaning individuals or groups ascribe to a social or human problem” (Creswell, 2009, p. 4). It is often used to study new phenomena or phenomena about which not much is known (Antwi & Hamza, 2015), and the phenomenon is studied from the participants’ perspectives (Williams, 2007). “Qualitative research involves an interpretive, naturalistic approach to the world” (Creswell, 2013, p. 74), which articulates participants’ experiences and perceptions within a particular context. The researcher becomes an active participant in the study and interacts directly with the subjects (Marczyk et al., 2005). The approach enables the collection of non-numeric data through multiple qualitative methods (Creswell, 2013), such as observation, interviews and documentation. Qualitative data analysis does not involve the extensive use of quantitative analysis (Kothari, 2004) but rather is an inductive iterative process in which the researcher identifies patterns, themes and categories emerging from qualitative non-numeric data (Creswell, 2013; Jaccard & Jacoby, 2010). Since this study sought to explore blockchain interoperability as a new phenomenon by investigating the views and experiences of individual blockchain experts, the qualitative approach was considered appropriate. Qualitative methods like interviews are flexible and can allow a researcher to gain an in-depth insight into the contextual issues pertaining to the organisation (Creswell, 2014). Accordingly, by using qualitative methods in this study, the researcher could gain detailed information on the participants’ views about blockchain interoperability in the banking sector.

The study triangulated several data collection methods, which included systematic literature reviews, interviews and webinars. Triangulation is a qualitative strategy for utilising multiple methods or data sources to provide a comprehensive understanding of a phenomenon (Patton, 2002). Hence, employing triangulation enabled the researcher to provide a more

comprehensive account and holistic understanding of the complexities associated with blockchain interoperability. In addition, triangulation ensures that the findings of a research study are credible and valid (Moon, 2019). Furthermore, triangulation can be useful for exploring complex problems and help address biases associated with using a single method (Noble & Heale, 2019). Moreover, blockchain interoperability is highly complex (Belchior et al., 2021a) and thus can benefit from a triangulation strategy.

Denzin and Lincoln (2018) note multiple ways of triangulating data. In data source triangulation, researchers can draw insights from multiple data sources at different times and locations and from differing perspectives. Triangulation might also involve multiple data analysis techniques or researchers to collect data and several methodologies, such as various forms of qualitative data collection methods like interviews, documents and observations (Merriam & Tisdell, 2016). This study triangulated multiple data collection methods to cross-validate the findings.

3.7 TIME FRAME

The time horizon refers to the time frame for data collection in a research study and can be cross-sectional or longitudinal (Saunders et al., 2015). A cross-sectional time frame represents a brief appraisal of a particular circumstance at a specific point in time and involves collecting data over a very short period, whereas a longitudinal time frame involves collecting data on several variables over a long period. This research is a cross-sectional study on blockchain interoperability.

3.8 DATA COLLECTION TECHNIQUES

Data collection is the process of acquiring data from respondents. The purpose of data collection in qualitative research is to gain relevant and sufficient information to provide an in-depth understanding of the target phenomenon. The qualitative data is collected within the context of the respondents' natural setting. The various data collection methods in qualitative research include participant observations, interviews, physical artefacts, archival records, and document analysis (Yin, 2017). The methods are used to solicit and collect qualitative data like the descriptive accounts of the phenomena, perceptions, opinions and experiences expressed by the subjects.

As previously mentioned, this study followed the methodological triangulation strategy, dominated by qualitative data collected through multiple data collection methods. The following discussion highlights the data collection methods applied in this study per the selected DSR process model as illustrated in Figure 3-7 below.

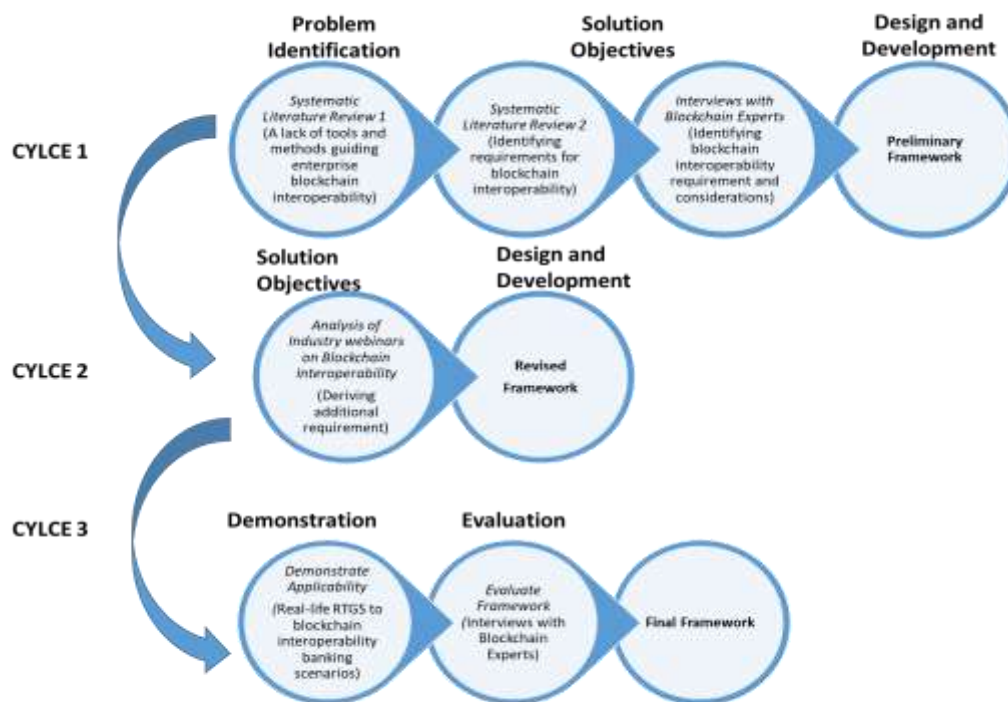


Figure 3-7 A summary of the data collection phases of the study

3.8.1 Systematic Literature Review

A systematic review (SLR) is a research method or process for identifying and evaluating relevant literature and collecting and analysing data from the selected literature to answer a specific research question (Liberati et al., 2009). The decision to conduct an SLR is driven by several factors, such as providing a theoretical grounding for future research, discovering the extent of research on a particular topic, and answering practical questions based on existing literature (Okoli & Schabram, 2010). In this study, two separate SLRs were used to collect data in two separate phases of the DSR process.

The first SLR informs the problem addressed in this study and forms part of the problem identification step of the DSRM. (Van der Merwe et al., 2019, p. 5) identified “establishing the requirements from the problem domain” as the first point for data collection within a DSR

study. Similarly, for this study, the requirements from the problem domain were identified during the problem awareness phase. The study employed an SLR as the data collection method to evaluate existing literature to identify open problems and challenges relating to blockchain technology within the financial sector. The systematic review evaluated scientific and grey literature focusing on blockchain implementation areas, challenges and objectives. The grey literature mainly consisted of reports from banks across the world. The articles were selected based on inclusion and exclusion criteria that focused on papers discussing blockchain implementation within the banking sector. The technology, organisation and environment (TOE) framework underpinned the analysis and organised the findings under the three TOE concepts of technology, organisation and environment.

The second SLR was conducted for the second step of the DSRM to identify and clarify the objectives of the proposed artefact. Following the adopted DSRM model, the objectives can be inferred from the problem domain. Though this may be true, the researcher argues that in this case, the objective inferred is general and points to the need for blockchain interoperability tools, standards and frameworks but does not clearly articulate the low-level functionalities and features required for such solutions. Therefore, the second SLR was conducted as part of the Define Objectives of the Solution step of the DSRM to evaluate existing blockchain interoperability approaches. The study intended to identify the weaknesses and strengths of these methods and also identify the requirements for the proposed blockchain interoperability framework. The data collected using the SLR would also be used as the foundation for the subsequent design and development phase.

3.8.2 Interviews

Interviews are data collection tools used to collect data either from individuals on a person-to-person basis or from a group of people (focus group) using a predefined set of questions (Paradis et al., 2016). Interviews can be structured, unstructured or semi-structured. A structured interview follows a rigid set of predetermined questions with little or no room for follow-up questions (Gill et al., 2008). In contrast, unstructured interviews allow for more flexibility regarding the questions posed. Semi-structured interviews include predefined questions but provide leeway for the researcher to ask follow-up questions (Gill et al., 2008).

This study conducted two sets of semi-structured interviews. First, the interviews were conducted as part of the design and development phase of the DSRM involving 13 blockchain experts within the banking industry. The interviews were conducted using online conference platforms such as Google *Meet* and *Zoom*. Using the aforementioned platforms was preferred to face-to-face interviews because they allowed the participants flexibility in choosing a suitable and convenient time for the interviews, which simplified the scheduling process. In addition, the researcher preferred using the platforms because they offered free one-hour sessions and recording capabilities. The interviews were conducted on a one-to-one basis with each participant, and the average duration for each interview session was approximately an hour. An interview guide (see APPENDIX B) containing a mix of close-ended and open-ended questions guided the interviews.

The researcher commenced each interview session by introducing herself to the participants and giving them an opportunity to introduce themselves. The researcher then explained the purpose of the study and the interview, provided an overview of how the interview would be conducted, and gave the participants an opportunity to ask questions. This process happened before starting the recording. At the start of the actual interview, the participants were requested to switch off their cameras to allow only the audio to be recorded to protect the participants' identities. The interview proceedings were recorded using the record feature offered by the conference platforms. An additional voice recording device was used to record the interviews for backup purposes.

Interviews are often conducted to collect individual views, experiences and beliefs on a specific topic and are believed to provide a detailed understanding of the phenomena of interest (Gill et al., 2008). In this study, semi-structured interviews with blockchain experts were conducted to assist in further eliciting the requirements for blockchain interoperability from the perspectives of the selected experts. Interviews are flexible and allow the researcher to gain an in-depth insight into the contextual issues of the organisation (Cresswell, 2014). From the interviews, the researcher acquired detailed information and explanations relating to the participants' personal views, opinions, professional experiences and meanings regarding blockchain interoperability.

The second set of interviews was conducted as part of the Demonstrate and Evaluate phases of the DSRM. Unlike the interviews above, which were intended to solicit requirements for the framework, the second set of interviews served to evaluate the proposed framework. These interviews involved three blockchain experts who were part of the first interviews. The interview guide (see APPENDIX B) included a mix of open-ended (qualitative) and close-ended (quantitative) questions.

3.8.3 Webinars

In addition to the data collection methods above, the study used webinars to augment the data collection process. The selected types of webinars focused on interoperability relating to blockchain technology in the banking sector and involved a two-way interaction between the host and either or both the presenters and the audience. According to Tiong and Sim (2020), two-way communication webinars offer the advantage of allowing the researcher to collect observational qualitative data (if required) and additional data through the question-and-answer sessions. The webinars enabled the researcher to obtain additional contextual insights and opinions from diverse industry players and experts who could not be accessed through traditional data collection methods. Furthermore, the webinars and podcasts identified additional requirements for the proposed framework and corroborated and compared the interview findings to enhance the proposed framework.

The webinars and podcasts used were identified through a search on YouTube. The search string “Blockchain interoperability in banking” was used to search the YouTube platform for potential webinars and podcasts. The relevant webinars were downloaded. The researcher listened to each webinar to determine the relevance to the study topic. The selected webinars were then edited using *Cap Cut* editing software to remove adverts. The edited videos were then transcribed and analysed. Thirteen webinars and podcasts were analysed and findings are presented in Section 8.2.

3.9 SAMPLING TECHNIQUES

3.9.1 Target Population

Specifying a population is a requirement for both qualitative and quantitative studies. According to (Asiamah et al., 2017), a researcher should specify the general, target and accessible populations. The general population refers to the largest group of potential participants restricted to a specific geographical area or institution who share at least one common attribute and from whom some information can be collected (Cresswell, 2014). The target population refers to all members of the general population who meet the criteria specified for a research investigation (Alvi, 2016).

In this study, the general population constitutes blockchain experts in the South African context. Blockchain experts in this study refer either to blockchain developers, blockchain software engineers, consultants or blockchain researchers from the banking sector and related fields.

3.9.2 Sampling Method

The study used a purposive sampling technique to select the appropriate sample. Purposive sampling is a nonprobability sampling where the researcher intentionally selects a specific target group (Sekaran & Bougie, 2016). Nonprobability sampling approaches are practical for qualitative studies (Merriam & Tisdell, 2016). In purposive sampling, the researcher has the prerogative to select specific participants who can provide the relevant information to answer the research question. There are two categories of purposive sampling, namely judgement and quota sampling; the study applied judgement sampling because it enabled the selection of the subjects who were best positioned to provide the requisite information (Sekaran & Bougie, 2016).

The participant recruitment process occurred in various ways. The first approach was to contact the South African Financial Blockchain Consortium (SANBA), a voluntary body investigating how blockchain can be used to transform the financial industry. Its members, which include banks, financial infrastructure players and regulators, are voluntary participants of the consortium. The consortium was the first contact to identify the main banks involved and potential subjects within each of the banks. The study assumed that the

individuals within the banks already had an interest in the technology and thus would be more willing to participate in the study. The second approach involved using *LinkedIn* to solicit participants. The researcher searched *LinkedIn* to identify potential candidates who were blockchain developers, software engineers, consultants or researchers. A private invitation was sent to each of the potential candidates identified via the search. In addition, the researcher used local blockchain conferences to identify and invite potential participants. The participants had to possess some professional experience relating to blockchain technology.

3.9.3 Summary of the Data Collection

Data collection method	Type of data collected	Purpose	Subjects	Number of subjects
Systematic literature review	Literature	Problem identification	Research articles and Company reports	0
Systematic literature review	Literature	Identification of Framework requirements and elements	Research articles and Company reports	0
Interviews	Qualitative	Identification of Framework requirements and elements	Blockchain Experts	13
Webinars	Qualitative	Identification of complementary Framework requirements and elements	Banking expert webinars on blockchain interoperability	13
Interviews	Qualitative and Quantitative	Framework evaluation	Blockchain experts	3

3.9.1 Sample Size

The determination of an appropriate sample size for research studies has been a contentious issue among researchers. Different researchers have suggested contradicting numbers of samples as appropriate. Typically, quantitative research designs are associated with large sample sizes, unlike their qualitative counterparts, which are generally associated with relatively small sample sizes of cases or individual participants (Asiamah et al., 2017). However, (Onwuegbuzie & Collins, 2007) argue against the dichotomised view associating small samples with qualitative designs and large sample sizes with quantitative research design. They argue that the sample size in both qualitative and quantitative designs can be small or large depending on the research objectives, research question and design. In methodological triangulation, different sample sizes may be used for each of the data collection methods. According to Onwuegbuzie and Collins (2007), the samples selected may be parallel, in which the samples are different yet drawn from the same population. Alternatively, the samples could be selected from different populations of the study.

As stated previously, this study followed a methodological triangulation strategy. As suggested by (Onwuegbuzie & Collins, 2007), the study included multiple samples. The main sample included 13 blockchain experts who participated in the interviews described earlier. The data collected from the 13 participants informed the design and development of the proposed blockchain interoperability framework. In addition, data were also collected from 13 webinars and were used to cross-validate the interview findings. Another sample consisted of three blockchain experts (selected from the original 13) who participated in the evaluation phase of the proposed framework.

3.10 DATA ANALYSIS TECHNIQUES

As previously stated, this study employed multiple qualitative data collection methods and performed different qualitative analysis techniques on the collected data. This study followed a triangulation approach whereby the data were collected in sequence. In addition, the study applied the DSR process, which consists of sequential steps that may be conducted in several iterations. Therefore, the analysis in this study was sequential and conformed to the

iterative nature of the DSR process. The upcoming sections explain the data analysis process for each of the data collection methods employed.

3.10.1 Analysis of the Systematic Literature Review Data

The data collected through the systematic literature reviews were analysed through a deductive thematic analysis approach. Braun and Clark (2006) define thematic analysis as a method for identifying, analysing, organising, describing and reporting themes found in the collected data. This method was adopted because of its flexibility and adaptability to different types of studies while still being able to provide a detailed account of the data (Braun & Clarke, 2006). The deductive thematic analysis process of the systematic review conducted as part of the problem awareness phase (Chapter 5) relied on the TOE framework to organise the findings, and for analysing the data from the systematic review in Chapter 6 relied on the European interoperability framework to analyse and organise the interoperability requirements.

3.10.2 Analysis of the Interview Data

This research study adopted the inductive thematic analysis approach to analyse the qualitative data obtained from the interviews with blockchain experts (see Chapter 7). In inductive thematic analysis, the data coding and theme development are guided by the collected data. Inductive thematic analysis neither uses a theory to guide the analysis nor an existing code scheme to code the data (Braun & Clarke, 2006). In inductive thematic analysis, the identified themes primarily reflect the data (Byrne, 2021), similar to grounded theory. Furthermore, inductive analysis is often descriptive and exploratory and used to provide a rich description of the collected data.

Furthermore, thematic analysis is employed because it affords researchers an effective way to examine the different perspectives of participants and identify new and unexpected information.

The study performed inductive thematic analysis on transcriptions of the interview data. The interview recordings were transcribed using *Otter.io* and Microsoft *Word 365*. The rationale for using two transcription platforms was that *Otter.io* is limited to only transcribing interviews with a maximum duration of 30 minutes, whereas *Word 365* allowed the researcher to transcribe longer interview recordings. During the transcription process, the research

ensured that the correct information was captured by the transcription software, and mistakes were corrected to ensure the accuracy of the information. After the transcription process, thematic analysis occurred through *Atlas.ti* analysis software, which entailed uploading the transcripts into the *Atlas.ti* software and coding. This analysis employed a mix of semantic and latent coding in which the researcher used the semantic meanings of participants and the researcher's interpretations to produce the codes.

The themes obtained from the inductive analysis were analysed to develop the proposed interoperability framework. The process of developing the framework was guided by the selected systems theory and thus fits the deductive approach. In deductive analysis, an existing theory or conceptual framework is used to guide the analysis. Deductive thematic analysis is analyst-driven and steered by the researcher's interest. Through deductive analysis, a researcher can focus on specific data as guided by the theoretical framework; however, it provides a narrow description of the overall data (Braun & Clarke, 2006).

The study applied content analysis to analyse the qualitative responses in the interviews conducted as part of the Demonstration and Evaluation phase. However, the study employed a descriptive statistical approach to the analysis of the quantitative data for the closed-ended questions.

3.10.3 Analysis of Webinar Data

The webinar data were analysed following a deductive content analysis approach in which the themes identified from the interviews with blockchain experts informed the analysis. Chapter 8 (section 8.3.3) contains a detailed explanation of the process. The tools used for the analysis were similar to the ones outlined for the analysis of the interview data.

3.11 RESEARCH RELIABILITY AND VALIDITY

The key purpose of all research is to produce valid and reliable knowledge, which must be produced ethically (Merriam, 2009). Thus, it is imperative that research produces verifiable and credible findings, meaning the researcher must conduct their research with rigour to ensure that their findings are reliable, valid and believable by other researchers and practitioners (Yin, 2018). These aspects imply that regardless of whether research is

quantitative or qualitative, it must be undertaken rigorously to ensure that the results obtained are credible. How credibility is addressed differs between qualitative and quantitative approaches. In quantitative research, credibility relies highly on the instrument of measurement (Golafshani, 2003). In a quantitative study, reliability depends on the repeatability of the measurements of variables and involves assessing the extent of errors in measuring a specific variable (Schwartz-Shea & Yanow, 2012). Researchers in a quantitative study must ensure that future researchers in different contexts can obtain the same results when the same variable is measured. In qualitative research, the researcher is the tool of measurement (Golafshani, 2003) and must provide a detailed description of findings instead of measurements (Merriam, 2009). The terms reliability and validity are often associated with quantitative research, while credibility, transferability and consistency are corresponding terms used in qualitative research (Golafshani, 2003; Merriam, 2009). For this discussion, these terms are used in conjunction.

Guba and Lincoln (1994) and Yin (2017) have identified three types of validity: internal validity (credibility), external validity (transferability), and reliability (consistency). Internal validity refers to how the research findings capture reality, and external validity refers to how generalisable the study's findings are (Merriam, 2009). Thus, external validity refers to how the study's findings can be applied or extended to another study. Reliability determines whether or not the study could result in the same outcomes when repeated.

3.11.1 Internal Validity

In this study, the researcher ensured internal validity by collecting data from multiple sources, including systematic literature reviews, interviews and expert webinars. The results were then triangulated to corroborate and cross-check the information obtained from the different sources. The triangulation also included cross-checking the information obtained from the interviews with different subjects who might have different views on the phenomenon. Merriam (2009) suggests respondent validation as another strategy for ensuring internal validity. Therefore, the researcher applied this strategy by periodically contacting the interviewed subjects, where necessary, to seek feedback and confirmation of any new findings. Merriam (2009) argues that doing so limited misinterpreting the participants' meanings and statements. In addition, the researcher ensured that the data

collection tools contained questions relevant and appropriate to answer the research questions and that the questions were related to the phenomenon being investigated.

3.11.2 External Validity

Merriam (2009) and Sekaran and Bougie (2016) state that external validity can be achieved by collecting rich, descriptive data. In this study, this was achieved by recording the interviews and collecting detailed transcriptions of the participants' responses during the interviews. The process was repeated when the researcher extracted data from the relevant documents. Recording the interviews ensured that no information was missed during the analysis.

3.11.3 Reliability

Reliability in qualitative research is expressed in terms of category reliability and inter-judge reliability (Sekaran & Bougie, 2016). The purpose of reliability is to minimise errors and bias (Yin, 2018). Category reliability refers to how well the researcher has defined the categories since well-defined categories lead to high reliability. The researcher used the same questions to interview the respective participants to ensure the reliability of the results, and the same codes ensured that the codes used were consistent. According to Sekaran and Bougie (2016) and Yin (2018), ensuring consistency in categorising the data during the analysis stage improves the reliability of the data and findings. The researcher also documented the procedures followed during the data collection to assist other studies that might wish to repeat the research. Baxter and Jack (2008b) further suggest that using a database to organise the data can also improve reliability. In this study, *Atlas.ti* software organised and categorised the qualitative data.

3.12 ETHICS CONSIDERATIONS

Ethical considerations are an important part of any research that must be considered to ensure the research process is ethical and to protect participants. The key considerations are informed consent and voluntary participation, anonymity and confidentiality, protection of the participants from harm, and ethical approval and access to participants (Arifin, 2018). The upcoming discussion demonstrates how this study addressed the above-mentioned considerations.

3.12.1 Ethical Clearance

Prior to the start of each data collection process conducted for the Identify the Objective of Solution and Demonstrate and Evaluate phases, the researcher sought ethical clearance from the University of Pretoria's Ethics Committee. Ethics clearance with reference numbers (EBIT/165/2022) and (EBIT/280/2023) were granted for the respective phases. On approval and obtaining the clearance, the researcher contacted the relevant participants and asked them to complete the informed consent forms (see APPENDIX A). Regarding the use of webinar data, it was not necessary to apply for ethics clearance. The reason being that the webinars used were obtained from YouTube, and YouTube provides a fair-use policy which allows researchers to utilise publicly available webinar videos in research.

3.12.2 Informed Consent

The principle of informed consent requires that participants are well informed about research and its associated risks and benefits. It also requires that participants be informed of their right to choose to participate or not to participate in the study, and this information should be in a language and format that participants can understand (Gajjar, 2013). As stated previously, a consent form was issued to potential participants to obtain permission from them to participate in the study and provide an explanation of the objectives and purpose of the research. The consent form informed the participants of their right to voluntary participation and, thus, the right to withdraw from the study at any time. Interviews were conducted with only participants who consented to participate in the study by signing the consent form, and the researcher sought permission to make audio recordings of the interviews. The consent forms were written in English, which is the official business language in South Africa; however, the researcher offered an explanation of the consent form at the start of the interview sessions to ensure that the participants understood their rights insofar as participating in the study.

3.12.3 Anonymity, Confidentiality and Protection from Harm

The anonymity and confidentiality principle requires researchers to protect the participants' identities (Arifin, 2018). In this study, the researcher ensured the privacy and confidentiality

of the respondents' personal identifying information (names and identities) by using codes to identify the different respondents during the data collection and analysis and when reporting the study's findings. Furthermore, during the online interviews, the recordings commenced after the introductions had been made, and when the recording started, the participants were advised to switch off their cameras to protect their identities. To protect the anonymity of the presenters and individuals shown in the webinars, the researcher did not use any names or personal identifiable information when presenting the webinar findings.

3.13 SUMMARY

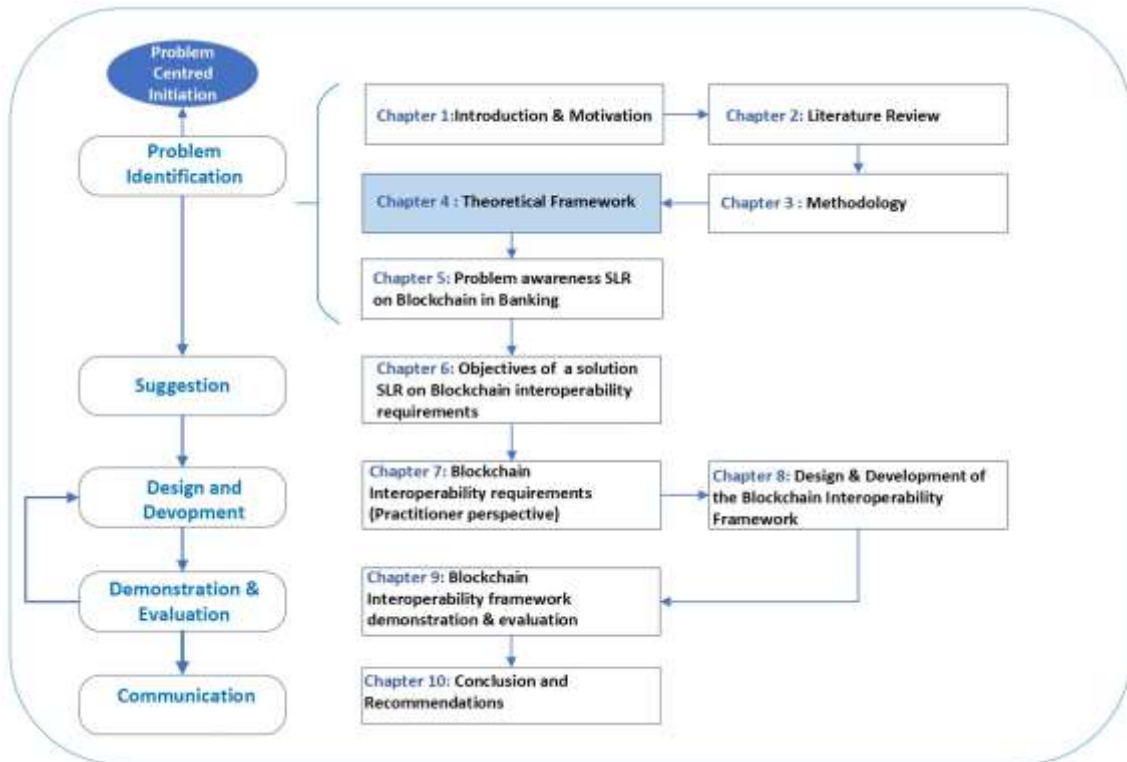
This chapter discussed the methodological choices used to achieve the objectives set out for this study. The chapter also introduced the selected pragmatist paradigm, and the researcher outlined the rationale for selecting this particular paradigm. The rationale for selecting the design science methodology (DSR) was also discussed. Chapter 3 outlined the data collection and analysis approaches, along with their associated rationales, as well as the validity, reliability and ethics of the research. Table 3-3 below summarises the research design choices adopted in this study.

Table 3-3 Overview of the methodological choices of the study

General methodological choices	Methodological choices adopted
Philosophy	Pragmatism
Approach	Inductive and Deductive
Strategy	Design Science Research
Choice	Qualitative
Time Horizon	Cross-sectional
Techniques and Procedures	<u>Data Collection</u> Systematic Literature Reviews Semi-structured Expert Interviews Webinars <u>Data Analysis</u> Thematic Analysis Content Analysis Descriptive statistics

CHAPTER 4

4 THEORETICAL FRAMEWORK



4.1 INTRODUCTION

This chapter presents the theoretical lens and perspective used to guide this study. The researcher presents an overview of the theories and models relevant to the study and those adopted in the different phases of the study. The research employed a technology adoption theory in the Problem Identification phase of the design science methodology (Chapter 5). The reason for this is that the lack of blockchain interoperability has been highlighted as one of the key barriers to the adoption of blockchain technology in organisations (Saheb & Mamaghani, 2021). From this perspective, technology adoption theories are considered relevant to the study, and therefore, this chapter commences with an overview of technology adoption theories/models. The chapter then continues with a discussion of key interoperability models and frameworks typically used to explain interoperability in

organisations. Thereafter, Chapter 4 presents the general systems theory selected as the main theoretical lens for this study. The discussion on general systems theory includes an overview of what the theory entails, a rationale for adopting the theory and its application within the study.

4.2 THE ROLE OF THEORY IN IS RESEARCH

The main purpose of undertaking research is to contribute towards building the body of knowledge within a specific subject area. This contribution is achieved through the building, testing, modifying and using theories that assist researchers in gaining a better understanding of the world and predicting future events (Bendassolli, 2013). According to Jaccard and Jacoby (2010), these theories are systems denoting worldly concepts or constructs and their relationships and can be used to describe, explain, predict and prescribe phenomena from different perspectives (Gregor, 2006).

The role of theory in research differs depending on the type of research being undertaken. In positivist quantitative research, an existing theory is used to formulate testable hypotheses (Bendassolli, 2013), in which case the hypothesis contains constructs or concepts extracted from the existing theory. In contrast, qualitative research does not generally use a theory to develop and test hypotheses but might develop a theory emerging from data without using any prior theory (Bendassolli, 2013) or involve using *a priori* theory to provide new explanations about a phenomenon (Jaccard & Jacoby, 2010; Reiter, 2017) by using empirical data to refine the existing theory. Alternatively, an existing theory can be used during data analysis to deduce and identify themes and patterns from the data according to the existing framework or theory (Bendassolli, 2013). Reiter (2017) adds that an existing theory can be used by assessing how well the theory explains or even predicts a phenomenon. This study adopted the approach of using an existing theory to build theory, as opposed to testing theory. This study drew from Von Bertalanffy's general systems theory (Von Bertalanffy, 1972) (henceforth referred to as systems theory) to develop a blockchain interoperability framework.

4.2.1 Types of Theories in IS Research

According to Gregor (2006), theories in IS research can be organised into five categories, which include theories for analysing, theories for explaining, theories for predicting, theories for predicting and explaining, and theories for design and action.

Gregor (2006) states that theories for analysing examine what is instead of providing explanations of why things are. These types of theories provide descriptions of the elements and relationships of a phenomenon. Analytical theories can make a phenomenon accessible for scientific investigation by providing abstract representations of a phenomenon, which allow researchers to identify patterns between various instances of the phenomenon (Mueller & Urbach, 2017). These abstract representations include schema, taxonomies and frameworks. Gregor (2006) argues that these theories do not merely describe a phenomenon but rather that as patterns emerge, analytical theories can provide explanations about phenomena.

Conversely, theories for explaining focus on providing explanations of the causal and conceptual relationships between the elements of a phenomenon (Mueller & Urbach, 2017). Theories for explaining provide researchers with answers to how and why a phenomenon occurs. Gregor (2006) states that these theories can also be used to understand different perspectives on the world and provide explanations for a set of circumstances from those perspectives. Theories for explaining can be developed through research approaches such as case studies and surveys, ethnographic, phenomenological and hermeneutic approaches, and interpretive field studies.

Theories for predicting provide a means to predict observations without explaining why the predicted outcome occurs. Accordingly, predictive theories do not explain the predicted observation or the causal relationship between the predicted observation or outcome and its cause. Instead, predictive theories can make predictions about possible outcomes from a set of explanatory factors (Gregor, 2006).

Furthermore, theories for explaining and predicting address the questions of what is, how, why, when, and what about a phenomenon (Gregor, 2006). These theories integrate explanations and predictions to provide a more comprehensive understanding of a phenomenon (Mueller & Urbach, 2017). Examples of this type of theory in IS include grand theories like the general systems theory adopted in this study and information theory (Gregor, 2006).

The last type of theory defined by Gregor (2006) is the theory for design and action. Gregor (2006) classifies theories for design and action as theories that explain how to do something. According to Venable (2006), design theories should be prescriptive about the utility of the solution to a given problem, such as methods, methodologies and prescriptions for constructing design artefacts.

This study applied various theories to serve different purposes at different data collection and analysis points of the DSR process. Chapter 5 presents the TOE framework applied as a priori theory from which themes were identified for the SLR. The purpose of the TOE framework was to assist the researcher in understanding the organisational, technological and environmental barriers and opportunities for blockchain technology in banking. Therefore, the TOE framework served the role of an explaining theory. As previously mentioned, the general systems theory was used as the main theoretical perspective guiding the design and development of the proposed framework. The general systems theory is a theory for explaining and predicting. In this study, the general systems theory explained and conceptualised the blockchain interoperability framework. The following discussion describes some of the IS theories used to explain various IS phenomena in organisational settings.

4.3 ORGANISATIONAL ADOPTION OF TECHNOLOGY INNOVATION

The lack of blockchain interoperability is highlighted as a significant barrier to the adoption of blockchain technology in organisations (Saheb & Mamaghani, 2021). Since this study focuses on addressing the lack of interoperability with blockchain, which is regarded as a key requirement for enabling mainstream adoption of blockchain, this chapter contains technology adoption-related theories which could be used to understand how the lack of blockchain interoperability influences blockchain adoption. The chapter discusses only

organisational theories that have previously been used to explain organisational adoption of technology innovations (Oliveira & Martins, 2010). This discussion is mainly because this study intended to investigate the adoption of blockchain at an organisational level. Specifically, the discussion below focuses on the diffusion of innovation (DOI) and technology organisation and environment (TOE) frameworks and also explains the role of TOE in this study.

4.3.1 Diffusion of Innovation Theory

DOI explains why and how new technologies and ideas proliferate through communities (Al-Jabri & Sohail, 2012; Oliveira & Martins, 2010). The theory elucidates diffusion as a process that occurs over time by which members of a community communicate about an innovation using particular channels (Rogers, 1995). According to (Rogers, 1995), four key elements influence the diffusion process: the actual innovation, how information about the innovation is conveyed, and the time and social community where the innovation is introduced. In addition, the theory proposes five constructs that influence the adoption of an innovation (Davis et al., 1989): relative advantage, complexity, compatibility, trialability and observability. These constructs are used to explore factors leading to the adoption of different innovations (Al-Jabri & Sohail, 2012; Folorunso et al., 2010) by different populations. In DOI, innovation can be any new idea, product or technology that is gradually adopted by different individual adopters at different times.

The different types of individual adopters are categorised into five groups, as illustrated by the innovation adoption curve shown in Figure 2-1 below. The categories of adopters are innovators, early adopters, early majority, late majority and laggards; these categories relate to the time it takes for each group to adopt an innovation. The characteristics of each category differ, with earlier adopters on the one end being much quicker in accepting and adopting innovations, and at the opposing end, laggards exhibit higher levels of resistance towards the adoption of an innovation. This categorisation plays a critical role in understanding the attributes of a target population that hinder or support that population in accepting and adopting innovations (Mwansa, 2015).

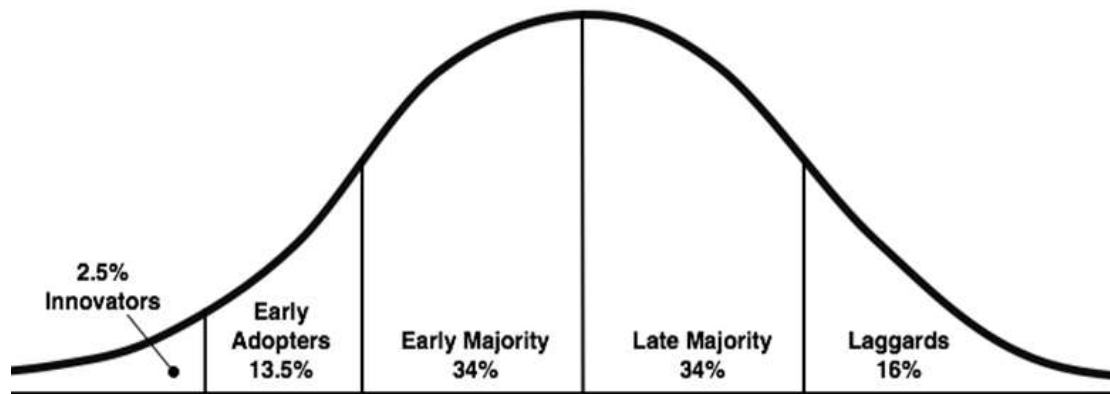


Figure 4-1 Innovation adoption curve (Rogers, 1995)

The diffusion and adoption of innovation do not only affect individual adopters but can also take place within organisations. However, at an organisational level, the diffusion and adoption process becomes more complex because it involves both proponents and opponents of the innovation, and these opposing views may also filter through to the decision-making process (Oliveira & Martins, 2010). To explain the complexities at an organisational level, Rogers (1995) extended the model to include characteristics of the individual decision-makers or leaders, the internal organisational structure, and the external characteristics of the organisation, as illustrated in Figure 4-2.

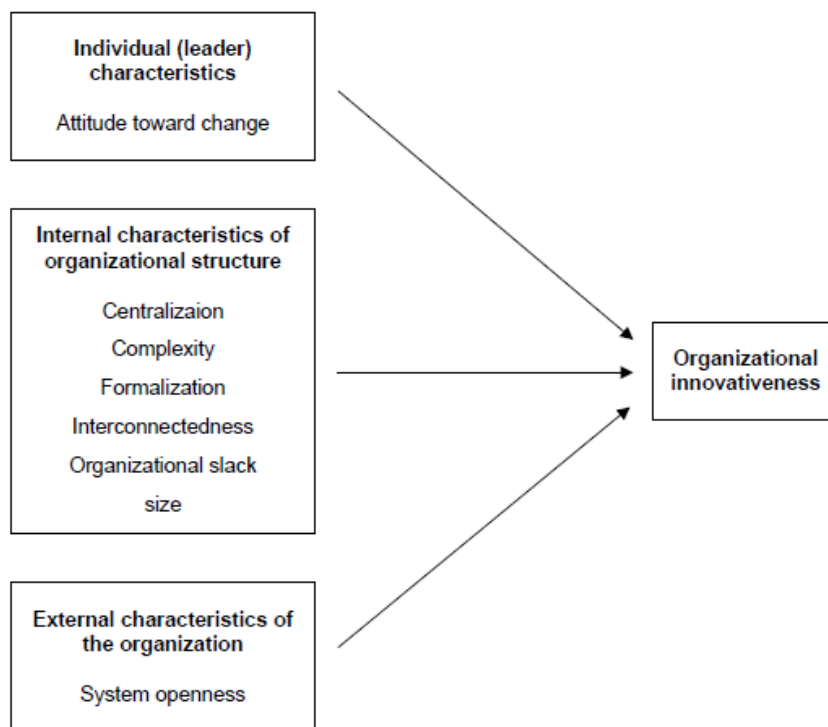


Figure 4-2 Diffusion of innovation at the organisational level (Rogers, 1995)

Leader characteristics represent a leader's attitude towards change. Internal characteristics of organisational structure include several factors, such as centralisation, which refers to whether the decision-making powers reside in one person or a group of individuals (centralised) or is decentralised. Complexity describes the extent of knowledge and expertise an organisation's members possess. Formalisation is the degree to which an organisation enforces compliance with rules and procedures, and interconnectedness expresses the level of interpersonal network links between different units of a social system. Organisational slack represents the availability of uncommitted resources in an organisation, while size refers to the number of employees in an organisation. The external characteristics of the organisation denote system openness.

Several studies have successfully applied DOI to determine factors contributing towards the adoption of various innovations (Oyedele et al., 2020; Peslak et al., 2010; Scott & McGuire, 2017; Zhang et al., 2015). However, the DOI has been criticised for falling short of providing constructs to explain the diffusion and adoption of complex network technologies (Lyytinen & Damsgaard, 2001) such as blockchain. Other criticisms have been that the framework does not consider the complexities and dynamic nature of cultural norms of the societies adopting the innovation. According to (Lyytinen & Damsgaard, 2001, p. 186), the framework lacks the “constructs to explain collective adoption behaviour”.

4.3.2 Technology, Organisation and Environment Framework

The TOE framework is a theoretical framework developed in 1990 by (Tornatzky et al., 1990) to explain the determinants of technological innovation adoption at an organisational level. TOE is a conceptual framework which explains how organisations adopt and use technological innovations based on three key elements of enterprise context, namely technology, organisation and environment (Tornatzky et al., 1990). Figure 4-3 below depicts the three contexts.

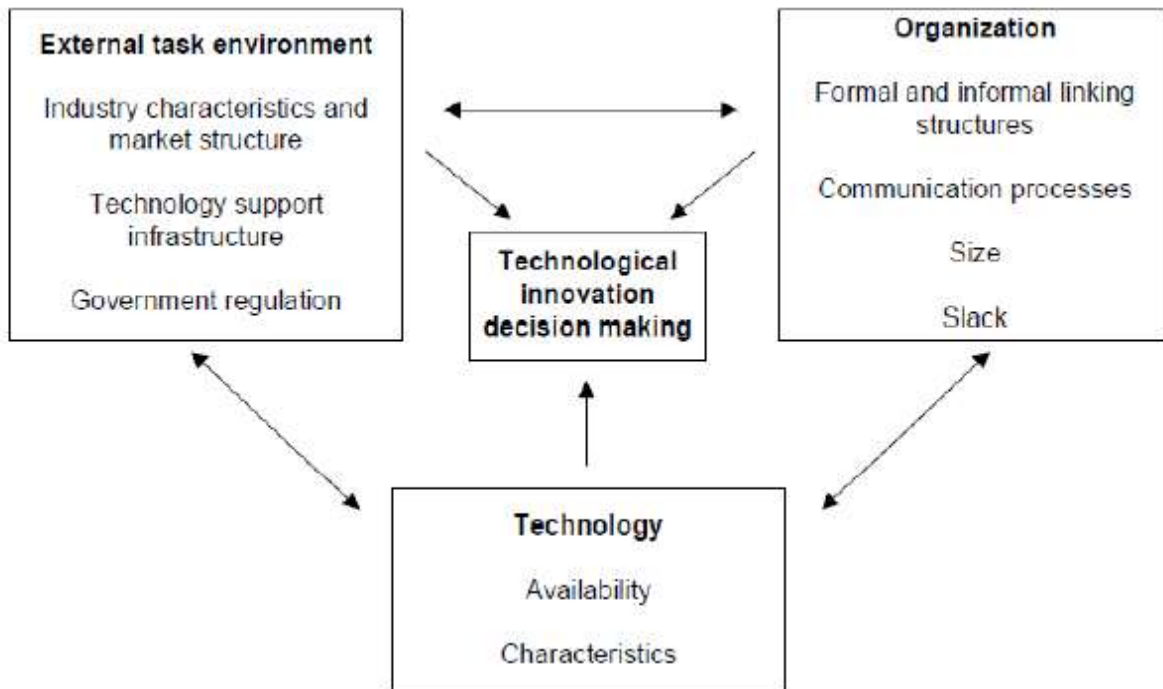


Figure 4-3 The three contexts of the technology, organisation and environment framework (Tornatzky et al., 1990)

The technological context describes the external and internal technologies of an organisation and may include already existing or emerging technology in the market. The descriptions of technology include their perceived usefulness, complexity, compatibility with the organisation and their associated learning curves (Awa et al., 2016).

The organisational context refers to attributes of the organisation which determine whether or not the organisation can adopt technological innovation. These attributes include the size of the organisation, informal and formal structures, human resources and communication processes. According to Rosli et al. (2012), these factors may also include the organisation's IS capabilities and IT infrastructure, readiness to adopt new technologies, organisational culture, experimentation and observability.

Environment describes the organisation's industry and the environment in which it operates. The environmental dynamics in which an organisation operates can either enable or hinder its operations (Awa et al., 2016). Environmental considerations include regulatory environment, clients, competitors (Chau & Tam, 1997; Low et al., 2011), governmental support, trading partner readiness, and access to relevant support skills (Awa et al., 2016).

Similar to DOI, the TOE framework emphasises the importance of perceived relative advantage, compatibility, complexity, trialability and observability of the target technology (Awa et al., 2016) in facilitating the adoption of new technological innovations. However, the TOE framework includes a critical aspect missing from the DOI, namely the environmental context (Cruz-Jesus et al., 2019). The TOE framework enhances the DOI and provides a more holistic explanation of organisational level innovation diffusion (Hsu et al., 2006), evident in the number of research studies underpinned by this framework.

Several studies (Awa et al., 2016; Low et al., 2011; Rosli et al., 2012) applied TOE as their theoretical basis to explain the adoption of various technologies, such as enterprise resource planning (ERP), accounting and auditing, cloud computing and customer relationship management (CRM). In their study investigating the adoption of ERP in small to medium enterprises in Nigeria, (Awa et al., 2016) found that the TOE framework adequately explained the adoption within the study populations. The researchers further observed that among the three contexts of TOE, the technological factors were the biggest drivers of ERP adoption among SMEs. Oliveira and Martins (2010) found that the TOE factors which support the adoption of CRM are technical competence, data quality integration and top management support, whereas pressure from competitors contributed negatively to adoption. A study by Siew et al. (2020) demonstrates the adequacy of the TOE framework in adoption. Their results show that environmental factors such as professional support and the complexity of existing systems affect adoption and organisation size, the skills and competence of IT staff, and top management support are the organisational factors that play a critical role in determining the adoption of computer-assisted auditing tools. The diversity of the applications of TOE demonstrates it is a generic framework and can be applied to study any technology, including complex, disruptive technologies such as blockchain (Zhu et al., 2006).

This study adopted the TOE framework in the problem awareness phases of the adopted DSR process. In particular, TOE was applied to analyse and organise the results of the systematic literature review (Chapter 5). The purpose of the systematic literature review was to explore the various applications, opportunities and barriers to the implementation and adoption of blockchain technology in the banking sector. The application of TOE enabled

the researcher to interrogate the barriers and considerations for blockchain interoperability from technological, organisational and environmental perspectives.

4.4 INTEROPERABILITY FRAMEWORKS

Currently, no theory exists specific to the study of interoperability; however, different types of framework perspectives have been applied to understand interoperability in organisations. The following discussions present some of the frameworks used to explore the interoperability of ICT solutions in organisational settings.

The interoperability of information technologies (IT) in enterprises has been a focal point in the information systems field for many years. IT increases the productivity and efficiency of organisational processes (Patel & Connolly, 2007); as such, it is critical for organisations to adopt technology innovation early and correctly to remain competitive (Yoo et al., 2012). However, realising these benefits depends considerably on interoperability (Hodapp & Hanelt, 2022). Moreover, achieving interoperability between technology innovations is generally a complex challenge for organisations, which is further perpetuated by the novelty of the new technologies for which there are either no standards or to which existing standards cannot be applied (Huber et al., 2021) as is the case with blockchain technology. Therefore, for organisations to realise value from adopting new technologies, they must understand the factors that support or inhibit the interoperability of these innovations. To achieve this, it is pertinent to draw from the existing knowledge and understand where and how the existing knowledge is adequate or inadequate in addressing the interoperability of novel technologies. The following discussion identifies prominent models and frameworks that have been used in the IS field to explain the interoperability of IT systems in organisations.

The following interoperability models are mostly cited and used within IS studies to explain the interoperability of different technology innovations in organisational settings: the ATHENA interoperability framework (AIF), the interoperability development for enterprise application and software (IDEAS), LISI and the European interoperability framework (EIF). Because this study intends to investigate the interoperability of blockchain in organisations,

the upcoming sections only discuss theories explaining interoperability within the context of enterprises.

4.4.1 ATHENA Interoperability Framework

AIF is a framework to explain the interoperability of enterprise applications and software systems (Berre et al., 2007). It provides a holistic view and explanation of interoperability that includes analysing and understanding business needs and technical requirements by adopting a multidisciplinary and model-driven approach to addressing interoperability challenges (Rezaei, Chiew, & Lee, 2014). In essence, the AIF explains how the model-driven development approach can be used in software engineering practice to support interoperability (Lemrabet et al., 2010). In addition, the AIF takes a solutions approach to addressing interoperability concerns. This approach involves synthesising the results of the different ATHENA project solutions relating to their technical and business requirements for interoperability (Rezaei, Chiew, & Lee, 2014). The framework elucidates interoperability as the capability of two or more systems or components to exchange information and use the exchanged information (IEEE Computer Society, 1991). The structure of AIF consists of three key levels or sub-frameworks that explain the interoperability process: the conceptual, technical, and applicative levels. Model-driven interoperability is defined at each of these levels.

According to Berre et al. (2007), the conceptual integration framework of the AIF focuses on concepts, meta-models, languages, and model relationships and provides a basis for systemising the nuances of software model interoperability. Technical integration relates to software development and execution environments and includes tools for developing software models and execution platforms for executing software models, whereas the applicative integration level mainly focuses on providing guidelines and patterns for solving the interoperability issues of software systems.

Furthermore, the AIF considers information interoperability from four different viewpoints (see Figure 4-4 below). The four viewpoints at which interoperation can be achieved are enterprise/business, process, service and information/data and a model-driven interoperability approach is prescribed for each viewpoint. The objectives of the viewpoints

differ, with enterprise/business interoperability focusing on enabling collaboration between organisations regardless of any existing differences in practices, cultures, legislative and commercial approaches. Achieving interoperability at this level requires the collaborating entities to have similar/compatible visions and goals (Lemrabet et al., 2010). Process interoperability concerns enabling processes from different organisations to collaborate and establish cross-organisational processes. Conversely, at the service level, interoperability is concerned with enabling different and independently developed ICT applications or organisational services to function together, whereas data interoperability involves enabling heterogeneous data models on different operating systems to operate collaboratively (Chen et al., 2008). However, this study did not use AIF because it was designed for a specific project (the Digital Interoperability Project) (ATHENA, 2005); in addition, it was not designed with blockchain in mind, and the current study aims to provide practical guidance on how organisations should implement blockchain interoperability.

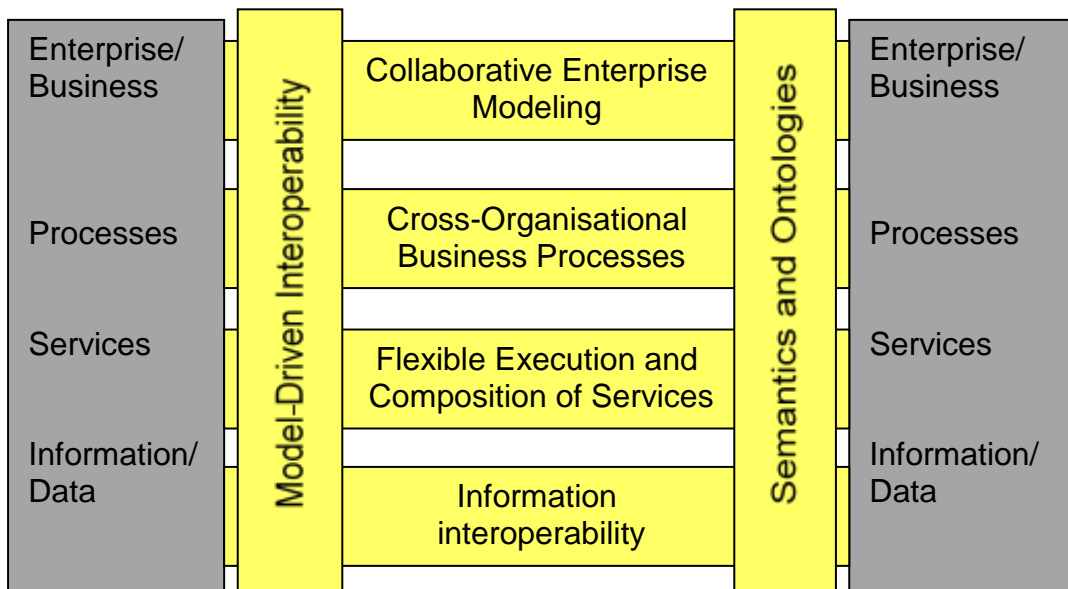


Figure 4-4 ATHENA Interoperability Reference Architecture (Berre et al., 2007)

4.4.2 Enterprise Interoperability Framework

The enterprise interoperability framework (INTEROP) is a barrier-driven framework which aims to address interoperability between enterprises by identifying the fundamental dimensions of enterprise interoperability, defining associated research domains, and establishing domain knowledge (see Figure 4-5) (Chen & Daclin, 2006). INTEROP explains interoperability between enterprises by identifying barriers to interoperability and using these barriers to structure domain solutions for enterprise interoperability (Rezaei, Chiew, & Lee, 2014). The framework adopts concepts from other models, such as the AIF and the European interoperability framework, to define enterprise research domains.

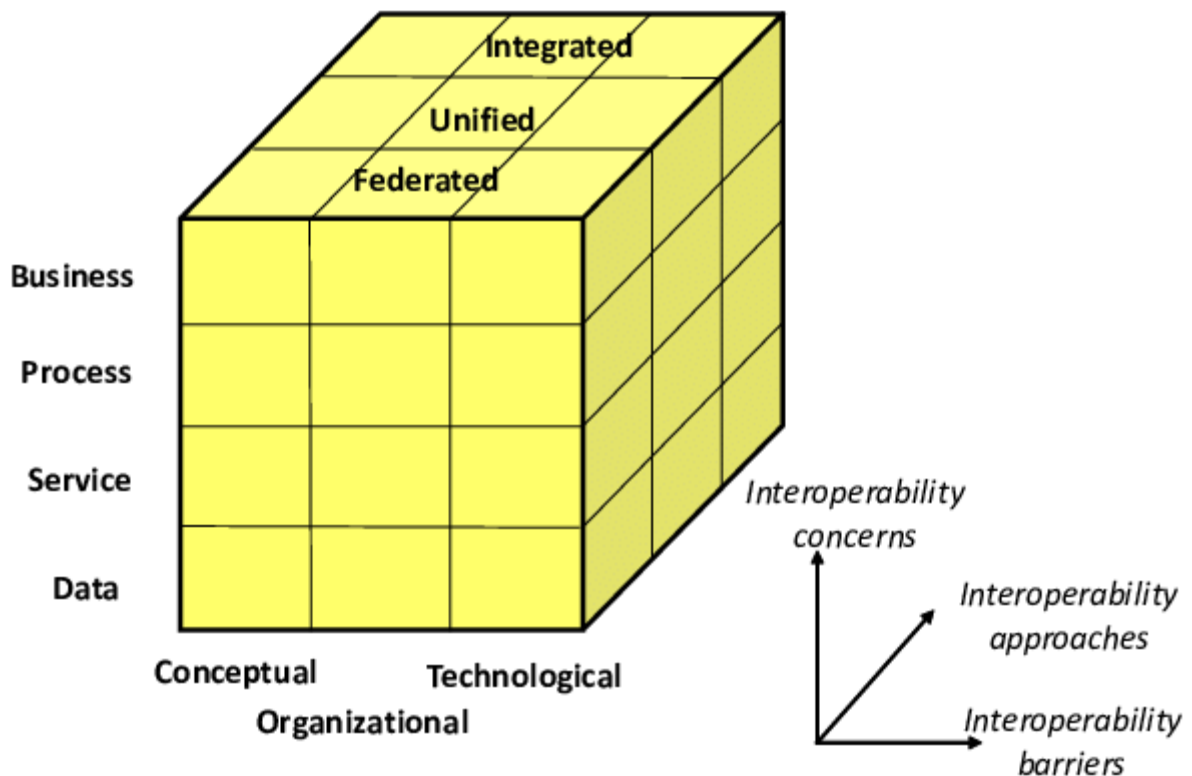


Figure 4-5 The enterprise interoperability framework (Chen & Daclin, 2006)

The INTEROP framework explains interoperability based on three dimensions: interoperability barriers, interoperability concerns and interoperability approaches. Interoperability barriers are defined as incompatibilities that hinder the exchange of

information and services between enterprises. In the framework, these are classified into three main categories: conceptual, technological and organisational barriers. Conceptual barriers relate to semantic and syntactic differences, whereas technological barriers concern differences and incompatibilities in information technologies, such as differences in technological platforms and architectures. Organisational barriers relate to incompatibilities between organisational structures (Chen & Daclin, 2006). The second domain defines four enterprise levels of interoperability concerns based on the AIF framework discussed above, while the third domain explains the three basic approaches for enabling interoperability between entities, namely integrated, unified and federated approaches. The integrated approach establishes interoperability between entities when the entities share a common format or model. Alternatively, a unified approach can be adopted if there is no common format, but there is a common meta-level structure (Guo et al., 2020). However, in the absence of a common meta-level structure, a federated approach can be used to establish interoperability by allowing entities to make specific accommodations as and when needed (Rezaei, Chiew, & Lee, 2014). Although this framework provides a mechanism for organising interoperability dimensions, it does not offer practical guidance on how to address interoperating for specific business problems (Chen & Daclin, 2006).

4.4.3 European Interoperability Framework

The European interoperability framework (EIF) is a set of guidelines for enabling interoperability between digital public services (European Commission, 2017). EIF defines interoperability in the context of public enterprises as the ability for organisations to interact towards reaching mutually beneficial goals by using ICTs to align business processes and share data (Kouroubali & Katehakis, 2019). The EIF provides recommendations on how public organisations and businesses can communicate. According to the European Commission (2017), the EIF framework is based on three main pillars: 1) Principles that provide guidance relating to the behavioural aspects that policymakers should consider to drive interoperability; 2) Interoperability layers, including technical, semantic, legal, and organisational perspectives from which interoperability can be achieved; 3) A conceptual model for integrated public services. The conceptual model promotes the idea that public services should be designed with interoperability in mind (European Commission, 2017).

The EIF defines 12 principles to guide the development of interoperable public services (see Figure 4-6). The principles are recommendations relating to the behavioural aspects that drive interoperability actions and are grouped into four categories: Principle 1 sets the context of EU actions on interoperability, Principles 2 to 5 are core interoperability principles, and Principles 6 to 9 concern generic user needs and expectations. The remaining principles guide how corporations are formed among public administrators within and across borders (Kouroubali & Katehakis, 2019).



Figure 4-6 Principles of the European interoperability framework (European Commission, 2017)

As mentioned above, the EIF defines four levels at which interoperability should be achieved (see Figure 4-7).



Figure 4-7 The four levels of interoperability (European Commission, 2017)

The legal interoperability level relates to ensuring organisations operating under different legal, policy and strategic frameworks can collaborate. In essence, legal interoperability facilitates the process of enabling legal rules to cooperate across jurisdictions and levels within the same country (Weber, 2014). Achieving legal interoperability requires either existing or new legislation and the corresponding data privacy requirements to be considered. However, how existing or new laws are applied depends on the context.

Organisational interoperability focuses on aligning business processes between organisations to achieve a commonly agreed upon and mutual goal. This requires respective business processes to be documented. Furthermore, it involves re-engineering existing business processes to achieve integration and alignment and enable a seamless exchange of information across organisational boundaries (Katehakis et al., 2018; Kouroubali & Katehakis, 2019). In addition, achieving organisational interoperability can help make user-centred services available, identifiable, and accessible, thus satisfying the requirements of the user community (European Commission, 2017).

The semantic interoperability level focuses on the semantic and syntactic elements of the data to be exchanged. The semantic aspects concern ensuring that the meaning of the exchanged data is unambiguous across organisational systems. Achieving semantic interoperability requires the use of standardised vocabularies and data formats to ensure that the exchanged data is understood by the communicating parties (Loutas et al., 2011).

On the other hand, the syntactic aspect focuses on describing the exact formats (grammar and format) of the information to be exchanged.

Technical interoperability relates to ensuring connectivity between systems and services and the applications and technologies they use. The technical interoperability aspects include interface specifications, interconnection services, data integration services, data presentation and exchange, and secure communication protocols. Ensuring technical interoperability may require the use of formal technical specifications.

4.4.4 European interoperability framework application

This study applied the European interoperability framework as a lens through which to identify the data collection and analysis of the blockchain interoperability requirements during the systematic literature review discussed in Chapter 6. The systematic literature review was undertaken as part of the Identifying the Objectives of Solution phase of the adopted design science methodology. The study employed the four levels of interoperability defined by the European interoperability framework to organise the requirements identified from the systematic literature review.

4.5 INTRODUCTION TO THE GENERAL SYSTEMS THEORY APPLIED IN THIS STUDY

General systems theory (GST) is an interdisciplinary study of systems whereby a system is viewed as a group of interacting and interconnected elements serving a common purpose and forming a unified whole (Von Bertalanffy, 1972). Systems theory defines a system as “an organised or complex whole consisting of an assemblage of things or parts forming a unitary whole” (Johnson et al., 1964, p. 367). A system and its associated elements (or subsystems) can be natural or artificial, such as a set of things, people, cells, molecules, et cetera as such, GST can be applied to any system regardless of the properties or elements of the system (Von Bertalanffy, 1972). The elements in a system can be homogenous, with similar properties and behaviour, or homogeneous, exhibiting varying properties and behaviour (Geiger et al., 2011b). The system and its elements interact with each other and

with the surrounding environment to produce patterns of behaviour that can be used to understand the whole. The essence of systems theory is understanding the wholeness of either or both a scientific and social phenomenon or problem (Bridgen, 2017). Understanding the system overall requires understanding the structures and patterns of behaviour that emerge because of the interactions between elements of a system (Lai & Huili Lin, 2017). Consequently, through systems theory, we can explain how systems collaborate to produce a more complex system (a whole) with emergent behaviour and characteristics. Due to the emergent properties, systems can be very different from each other (Lai & Huili Lin, 2017).

4.5.1 Open and Closed Systems

Systems theory distinguishes between two types of systems: open systems and closed systems. An open system is a system that can interact with the surrounding environment such that information is shared between the system and its external environment. In open systems, the input information from the environment can transform the system's behaviour and influence its evolution in some way (Ducq et al., 2012). Conversely, a closed system is typically isolated and does not exchange any information with the environment and thus cannot be altered by external input from the environment.

Open Systems

An open system receives information, energy or material from its environment and also sends back information, energy or material to its environment. The open interactions with the environment enable the system to grow and survive to avoid deterioration (negative entropy) (Lai & Huili Lin, 2017). The system uses the exchange with the environment to regulate its state (homeostasis). The open systems concept draws from the field of cybernetics, which "revolves around the theory of regulation and command in mechanical and living systems" (Adams, 2012, p. 213). Cybernetics advocate for feedback and control mechanisms to assist the system in regulating its internal state (Lai & Huili Lin, 2017).

According to Katz and Kahn (1978), open systems are characterised by the following elements:

- Input: The energy, information or material the system receives from the environment
- Transformation: The process of converting input into output
- Output: The final product produced by the system
- Interrelationships: The relationships between components of a system and the whole systems
- Boundaries: Interfaces that either or both connect and demarcate the system from its environment

The relationship between the elements above is illustrated in the models depicted in Figure 4-8.

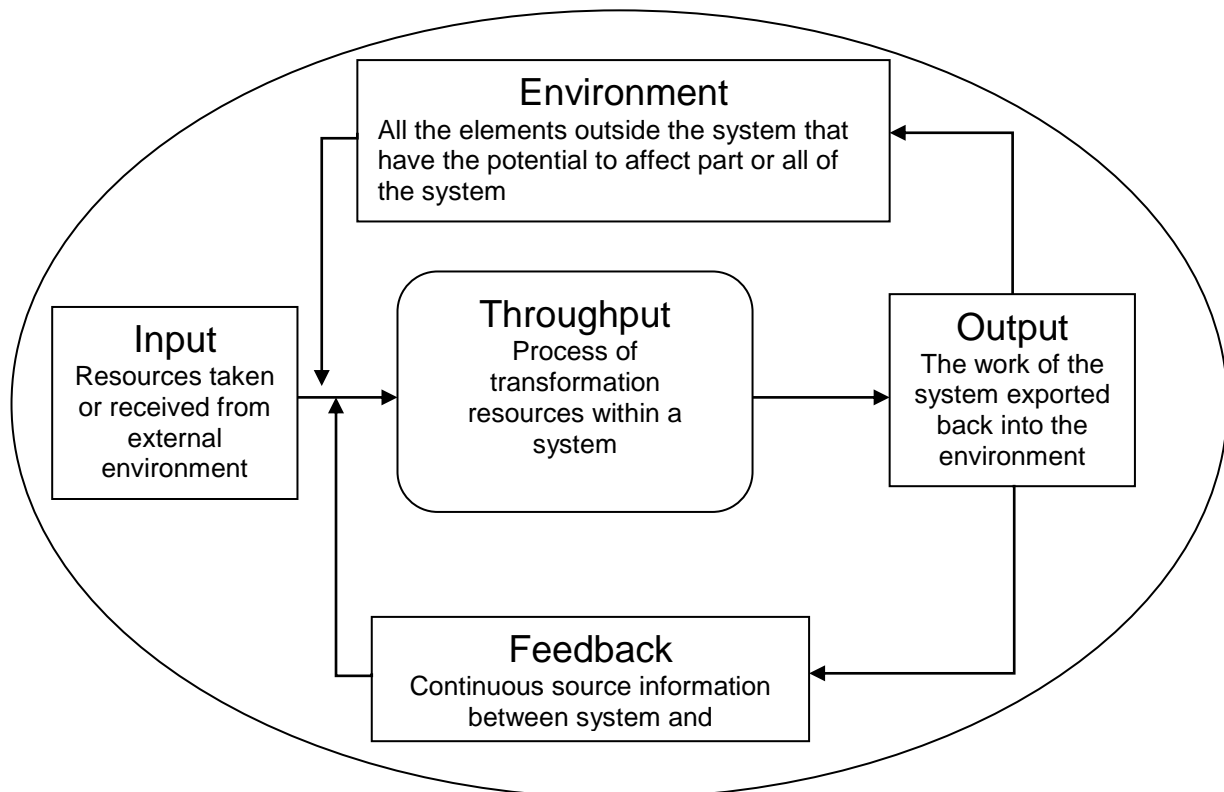


Figure 4-8 Open systems model (Katz & Kahn, 1978)

Closed systems

The term closed systems typically refers to systems that do not exchange any resources (information, energy or material) with the external environment or other systems. These types of closed systems are isolated from their environment, tend to be self-contained and self-sufficient and have fixed, impermeable boundaries (Ham et al., 2015). However, this notion of closed systems varies across disciplines. For instance, in the science and biology fields, closed systems are defined based on the degree of the permeability of their boundaries. In particular, closed systems in science and biology are systems of which the boundaries only allow energy through but not material or information (Shadab et al., 2022).

4.5.2 General Concepts in Systems Theory

Systems theory is founded on several concepts or principles which can explain different systems. Kast and Rosenzweig (1972) identified goal-seeking, holism, subsystems, input transformation output model, feedback, homeostasis, equifinality, system boundaries and open systems view. The concepts are briefly explicated as follows:

- **Goal Seeking:** This principle states that a system and its behaviour are purposeful and geared towards a specific goal. A system can seek to achieve multiple goals (Kast & Rosenzweig, 1972). Such goals are not inherent to the system but may be ascribed by the researcher (Ansari, 2004).
- **Holism:** States the whole is “not just the sum of its parts”, and explaining the system requires explaining it in totality. Thus, the system overall is greater than the sum of its parts, and to understand the whole, one must understand the interactions between the interrelated subsystems that comprise the whole system (Ansari, 2004).
- **Subsystem:** Refers to a system only being regarded as such if it has two or more interrelated elements or components. The subsystems are distinct parts of a system (Lom & Pribyl, 2021).
- **Open system view:** Systems can be viewed in two ways: either open or closed. Open systems have permeable boundaries and can exchange information, matter

and energy with their environment (Sheather, 1968); closed systems do not exchange anything with their environment.

- **Input transformation output model:** This principle primarily applies in open systems and states that a system is continuously transforming input from the environment into output back to the environment.
- **System boundaries:** Systems are delineated from the surrounding by boundaries. Boundaries outline the system and separate it from other systems and the environment. The boundaries can be permeable as in the case of open systems or non-permeable relating to closed systems.
- **Feedback:** Relates to how a system self-regulates and maintains a steady equilibrium state. The feedback is the output of the system's process, which is then fed back into the system as input. There are two types of feedback: negative and positive. Negative feedback relates to the information passed back to a system when an error has occurred; it is essentially error control feedback (Ansari, 2004). Thus, the purpose of negative feedback is to warn or indicate to the system an unexpected outcome; as such, the system should take corrective measures and readjust to a new steady state (Kast & Rosenzweig, 1972).
- **Homeostasis:** The ability of a system to alter its structure to adapt to its environment. The purpose of the alteration is to achieve a state in which there is a balance between the system and its surrounding environment (Von Bertalanffy, 1972). A system might remain in a state of dynamic equilibrium by continuously exchanging matter and energy with the surrounding environment (Kast & Rosenzweig, 1972). Dynamic equilibrium implies that the systems may attain various equilibrium states, which might vary from the original state at which the system started.
- **Equifinality:** A principle relating to open systems which suggests there are multiple ways of achieving a particular result or goal. Hence, the same outcome can be obtained in several ways, which might include chance events (Cicchetti & Rogosch, 1996). Cicchetti and Rogosch (1996) further elaborated that equifinality could also

refer to the process whereby the same end state is reachable from various initial states, conditions or processes.

4.5.3 The Rationale for Selecting Systems Theory

The following were considered in selecting systems theory as the theoretical framework for this study. Systems theory's primary purpose is to understand the wholeness of a scientific or social problem; hence, employing systems theory enables a researcher to study, understand and explain a problem holistically. Therefore, the study selected the theory was selected on the basis that it would help provide an in-depth explanation and understanding of blockchain interoperability and thus assist the research in developing a more comprehensive blockchain interoperability framework. In addition, system theory focuses on evaluating interactions and relationships between parts of a system to understand the whole system (Mele et al., 2010). This study aimed to explore the phenomenon of blockchain interoperability. The definition of interoperability is "the ability of two or more systems or components to exchange information and use the information" (IEEE Computer Society, 1991, p. 114). Information exchange is a form of interaction between two entities; therefore, understanding how two systems or components interoperate can be explained by evaluating the interactions between them. Accordingly, the study of interoperability is well suited to be explored from a systems theory perspective. This is supported by Naudet et al. (2010, p. 176), who reason that interoperability can generally "benefit from a systems approach" because the systems theory provides a generic framework that applies to any domain. Furthermore, systems theory not only focuses on the system in isolation but also considers the environment and how it influences the behaviour of the system. This aspect assisted the researcher in understanding the external environmental factors that influence blockchain interoperability. Table 4-1 shows a list of some studies that have applied systems theory and its variations.

Table 4-1 A list of studies that used systems theory

Title	Type of Systems theories	Study focus	Role of theory
A contribution of system theory to sustainable enterprise interoperability to science base (Ducq et al., 2012)	General systems theory	Enterprise Interoperability	Modelling and representation
Requirements for supporting enterprise interoperability in dynamic environments (Weichhart, 2014)	Complex adaptive systems theory	Enterprise Interoperability	Analysis and discussing initial requirements for the interoperability platform
Ontology of enterprise interoperability extended for complex adaptive systems (Weichhart & Naudet, 2014)	Complex adaptive systems theory	Enterprise Interoperability	Modelling and representation
Supporting interoperability in complex adaptive enterprise systems: A domain specific language approach (Weichhart et al., 2016)	Complex adaptive systems theory	Enterprise Interoperability	Modelling and representation
A systems theoretical approach to interoperability of information (van Lier & Hardjono, 2011b)	Luhmann's systems theory	Hybrid systems	Understanding through modelling and representation
Extending the Ontology of enterprise interoperability (OoEI) using enterprise-as-system concepts (Guédria & Naudet, 2014)	General systems theory	Enterprise Interoperability	Modelling and representation
Sustaining interoperability of networked liquid-sensing enterprises: A complex systems perspective (Agostinho & Jardim-Goncalves, 2015)	Complex systems theory	Enterprise Interoperability	Modelling and formalisation
Crowdsourcing information systems – a systems theory perspective (Geiger et al., 2011a)	General systems theory	Crowdsourcing information systems	Modelling and representation

4.5.4 Systems Theory Application

As stated above, this study applied the systems theory as a theoretical lens. A theory can be used in different phases of the research process and for various purposes. Gregor (2006) defines four primary goals of applying theory in IS research: to analyse and describe a phenomenon, explain, predict and prescribe. In this study, the goal of adopting the systems theory was to analyse and explain the phenomenon of blockchain interoperability. When theory is used to analyse and explain, the intention is to answer the question of what, how, when and where—without providing any predictions or testing propositions (Gregor, 2006). Regarding the use of theory in the research process, Stewart and Klein (2016) outline that theory can be applied to provide a rationale for a research study, to define the aim and research questions, as part of the methodology and for data collection, analysis, and interpretation. Similarly, Bernard and Ritti (1990) state that an explicit theory is essential in defining the research question as a scientific question, as a guide for selecting variables, and interpreting results. In addition, an existing theory can be used during data analysis and following an initial inductive analytical process, which allows themes to emerge from the data, followed by using concepts identified from an existing theory to deduce themes (Bendassolli, 2013). Moreover, an existing theory can be used for comparison purposes and to measure how well the theory measures the constructs of the emerging theory (Reiter, 2017). For this study, the selected theory was used as a framework for data analysis and interpretation as well as in the construction of the proposed framework. In particular, the systems theory was used to organise the themes and concepts obtained from various data collection phases for the construction of the proposed blockchain interoperability framework.

4.5.5 Criticism of Systems Theory

Although systems theory has been commended for enabling the study of complex systems and its adaptive and dynamic nature, making it applicable to a variety of systems, it has also been criticised in many aspects. Von Bertalanffy (1972) criticises the theory for not being able to provide explanations of why phenomena occur in a particular way. Hutchinson and Oltedal (2014) argue that the theory does not accommodate questions around morality and ethics. In addition, Bauer and Schneider (2007) criticise the theory for its limited ability to make predictions regarding the future state of the systems. Furthermore, issues have been

raised regarding the difficulties about defining systems boundaries and explaining interactions for various adaptive systems (Drover & Shragge, 1977).

The limitations stated above do not prevent the applicability of systems theory to the present study because this study does not intend to explain the lack of interoperability *per se* but rather to provide a solution to address the lack of interoperability concerning blockchain systems. Furthermore, this study did not follow the critical realism paradigm, which relates to issues around power dynamics, morality and ethics. Rather, the present study followed the pragmatism paradigm, which relates to actions to address interoperability. Regardless of the aforementioned limitations of the systems theory approach, the researcher believes that applying systems theory allowed for a comprehensive examination of blockchain interoperability.

4.5.6 Overview of Selected Theories and Models

Theory/model	Phase applied	Application
Technology, environment and organisation framework (TOE)	Chapter 5 DSRM phase: Problem Identification	Systematic literature review Data collection and analysis
European interoperability framework	Chapter 6 DSRM phase: Identify Objectives of the Solution	Systematic literature review Data collection and analysis
General systems theory	Chapter 7 and 8 Overarching Theory for Study DSRM: Design and Develop	Construction of the proposed blockchain Interoperability framework

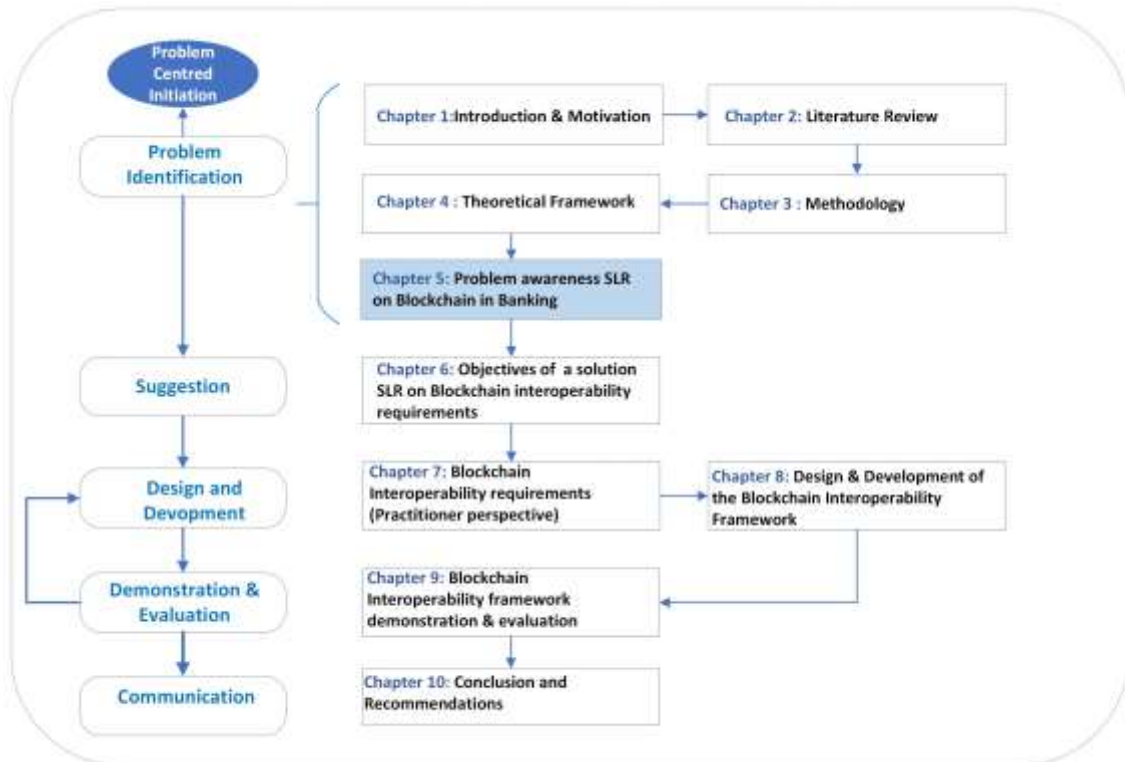
4.6 SUMMARY

This chapter presented the main models and theories underpinning the current study. The chapter commenced with a discussion of key innovation theories, in particular, the TOE framework, which underpins the systematic literature review (Chapter 5) conducted as part

of the Identifying the Problem phase. The chapter also presented the various interoperability models and frameworks relevant to the study. The discussion included the European interoperability framework, which was applied to guide the data collection and analysis of the systematic literature review discussed in Chapter 6. Chapter 4 presented systems theory as the overarching theoretical perspective of the study. The discussion of systems theory included a description of the theory and its associated principles, a rationale for selecting the theory, and a discussion of the theory's application in the study. The next chapter presents the systematic literature review that informed the problem awareness phase of the study (Chapter 5).

CHAPTER 5

5 PROBLEM AWARENESS (A SYSTEMATIC LITERATURE REVIEW)



5.1 INTRODUCTION

The current chapter corresponds to the Problem Identification step in the DSR process adopted for this study. This chapter aims to answer the following sub-research question:

- *What are the use cases, challenges, and considerations for blockchain implementation in the banking sector?*

The study adopted a systematic literature review method to answer the research question above. The chapter articulates the process followed in conducting the systematic literature review approach applied to identify the problem this study intends to solve. The chapter also elaborates on the findings of the systematic literature review. The chapter was published as follows:

Mafike, S.S. & Mawela, T. 2022. Blockchain Design and Implementation Techniques, Considerations and Challenges in the Banking Sector: A Systematic Literature Review, *Acta Informatica Pragensia*, Prague University of Economics and Business, vol. 2022(3), pages 396–422.

5.2 SYSTEMATIC LITERATURE REVIEW

A systematic literature review is a rigorous and methodological-based exercise aiming to identify, collate and synthesise empirical studies to address a particular research question by using a systematic and explicit methodology that minimises bias (Higgins et al., 2011). These types of investigations have several advantages. The SLR enables researchers to access a wide range of studies beyond their particular fields through extensive search methods, predefined search strings and inclusion and exclusion criteria (Robinson & Lowe, 2015). In addition, a SLR allows researchers to examine information relating to a particular phenomenon from different settings and methodological perspectives (Kitchenham, 2004).

There are several approaches to conducting systematic literature reviews (Kitchenham, 2004; Mohamed Shaffril et al., 2021; Nightingale, 2009; Okoli, 2015; Okoli & Schabram, 2010). The guidelines for conducting systematic literature reviews by (Kitchenham, 2004) and the Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) were adopted for this SLR. According to (Kitchenham, 2004) guidelines, conducting an SLR can be accomplished by following three phases: Planning, Conducting the Review and Reporting the Review. Each phase has specific steps and guidelines, as stipulated below.

Planning:

1. Identification and need for review
2. Development of a review protocol

Conducting the review:

3. Identification of research
4. Selection of primary studies
5. Study quality assessment
6. Data extraction and monitoring

7. Data synthesis

Reporting:

8. Reporting the review

The phases and their respective steps were conducted under the guidelines described below.

5.2.1 Planning: Identification and need for review

According to Kitchenham (2004), there are several reasons for conducting a systematic review:

- To provide a thorough and unbiased synthesis and summary of the existing information relating to a specific phenomenon
- To identify deficits in existing research towards identifying new research areas
- To establish a framework for organising existing literature and positioning new research activities appropriately.

The purpose of conducting an SLR in this study relates to the second motivation outlined above, namely to identify existing deficits and uncover opportunities relating to research on blockchain implementation and adoption within the financial sector. In particular, the purpose of the SLR in this study is to identify research deficits by assessing the evidence from scholarly and practitioner literature on practical techniques, challenges and opportunities for implementing blockchain technology in the banking sector.

The need for conducting the SLR was further necessitated by the limitations of existing studies on blockchain within the banking sector. Existing studies and reviews mainly focus on identifying specific use cases and some challenges and perceived benefits of blockchain in the financial sector. However, such studies do not offer any insights into the practical challenges related to implementing blockchain in the sector. In addition, current studies do not sufficiently cover the implementation practices, techniques and considerations organisations need to weigh to enhance the development and adoption of the technology in the sector. Furthermore, most of the literature covering the practical implementation of blockchain in the banking sector originates from practitioners and industry and, thus,

highlights the need for a detailed examination of this topic from an empirical perspective to supplement the practitioners' work and promote a better understanding of the nuances of blockchain implementation in the sector.

5.2.2 Planning: Development of a Review Protocol

Following the guidelines for conducting an SLR by Kitchenham (2004), a protocol was developed. The review protocol stipulated the methods for identifying, screening and selecting the relevant article, but importantly, the review protocol involved the formulation of the research questions addressed by the SLR. The SLR research questions were based on the main Sub-Research Question 1 stated above:

***RQ1:** For which banking operations have banks piloted or implemented a blockchain-based proof of concept?*

***RQ2:** What are the challenges experienced with blockchain implementation in banking operations?*

***RQ3:** What design and implementation considerations are reported in the literature on blockchain-based banking systems?*

***RQ4:** What are the future research directions for blockchain implementation in the banking sector?*

The protocol was subjected to several iterations of a peer-review process to mitigate the possibility of bias. Once the researcher and the supervisor had reached a consensus regarding the protocol, the review was conducted as outlined below.

5.2.3 Conducting the Review: Identification of Research

The identification of research articles was based on two categories of articles: 1) peer-reviewed scholarly articles and 2) grey literature in the form of company technical reports on blockchain adoption and implementation. The decision to include grey literature was made for several reasons. First, academic literature on blockchain implementation is relatively scarce compared to industry-based research; therefore, grey literature was included to augment the findings of the SLR. Second, the inclusion of grey literature in an SLR

minimises publication bias, leading to a more comprehensive and balanced view of the evidence (Paez, 2017). Lastly, it can provide additional insights that may have been overlooked in the academic literature (Paez, 2017).

The two categories of articles were sourced using different approaches and resources. Electronic databases were used to source academic literature. In particular, a systematic search was conducted on the following electronic databases to search for peer-reviewed academic articles: *Scopus*, *IEEE Xplore*, *ACM Digital Libraries* and *ScienceDirect*. The databases were queried using search strings formulated with the following primary keywords: “blockchain implementation” and “banking”. In addition, synonyms of the above-stated keywords, for example, “distributed ledger”, “DLT”, “proof-of-concept”, “experimentation” and “financial”, were used to formulate alternative search strings to enhance the search efforts and ensure that the search results were comprehensive. In addition to the databases, the top eight (Basket of Eight) IS journals were also searched for potential articles; however, at the time, they did not yield any results. Table 5-1 depicts the search strings applied to selected databases and journals.

Table 5-1 Databases used and respective search strings

Search string	Database
(blockchain OR “distributed ledger” OR DLT) AND (implementation OR design OR “proof of concept” OR develop*) AND (bank OR finance)	<i>Scopus</i> , <i>IEEE Xplore</i> , <i>ACM Digital Libraries</i> and <i>ScienceDirect</i> ,
("blockchain implementation" OR "blockchain design" OR "blockchain proof of concept" OR "blockchain development" OR "blockchain system" OR "blockchain-based system" OR "distributed ledger implementation" OR "distributed ledger design" OR "distributed ledger proof of concept" OR "distributed ledger development") AND (bank OR finance OR banking)	<i>Scopus</i> , <i>IEEE Xplore</i> and <i>ACM Digital Libraries</i>
<p>Sub-key 1</p> <p>("blockchain implementation" OR "blockchain design" OR "blockchain proof of concept" OR "blockchain development" OR "blockchain system" OR "blockchain-based system" OR "distributed ledger implementation")</p> <p>Sub-key 2</p> <p>("distributed ledger design" OR "distributed ledger proof of concept" OR "distributed ledger development") AND (bank OR finance OR banking)</p>	<i>ScienceDirect</i> (the second search key above had to be broken down into two substrings because <i>ScienceDirect</i> has a limit on the number of terms in the search string)

Company reports were sourced from institutional websites. A Google search was undertaken to identify banking and financial institutions involved in blockchain development. Table 5-2 indicates the search strings used to identify the institutions. The identified institutional websites were searched for relevant reports and working papers (Table 5-3). Institutional websites and publications provide credible sources of grey literature for an SLR because the knowledge and authority of such sources are well established (Adams et al., 2017; Garousi et al., 2019).

Table 5-2 Search keys for identifying financial institutions involved in blockchain experimentation

Seach Engine	Search string
Google	Central bank blockchain projects
Google	Banks experimenting with blockchain

Table 5-3 Banks experimenting with blockchain

Central Banks	
<ul style="list-style-type: none"> • Bank of Lithuania • Bank of Thailand • Hong Kong Monetary Authority • Saudi Arabian Monetary Authority • South African Reserve Bank • Monetary Authority of Singapore • Bank of Canada 	<ul style="list-style-type: none"> • Swedish Central Bank • National Bank of Cambodia • Central Bank of Brazil • German Central Bank • Bank of France • European Central bank • Bank of Japan

5.2.4 Selection of primary studies

Identifying and selecting the final articles for the review was initiated by searching the selected databases, and the results were exported to the reference manager software *Mendeley*. Duplicated articles were removed using *Mendeley*. The removal of duplicates of technical reports was done manually. A title and abstract screening was then performed on the remaining articles, and articles irrelevant to the research questions were excluded. In cases where the relevance of the paper could not be determined from the title and abstract, a full copy was obtained and assessed by the researchers, who agreed on the relevance of each paper. Full-text copies of the articles identified as relevant were downloaded and

reviewed. The decision to determine the final articles to review was made based on the following pre-defined inclusion and exclusion criteria.

Inclusion criteria:

- The study was written in English. The researchers only understand English.
- The study was published between 2008–2021. The indicated period is relevant because the first publication on blockchain was published in 2008 (Nakamoto, 2008).
- The study focused on the implementation of blockchain technology (distributed ledger) in the banking sector.
- The study covered blockchain implementation or design guidelines and considerations within the banking sector.
- The study was available in an electronic format.

Exclusion criteria:

- Studies not written in English.
- Systematic literature reviews. The authors only considered studies that had used primary data, not secondary data.
- Studies that did not focus on either or both blockchain implementation and design implementation considerations within the banking sector
- Non-peer-reviewed academic studies and practitioner reports not from the banking sector.

A study was excluded if it met any of the exclusion criteria. In addition, forward and backward searches were performed on the selected articles to identify relevant articles that may have been missed during the initial database searches. These were included in the final list of articles selected for review, as shown in the PRISMA chart in Figure 5-1. The PRISMA chart depicts the steps explained above as well as the number of articles found and excluded at each step of the process.

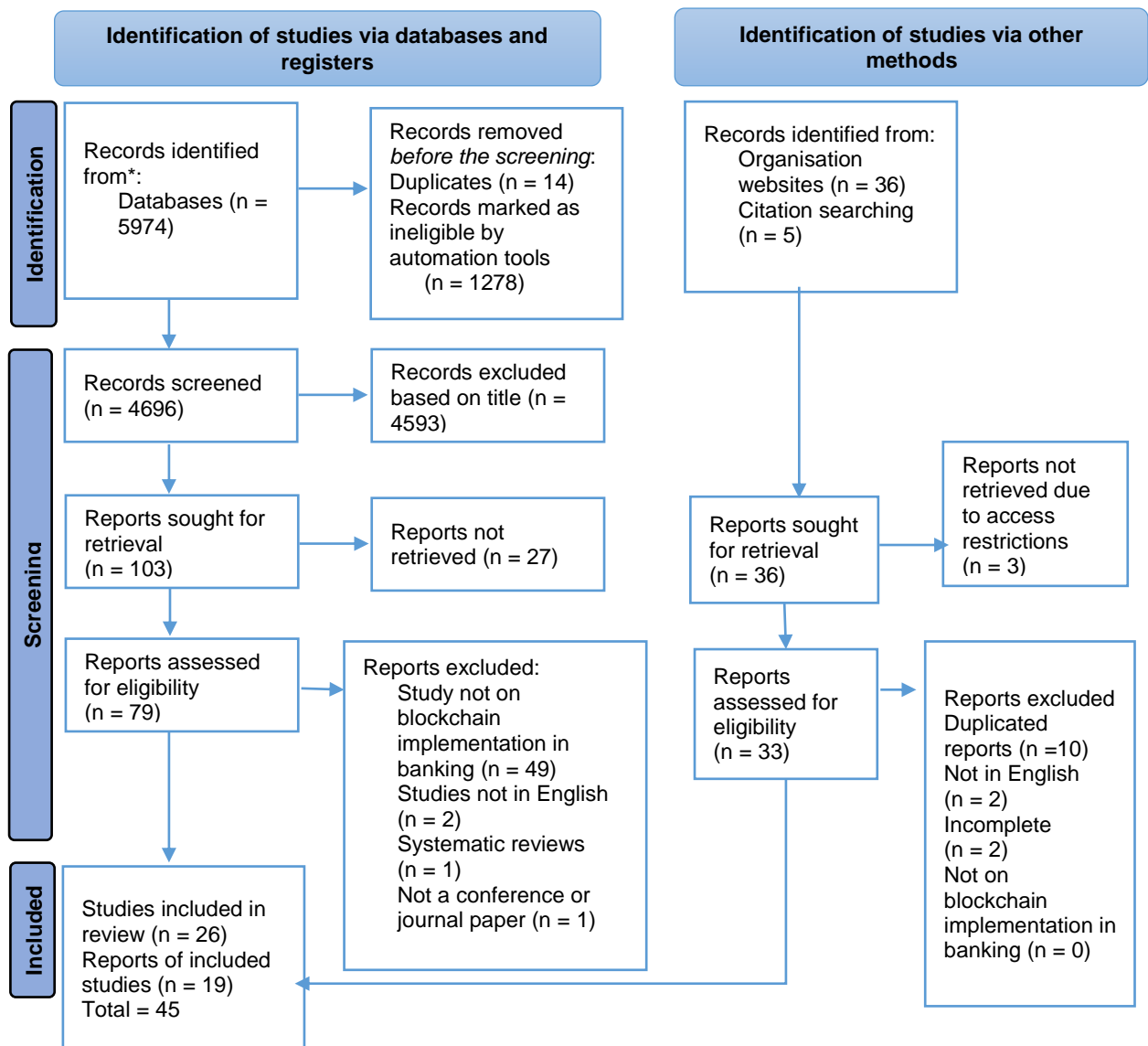


Figure 5-1 PRISMA 2020 chart of the selection strategy (Adapted from Page et al., 2021)

5.2.5 Study Quality Assessment

According to Kitchenham (2004), the studies selected for inclusion in the review should undergo a quality assessment to weigh their relevance when synthesising the results and guide recommendations for future research. The quality assessment criteria proposed by (Dybå & Dingsøyr, 2008) and (Garousi et al., 2019) were applied to assess the quality of the

45 selected studies. In particular, the assessment criterion used to evaluate academic studies was adopted from the quality checklist by (Dybå & Dingsøy, 2008), as shown in Table 5-4. However, some questions from the list by (Dybå & Dingsøy, 2008) were excluded because they did not apply to the type of studies selected for the review. For instance, questions on sampling, control groups and participants were excluded because the studies used in this review were implementation papers, which, in most cases, did not require the involvement of participants. Only the organisational technical reports were assessed per the checklist by (Garousi et al., 2019), as shown in Table 5-5. The rationale for using different criteria to assess the academic and grey literature was based on the argument by (Garousi et al., 2019), who argue that assessing the quality of grey literature requires a more fine-grained approach than for academic literature because the process of developing grey literature is less controlled.

Table 5-4 Assessment criteria to evaluate academic studies (adapted from Dyba & Dingsøy, 2008)

Quality criteria	Yes	No
QC1. Are the aim and objectives stipulated clearly?		
QC2. Is there a rationale explaining clearly why the study was undertaken?		
QC3. Is the idea presented clearly?		
QC4. Are there clearly stated findings with credible results and justified conclusions?		
QC5. Is the context of the study articulated clearly?		
QC6. Do the findings provide value for research or practice? (Does it enrich or add something unique to the research?)		
QC7. Does the paper specify the research design for the study?		
QC8. Does the paper justify the appropriateness of the research design?		
QC9. Does the paper specify the limitations of the study?		

Table 5-5 Assessment criteria to evaluate grey literature (adapted from Garousi et al.,2019)

Quality criteria	Yes	No
QC1. Is the source published by a reputable organisation?		
QC2. Is the author associated with a reputable institution?		
QC3. Does the author have expertise in the area?		
QC4: Are the aims and objectives clear?		
QC5: Is the methodology clearly stated		
QC6: Is the source presented in an objective manner?		
QC7. Are there clearly stated findings with credible results and justified conclusions?		
QC8. Is the context of the study clearly articulated?		
QC9. Do the findings provide value for research or practice? (Does it enrich or add something unique to the research?)		

5.2.6 Data Extraction and Synthesis

The final sample of 45 articles was subjected to a systematic literature review to analyse the demographics of the paper, such as the type of paper, year of publication, the author's affiliation, and the geographical location of the publication. Second, an automated, qualitative content analysis using *Leximancer* software was executed to analyse the academic studies and practitioner reports separately. The analysis for the studies and reports was performed separately to compare scholarly work and practitioner work to identify differences and similarities between the two. *Leximancer* is machine learning, data mining software used for automated content analysis. It enables the analysis of large, complex volumes of text without the need for a researcher to develop codes and concepts manually (Angus et al., 2013). Using *Leximancer* to generate concepts reduces analytical bias (Lemon & Hayes, 2020), which is typical of manual analysis; in addition, it is more statistically reliable and reproducible (Angus et al., 2013).

The analysis was initiated by uploading PDF versions of the studies and reports into *Leximancer*, which then generated the concepts automatically. The themes and the associated concepts generated by *Leximancer* were generated at a visibility concept setting of 100% and a theme size of 51%. The generated concepts were evaluated, and all irrelevant concepts were removed. The concepts were evaluated for relevance to answer the research questions. The authors adjusted the settings to include user-defined concepts relating to the research questions to refine the map. The user-defined concepts included, bank, blockchain, implementation, and system. A second automatic regeneration of the concept map was executed to include the user-defined concepts. The results of the analysis are presented in Section 5.2.7 below.

5.2.7 Data Synthesis (Results)

Data synthesis involves summarising the results extracted from the selected articles. Synthesising the information from the articles could follow a qualitative or quantitative approach. In this case, a qualitative approach was taken, and the results were synthesised

to answer the respective sub-research questions outlined below. The following discussion presents the key findings concerning each research question.

SRQ1: For which banking operations have banks piloted or implemented a blockchain-based proof-of-concept?

The results of the content analysis performed on the selected studies to identify the banking operations where blockchain technology was being used revealed a growing interest in the technology among global central banks. The results showed that the majority of central banks were exploring the use of blockchain in addressing inefficiencies with traditional payment systems, such as in cross-border and remittance systems (Bank of Canada & Monetary Authority of Singapore, 2019), inter-bank settlement (Payments Canada et al., 2017) and security settlements (Monetary Authority of Singapore, 2017b). Another area of application identified in the literature relates to the use of blockchain in developing central bank digital currencies (CBDCs). From the reviewed literature, the most common application of CBDC relates to cross-border payments. According to Han et al. (2019, p. 268), this is because CBDC systems offer “real-time settlement and reduce costs” associated with traditional payment systems. For example, several banks Hong Kong Monetary Authority and Bank of Thailand (2018) and Raphael Auer et al. (2021) have explored the use of multi-CBDCs to enable interoperability in multi-currency cross-border payments to reduce risk and high transaction costs typical to these types of payments. In addition to the applications above, some banks have also explored the use of blockchain in trade finance operations and for enhancing know-your-customer (KYC) and anti-money laundering (AML) compliance processes.

SRQ2: What are the challenges experienced with blockchain implementation in banking operations?

Regarding the question of what challenges are experienced when developing blockchain in the banking sector, the reviewed literature highlights some key challenges relating to the scalability of blockchain systems, performance issues, regulatory limitations and challenges with enabling interoperability between blockchain systems. The following discussion elucidates these challenges as identified in the reviewed literature.

Scalability and performance issues

The reviewed literature cited scalability and performance issues as some of the challenges limiting the implementation of blockchain technology in the sector. Specifically, scalability and performance issues were reported concerning blockchain platforms that utilised the traditional proof-of-work (PoW) consensus mechanism. According to the Monetary Authority of Singapore (2017a), PoW-based platforms have lower transaction speeds compared to alternative and newer blockchain platforms such as *Corda*, *Quorum* and *Hyperledger*, mainly because PoW platforms require the entire ledger to be duplicated on every node in the network. However, some studies also highlighted challenges relating to the scalability and performance of the newer platforms. For example, the Bank of Thailand (2018) found that the *Corda* platform resulted in reduced performance when multiple consecutive transactions were initiated by the same node due to the sequential transaction processing mechanism *Corda* uses to process transactions. Others European Central Bank and Bank of Japan (2020) and South African Reserve Bank (2018) reported that the overall performance of the newer platforms was reduced significantly when the number of transaction requests increased with increased network sizes.

Legal and regulatory challenges

Legal and regulatory challenges are other areas of concern relating to the implementation of blockchain technology in the banking sector. The provision of banking services is a highly regulated process, and banks are required to comply with domestic and cross-jurisdictional laws and regulations. Similarly, banks adopting blockchain in their operations have to comply with local and global financial regulations. However, despite the requirement of compliance within the sector, several organisations (Hong Kong Monetary Authority & Bank of Thailand, 2018; Sveriges Riksbank, 2017) have highlighted regulatory and legal issues concerning the implementation of blockchain-based payment systems. The studies point out that current legal and regulatory frameworks governing financial market systems are not suitable for blockchain-based payment systems in their current state. As a result, the Hong Kong Monetary Authority and Bank of Thailand (2018) and Zhang (2020) argue that amendments to current regulatory frameworks are necessary to suit the nature of transactions on the blockchain better and meet the required operations and management of blockchain-based payment systems.

Platform interoperability issues

The lack of interoperability between different blockchain platforms used within the banking sector was also identified by some of the literature as a significant inhibitor of blockchain implementation in the industry. The lack of interoperability between the platforms means transaction information cannot be shared between blockchain payment systems, as required. The literature outlined several factors contributing to the lack of interoperability. According to the South African Reserve Bank (2018), the traditional banking systems and core technology used to support these banking systems were not designed to support blockchain technology. As a result, the emerging blockchain-based payment systems are not interoperable with the existing systems.

The South African Reserve Bank (2018), further states that additional interoperability issues stem from variations in the technologies used across different financial payment ecosystem players. Typically, the financial payments ecosystem involves global participation that often involves differing technologies. Similarly, the choice of blockchain platforms varies significantly across participants in the ecosystems. The heterogeneity in the blockchain platforms used complicates the transfer of transaction information between participants. Chapman et al. (2017) state that the lack of interoperability resulting from the heterogeneity of the blockchain platforms used in the sector is a critical obstacle for cross-border and remittance payments where transactions span multiple jurisdictions.

SRQ3: What design and implementation considerations are reported in the literature on blockchain-based banking systems?

This section discusses the practical strategies and considerations adopted by the banking enterprises to implement blockchain. The principles and strategies presented are mainly the principles that are common to all the use-cases identified and addressed in SRQ1 above. The identified principles are categorised according to the TOE framework for technology adoption explained in Section 4.3.2. The three tenets of the TOE framework were used to categorise results into three themes, namely, the Technical consideration theme, Organisational considerations theme and the environmental considerations theme. The discuss therefore includes the technical, organisational, and broader environmental principles and strategies to provide a comprehensive interrogation of the considerations for implementing blockchain in the banking sector. The theme Technical considerations, represents the technological aspects that should be considered when implementing

blockchain interoperability. The Organisational considerations theme represents the business decisions and considerations that impact and influence how the process of interoperating blockchain technology into the business is handled. In addition, the Environmental considerations theme denotes the legal and regulatory elements that should be considered when implementing blockchain technology.

Technical Considerations

- *Blockchain platform selection*: The reviewed literature identified the selection of the correct blockchain as a critical consideration. Banking institutions can choose from several blockchain platforms in the market depending on the intended use case, and each platform offers different capabilities and features. For instance, platforms such as *Quorum*, *Corda* and *Hyperledger Fabric* are preferred over public blockchains due to their security and privacy features. However, even these platforms have significant differences in performance and security metrics. Therefore, the choice of the right platform that is fit for purpose requires careful consideration and assessment of its functionalities, adaptability and compatibility with existing enterprise systems (Farshidi et al., 2020).
- *Privacy*: The literature indicates the necessity of ensuring blockchain banking solutions are designed in a manner that protects the privacy of the participants on the blockchain. In addition, blockchain banking systems should offer privacy levels comparable to current systems. In particular, the literature recommends solutions that leverage the inbuilt privacy and security features of the blockchain platform, such as the use of confidential identities in *Corda* (Monetary Authority of Singapore, 2017a), the use of channels in *Hyperledger* and the use of constellations, whispers and Pedersen commitments in *Quorum* to hide transaction information from parties not involved in the transaction (South African Reserve Bank 2018).
- *Scalability*: Designing scalable blockchain systems is also cited as a key consideration in developing blockchain banking systems. Scalability in the context of banking systems refers to the notion that blockchain payment systems should be designed to accommodate the current transaction volumes of traditional payment systems and should also be designed to anticipate growth in future transaction volumes. In addition, they should be designed to accommodate future additions of

new participants with no or limited changes to the system design (Saudi Central Bank, 2019).

- *Resilience*: Blockchain financial solutions should be developed to be resilient to failure, i.e., their design should incorporate disaster recovery mechanisms to contend with various system failures and reduce system downtime (Hong Kong Monetary Authority & Bank of Thailand, 2018). All network participants should provide the necessary “operational capacity and sound risk and data management” to ensure a resilient environment (Morales-Resendiz et al., 2021, p. 7).
- *Existing systems and frameworks*: According to the South African Reserve Bank (2018), existing systems and frameworks should be considered. The SARB suggests that the existing systems should be evaluated to ensure their suitability and compatibility for integration and interoperating with new blockchain-based systems. Similarly, potential risks to existing systems should be evaluated, and changes to these systems should be controlled to avoid unintended disruptions to existing business processes (Saudi Central Bank, 2019).

Organisational Considerations

- *Scope*: The literature highlighted the importance of defining a clear and confined scope of the *application* of blockchain technology in the sector. The scope of application is an important consideration because it influences other considerations, such as the nature of the blockchain, platform selection, the protocols, and the number of participants (nodes) to use for a specific case (Bank of Canada, 2018; Bank of Thailand, 2018).
- *Definition of roles*: Conventional payment systems involve an orchestration and coordination of multiple participants, which often include various players, such as central banks, commercial banks and other financial service institutions. Similarly, blockchain payment systems require a significant amount of coordination and operational effort to enable interoperability with the financial ecosystem. Therefore, when designing blockchain systems, the roles of individual stakeholders should be clearly defined to simplify collaboration and accountability (Morales-Resendiz et al., 2021).

- *Governance*: The traditional banking ecosystem follows a centralised governance model in which the central bank is the sole party responsible for regulating and supervising other financial players (Nier, 2009). This is in contrast to the decentralised governance model used to manage participation in blockchain systems. These variations call for new governance structures and frameworks to ensure harmony and standardisation among participating banks using blockchain technology (Monetary Authority of Singapore & Bank of Canada, 2019). New governance models should be developed for blockchain systems to govern the consistency of the blockchain network and ensure no banking node is favoured over the others (Monetary Authority of Singapore, 2017a).

Environmental Aspects and Considerations

- *Legal and regulatory compliance*: The reviewed literature highlighted the need for blockchain payment systems to be designed in compliance with local and global regulatory frameworks, and wherever existing frameworks are not suitable, newer and more suited regulations should be developed (Hong Kong Monetary Authority & Bank of Thailand, 2018). In addition, the literature has highlighted legal aspects to consider when developing blockchain payment systems. These include the legalities of smart contracts (European Central Bank & Bank of Japan, 2018; Monetary Authority of Singapore, 2017a), legal settlement finality (South African Reserve Bank, 2018), and legal issues relating to service-level agreements (National Bank of Cambodia, 2020).

SRQ4: What are the future research directions for blockchain implementation in the banking sector?

The review of the blockchain use cases and applications in the banking sector revealed that implementing the technology has the potential to yield results for the sector. However, this potential is hindered by some challenges relating to the implementation of the blockchain in the sector. The literature review results indicated that the sector was not fully realising the

benefits of the technology due to limitations relating to interoperability, privacy and security, scalability, regulation and governance. Based on these results, the following opportunities were identified for future research and the basis for conducting this study.

Governance

The banking sector involves several participants with varying interests. Governance models play an important role in ensuring the success of these collaborative networks. However, introducing blockchain into the banking ecosystem requires new governance models to be developed. Introducing blockchain technology in the sector introduces disparities between the typical centralised governance models used in the sector and the blockchain-based decentralised consensus-based models. Therefore, there is a need for researchers to investigate ways of reconciling the traditional governance models and emerging blockchain technology. Furthermore, researchers could explore the impact of blockchain on existing governance models and might also propose new blockchain-centric governance models.

Security

Blockchain technology is designed to be highly secure yet is not without limitations. Blockchains consist of several layers contributing to their desirable properties but may also lead to security concerns. Blockchain technology features, such as consensus mechanisms, smart contracts, and protocols, have security vulnerabilities which can be exploited to compromise the security of the blockchain system (Hasanova et al., 2019). Therefore, it is critical for organisations adopting the technology to understand the security risks posed by the technology at different levels. Researchers have to explore and understand the security and privacy implications of integrating blockchain into their business processes to address these concerns. Future studies could investigate the various security vulnerabilities of blockchain systems and propose possible mitigation strategies and controls.

Interoperability

The disjointed nature of blockchain projects in the banking sector has resulted in several disparate and distinct systems that are unable to communicate (South African Reserve Bank, 2018). This lack of communication between blockchain systems in the sector presents a challenge for cross-border payments, which require transactions to be processed across multiple different networks. Furthermore, the application of the technology in the sector leads

to further interoperability issues between the technology and existing core banking legacy technologies used to support payment systems. The challenges are further complicated by the absence of suitable standards, frameworks and protocols for enabling interoperability in blockchain banking systems (South African Reserve Bank, 2018).

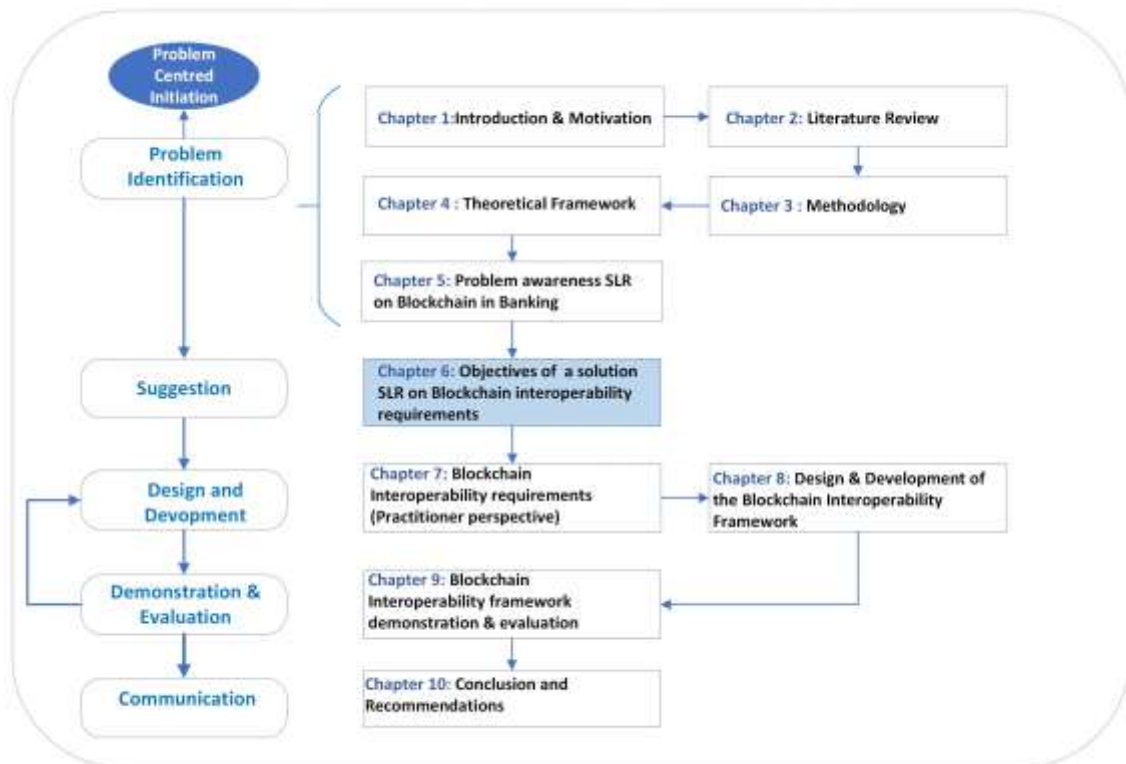
The following opportunities were identified from the limitations described above. Future research could focus on conceptualising and developing standards and frameworks for blockchain implementation in general. Future research could also investigate interoperability methods and protocols for achieving domestic and global financial market interoperability, including cross-border payments and CBDC. In addition, future studies might focus on privacy issues related to the interoperability of blockchain systems in the financial and banking sectors. Another important potential area for future exploration is blockchain-to-legacy enterprise system interoperability. Researchers and practitioners could explore approaches to enabling blockchain-to-legacy system interoperability. At the same time, a broader research area is understanding blockchain interoperability at all levels, including semantic, syntactic, organisational and technical levels. This study aims to address the deficiency relating to two of the challenges identified above 1) The lack of interoperability between blockchain systems and existing legacy systems within the banking sector and 2) The lack of interoperability between blockchain platforms used in the sector.

5.3 SUMMARY

Chapter 5 outlined how the problem addressed by this study was identified using a systematic literature review method. The chapter presented the procedure for conducting the review and the associated key findings. The next chapter relates to the Solution Suggestion step of the DSRM process and presents the objectives of the solution proposed in this study.

CHAPTER 6

6 OBJECTIVES OF A SOLUTION (A SYSTEMATIC LITERATURE REVIEW)



6.1 INTRODUCTION

Chapter 5 outlined the process of identifying the problem that this study addresses. The current chapter presents the next step in the DSRM process, which relates to identifying the objectives of a solution required to address the study problem. In particular, this chapter presents the systematic literature review approach adopted to identify the solution objectives which are in the form of requirements for enabling blockchain interoperability. This chapter was published and presented at a conference as follows:

Mafike, S.S., Mawela, T. (2023). Requirements for interoperable blockchain systems: A systematic literature review. In: Younas, M., Awan, I., Benbernou, S., Petcu, D. (eds) The 4th Joint International Conference on Deep Learning, Big Data and Blockchain (DBB 2023). Deep-BDB 2023. Lecture Notes in Networks and Systems, vol 768. Springer, Cham. https://doi.org/10.1007/978-3-031-42317-8_4

6.2 SYSTEMATIC LITERATURE REVIEW

The systematic literature review was conducted following a similar process to the one followed in Chapter 5. The systematic literature review process presented in the current chapter also followed the guidelines for conducting systematic reviews by (Kitchenham, 2004) and the PRISMA reporting guide (Page et al., 2021). However, in this chapter, the purpose of the review was to address the following research question:

- *What are the requirements for technical, semantic, organisational and legal interoperability in blockchain systems?*

The upcoming sections present the process followed to address the research question stated above. In addition, the sections discuss the requirements identified in the process.

6.2.1 Planning: Identification and Need for Review

As stated in Chapter 5, Kitchenham (2004) suggests that the first step of conducting a systematic review is planning the review by first identifying the purpose of the review, formulating the research question, and developing a review protocol. The purpose of this review is guided by the DSRM process followed. Under DSRM, once a problem has been identified (as outlined in Chapter 5), the objectives of a possible solution must be ascertained. In this instance, the main purpose for conducting the review was to identify the requirements a solution would have to fulfil to address the lack of interoperability between blockchain systems and other systems within enterprise settings.

An additional motivation for conducting the review was that currently, the majority of these solutions are designed to address interoperability issues in public blockchain networks and overlook interoperability concerns in private and consortium blockchains used in enterprise settings.

Furthermore, existing solutions and studies mainly focus on addressing interoperability from a technical and semantic perspective. However, to achieve true interoperability, many other aspects must be considered, such as legal agreements, governance structures, data formats, semantic choices, applications, technical infrastructure, privacy and security issues

(Ndlovu et al., 2021). Hence, fully understanding blockchain interoperability requires extending the focus beyond public blockchain interoperability and the technical and semantic aspects. It is critical to understand interoperability in the context of blockchain systems within enterprises. Other forms of interoperability, such as organisational and legal interoperability (European Commission, 2017) and the interoperability between blockchain and legacy systems, should be explored to achieve such interoperability.

6.2.2 Conducting the Review: Identification of Research

This step consisted of identifying the literature, searching for the literature and making decisions regarding the suitability of the literature to be considered for the review (Cooper, 1988). In this review, two forms of literature were identified: academic peer-reviewed literature in the form of journal and conference papers and grey literature in the form of practitioner reports. Typically, SLR studies include only academic literature; however, this review included grey literature to expand the scope of studies included, thereby providing a comprehensive view of the available evidence (Mahood et al., 2014). In addition, grey literature provides a valuable data source for research intended for academics and practitioners as it builds trust between academics and practitioners and enhances the applicability of academic research work to industry settings (Garousi et al., 2019).

The search strategy used to identify prospective literature was as follows. Academic peer-reviewed articles were sourced from digital databases, which included *ACM Digital Libraries*, *IEEEExplore*, *ScienceDirect*, and *SpringerLink*. The grey literature was sourced through a Google search. The literature search was operationalised using search strings (see Table 6-1) formulated using the following main keywords from the research questions: blockchain interoperability, requirements, elements, framework, and solution. In addition, synonyms, related terms and abbreviations were used to compile additional search strings to enhance the search effort.

Table 6-1 Search strings used to identify the literature

Search string for academic literature	Search keys for practitioner reports
“blockchain interoperability” AND Requirements	Blockchain interoperability requirements
“blockchain interoperability” AND elements	Blockchain interoperability framework
“blockchain interoperability” AND framework	Cross-chain communication requirements
“blockchain interoperability” AND solution	
“DLT interoperability”AND requirements	
“cross-chain” AND interoperability AND requirements	
“cross-chain communication’ AND requirements	

6.2.3 Selection of Primary Studies

The search strategy described above retrieved 196 academic articles from the databases and five industry reports. The retrieved articles were then subjected to a screening process in which duplicate articles were removed. The remaining articles were then screened using predefined inclusion and exclusion criteria shown in Table 6-2. The remaining papers were further screened by reviewing their abstracts, and studies found to be irrelevant based on their abstracts were also removed. Full-text screening and review were performed on selected remaining articles. Eighty-three conference and journal articles and five industry reports were selected for the review. The details of the search and selection processes are outlined in the PRISMA chart shown in Figure 6-1 below.

Table 6-2 The Inclusion and Exclusion criteria

Inclusion criteria	Exclusion criteria
Conference and journal papers, and industry reports on blockchain interoperability and related topics: cross-chain communication or blockchain integration	Generic studies and reports on blockchain but not relevant to blockchain interoperability and related concepts
Peer-reviewed articles and industry reports on blockchain design or decision frameworks	Duplicated studies
Papers are written in English	Editorial, opinion pieces, abstracts, summaries and any incomplete studies because they do not provide sufficient information
Year of publication 2009–2023	

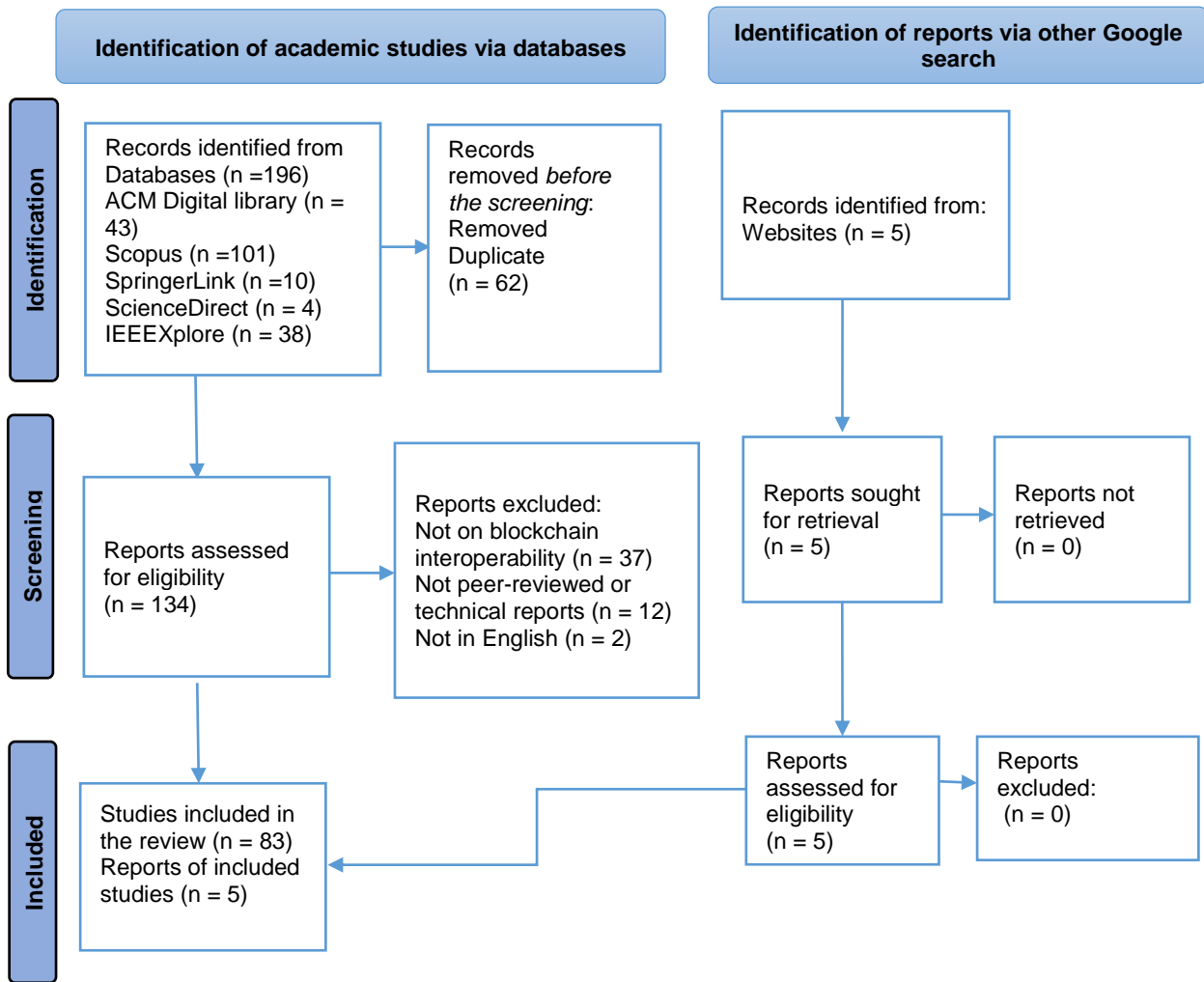


Figure 6-1 PRISMA 2020 chart representing the search process. (Adapted from Page et al., 2021)

6.2.4 Data Extraction

The data were extracted from the selected articles using *Leximancer* text mining software. The articles were saved in PDF format and exported to *Leximancer*. The software then automated the process of identifying concepts and themes from the studies. In addition to the automated concepts, additional user concepts such as organisational, legal, semantic and technical requirements were included to help streamline and focus the data extraction on the requirements.

6.2.5 Data Synthesis

The researcher analysed the final selection of studies and reports using the thematic analysis approach. Thematic analysis is a qualitative data analysis approach in which patterns and meanings in a dataset are identified and analysed (Braun & Clarke, 2012). Thematic analysis can be used to analyse any form of qualitative data, such as interview transcripts, field notes, documents, videos and audio (Joffe, 2012). In addition, thematic analysis is independent of theory and epistemology and thus can be applied in studies underpinned by different epistemologies. The analysis and review of the selected literature was based on the four levels of interoperability defined by the (European Commission, 2017). *Leximancer* analysis software then automated the analysis process.

The four levels of interoperability (technical, semantic, organisational and legal levels) were selected as the themes for identifying and classifying the different requirements. As elaborated in Chapter 4, the technical interoperability layer relates to ensuring connectivity between systems and services and the applications and technologies they use. The organisational interoperability level focuses on aligning business processes between organisations to achieve a commonly agreed upon and mutual goal. The semantic interoperability level focuses on the semantic and syntactic elements of the data to be exchanged. Lastly, the legal interoperability level ensures that organisations operating under different legal, policy and strategic frameworks can collaborate.

The following discussion presents the key interoperability requirements identified from the reviewed literature. The requirements are presented and categorised under the four themes corresponding to the four levels of interoperability mentioned above. The analysis revealed that the majority of the studies did not distinguish between technical and semantic interoperability requirements. Therefore, the requirements identified under these themes are presented under one section that includes both these levels of interoperability. The requirements for organisational and legal interoperability were not explicitly stated in most of the reviewed articles. The study also noted that the reviewed literature distinguished between interoperability requirements for permissioned and permissionless blockchain types. Following this observation, we present the findings on the interoperability requirements and categorise them according to whether they are requirements for permissioned or permissionless blockchain types.

6.2.6 Technical and Semantic Interoperability Requirements (TSR)

TSR1: *Security, Privacy and Data Confidentiality*

Security is cited as a fundamental requirement for interoperability in permissioned and permissionless blockchains, which are both required to store and exchange arbitrary data and digital assets in a way that does not compromise the authenticity and validity of the data. Hence, providing interoperability should not compromise the security of the communicating blockchains, and the mechanisms, methods, and operations used to enable interoperability between the blockchains must be secure.

Achieving this requires that the data exchange between different blockchains should be protected at the source blockchain, when in transit, and at the destination blockchain (Jin et al., 2018). Thus, the communicating blockchains have to provide measures for ensuring the data are secure and cannot be tampered with. The following requirements are stipulated for securing data at the source and destination blockchains: The source chain must have measures to record and ensure the data or digital assets to be transmitted are reliable and valid, and the destination chain must be able to verify and validate the received information (Jin et al., 2018).

According to the literature, the security of data in transit relies on the interoperability or integration mechanisms used. This reliance is mainly because interoperating blockchain systems often require using some integration mechanisms to connect the communicating systems. As a result, the integration mechanism should also fulfil some security requirements to protect the data in transit; accordingly, the integration mechanism must be credible and trustworthy. Credibility and trustworthiness are key requirements for integration mechanisms relying on central parties, such as third-party integration schemes, single notary schemes and bridges. The integration mechanism should not be less secure than the blockchains it is connecting, as this would compromise the security of the connected chains (Pillai et al., 2023). Furthermore, the integration mechanism must be fault-tolerant to ensure the continuous availability and accessibility of the data (Pillai et al., 2023).

Concerning data confidentiality and privacy requirements for interoperability in permissioned and permissionless blockchains, permissioned blockchains tend to have more stringent requirements for data privacy than their permissionless counterparts because permissioned

networks are often used within enterprise settings and thus may be used to store confidential and sensitive business information. Thus, enabling interoperability involving permissioned networks requires the confidentiality of the data exchanged during cross-chain communication to be preserved (Hardjono et al., 2020). Such confidentiality is particularly critical for cross-chain communication in which a permissioned blockchain may need to interact with a permissionless blockchain, which offers more data transparency.

Table 6-3 Security, Privacy and Data Confidentiality

TSR1	Security, Privacy and Data Confidentiality
TSR1 : a	The mechanisms, methods, and operations used to enable interoperability between the blockchains need to be secure
TSR1 : b	An integration mechanism that is fault-tolerant
TSR1 : c	Ensure confidentiality of data: access control, authentication and encryption

TSR2: Distinguishability of Blockchains

The second requirement cited in the literature concerns the distinguishability of the blockchains involved in a cross-chain data exchange. The distinguishability requirement refers to the notion that blockchains should be uniquely identifiable to be interoperable. Accordingly, blockchains must have some form of unique identifier or address to identify the source of the data being transmitted for routing and addressing purposes (Hardjono et al., 2020) or have a unique key for identification purposes during the authentication and routing of the exchanged data (Sonkamble et al., 2021).

The identifiability of blockchains is paramount for permissioned blockchains because, in permissioned blockchains, the data exchange relies much on the ability of the network to

authenticate and validate requests and for signature proofs to accompany the data (Ghosh et al., 2021). Therefore, in cross-chain interactions involving permissioned blockchains, the communicating blockchain networks may be required to have and know the identifiers of each other's members (Hardjono et al., 2020). For instance, in consortium blockchain arrangements involving multiple member organisations, it may be required that all member nodes are identified and registered (Hardjono et al., 2019).

However, there may be differences in how distinct networks handle membership identities; thus, a cross-network identity management mechanism is required when multiple blockchains interact (Ghosh et al., 2021). Whenever a cross-network identity management scheme is used, additional requirements must be fulfilled. First, the identity management mechanism must adhere to the privacy and security requirements of the network. Second, the mechanisms should allow external entities or networks to verify member identification independently.

In addition, fulfilling the distinguishability requirement requires the use of decentralised identity registers to map external identities to network-specific identities and also requires each network to maintain the integrity of the network's membership and ensure the availability of its membership list to a communication peer during an interoperability session (Ghosh et al., 2021). Furthermore, the digital identity of each blockchain and its members should be verifiable (Liu et al., 2022). Thus, any blockchain receiving the identity credentials from another blockchain should be able to query the identity register and obtain the identity certificate as proof that the credentials are valid (Liu et al., 2022).

Table 6-4 Distiguishability requirements for blockchains

TSR2	Blockchains should be distinguishable
TSR2 : a	Should have a unique identifier for routing purposes
TSR2 : b	Identity management mechanisms should adhere to privacy and security requirements of a network
TSR2 : c	Digital identity of each blockchain and its members should be verifiable

TSR3: Cross-Chain Communication Protocol

Enabling cross-chain communication or interoperability between disparate blockchain networks requires a common, standard cross-chain communication protocol (Pillai et al., 2022). Standard cross-chain protocols are required to facilitate data and asset transfer between different blockchains and to perform value conversions of incoming and outgoing data (Lipton & Hardjono, 2022). The protocols should ensure that minimal modifications to the existing protocol of each system are needed when a new blockchain is introduced to the ecosystem (Jin et al., 2018). Cross-chain protocols should be designed to fulfil several requirements to achieve this. Generally, cross-chain communication protocols should be designed to fulfil the verification requirement, i.e., they should enable the destination blockchain to verify the existence and validity of a transaction that occurred on the source blockchain (Sober et al., 2022). In addition, cross-chain protocols must fulfil the atomicity and liveness requirements (Robinson, 2021), prevent the double spending problem and ensure the finality of transactions (Sober et al., 2022).

The liveness property states that the atomic cross-chain transaction protocol eventually (after a finite amount of time) terminates (Robinson, 2021). It ensures that during atomic swaps, assets are not locked indefinitely. The atomicity requirement ensures consistency in the states of the blockchains involved in cross-chain communication. In the context of cross-chain communication, atomicity refers to the notion that unless all parts of the transfer are committed, the transaction is rolled back. Atomicity ensures that there is no burn without a claim (Sober et al., 2022). Furthermore, for permissionless blockchains, cross-chain protocols are required to have an incentive mechanism to encourage good behaviour (Robinson, 2021). However, for permissioned blockchains, a reputation mechanism or external enforcement, such as legal action, may be required.

Table 6-5 Cross-chain protocol requirements

TSR 3	Cross-chain communication protocol
TSR3 : a	Should enable data and asset transfer between different blockchains and to perform value conversions

TSR3 : b	Should fulfil the atomicity and liveness requirements
TSR3 : c	Should ensure finality of cross-chain transactions
TSR3 : d	Should prevent double spending

TSR4: Customisation or Standardisation of Data

Standardised data formats have also been cited as a requirement for enabling semantic interoperability. According to Al-Rakhami and Al-Mashari (2022), the data formats used on blockchains must be standardised to enable all participants in the data exchange to verify the reliability of the information and for the communicating parties to have a shared understanding of the data. Specifically, having standardised data formats is required for asset exchanges (atomic swaps) to define asset profiles to ensure the communicating participants have the same definition and value of the asset being exchanged (Lipton & Hardjono, 2022).

Table 6-6 Data standardisation requirements

TRS4	Standardised or common data formats
-------------	--

6.2.7 Organisational Interoperability Requirements (OR)

Organisational interoperability relates to the ability of autonomous enterprises to form strategic collaborative relationships despite any differences that may exist in terms of business practices, culture, legislation and business models (Lemrabet et al., 2010). The organisational interoperability level depends on the agreed definitions of technical and semantic interoperability between enterprises and includes procedures and rules of how collaborative participation is governed (Al-Rakhami & Al-Mashari, 2022). In the context of blockchain technology, organisational interoperability concerns the use of blockchain technology to support specific business processes of enterprises in strategic collaborations.

The enterprises may have different blockchain systems designed to meet specific business goals; however, interoperability between these systems may be required to facilitate data exchanges (Al-Rakhami & Al-Mashari, 2022). The following discussion focuses on some of the key requirements for enabling organisational interoperability in cases where blockchain technology is needed or used to support collaboration between enterprises.

OR1: *Business Model Requirements*

Blockchains, particularly permissioned blockchains, can be used to establish thriving business alliances between different enterprises to provide newer and improved services to themselves and their customers. Conventionally, enterprises can form different types of collaborative relationships. In particular, enterprises can be in vertical relationships in which an enterprise becomes a customer of another enterprise to obtain goods and services that enable the enterprise to deliver products to its customers (Bedin et al., 2021). Alternatively, organisations can establish horizontal business relations with other organisations. In this case, an alliance is formed between two or more competing companies for value creation and the benefit of their customers. Blockchain technology can be used to establish these alliances. However, achieving this requires such organisations to have a shared collaborative blockchain business model for information sharing (Reegu et al., 2022).

Table 6-7 Business model requirements

OR1	Blockchain-driven collaborative business model that enables inter-organisational data exchange
------------	---

OR2: *Trust Requirements*

The reviewed literature highlighted that establishing strategic alliances and collaborations between enterprises requires trust. Trust is critical in inter-organisational collaborations whereby organisations have to share business processes even when the collaborating organisations do not have strong trust relationships, and yet, they have to collaborate to perform a mutually beneficial process (Carminati et al., 2018). Trust ensures that business processes are executed correctly. Traditional mechanisms for establishing trust among organisations include mutual agreements and reputation systems. Similarly, blockchain

technology can be leveraged to increase trust in collaborative business processes (Mendling et al., 2018). However, rather than using mutual agreements, smart contracts can act as a central broker to orchestrate and monitor the execution of business processes (Carminati et al., 2018). In addition, smart contracts can be utilised to enforce the executions of transactions and ensure the satisfaction of contractual conditions and obligations between untrusted stakeholders (Viriyasitavat et al., 2022).

Table 6-8 Trust requirements

OR2	Trust mechanisms such as smart contracts to orchestrate cross-organisational business processes and to enforce contractual obligations
------------	---

OR3: Governance Requirements

Governance requirements relate to the requirements that must be fulfilled to manage and coordinate tasks between multiple organisations in a strategic partnership. Coordinating these tasks requires compatible and comparable governance models between all partners (Lehmann, 2019). In instances where the existing governance models are incompatible, a composite governance model may be required to enable the effective management and coordination of cross-organisational processes and enforce trust between the collaborating partner organisations (Hewett et al., 2020). In consortium networks, blockchain technology itself can be harnessed to facilitate new governance models and approaches that differ from conventional centralised governance models to manage decision rights, accountability and incentives (Beck et al., 2018).

Table 6-9 Governance requirements

OR3 : a	Governance models must be comparable and compatible
OR3 : b	Composite or decentralised governance models in consortium blockchain

6.2.8 Legal Interoperability Requirements (LR)

Legal interoperability relates to “ensuring that organizations that operate under different legal frameworks, policies and strategies are able to share information” (European Commission, 2017). In the context of blockchain technology, legal interoperability is considered to relate to the legal and regulatory dimensions associated with enabling blockchain interoperability. Particularly, it involves identifying the domestic and international legal and regulatory aspects, the legalities of smart contracts used to enable cross-blockchain communications, and any other legal issues concerning the exchange of data and assets across organisational and jurisdictional boundaries. The discussion below includes general legal requirements that are not specific to any industry or jurisdiction. However, additional requirements specific to business contexts and legal environments would have to be considered when developing applications that require interoperability between blockchains.

LR1: *Identification Requirements*

The identification requirement relates to the notion that blockchains should be identifiable. In the context of legal interoperability, the identification requirements pertain to the identification of participants involved in the cross-chain communication process. In this case, the identification is not required for routing purposes; rather, it is required to enforce legal and regulatory compliance with domestic and international laws and regulations (Pang, 2020). For example, some domestic and national contract laws may require parties in a contractual agreement to be identifiable (European Commission, 2020). For instance, in asset exchange processes, where assets are exchanged as payment for goods or services, the parties involved in the transactions may be required to be identified for compliance with tax laws. In other instances, participants may be required to identify themselves for authentication purposes and compliance with know-your-customer and anti-money laundering regulatory requirements (World Bank Group, 2020). However, it should be noted that this requirement may require other requirements, such as the privacy requirement, to be compromised.

Table 6-10 Identification requirements

LR1	Identification of participants in cross-chain communication for legal and regulatory compliance
------------	--

LR2: Jurisdictional Requirements

Blockchain interoperability is not limited to connecting blockchains in the same industry or locality but can also enable blockchains across different geographical locations to connect. Legislation diverges greatly across different countries; therefore, in situations involving collaboration between blockchain systems in different jurisdictions, the systems and parties involved in the data and asset exchanges may have to comply with different laws. As a result, the design of the interoperability mechanisms and smart contracts may be required to anticipate the jurisdictional variations and include policies and legal controls to address the jurisdictional uncertainties (European Commission, 2020; World Bank Group, 2020). In addition, enabling legal interoperability across jurisdictions may require the development of a compliance framework for blockchain systems by establishing multilateral agreements and memorandums of understanding (Zhang, 2020).

Table 6-11 Jurisdictional requirements

LR2	Compliance with cross-jurisdictional regulations and legislations
LR2 : a	Design interoperability mechanisms and smart contracts controls for legal uncertainty
LR2 : b	Legal compliance framework for blockchain

LR3: Smart Contracts Requirements

Smart contracts can play a critical role in supporting blockchain interoperability because they can be written in traditional programming languages and, as a result, can be deployed and executed by any blockchain peer or node. In addition, smart contracts can invoke other smart contracts within the same network and across networks by sending remote procedure calls (Khan et al., 2021). Furthermore, because smart contracts enable parties to set and agree on contractual clauses, they can also be used to implement some of the requirements for enabling legal interoperability. To achieve these, smart contracts are required to satisfy some legal requirements, like being legally enforceable in cases where no separate agreement written in natural language exists. In this case, the smart contract “must satisfy the relevant validity requirements in domestic contract law” (European Commission, 2020) and should be considered legally enforceable and a binding expression of the agreement between parties (Governatori et al., 2018). In some instances, smart contracts may be required to co-exist with traditional agreements, and the smart contract is then used to automate the contents of the traditional agreements (Governatori et al., 2018).

Table 6-12 Smart contract requirements

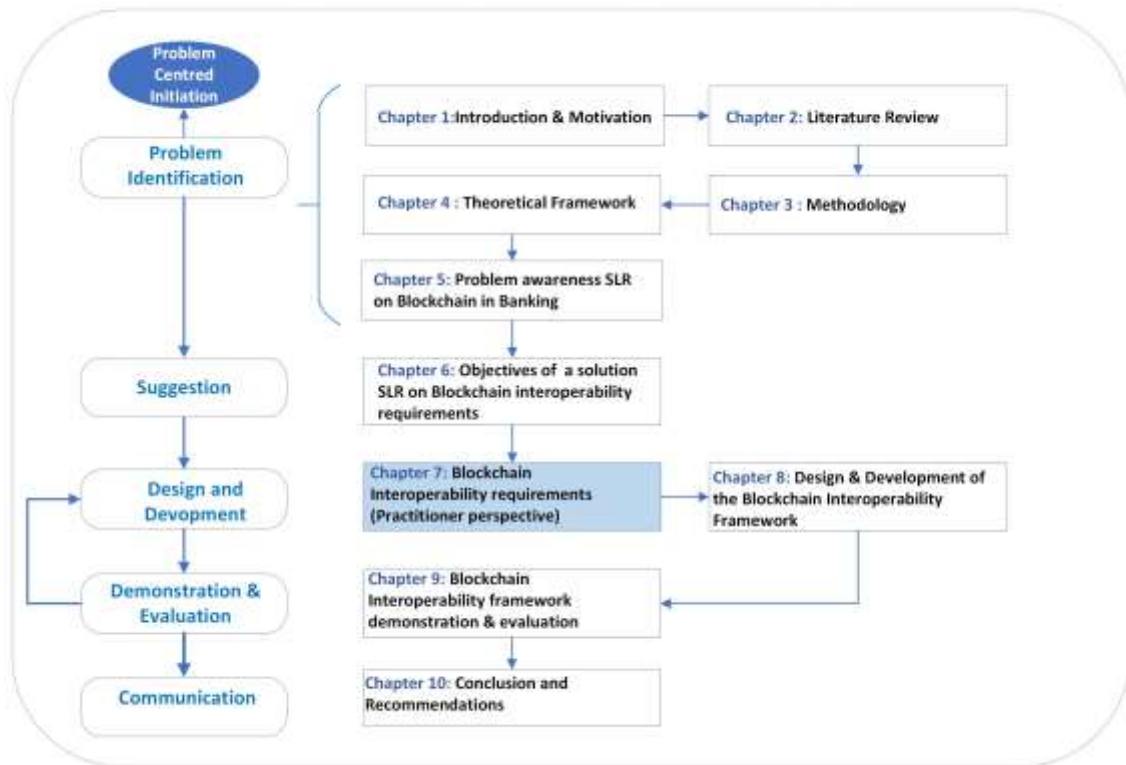
LR3	Smart contracts should be legally enforceable and satisfy relevant domestic contract laws
------------	--

6.3 SUMMARY

This chapter discussed some key requirements for enabling blockchain interoperability. The chapter also outlined how the requirements were identified through conducting a systematic literature review in which a total of eighty-eight articles were reviewed. The chapter elaborated on the process of conducting the systematic literature review. The requirements identified in this chapter were used to inform the design and development of the proposed interoperability discussed in subsequent chapters.

CHAPTER 7

7 OBJECTIVES OF A SOLUTION (EXPERT INTERVIEWS)



7.1 INTRODUCTION

This chapter forms part of identifying the objectives of a solution step of the DSRM process. The chapter comprises two main sections. The first section details the analysis of interviews conducted with blockchain experts. The purpose of the interviews was to understand the nuances of blockchain interoperability from a practical perspective. The second section details the analysis of practitioner webinars on interoperating blockchain from a banking industry perspective. The webinars supplemented insights from the interviews and the systematic literature review discussed in the previous chapter (Chapter 6). The webinars were included to provide a broader coverage of contextual issues relating to blockchain interoperability in the sector. The insights from these two sources then informed the

interoperability framework presented in the next chapter. The chapter addresses the following sub-research questions.

- *What are the requirements for interoperable blockchain systems?*
- *What are the critical elements required to formulate a blockchain interoperability framework?*

7.2 BLOCKCHAIN EXPERT INTERVIEWS

This section discusses the analysis of the data obtained from semi-structured interviews with blockchain experts within the South African banking and financial sector. The aim of the interviews was to identify the key requirements for enabling the interoperability of blockchains in the sector and the different elements/components relating to the interoperability of blockchain systems from the context of the banking sector. An interview questionnaire (APPENDIX B) guided the interview process with the blockchain experts. A blockchain expert in the context of this study refers to anyone with some experience working with blockchain systems either or both as a developer, software engineer, systems architect and in the regulation of blockchain technology or related technologies such as cryptocurrencies within the banking sector or financial services industries. In this phase of the study, thirteen blockchain experts were interviewed. The following discussion details the process followed for conducting the interviews and outlines the profiles of each of the experts.

7.2.1 Interview Process Overview

As outlined in the methodology in Chapter 3, a qualitative, semi-structured interview questionnaire was developed and used to guide the interview process. The questionnaire contained open-ended questions formulated around the four levels of interoperability defined by the European interoperability framework. The interviews were conducted intermittently over four months due to the limited availability of blockchain experts in South Africa. The interviews were conducted online via the *Zoom* Conferencing platform; each

interview session lasted approximately an hour. The profiles of the interview participants are outlined in Table 7-1 below.

Table 7-1 The profiles of the interview participants

7.2.2 Participant No.	Blockchain Experience		
	Roles	Years	Focus
1	<ul style="list-style-type: none"> Chief Technology Officer Chief Digital Officer Blockchain Developer 	6	<ul style="list-style-type: none"> Banking Decentralised Finance(DeFI)
2	Software Engineer	7	<ul style="list-style-type: none"> Banking Blockchain Regulatory Technology
3	DLT Research Group Leader	7	<ul style="list-style-type: none"> Blockchain Regulatory Technology
4	Software Developer	3	<ul style="list-style-type: none"> Permissionless blockchains Smart contracts
5	Systems Architect	5	<ul style="list-style-type: none"> Banking Payment systems Regulation
6	Senior Software Engineer	3	<ul style="list-style-type: none"> Smart contracts
7	Software engineer	4	<ul style="list-style-type: none"> Cryptocurrencies
8	Senior Systems Analyst	5	<ul style="list-style-type: none"> Cryptocurrencies Public blockchains Blockchain Speaker (Blockchain Special interest group)
9	Blockchain Developer	6	<ul style="list-style-type: none"> Permissioned, Permissionless, consortium blockchains, Smart contracts, DApps, DeFi

			<ul style="list-style-type: none"> • Payments and Cross-chain technologies
10	Software Developer	1	<ul style="list-style-type: none"> • Permissioned blockchains
11	Blockchain Researcher	1	<ul style="list-style-type: none"> • Non-Fungible Tokens
12	Blockchain Researcher	3	<ul style="list-style-type: none"> • Permissioned • Permissionless blockchains
13	Software Engineer	4	<ul style="list-style-type: none"> • Permissionless blockchains • Smart contracts

7.3 INTERVIEW RESULTS

This section presents the findings from the analysis of the data obtained from the interviews with blockchain experts. The participants responded to questions aligned to the sub-research questions stated above. The data were analysed following a thematic analysis approach (see Chapter 3, Section 3.10.2), through which seven main themes were identified. The first theme is the Branch of blockchain interoperability which comprises two sub-themes; blockchain-to-legacy interoperability and blockchain-to-blockchain interoperability. The second theme, is the Business perspective, the third is the Legal and regulatory compliance theme comprising three sub-themes, Vague regulatory frameworks, Regulatory compliance through existing laws, and Types of regulations for blockchain interoperability. The fourth is the Interoperability techniques theme, followed by the Interoperability mechanisms theme. The sixth and seventh themes are the Data and Interoperability through standardisation.

7.3.1 Theme 1: Branch of blockchain Interoperability

The thematic analysis of the interview transcripts revealed that the concept of blockchain interoperability can be viewed from different angles or branches. From the analysis, two main branches of blockchain interoperability were identified. According to Respondent 6, *“There’s (sic) two main aspects of, that we could be talking about. The first is blockchain interoperability with existing infrastructure. Ok so if you have existing systems how does*

blockchain interoperate with it [...] the 2nd branch is how do multiple blockchains talk to each other”.

The forms identified from the extract above were respectively identified as blockchain-to-legacy interoperability and blockchain-to-blockchain interoperability. The identified forms are presented as sub-themes below.

Sub-theme: blockchain-to-legacy interoperability

This sub-theme relates to the form of interoperability involving blockchain systems and other traditional/legacy systems that are not blockchain-type systems. According to the data, this form of interoperability is required in cases where blockchain is adopted into organisations with preexisting systems. For instance, Respondent 5 stated that *“It’s a very complex space [...] trying to figure out ways to make it interoperable with our current ways because you cannot drop what you are doing today because of this blockchain and replace it entirely”*. In support, Respondent 8 stated that *“It also has some interoperability challenges because you have to be able to integrate your blockchain with your enterprise systems that corporates normally have, so, for example, they may have SAP or they may have some other kind of enterprise system”*.

The data also indicated that blockchain-to-legacy interoperability may present in various ways within the banking sector, depending on the type of legacy system. For example, blockchain-to-legacy can mean interoperability between traditional fiat currency and new blockchain-driven currencies (digital currencies), as stated by Respondent 3, who alluded that *“when it comes to issues of interoperability between fiat and digital currency that’s a big difficult one to solve”*.

On the other hand, it may refer to interoperability between blockchain and legacy infrastructure and applications. This is evidenced in the response provided by Respondent 8: *“...and they are used in various of mechanisms to be able to integrate into the existing reserve bank applications”*. Legacy infrastructure refers to the legacy financial systems used to facilitate accounting and bookkeeping in financial payment transactions. Respondent 3 alludes to this and purports that *“in terms of normal accounting and bookkeeping, there is also no interoperability. We don’t even know how to account for digital assets”*. Mentioning “normal accounting and bookkeeping” suggests the traditional way of accounting used in

financial systems, and the quote suggests there is no interoperability between the new blockchain technology and the financial systems used for normal accounting and bookkeeping functions. This is supported by the following extract:

“Okay, with a problem like interoperability, I think I think it is this. So for finance, so if you take finance for financial systems, financial systems is extremely old [...] It was used as it is as it was designed for the current time. The bookkeeping at the back between banks is also not standardised between financial systems [...] wasn’t designed to work with the internet [...] so I think that’s, that’s probably the the major thing that financial services institutions are struggling to get grip on except for the fact that cryptocurrency was made for the internet and blockchains systems were made for the internet” (Respondent 3).

The above thematic analysis findings regarding blockchain-to-legacy interoperability correspond to the findings of existing literature on blockchain interoperability. Some studies focusing on the use of blockchain technology in organisational settings have identified the need to address the lack of interoperability between new blockchain systems and incumbent systems that are already in use in those organisations (Belchior, Vasconcelos, et al., 2022; Bhatia, 2020). According to Bhatia (2020), different blockchain ledgers need to interact with each other and with legacy systems to enable blockchain technology to meet the needs of today’s world. Similarly, Belchior, Vasconcelos, et al. (2022) highlighted that the lack of seamless communication between private blockchains and legacy systems is a critical area that must be addressed to improve the adoption of blockchain technology in enterprises.

Sub-theme: blockchain-to-blockchain interoperability

As stated in the discussion above, the second branch of interoperability is blockchain-to-blockchain interoperability. Blockchain-to-blockchain interoperability speaks to the concept of enabling interoperability between different types of blockchains. The concern with this branch of interoperability *“is how do multiple blockchains talk to each other”* (Respondent 6). This notion of blockchain-to-blockchain interoperability is also identified by Respondent 8 who stated that *“interoperability between blockchains, that’s also an issue as well because there is no general standards”*. Similarly, Respondent 2 alluded to this type of interoperability when stating that it is *“kind of a steep learning curve in terms of trying to integrate other blockchains that is why for now we are limiting our scope for now to bitcoin blockchains”*.

In addition, the interview data indicates that the branch of blockchain-to-blockchain interoperability may represent interoperability between different blockchain platforms (cross-platform interoperability), such as between an *Ethereum* blockchain and a *Bitcoin* blockchain. Respondent 8 stated that *“But then when we talk about interoperability between blockchains there’s also a challenge [...] also blockchain and you can’t easily move from one to the other so in order to do simple things like you know example to use your Ethereum to buy Bitcoin for example you would have to go to the exchange, exchange your Bitcoin to perhaps you know like \$2”*. This is corroborated by Respondent 4, who stated that *“so if you have a tokenised say for instance a Rand or say Bitcoin or an Ethereum blockchain, now you can trustlessly and decentrally trade your tokenised Rand with whatever asset that is on the Ethereum blockchain”*.

In addition, the analysis revealed that the branch of blockchain-to-blockchain interoperability may give rise to more nuanced forms of interoperability, depending on the nature of the difference between the blockchains. Another type of interoperability is alluded to in the extracts stated above. The quotes above refer to *Bitcoin* and *Ethereum* as blockchain platforms and also the tokens (data) used on those platforms. The quote from Respondent 3 *“that allows for decentralised switching and trustless switching between us the switching between fiat currency of any digital assets, cryptocurrency or any digitise real-world assets, it doesn’t have to be cryptocurrency, it could be for instance a share certificate or digit token of a real-life asset.”*, indicates that enabling interoperability between different blockchain platforms can enable interoperability between different forms of data (tokens) on those blockchain platforms, implying that interoperability may be required at the level of the data (data interoperability). Data interoperability refers to the form of interoperability which enables data with different formats and from different sources to be unified, used and exchanged seamlessly across systems. The concept of data interoperability is supported by existing literature on blockchain interoperability. In particular, this form of interoperability is often classified as semantic interoperability in the literature. In the context of blockchain-to-blockchain interoperability, data interoperability represents a semantic dependence between heterogeneous blockchains for data exchange while at the same time ensuring the validity and variability of the shared data (Abebe et al., 2019a). In support, Hardjono et al. (2020, p. 11) explain that facilitating interoperability between permissioned and permissionless blockchains can be achieved through semantic interoperability at the values

level to provide semantically compatible meanings of the shared data (coins or tokens) stored on the blockchains.

Another form of blockchain-to-blockchain interoperability can relate to interoperability between smart contracts. This form of interoperability is identified from the following quote “...*how we can get a smart contract on one blockchain to work on another and that is itself is again also a completely none trivial task. Fundamentally, the reason for this is because, different blockchains they have their own virtual machine ok so they run their own software and if the software can execute smart contracts then it understands a very specific language... and so if you have different blockchains that all speak different languages, getting smart contract from one to be used on another it's not easy.*” (Respondent 6). The extract above implies that enabling interoperability at the platform level (between blockchains) may support interoperability at the smart contract level. This may be the case where the blockchain platforms being used provide smart contract capabilities, and an organisation wants to leverage those capabilities in the business processes or logic. Khan et al. (2021) concur that for true interoperability, smart contracts created on different blockchain platforms using different programming languages should be interoperable. The authors refer to this form of interoperability as code-level interoperability, in which smart contracts on heterogeneous blockchains can interact by referring to each other's contract code. Similarly, Schulte et al. (2019a) concur that achieving blockchain interoperability can enable interoperability between smart contracts or cross-blockchain smart contract interactions, in which smart contracts running on different blockchains can interact and be transferred across blockchains.

This interpretation of blockchain-to-blockchain interoperability as a means for facilitating digital asset transfers and exchange is consistent with the findings of the systematic literature review discussed in Chapter 5 and the extant literature, as evidenced by (Borkowski et al., 2019), who discuss interoperability between blockchains as a form of interoperability for enabling the exchange of digital tokens between different blockchains. In support, Schulte et al. (2019a) present blockchain-to-blockchain (or what they term cross-chain interoperability) from two angles: cross-blockchain token transfer and cross-blockchain smart contract interactions. Their view of cross-blockchain token transfer refers

to a method enabling the transfer of digital tokens, such as cryptocurrencies, from one blockchain to another. Their second view aligns with the findings above, which indicate that blockchain-to-blockchain interoperability can be considered from the perspective of cross-blockchain smart contract interactions, which involve invoking smart contracts on different blockchains.

Theme summary

The following discussion provides a summary of Theme 1. Theme 1 detailed the findings regarding the types or branches of blockchain interoperability that may be present in a banking institution. Two overarching branches of interoperability were identified from the analysis, namely blockchain-to-legacy interoperability and blockchain-to-blockchain interoperability, respectively. As explained above, the blockchain-to-legacy branch of interoperability refers to a form of interoperability involving a blockchain system and a traditional system that is not blockchain-enabled. Conversely, the blockchain-to-blockchain branch concerns interoperability between different blockchain systems or between blockchain derivatives that may be used within the organisation.

Key theme insights

One of the key insights identified from the theme is that banking institutions adopting blockchain must consider effective ways to address blockchain-to-legacy interoperability. This is necessary because banks rely on legacy core banking systems, and it is impractical to overhaul and replace the core system with blockchain technology; therefore, careful considerations are necessary regarding how blockchain technology can be incorporated into existing legacy core banking systems. The second insight is that banking organisations may opt to adopt multiple blockchain systems that might also have to interact. This is because different blockchain systems are designed for specific use cases and thus offer different capabilities. Therefore, a banking institution might need to adopt different blockchains to satisfy various business requirements.

7.3.2 Theme 2: Business Perspective (Case)

The second theme identified from the thematic analysis of the interview transcriptions relates to the business aspects of blockchain interoperability. The theme pertains to business aspects relating to enabling the interoperability of blockchain technology in organisations.

One of the aspects identified from the analysis concerns the concept of a business case as a factor that drives blockchain adoption and, consequently, how the adopted blockchain can then be integrated and interoperated within enterprise settings. This theme explains that an organisation's choice to adopt blockchain mainly depends on the availability of a compelling business case for blockchain technology that stipulates the purpose of adopting blockchain and the overall value proposition for adopting blockchain. The purpose relates to the business reasons for adopting the technology and answers the question of why blockchain is required. Answering this question, in turn, influences the technological choices regarding the nature of the blockchain, the platform, and the type of information to be shared, thus also influencing the considerations for interoperating the technology into the existing business systems and processes. This view is evident in the following response: *“So you need to think carefully about your business case to say, what are the elements of this business case that I'm trying to realise. If I was to put it onto the blockchain platform which of these laws would I potentially tamper with?”* (Respondent 5). Another respondent puts forward a similar argument by explaining that the decision on what approach to take when integrating blockchain into an organisation depends on whether or not it makes business sense and also depends on the purpose or goal the organisation wishes to achieve by adopting blockchain. This argument is supported by the following quote from Respondent 4: *“The integration it comes, you need to check if it makes sense to integrate with blockchain and also what goals you want to achieve on the blockchains.”*

In addition, the analysis indicates that the business case influences the scope of interoperability and also the form/branch of interoperability required. In this case, the scope refers to whether the technology would be used to replace existing systems or to enhance existing systems. The scope then determines the types of other systems that need to communicate with the blockchain, which essentially also influences the domain/branch of interoperability.

This argument emerges from the following responses: *“So, if the technology itself is not a major overhaul, it may be let’s say no no, by for instance, if it’s actually, it doesn’t change the whole underlying system entirely, but it actually improves the existing system portion of the system and it will bring like a significant revenue they will actually go into implementation”* (Respondent 2). Similarly, Respondent 6 stated that *“if you’re adding blockchain into your existing systems, make sure that you know blockchain is serving very specific purpose [...] the reason for that is you know a lot of these blockchains handle things differently. They’re all incredibly unique [...] and that changes how you need to interact with it right”*. Both of these quotes demonstrate a link between the purpose (business case) and the scope and form of blockchain interoperability.

Such a discussion concerning the business case as one of the factors influencing the choice of blockchain technology and, consequently, the integration and interoperability process within organisations is rare in the interoperability literature in general, even in studies focused on the organisational aspect of interoperability. However, some existing literature has vaguely alluded to this relationship. For instance, Dimitrov and Gigov (2020) relate the choice of blockchain interoperability solution to the specific industry in which the organisation operates, although they do not provide a detailed discussion.

Theme summary

Theme 2 addressed the different business aspects relating to enabling blockchain interoperability. Specifically, the theme highlights the relationship between the business case and blockchain interoperability. The theme shows that the purpose of adopting a specific blockchain in an enterprise influences the form of interoperability required as well as the techniques and considerations that can be applied to enable the blockchain interoperability.

Key theme insights

The following insights were obtained from Theme 2. The business case or use case for blockchain in an organisation is a critical driver of how blockchain interoperability is handled in the organisation because the business case influences why the blockchain is required in the first place. Thus, the purpose of the blockchain determines the choices regarding the

scope of interoperability, meaning that it determines the form of interoperability required, the systems involved, the type of data to be shared and, consequently, the technical methods used to enable the required interoperability.

7.3.3 Theme 3: Legal and Regulatory Compliance

Legal and regulatory compliance is another common theme that emerged from the interview analysis. Several respondents highlighted regulatory compliance as an important aspect of enabling blockchain interoperability in the banking sector. The succeeding discussion highlights some of the salient views of the respondents concerning the role of regulation and regulatory compliance in enabling blockchain interoperability. These views are represented as sub-themes below.

Sub-Theme 1: Vague regulatory landscape

The observations obtained through the analysis of the interview transcripts reveal that compliance with regulations is an important consideration for enabling blockchain interoperability in the banking and financial sectors. However, it was noted that even though compliance with regulation was a critical consideration, the regulatory aspects of blockchain adoption and interoperability in the sector remain uncertain due to vague regulations. One respondent highlighted this aspect regarding the regulation of blockchain technology in banking “...but generally, globally, even in SA there is still regulatory uncertainty around this thing as a technology [...] the way regulation works is that you don’t want to disrupt the innovation process. Yeah, you need to wait for some time to see... at what point you need to establish at what point you need to step in without stifling the innovation process” (Respondent 5). This was supported by another respondent who reported that banks “all had to basically stand back because of the vague regulation. So the regulator is laying some of the foundations to enable them to participate more actively” (Respondent 4). Respondent 1 corroborates this as follows: “Regulation moves slower than technology. Innovation is always faster than regulation is lagging behind. So in this case, we have a similar situation where regulation is lagging behind”.

Similarly, regarding the use of smart contracts in enabling interoperability, another Respondent stated that *“100 % they could the problem isn’t whether or not they can. The problem is regulating that and actually having some sort of regulation that stipulates yes”* (Respondent 6).

The findings above regarding vague regulations being a hindrance to enabling blockchain adoption and interoperability agree with the findings reported in the existing literature on blockchain technology, namely a general lack of appropriate regulations for blockchain across various industries (Abu-elezz et al., 2020). For example, Duque and Torres (2020) argue that the operability of blockchain or distributed ledger in areas such as e-commerce raises important regulatory challenges, which have to be addressed through new policies. Similarly, Wilkie and Smith (2021, p. 168) highlight regulatory uncertainty as a hurdle for wider implementation of the technology in organisations. However, they further argue that the ambiguous regulatory framework from tax, accounting, financial and operational perspectives might also provide *“an opportunity for organisations to take advantage of the regulatory sandbox to test and develop new methods of integrating blockchain with existing technologies”*.

Sub-Theme 2: Regulatory compliance through existing laws

However, the analysis also revealed that despite the absence of clear regulations governing blockchain technology in the sector, banking and financial institutions should still find ways to comply with existing laws and regulations to protect consumers. The interview data indicate that in the absence of blockchain-focused regulations and laws, organisations should consider existing regulations. This argument is presented in the following extract:

“If we speak of the POPI Act today. It’s not a blockchain rule or law. But you know if you’re dealing with personal information you’re obliged by law. It’s not gonna say there are exceptions because now you’re on the blockchain [...] But it’s not a blockchain law, it is a law that exists for you as an entity in operation, so the lines [...] because the lines become blurred you need to be at all times be sure where when you’re about to cross them, and when not to cross them” (Respondent 5).

The statement above was supported by Respondent 1, who stated that *“For that innovation to be realised, there has to be some kind of regulations. I want to say like I think regulatory*

sandbox whereby some other traditional regulations no longer apply to this new way of building or I mean of exchanging data, of exchanging information that is powered by blockchain. So you almost need that kind of Okay great. This is we know how the regulations looks like however, for this new piece of technology we understand that it basically, it doesn't fully comply with the traditional regulation, so we need to give It a sandbox like Okay the blockchain technology we are willing to be a little bit lenient to see where it's going".

Another respondent put a similar statement forward regarding the importance of complying with existing laws to protect consumers when considering interoperability: *"Say, for example, your company handle user data and we know that user data is an incredibly touchy subject and it's a lot of laws and regulation like [the] POPI Act so if our current infrastructure, this is an example right, handles user data and has to secure this sort information that is the one thing you should be thinking about [...] You 100 % should make sure that you are not putting the user at risk"* (Respondent 6).

The suggestions above for organisations to select and use existing laws are consistent with the idea of using a regulatory sandbox reported in the literature. A sandbox is an allowance given by regulators to organisations to enable them to implement new technologies by removing the requirements to comply with the full scope of the existing regulations (Wilkie & Smith, 2021). The purpose of a regulatory sandbox is to ensure that regulation, or the lack thereof, does not stifle innovations in organisations.

In addition, other respondents supported the notion of legal and regulatory compliance as an important consideration for interoperability for digital asset exchange. However, they did not relate this to the banking sector in particular but instead highlighted the importance of regulation in the context of cryptocurrency exchanges. Cryptocurrency exchanges are centralised companies that offer services to customers who wish to trade cryptocurrencies. Cryptocurrency exchanges enable interoperability by facilitating crypto-asset/cryptocurrency exchanges, typically referred to as atomic swaps. In this context, the findings indicate that cryptocurrency exchanges should comply with existing regulations that regulate other financial institutions, such as banks. For instance, regarding regulation, Respondent 3 stated that *"now the next step would be to enforce cryptocurrency in companies like your exchanges to register as accountable institutions which means that they, they would have the same regulation, exactly the same regulations as other banks"*. Other respondents

expressed similar views and specified that “*centralised finance platforms obviously are more in line with regulations, so they they try to be like your normal banking sector where you know you, you have to do your normal regulatory KYC anti money laundering*” (Respondent 8). In addition, Respondent 7 stated that “*the law needs to be enforced on centralised exchanges. They should abide country laws to protect citizens*”.

The findings regarding the need for regulation of crypto exchanges are not the focus of this study; however, they provide a good demonstration of the importance of regulation in crypto asset transfers. Enabling crypto asset transfers between blockchains is one of the significant applications of blockchain interoperability. Therefore, the discussion above can be extended to understanding the role of regulations in the exchange of digital assets in organisational settings. In this respect, the findings support the current literature on blockchain interoperability. The findings specifically align with (Belchior, Vasconcelos, et al., 2022), who affirm that establishing seamless interoperability for asset exchange purposes between organisations requires compliance with various regulations and interoperability solutions that comply with legal frameworks and regulations. In addition, the findings above correspond to the proposal by Mohanty et al. (2022), who proposed that future cross-chain interoperability applications supporting transactions in the banking and financial sector should comply with legal frameworks, particularly at the level of cryptocurrencies and for interoperability mechanisms.

Sub-theme 3: Types of regulations for blockchain interoperability

The analysis of the interview data highlighted another interesting aspect of regulatory compliance raised by the respondents; this aspect relates to the types of regulations they mentioned. The analysis revealed the respondents consider compliance with data privacy laws and anti-money laundering regulations critical when enabling blockchain interoperability in the banking sector. The following discussion presents the types of regulation mentioned.

Data Privacy laws:

Some respondents mentioned compliance with data privacy laws as a critical regulatory consideration banks must consider concerning blockchain interoperability. Specifically, they referred to the Protection of Personal Information (POPI) Act of 2013 as an example of a

data privacy law banks must consider when sharing information on the blockchain. The POPI Act is a South African data privacy law which stipulates conditions for access to personal information by private and public institutions. The purpose of the Act is to protect the processing of personal information by balancing the right to protection with the right to access information, as illustrated by the following quotes. For example, Respondent 5 mentioned the need for organisations to consider privacy issues and relevant privacy laws when connecting to the blockchain. This argument is exemplified by the following quote: *“Privacy issue[s], you need to think about what the laws says if people be playing with people’s personal information as an example as part of a business case”*. This is supported by a respondent who asserted that *“we know user data is an incredibly touchy subject and it’s a lot of laws and regulation as the POPI Act”*. Another respondent also mentioned the POPI Act as an example of law that must be complied with regarding user data: *“If we speak of the POPI act today it’s not a blockchain rule... but you know if you dealing with personal information, you’re obliged by law”* (Respondent 5). The same idea was presented by Respondent 1 who stated that when interoperating blockchain with other systems, *“there’s a regulatory requirement, so you need to ensure that POPIA and all these Acts are catered for. GDPR, of cause GDPR you have the right to say an organisation forget me, delete everything”*. The points above raised by the respondents regarding the need for compliance with privacy laws relate to another critical technical consideration (Section 6.2.6).

The issue of compliance with privacy laws is not unique to the respondents. Similar arguments regarding the need to comply with privacy laws when considering blockchain interoperability have been reported in the literature. In the study on cross-chain blockchain networks in Europe, Senthilkumar (2020) points out that the development of cross-chain blockchain platforms for domestic and global contexts is limited by sectoral, national and regional regulatory barriers. In particular, the author highlights that privacy laws like the European General Data Protection Regulation (GDPR) (CMR 2019) have the potential to discourage organisations from adopting blockchain technology due to the transparency feature on blockchains, which makes it difficult for organisations to hide sensitive information (Senthilkumar, 2020).

In addition to the privacy laws above, the respondents also identified laws relating to the prevention of financial crimes. In particular, the know-your-customer (KYC) and anti-money laundering (AML) laws emerged as some of the laws that should be considered when

addressing interoperability involving blockchain technology. For example, Respondent 2 stated that “*virtual asset providers need to do the KYC, know your customer you know so that they can be able to identify the customers and stuff*”.

These findings correspond to the findings presented in the systematic literature review (see Section 5.2.8) in which Pang (2020) reports that blockchains and participants on the blockchain should be identifiable for compliance with KYC and AML regulations. Similarly, the findings correspond to other literature on blockchain technology in banking, which indicates that KYC and AML compliance is critical for blockchain-centric solutions involving the exchange of crypto assets or digital assets (Moreno & Seigneur, 2022), such as in the exchange of CBDCs (Pocher & Veneris, 2021) and cross border payments (Zetsche et al., 2022).

Theme Summary

Theme 3 explored the respondents’ views regarding legal and regulatory elements and their role in blockchain interoperability in organisations. The theme comprised three sub-themes. The first sub-theme explored the lack of appropriate statutes and regulations focusing on blockchain. The second sub-theme discussed the respondents’ views relating to the use of existing laws and regulatory frameworks to ensure that banking institutions using blockchain technology do not violate current domestic and international laws that govern the sector. The last sub-theme presented key regulations the respondents identified as critical to blockchain interoperability. Mainly, the sub-theme showed that the respondents considered compliance with privacy laws and anti-money laundering regulations key to blockchain interoperability.

Theme insights

Insights obtained from the above are as follows. The first insight is that the banking sector is highly regulated, and the scope of regulation is not limited to the overall functions and operations of banking institutions but also includes the regulation of technological innovations adopted and used by banking institutions. Accordingly, the process of introducing new technologies has to be guided by relevant regulatory and legal frameworks. The second insight is the lack of appropriate regulations to guide the use of blockchain in the sector because blockchain technology is decentralised, and issues relating to the

governance and management of the technology are handled by the technology itself, contradicting traditional centralised ways of governance and management. However, despite this lack, the adoption and use of the technology in the sector are still required to align with sectoral regulations. Therefore, organisations must carefully consider how to identify potentially relevant regulations or parts of regulations applicable and relevant to a specific use case of the technology within the organisation. Regarding interoperating the technology, a process that requires the exchange of data, the study gained the insight that existing privacy laws (local or global) should be complied with to protect customers' right to privacy. Thus, organisations should devise appropriate ways to protect the privacy and security of the customer information shared across the blockchain.

7.3.4 Theme 4: Interoperability Techniques

This theme relates to the types of interoperability techniques identified during the analysis of the transcripts. In this context, interoperability techniques are identified as the methods used to enable different forms of blockchain interoperability. The techniques are discussed in relation to the two branches or forms of blockchain interoperability discussed in Theme 1 (blockchain-to-legacy and blockchain-to-blockchain).

The respondents identified APIs as a technique that can be used or is being used to connect blockchain to non-blockchain systems and connect different blockchain systems. According to Respondent 2, *“to integrate with other blockchains, so you actually need to build like a different API that integrate with different blockchains”*. Other respondents stated that *“everyone has their own approach to that, they can use APIs or oracles for integration”* (Respondent 5). Similarly, Respondent 1 notes that APIs can indeed be used to facilitate blockchain interoperability; however, the respondents clarify that these APIs should be standardised to avoid introducing additional interoperability challenges resulting from the differences in the actual interfaces themselves. For example, Respondent 1 stated that *“the core technical challenge is about what we call the application programming interfaces which is APIs. We have different APIs and these are designed by different people [...] so the fact that two different entities design or define interfaces, and the fact that we are different standards and we don't follow like a unified mechanism that can be used and accepted as the standard of building APIs is a challenge”*. The use of APIs as a mechanism for enabling interoperability between blockchain systems and non-blockchain systems corresponds with

the existing literature. For example, (L. Zhang et al., 2021) demonstrate the use of APIs in enabling interoperability between multiple blockchain systems in the tourism sector. The authors used rest API to connect multiple blockchains to external systems. Similarly, (Hegnauer, 2019) developed an interoperability API that enables user applications to interact with different private and public blockchains. In support, (Belchior et al., 2021b; Jin et al., 2018) suggest that APIs, particularly cross-chain APIs, can support the exchange of data between different blockchain systems.

In addition, oracles were mentioned as another form of interoperability technique that can enable blockchain-to-legacy interoperability. Oracles are systems that provide means to collect data and transfer it from external sources to the decentralised blockchain systems. The respondents mentioned that *“we have things they call oracles, not to be confuse[d] with oracle databases. It is just a tool or way to integrate the distributed peer-to-peer network is blockchain and our traditional networks”* (Respondent 5). Similarly, Respondent 6 said that *“the whole reason why we have oracles that bring in off chain data into the network is because smart contracts and blockchain network can’t actually really access lots of information by itself”*. Oracles are also reported in the literature as a way to enable cross-chain communication between blockchain and enterprise systems. According to Lu et al. (2023), blockchain oracles can be utilised not only to connect permissioned blockchains but also to connect consortium blockchains between enterprises. Likewise, Gao et al. (2020) illustrate how oracles can be applied to facilitate the migration of data between two heterogeneous blockchain systems. Other studies on blockchain interoperability solutions also identify oracles (Belchior et al., 2021b; Buterin, 2016). Even though oracles have been noted as possible interoperability solutions, the respondents highlighted that current oracles are often third-party products and may, therefore, not fully meet the data exchange and security requirements for enterprise settings. According to Respondent 4, *“oracles operate in a similar fashion where what essentially you have is off chain network that has its own you know agreement or consensus protocol and they aggregate data... And again you are relying on this third party to provide this solution and that third party you know if something happens with the oracle your assets can be lost”*. This argument was presented by Al-Breiki et al. (2020, p. 1), who argue that even though oracles allow data to flow from external systems to the blockchain, “there is always a risk of oracles providing corrupt, malicious or inaccurate data”.

Furthermore, the analysis of the transcripts revealed bridges as an alternative technique that can be used to connect heterogeneous blockchain systems. One Respondent stated that *“blockchain interoperability requires some mechanisms where you introduce bridges”* (Respondent 1). Similar to the security issues stated above regarding oracles, the Respondents highlighted that using bridges may compromise the security of the blockchain system. *“the problem with bridges is that they are great unless they are not built properly, which then they become an attack vector right! If a bridge is not built properly it becomes an attack vector”*. In support, Respondent 6 states that *“There’s different techniques of interoperability and they use a bridge and from the research I’ve done and anecdotally what we’ve seen bridges are slower things... they are extreme. Wormhole got hacked for how many millions or something”*. The sentiments above regarding the use of bridges and their limitations align with those reported in the literature (Bhatia, 2020; Mohanty et al., 2022; Wang et al., 2023). In their classification of blockchain interoperability solutions, Wang et al. (2023) classify bridge-based solutions as interoperability solutions that connect heterogeneous blockchain systems through a bridge placed between the communicating blockchains to protect the integrity and consistency of the systems. Similarly, (Khan et al., 2021) and (Mohanty et al., 2022) explain how various industry blockchain interoperability solutions use bridge-based solutions such as smart contracts to connect different blockchain systems.

Theme Summary

Theme 4 discussed various techniques that can be employed to enable interoperability between blockchain and legacy systems and between different blockchain systems. Within the theme, oracles, APIs and bridges were identified as technologies that can enable blockchain systems to exchange information with legacy technologies. Regarding interoperability between different blockchain systems, the respondents identified bridges and interoperability protocols as techniques that can facilitate data exchange. However, the respondents mentioned that the techniques above have security and performance limitations of which organisations need to be aware. Furthermore, the theme included a discussion on third-party solutions as alternative solutions to facilitate blockchain interoperability in organisations. However, due to the security risk associated with third-party solutions, the respondents recommended using custom interoperability mechanisms and techniques.

Theme Insights

The results above indicate that enabling blockchain interoperability requires some form of a connection mechanism to act as an interface between the communicating systems. Therefore, selecting the correct mechanism requires organisations to understand the available solutions regarding the benefits they offer and the associated limitations. In addition, interoperability mechanisms or techniques must provide sufficient security and privacy capabilities to protect the data exchange. Hence, security and privacy requirements and compliance with privacy laws are paramount to selecting or designing an effective interoperability mechanism.

7.3.5 Theme 5: Interoperability Mechanism Properties

The current theme describes the required features and functions of an interoperability mechanism, as described by the respondents. As discussed in Section 6.2.6 above, blockchain interoperability relies on interoperability mechanisms such as APIs and oracles. The theme discussed in this section describes the features/requirements these mechanisms must fulfil to provide efficient and effective interoperability between communicating systems.

The discussion above on privacy laws underlined privacy as a paramount requirement for developing effective blockchain interoperability solutions. The majority of the respondents explained that due to the inherent transparency and immutability properties associated with blockchain technology, banking institutions and organisations adopting the technology should carefully consider the type of information to store and share and how and when such information is shared. They further explained that the organisational decision to share information on the blockchain should be considered in relation to the relevant data protection laws to ensure that the privacy of business and customer data is protected. Regarding the aforementioned, Respondent 8 stated that *“the enterprise and the corporate sector also need privacy you know if they want to participate in blockchain technology that’s there’s also another challenge because you can’t have the same operation because with a public blockchain you can see every transaction [...] but corporates don’t necessarily want to do that, that’s where you get your private blockchain”*. Similarly, Respondent 6 explains that *“blockchains fundamentally, or at least blockchains that we know that are mainstream permissionless public blockchains. Those blockchains have transparency and auditability, traceability all of this in mind. From a business perspective you just 100 % should make sure*

that you are not putting the user at risk that you are putting user identifiable information on blockchain. In agreement, Respondent 1 explained that “the property of blockchain technology is 1) is decentralised, so its not trusted, 2) which is like the biggest challenge is the fact its immutable [...] the record is there forever. It presents certain technical decisions that you need to make which are a challenge. It means the way you store information it must be such that information is not personally identifiable”.

Another Respondent explained the need for banking organisations not only to consider data privacy issues internally but also to consider privacy issues relating to sharing data across jurisdictions. This is explained in the following extract by Respondent 5 who alludes that *“there is also the issue of data residency it’s a huge thing in banks today that certain pieces of information are required within the national borders and cannot or may not exists outside and blockchain is borderless by design... so you need to think carefully about your business case [...] if I was to put it onto the blockchain platform which of these laws would I potentially tamper with?”.*

In addition, the respondents indicated that security control must be considered a requirement to protect the integrity and privacy of the data exchange process. According to Respondent 8, enterprises need to consider solutions that enable a seamless and secure flow of information between existing enterprise systems and blockchain systems. Respondent 8 recommends that organisations should determine *“how do you go from your corporate system into a blockchain transaction safely and seamlessly?”*. Other respondents made recommendations regarding possible security controls organisations can consider in securing data exchange. For instance, Respondent 3 suggests that *“for interoperability you can also look at zero knowledge proof which is a game changer not only for blockchain but for general financial services because banks may not want to share the transaction information with their competitors, so zero knowledge proofs is really a technical method that can be used to share information with competitor without that competitor reading that information”*. Likewise, Respondent 6 explains that organisations should think about *“how do we secure the state now?”* and suggests that *“the idea is that we can use state proofs that are post quantum secure to verifiably say no this was indeed the state of the blockchain at the certain period”*. Similarly, another respondent explains as follows: *“So, when they try to do a blockchain based solution. So there is private networks, and those private networks you don’t want the external parties to be able to access the private networks. You don’t want*

the external party to be able to access the private network. So, that's why you could you know you would put all the various other security layers like you know traditional cryptography on" (Respondent 4).

Theme summary

The findings above align with the literature, which states that the lack of adequate privacy preservation during blockchain interoperability could compromise the security of the shared data and allow attackers to steal sensitive user information, track users' transactions, and make inferences regarding private and sensitive user information (Yin et al., 2023). Furthermore, they align with the argument that organisations must provide the correct security and privacy policies to mitigate attacks when connecting heterogeneous blockchain systems (Haugum et al., 2022b).

Theme insights

The main insight from the theme is that privacy and security features are key considerations for selecting an interoperability mechanism. The theme revealed that banking organisations should ensure that the mechanism used to facilitate the data exchange across systems does not compromise the integrity of the shared data.

7.3.6 Theme 6: Data

The fundamental purpose of interoperability is to facilitate seamless data exchange between systems regardless of their differences. Therefore, it is essential to understand the type of data shared during the interoperability process. The theme, Data, explores the different aspects relating to data, as mentioned by the respondents.

The respondents highlighted several factors that must be considered regarding data. Some respondents highlighted the need to consider the types of information that can or cannot be shared on the blockchain. They explain that organisations should determine what information to share, when and how it is shared on the blockchain, and this decision should be guided by the relevant regulations. For example, Respondent 1 said, "*at point-to-point where these things connect... you know data structure is also a challenge that prohibits that you need to think about your entities. What are some [of] your data artefacts that you are looking for and how they're structured*". The preceding quote highlights another important

aspect of formatting the data that had been exchanged. The quote indicates that organisations must also consider how data can be formatted to enable seamless interoperability. Similarly, Respondent 5 stated that organisations must determine if the data they want to share can indeed be shared on the blockchain. *“You need to think about what are the laws saying when playing with people’s personal information... is it something that I can share on a blockchain?”*.

The respondents also indicated how sensitive data is handled must be considered. According to Respondent 6, sensitive business and user data should not be shared across blockchain systems or between traditional business systems and a blockchain. The respondent stated that organisations should *“make sure the blockchain is serving a particular purpose but that purpose should not be to store or share sensitive data or user data. One thing you should not be doing [is] it should not be used to share and store secrets like password keys user information or identifiable information”*. In support, Respondent 1 noted that *“it present (sic) certain technical decisions that you need to make ... for instance, the fact that its immutable, it means that the way your store information it must be such that, that information is not personally identifiable”*.

Furthermore, regarding the type of contextual data that can be shared, there is consensus among some respondents that blockchain interoperability should enable the exchange of digital assets; however, the respondents did not provide specific examples of such data. Respondent 3 indicated that *“the friction we have is exchanging data, for instance, your digital assets where we cannot create software protocols that allows (sic) for decentralised switching and trustless switching between fiat currency or any digitised assets, cryptoassets or any digitised real world assets”*. Likewise, Respondent 1 stated *“when we talk about interoperability if you think about two networks what you care about is who is moving in this path. It’s the assets, the tokens. If I want to Bitcoin to move from traditional Bitcoin into Ethereum how do I achieve that?”*. The respondents also suggested business data might be shared between different systems. The following quote suggests that organisations can share some of their transaction data. For instance, Respondent 4 stated that *“so you get a network of corporates that want to do some business... they want to use blockchain, they don’t want keep their transactions isolated from each other”*.

The findings above regarding the data consideration for organisations correlate with existing literary findings, which state that sharing data between blockchain applications requires data to be shared selectively among communicating parties while at the same time adhering to the security and validation requirements of the blockchain (Bhaskaran et al., 2018). The authors state that this particularly pertains to the banking sector, whereby banks may need to share confidential KYC data on the blockchain. This precaution is necessary because blockchains have some deficiencies in handling the privacy and security of financial data, and therefore, banks must consider ways to manage the data shared on the blockchain hierarchically to comply with existing laws, regulations and guidelines on banks' operations and customer management (Wang et al., 2020).

Concerning the findings on the types of contextual data that can be shared, the existing literature agrees that using blockchains in enterprise settings, such as banks, leads to the emergence of new forms of data like digital assets, which may have to be shared across different systems within the enterprise (Abebe et al., 2019b). According to Themistocleous et al. (2023), emerging technological innovations like blockchain technology have introduced new representations of money and assets, such as crypto assets and CBDBs, which may need to be stored and shared across different systems.

In addition, the respondents affirmed the need to develop data formatting standards to simplify and facilitate blockchain interoperability. Respondent 3 referred to this in the following statement: *“So, once you have a stable coin or once you have a tokenised version of the CBDC on the blockchain then it becomes instantly interoperable with other assets on the blockchain. We see that with Ethereum for instance, like in standard ERC-20 and ERC 721. If you design a tokenised asset with ERC-20 standard, it's immediately interoperable with any other assets on the Ethereum blockchain”*. In the same way, Respondent 1, mentioned the need for standardisation when he stated that organisations should think about *“what are some of the standards that you put in place now? The challenge now is that two different networks don't follow similar standards. The fact that two different entities design or define interfaces, the standard is at principal level”*. These findings correspond to the general literature on interoperability, which advocates for the development of standard data formats to facilitate semantic interoperability between heterogeneous information systems. For example, the findings align with the argument that industry stakeholders should develop and implement technical standards to facilitate seamless data exchange (Burns et al., 2019;

Hosseini & Dixon, 2016). Furthermore, the findings concerning data format standards explained above correlate with the reports by various studies on blockchain interoperability, which explains that the lack of interoperability between blockchains is a consequence of the absence of universally accepted interoperability and compatibility standards (Lima, 2018). These findings imply there is indeed a need for interoperability standards to simplify the process of connecting different blockchains. Detailed findings on standardisation are presented in Theme 7 below.

Theme summary

The Data theme addresses aspects that should be considered in relation to the data to be exchanged. The theme highlighted that the respondents consider understanding the type of data to be shared and data standards as critical for enabling blockchain interoperability.

Theme insights

The theme provided the following insights: First, enabling blockchain interoperability requires organisations to identify and understand the data to be shared. Understanding the data means understanding the data types, formats, ontologies, and value representations across the communicating systems. The second insight is that organisations should consider creating and adopting common data standards for tokenised assets to simplify the interoperability process.

7.3.7 Theme 7: Interoperability Through Standardisation

The current theme discusses the respondents' views regarding the necessity for standardised methods for developing blockchain systems to facilitate blockchain interoperability. Two main areas concerning standardisation emerged from the analysis.

First, some respondents highlighted that the challenge with blockchain interoperability stems from the lack of standardised methods guiding the development of blockchain systems, thus resulting in the emergence of various heterogeneous blockchain systems that are not interoperable. For example, Respondent 3 explains that with accounting and bookkeeping processes involving blockchain transactions, *“there is no clear guideline from any standardised industry in terms of standardisation we know exactly how to do that in normal finance ... but you don't know what, how that is handled for digital assets, that's also a*

problem for institution[s] that keep these assets on their treasury and on their balance sheet". In agreement, Respondent 1 stated that *"the challenge we have with all these blockchain networks is that we are not following the same standard which makes it very difficult to communicate*". The same sentiments were expressed by Respondent 6, who stated that one of the considerations for enabling blockchain interoperability is to deliberate *"about is there is a standard way or procedure for one blockchain to talk to another"*. These findings regarding the lack of standards as a barrier to blockchain interoperability correspond to several studies on interoperability in general and blockchain interoperability specifically. The studies purport that a barrier to the widespread deployment of blockchain technology is the lack of standardisation among blockchain platforms (Andoni et al., 2019; Belchior et al., 2021b). In addition, the findings above align with Deshpande et al. (2017, p. 16), who explain that *"using standards to establish stronger consensus on consistent terminology and vocabulary could improve understanding of the technology and help progress the market"*.

The second aspect the respondents expressed is related to the different areas in which standardisation could play a role in enabling interoperability. Some respondents revealed that enabling blockchain interoperability requires standard data formats between the communication systems, as mentioned in Theme 6 above. For instance, Respondent 3 explained that *"if you design a token based on the ERC20 standard its immediately interoperable with any other asset that's on the Ethereum blockchain"*. They added that it is also necessary to standardise the design and development of CBDCs. The respondent believes current central bank initiatives focused towards the development of CBDCs are disjointed because of a lack of standards guiding these developmental efforts. This view is implied in the following quote on CBDC development: *"The challenge with these institutions that issue these currencies, they are by nature centralised and also operating in silos. So you know there is some direction from the Bank of International Settlements to create standards for doing this. There is nothing here, it's free for all so every central bank is designing their own CBDC"*.

Others suggested that enabling interoperability requires standardised interfaces between the communicating systems. For instance, according to Respondent 1, the lack of standardised blockchain-focused APIs is an additional barrier to interoperability. The respondent explained that *"you have disparate application integration or application programming interfaces because we don't follow a standardised approach in terms of*

designing this". A similar argument was put forward by Respondent 6 regarding the use of smart contracts as interoperability interfaces: *"Smart contracts are developed using different programming languages, in this case they are completely different. We need to have a standard that allows them to talk to each other"*.

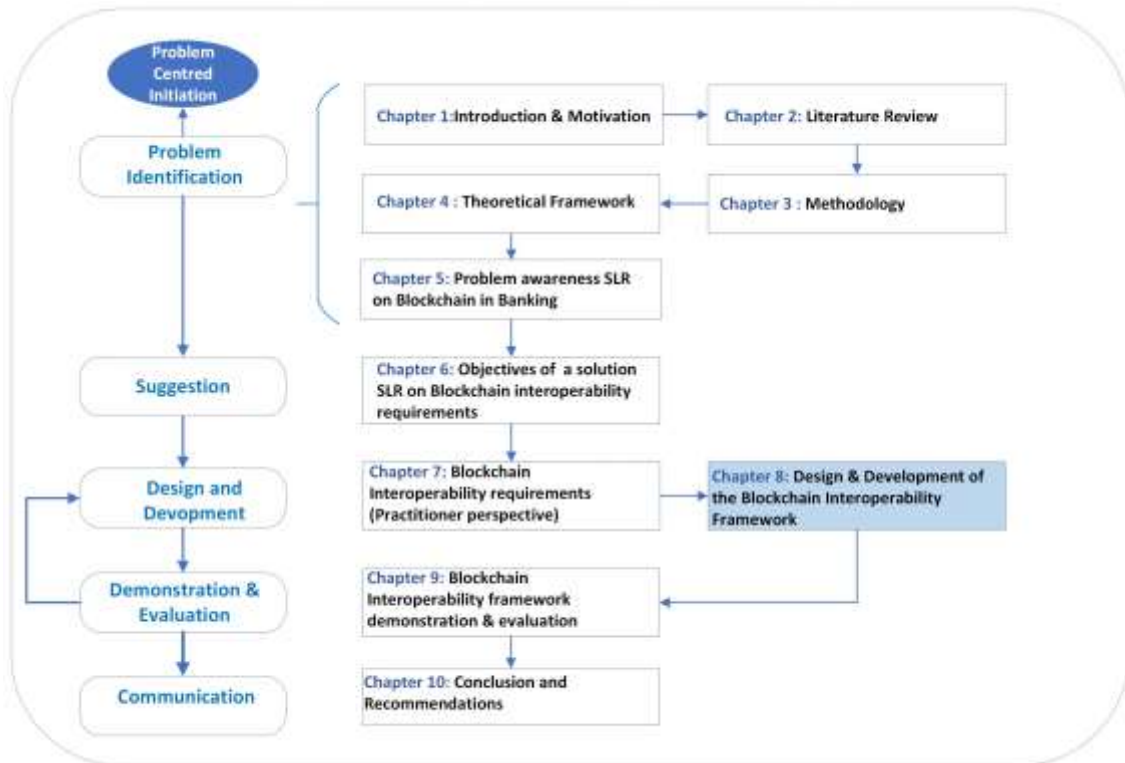
The findings above regarding the need to standardise data formats and interfaces among blockchain systems are similar to those expressed by (Hardjono et al., 2019). Hardjono et al. (2019) proposed that a common standardised transaction format and syntax for blockchain systems should be developed to enable interoperability. Similarly, the findings back up the argument by Jung and Jeong (2021), who explain that enabling interoperability between digital assets like CBDCs requires the development of common technical standards for message formats, encryption technology, data, and user interfaces. Concerning the suggestion that smart contracts should be standardised, (Capocasale & Perboli, 2022) concur about the compelling need to create standard definitions, guidelines and best practices for smart contracts. Cali et al. (2022) reiterate that appropriate standardised frameworks should be developed for distributed ledger technologies (blockchains) and other related DLT-based technologies, such as smart contracts, to support comprehensive industrial implementation of the technology.

7.4 SUMMARY

This chapter narrated the findings from the thematic analysis conducted on interview responses of thirteen blockchain experts. The inductive thematic analysis revealed seven themes, which identified forms of blockchain interoperability, business perspectives, interoperability mechanisms, properties of interoperability mechanisms, regulatory compliance, data, privacy and security, and interoperability through standardisation. The chapter further presented key insights obtained from each of the themes. The themes and associated insights informed the development of the proposed framework in Chapter 8.

CHAPTER 8

8 DESIGN AND DEVELOPMENT



8.1 INTRODUCTION

This chapter discusses the development of the proposed blockchain interoperability framework that banking organisations can use as a reference to guide the process of interoperating blockchain systems with existing systems and other blockchain systems. The purpose of the framework is to guide the different considerations to enable a seamless exchange of data involving blockchain banking systems. The chapter explains the process followed when developing the framework. In particular, the chapter elucidates how the framework was formulated using concepts borrowed from the general systems theory and the European interoperability framework (see Chapter 4 for an overview of the Systems theory and the EIF framework).

The section further explains how the development of the proposed framework was informed by the requirements identified in the systematic literature review (Chapter 6) as well as the

results obtained from the data collected from the interviews presented in Chapter 7. The resulting blockchain interoperability framework is presented at the end of the chapter.

8.1.1 Overview of General Systems Theory and Its Concepts

Systems theory is an interdisciplinary theory for studying how systems interact to form a large, more complex system, such that the behaviour and properties of the larger system are derived from the collective characteristics of the smaller systems. The key purpose of systems theory is to explain real-life systems to enhance the understanding of systems and the predictive ability of other real-life systems (Adams et al., 2014). Due to its interdisciplinary nature, systems theory can take different forms. In organisational studies, systems theory is applied to explain organisations as complex systems consisting of interconnected systems that interact and collaborate to achieve a common goal; it is used to explain how organisations behave, change and develop (Millett, 1998). In the communication field, systems theory explains the interconnectedness of communication systems, while in engineering and related fields, such as information technology and information systems, explains communication between artificial systems such as information systems and sociotechnical systems and machines (Lai & Huili Lin, 2017). Despite its multidisciplinary application, the theory is founded on common concepts.

The key focus of systems theory is the system. A system is viewed as an organised group of interdependent and interrelated components or subsystems and is defined by its goals or purpose (Pokharna, 2013). Thus, understanding a system requires understanding its goal. Goals are negotiated and vary according to needs. Furthermore, a system is formed based on relationships emerging from the interactions and mutual feedback between its components or sub-systems. Therefore, a system is not viewed as a mere collection of its parts but as a whole that is greater than the sum of its parts. Hence, the system has properties and behaviour that differ from the behaviour of its individual components (Lai & Huili Lin, 2017), and these emergent properties differentiate different systems. In addition, general systems theory views systems as open systems, meaning they are open to their environment and have permeable boundaries that enable information and resources to flow into the system and out to its environment constantly. As a result, the environment surrounding the systems influences and helps regulate how the system functions. Another concept relates to feedback, which can be either negative or positive. Positive feedback

helps to enhance and grow the system, while negative feedback seeks to correct or reduce deviations or errors in how the system functions. Lastly, systems require constant maintenance to ensure balance and prevent deterioration. Systems theory argues that if left alone, any system will deteriorate and move away from its goals (or reach a state of entropy). Therefore, systems must be maintained continuously to prevent this deterioration. The System theory and associated concepts are shown in Figure 8-1 and Figure 8-2.

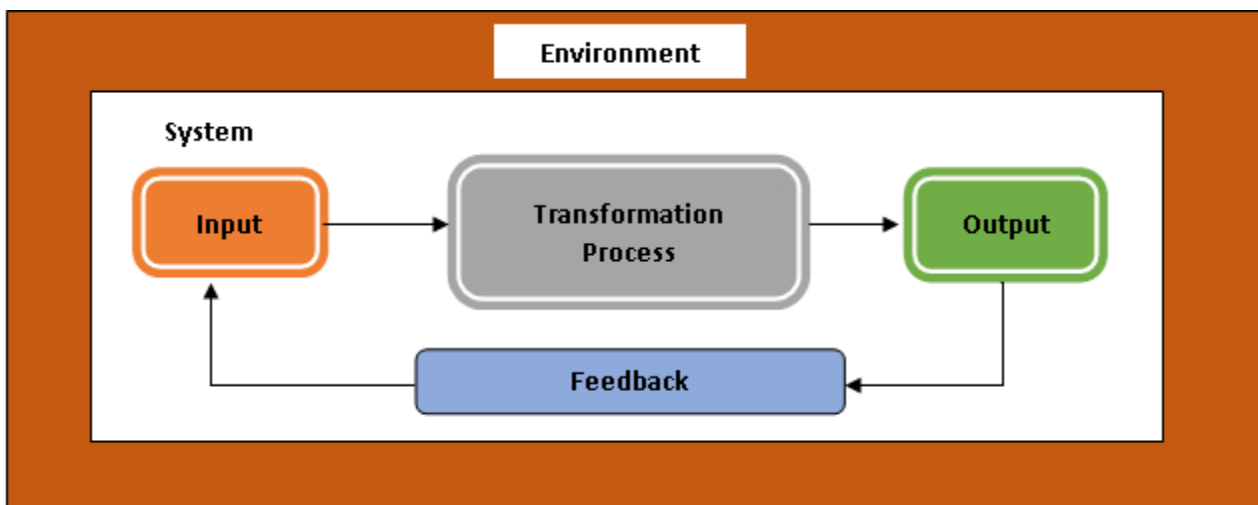


Figure 8-1 Pictorial representation of systems theory elements

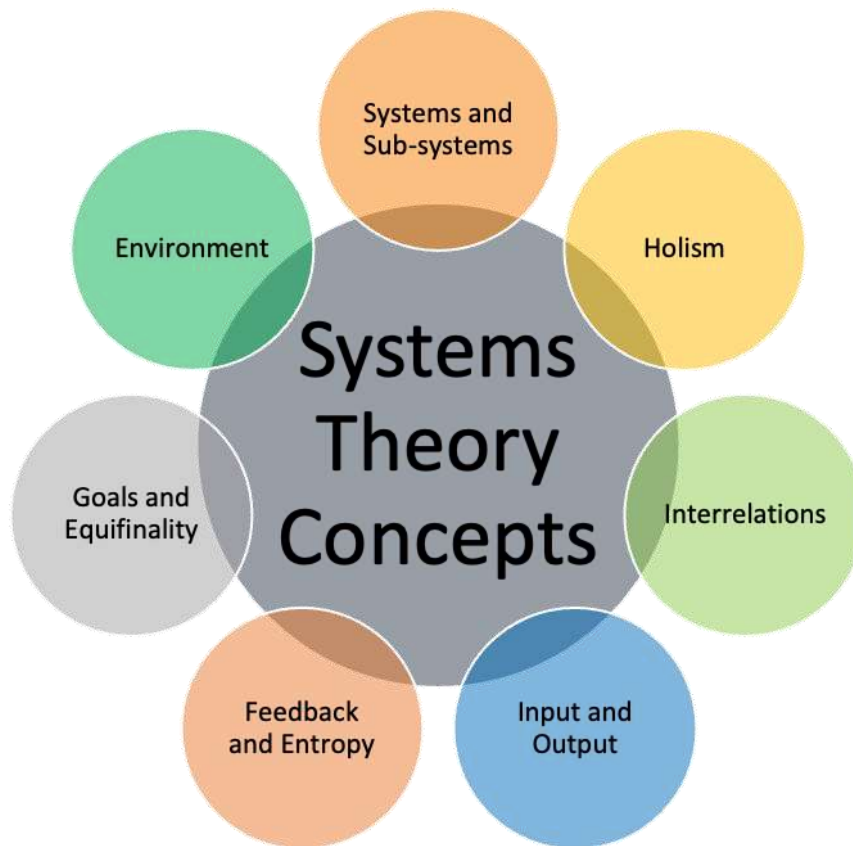


Figure 8-2 Overview of systems theory concepts

8.1.2 Application of Systems Theory Concepts to Develop the Interoperability Framework

Identification of Systems

As stated in Chapter 4 and the preceding section, one of the main emphases of systems theory is the understanding of systems and the interaction and relationships between them and their sub-systems. Interactions between systems and their components involve the exchange of information and resources (Katrakazas et al., 2020). This exchange of information can be viewed as interoperability. Systems interoperability is a critical feature of any system to be able to interact with other systems to achieve its goals (Chapurlat & Daclin, 2012). Because systems interoperability enables the exchange of information in different ways, it can, as a result, create a foundation for the development of new forms of communication between systems (Van Lier & Hardjono, 2011a). Establishing these new forms of communication requires an understanding of the participating systems and an

agreement between the systems regarding the technology and semantics to use (Van Lier & Hardjono, 2011a). Therefore, understanding the communication (interactions) systems requires first identifying the systems involved in the interaction. Therefore, in the context of understanding blockchain interoperability, organisations must first identify or determine the blockchain system(s), its components, and how these components interact, as well as other systems required to interact with the blockchain to satisfy specific business goals.

Regarding the concept of systems in the context of blockchain interoperability, the findings obtained from the SLRs (in Chapters 5 and 6) and the analysis of the interview data in Chapter 7 present systems as follows. The interview data revealed that systems in the banking institution context refer to the bank itself as a system. The bank comprises other systems that need to interact to meet a specific objective. The other systems are identified as permissioned blockchain systems, as well as traditional core banking systems that enable payments. The systematic literature reviews also indicated that the systems might be permissionless blockchain systems, which could be external to the institution but might be required to facilitate collaboration with external parties for strategic reasons. In particular, SLR 1 (Chapter 4) revealed specific types of blockchain systems or platforms deployed in the banking sector. The discussion on technical considerations in the SLR in Chapter 4 showed that banking institutions preferred Quorum, Corda, and Hyper Ledger Fabric to their permissionless counterparts because of their security and privacy features. Furthermore, the data revealed that blockchain could be further deconstructed into various components that might also need to interact. As discussed in Theme 1 (Section 7.3.1), some blockchain systems consist of smart contracts that might need to interact to enable blockchain interoperability. Therefore, smart contracts can also be viewed as sub-systems. The information above implies that addressing blockchain interoperability requires understanding the systems involved, their components and how they interact. Thus, from the discussion above, it can be inferred that an interoperability framework should include a component focusing on the systems involved, their features and properties. The systems components proposed for inclusion in the framework are shown in Figure 8-3. The elements of the component are based on the findings discussed earlier.

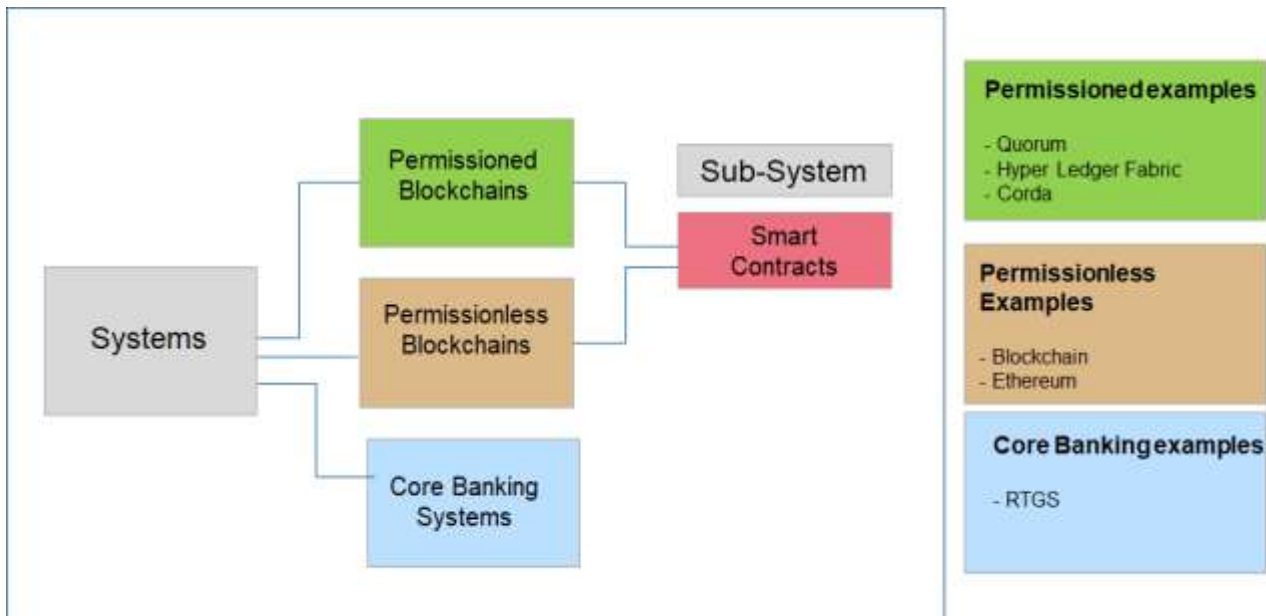


Figure 8-3 Overview of systems involved for blockchain interoperability in banking

Systems Goals

Systems theory states that a system should serve the purpose(s) of both its parts and the system of which it is part (Habbershon et al., 2003), thereby implying that every system and its sub-systems should collaborate towards a particular goal. In the context of blockchain interoperability in banking organisations, the collective goal of the systems above is to exchange information seamlessly, regardless of any differences between the systems, ultimately to meet the overall goal of the banking organisation. According to the interview data as well as the results from the SLR (Chapter 5), the choice of the systems above and, ultimately, the goal they serve is driven by the business goals and objectives. The interview data revealed that the choice of the type of blockchain deployed in the organisation depends on the business case, i.e., an organisation should select a particular blockchain to fulfil a specific business purpose. Likewise, the SLR revealed that the choice of the system, particularly the choice of the blockchain system, is guided by the business model. This finding has the following implications for enabling blockchain interoperability.

The first implication is that the business objective determines the blockchain platform (system) that is deployed. Second, the objective/goal further influences the area of application of the technology within the organisation and, consequently, the selection of

other systems that would need to communicate and share information with the blockchain. Hence, the organisation must determine what systems to apply, when and how to interoperate (how they interact). Understanding the systems requires understanding their features, limitations, capabilities and scope of application. For blockchain systems, this means understanding the consensus mechanisms, features, determining whether or not it has smart contract capabilities, the data formats, the transaction speed, interfaces, et cetera. Based on the findings above, the inference is that the framework should incorporate a component to represent the business aspect that influences interoperability. The business-related concepts, design elements and guidelines inferred from the interviews and the SLRs are shown in Figure 8-4.

Table 8-1 Conceptualisation of system and their goals

#	Findings (requirements or objectives)	Design element/Principle
1	<ul style="list-style-type: none"> • Business case for blockchain and blockchain interoperability <p style="text-align: center;">Or</p> <ul style="list-style-type: none"> • Blockchain-centric business model 	<ul style="list-style-type: none"> • Determine business case for blockchain (Section 7.3.2) • Identify scope of application of blockchain (Section 6.2.7) • Identify suitable blockchain platform (Section 6.2.7) includes the following: <ul style="list-style-type: none"> * Understanding feature * Understanding function * Understand data * Identify system components * Identify other systems including existing and new • Identify other systems that need to interact with blockchain (Section 7.3.2) • Determine type or level of interoperability required (Section 7.3.2) • Identify types of data to be exchanged (Section 7.3.2) • Evaluate compatibilities and incompatibilities between system (Section 7.3.2)

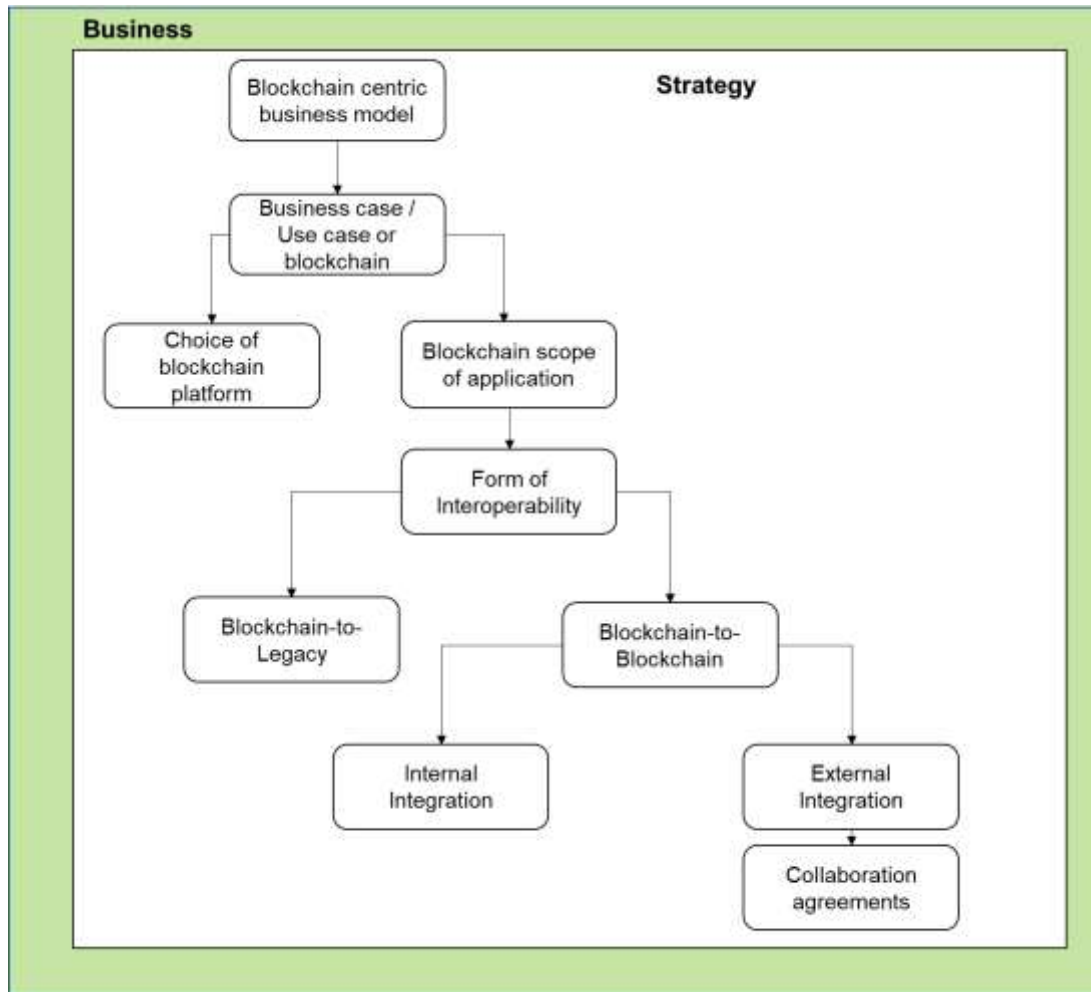


Figure 8-4 Business related aspects and guidelines

Environment

As stated previously, the systems theory approach encompasses the idea that an open system can interact with its external environment. Organisations as forms of open systems are influenced by the external environment. Systems theory recognises that an organisation relies on the environment, which is a larger system, such as the industry in which the organisation operates, the economic system and the society. The environment provides essential input to the organisation and may also be an outlet for the output produced by the system (Chikere & Nwoka, 2015).

Additionally, systems theory provides a means to describe the external and internal relationships of an organisation. Internally, the theory helps explain why and how people interact with each other and with technical systems within the organisation. It can also assist

in describing how technical systems interact with each other. Externally, the theory helps explain how an organisation interacts with its environment, such as other external organisations and the industry and society at large. Borrowing from the systems theory, the environment concept was adopted to represent the role and influence of the environment in the process of enabling blockchain interoperability in the banking sector.

The findings from interviews and the SLRs indicated that in the aforementioned context, the concept of the environment refers to regulations governing how banking institutions operate, as well as other external organisations involved in the strategic collaboration with the bank. The regulatory aspect refers to industry-specific regulations, country-wide regulations and cross-jurisdictional/global regulations, whereas other organisations can be other banks or organisations that may need to share information with an organisation. The regulatory environment provides input to banking organisations and thus influences strategic decisions regarding internal business processes, such as what systems are used and how they operate and interact. Similarly, external organisations involved in strategic collaborative relationships with an organisation can also provide input to that organisation. As the findings of the SLR in Chapter 6 indicated, this process might require interoperability at the organisational level to ensure collaborating organisations' processes are aligned. Therefore, both the external regulations and external organisations influence the interoperability process. The next discussion outlines the relationship between the environment and the blockchain interoperability process.

The process of enabling interoperability between different systems involves the transfer of data between systems that may have different security measures and controls. In a banking institution, this information might include sensitive business, transaction and customer data. To protect this information, banking institutions are required to comply with the relevant regulations related to the protection of private information and rules regulating payment systems. Therefore, as suggested by the interview and SLR findings, banking organisations should consider appropriate regulations when interoperating blockchain systems. In particular, the recommendation is that the banking industry should develop a blockchain-centric regulatory framework to address the lack of appropriate regulations. In addition, in the absence of the appropriate legal and regulatory frameworks, organisations should evaluate and identify existing regulations that could be applied to regulate blockchain systems in the interim to support innovation. Further regulatory implications were mentioned

regarding the usage of smart contracts in enabling blockchain interoperability. According to the SLR findings (Chapter 6), organisations using smart contract capabilities to enable interoperability should consider the legal implications of such contracts. Drawing from the findings above, the environment concept was conceptualised, as illustrated in Figure 8-5 below. The environmental elements included in the figure are based on the findings as outlined in Table 8-2. The key environmental elements that influence the choice of interoperability strategy and approach include industry and global standards and regulatory policies. Specific elements relating to standards include, identifying and developing data and interface standards to ensure that data on various systems follows the same data standards and formats. On the other hand, the regulatory policy elements represent the legal and regulatory considerations that should be considered to enable blockchain interoperability in the banking sector. Examples of existing standards and regulations suggested by the respondents are also included Figure 8-5.

Table 8-2 Conceptualisation of the environment

#	Findings (requirements or objectives)	Design element/principle
1	<ul style="list-style-type: none"> • Blockchain-centric regulatory framework 	<ul style="list-style-type: none"> • The banking industry should develop a blockchain-centric regulatory framework (Sections 6.2.8, 7.3.3)
2	<ul style="list-style-type: none"> • Compliance with regulations 	<ul style="list-style-type: none"> • Identify potential regulations concerning interoperability (national and global where relevant) (Sections 6.2.8 and 7.3.3) • Evaluate existing regulations for applicability to blockchain interoperability (Section 7.3.3) • Select the relevant regulations / parts of regulations that are applicable to blockchain systems (Section 7.3.3) • Customise existing data privacy and protection policies to include provisions for blockchain interoperability (Section 7.3.3)

3	<ul style="list-style-type: none"> • Smart contract requirements 	<ul style="list-style-type: none"> • Evaluate existing national contract laws for applicability to smart contracts (Section 6.2.8) • Include provision for smart contract enforceability in contract laws (Section 6.2.8) • Develop guideline for harmonisation of smart contract and traditional contracts (Section 6.2.8)
---	--	--

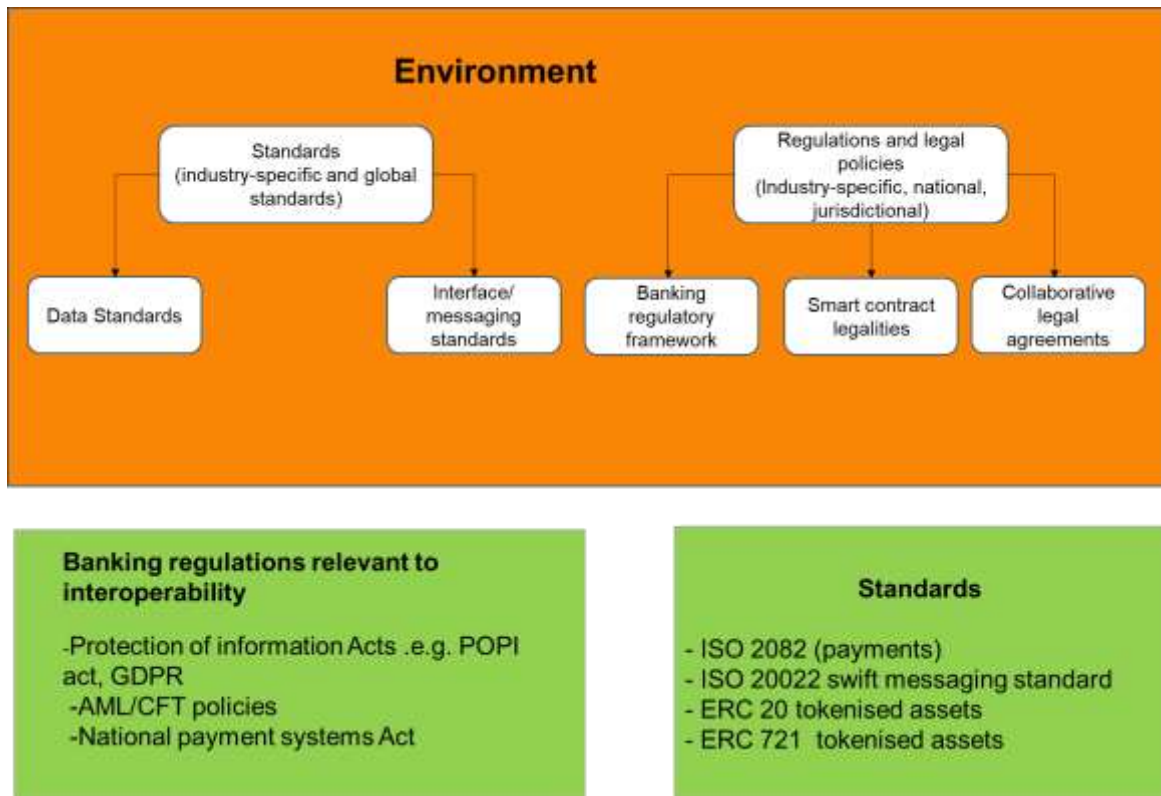


Figure 8-5 Environmental aspects of blockchain interoperability

Input and output

In systems theory, systems exchange information as input and output with the environment and other systems. Inputs refer to elements that come into the systems to enable

interactions between system components, while outputs denote products or elements leaving the system or elements that change the system to execute certain tasks. The type of input or output varies depending on the type of system.

For this study, the input and output elements are conceptualised as the information/data exchanged between systems and subsystems. As the findings from the SLRs and the interview analysis revealed, the data can be normal business data (arbitrary data), transaction data or digital assets. In the blockchain interoperability context, the aim is to exchange normal as well as digital assets (crypto assets) across system boundaries. However, variations in how the data is represented across systems complicate the interoperability process. Therefore, understanding the data being shared is critical to addressing challenges that stem from the aforementioned variations in data formats across the communicating systems. Thus, the proposed interoperability framework should include data-related aspects.

In particular, the input/output or data component of the framework is derived from the findings discussed in Theme 6 and the findings of the SLR (Section 6.2.6) and includes the following aspects. First, the requirement (TRS 4 in Section 6.2.6) and findings in Theme 6 indicated that data formats should be standardised across communication blockchain systems. Furthermore, the results indicated that organisations should define standard units of value for the digital asset to ensure that the communication systems have the same understanding and representation of the data. The various elements identified concerning data are illustrated in Table 8-3 and Figure 8-6 below.

Table 8-3 Conceptualisation of data (input/output)

#	Findings (requirements or objectives)	Design element/principle
1	<ul style="list-style-type: none"> Identify forms of data that were exchanged 	<ul style="list-style-type: none"> Organisations should identify the kinds of data that need to be shared to fulfil the business goal (Section 6.2.6)

		<ul style="list-style-type: none"> • Determine level of compatibility between data across systems (Section 6.2.6) • Determine and understand level of compatibility between message formats across systems (Section 6.2.6)
2	<ul style="list-style-type: none"> • Communicating systems need to have a shared understanding of the data 	<ul style="list-style-type: none"> • Banking industry should develop industry-wide standards for blockchain used in the sector (Sections 6.2.6 and 7.3.7) • Data formats should be standardised across the banking industry (Sections 6.2.6 and 7.3.7) • In the interim while standards are being developed: <ul style="list-style-type: none"> *Collaborating organisations should agree on data formats (Section 6.2.6) *Organisations should agree on asset definition and values (Sections 6.2.6 and 7.3.7)

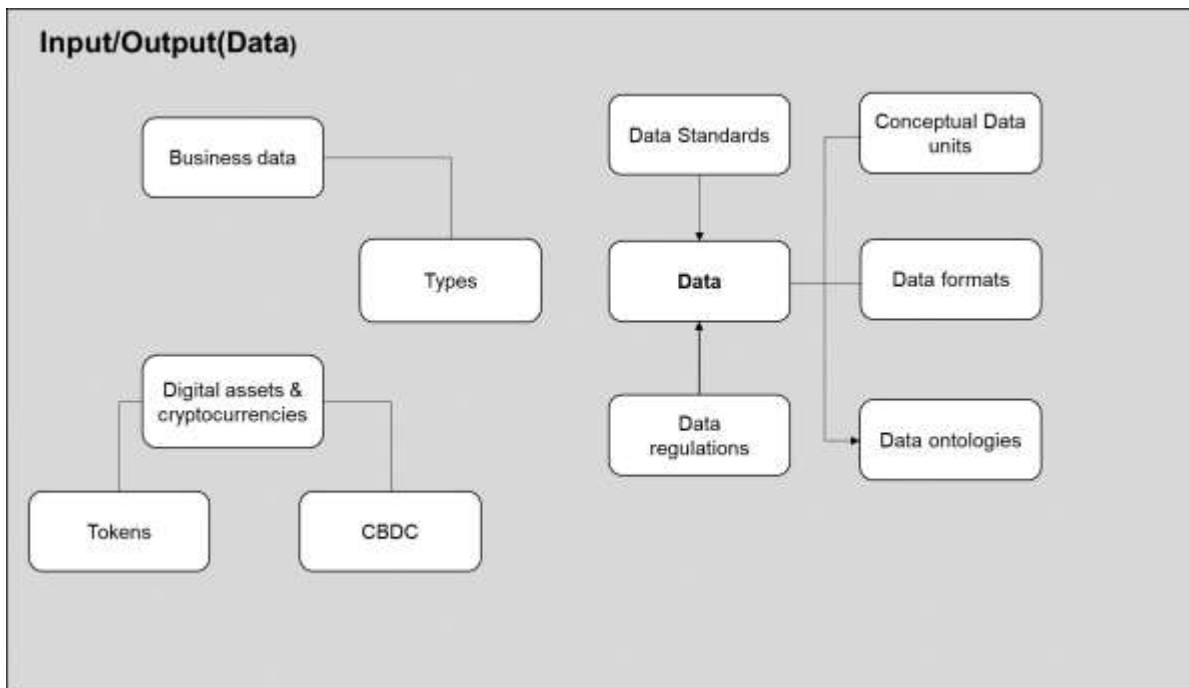


Figure 8-6 Data elements for blockchain interoperability

As illustrated in Figure 8-6, the main data elements that should be considered include, the types of data to be shared and data formats. The types of data denoted in the figure are business data and digital assets and cryptocurrencies. The data format elements that include, data standards and data regulations.

Transformation

The transformation component of systems theory represents the manipulation or reorganisation of input to produce outputs. It represents the process of transforming or converting resources or data within a system and also indicates how systems and sub-systems are interrelated (Ham et al., 2015). In essence, transformation can help in understanding how systems and their components exchange data and resources (Scott & Davis, 2015). On this basis, the transformation component in this study is used to represent the concept of interoperability between the different systems in the banking context. Hence, the transformation component includes elements relating to enabling interoperability between blockchain systems and other systems. According to the findings in Chapters 6 and 7, the interoperability elements refer to the techniques and mechanisms used to enable interoperability (Section 7.3.4, Theme 4), properties and functions pertaining to the mechanisms (Section 7.3.5, Theme 5), level of interoperability adopted from the European interoperability framework (discussed in Section 6.2.6), and all the necessary considerations to facilitate the blockchain interoperability process, as discussed in the SLR in Chapter 6. The conceptualisation of the transformation component is shown in Figure 8-7. The elements of the component are derived from the findings shown in Table 8-4.

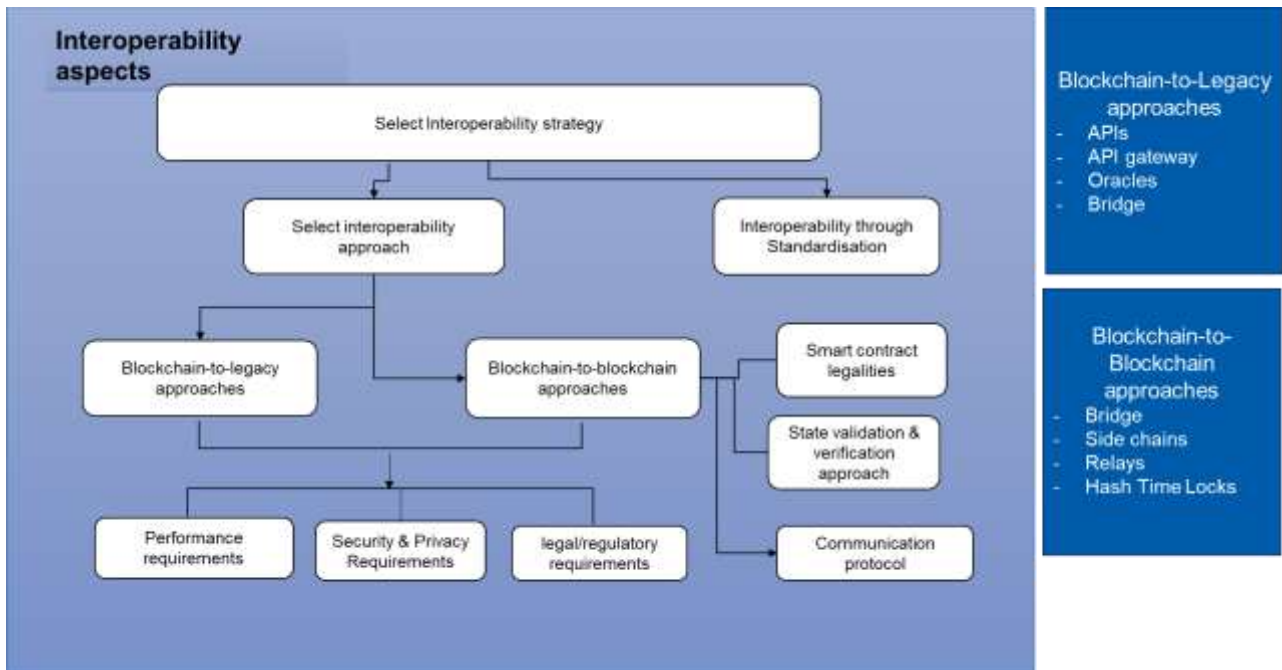


Figure 8-7 Conceptualisation of the Transformational Component

Figure 8-7 illustrates the elements that should be considered when deciding on the interoperability strategy to follow. There are two main strategies that can be adopted, the first is a strategy in which interoperability is achieved through standardisation. This strategy is appropriate in cases where the systems to be interoperated utilise the same data standards and formats. The second strategy is denoted as ‘selecting an interoperability approach’ and is required when there are data format incompatibilities between the systems to be interoperated. Selecting an interoperability approach depends on the desired type of interoperability, that is, blockchain-to-blockchain or blockchain-to-legacy. However, both types of interoperability require consideration to be given to the performance, security and privacy and legal requirements as shown in Figure 8-7. In addition, Figure 8-7 shows that when selecting a blockchain-to-blockchain approach, organisations should consider smart contract legalities, understand the state validation approach employed by each blockchain and identify the communication protocols to be used.

Table 8-4 Conceptualisation of interoperability

#	Findings (requirements or objectives)	Design element/Principle
1	<p>A cross-chain communication protocol</p> <ul style="list-style-type: none"> • Should enable data and asset transfer between different blockchains and perform value conversions • Should fulfil the atomicity and liveness requirements • Should ensure finality of cross-chain transactions • Should prevent double spending 	<ul style="list-style-type: none"> • A blockchain interoperability framework should provide considerations for the selection of a cross-chain communication protocol (Section 6.2.6) • Organisation should identify or develop appropriate protocols suited to blockchain and data (Section 6.2.6)
2	<p>Cross-chain mechanism</p> <ul style="list-style-type: none"> • Should protect the security and integrity of exchanged data • The mechanism, methods, and operations used to enable interoperability between the blockchains need to be secure • An integration mechanism that is fault-tolerant • Ensure confidentiality of data: access control, authentication and encryption 	<ul style="list-style-type: none"> • Organisations should identify available cross chain technique and mechanism (Section 7.3.4) • Organisations should evaluate available cross chain mechanism (Section 7.3.4) • Organisations should be able to select the right cross chain mechanism (Section 7.3.4) • Organisation should consider security control required to protect the integrity and privacy of the data exchange process (Section 7.3.4) • Organisation should ensure that the interoperability process complies with relevant data laws (data protection laws) (Section 7.3.4)
3	<p>Form of interoperability</p>	<ul style="list-style-type: none"> • Organisations should identify the form of interoperability required basis of business case i.e., blockchain-to-blockchain or blockchain-to-legacy (Section 7.3.1)

4	Interoperability levels	<ul style="list-style-type: none"> Organisations should identify appropriate level(s) of interoperability they desire to achieve (Section 7.3.1)
---	--------------------------------	---

8.2 CYCLE 1: FRAMEWORK DEVELOPMENT

The proposed blockchain interoperability framework was developed in two forms, namely the layered architectural component framework (see Figure 8-8) and the blockchain interoperability process flow framework (see Figure 8-9). The architectural component framework is a high-level representation of the key components required to enable blockchain interoperability. The framework components were derived from the systems theory components as discussed in section 8.1.2 and illustrate the different elements that contribute to enabling blockchain interoperability. The architectural components are outlined in Section 8.3.1 below. The blockchain interoperability process flow framework illustrates the relationship between the components as well as the process organisations should follow to interoperate blockchain technology with other organisational systems. The frameworks are complemented by a set of guidelines and a technology stack to support the decision processes (see Figure 8-10). The guidelines were derived from the suggested made by the participants as discussed in Chapter 7.

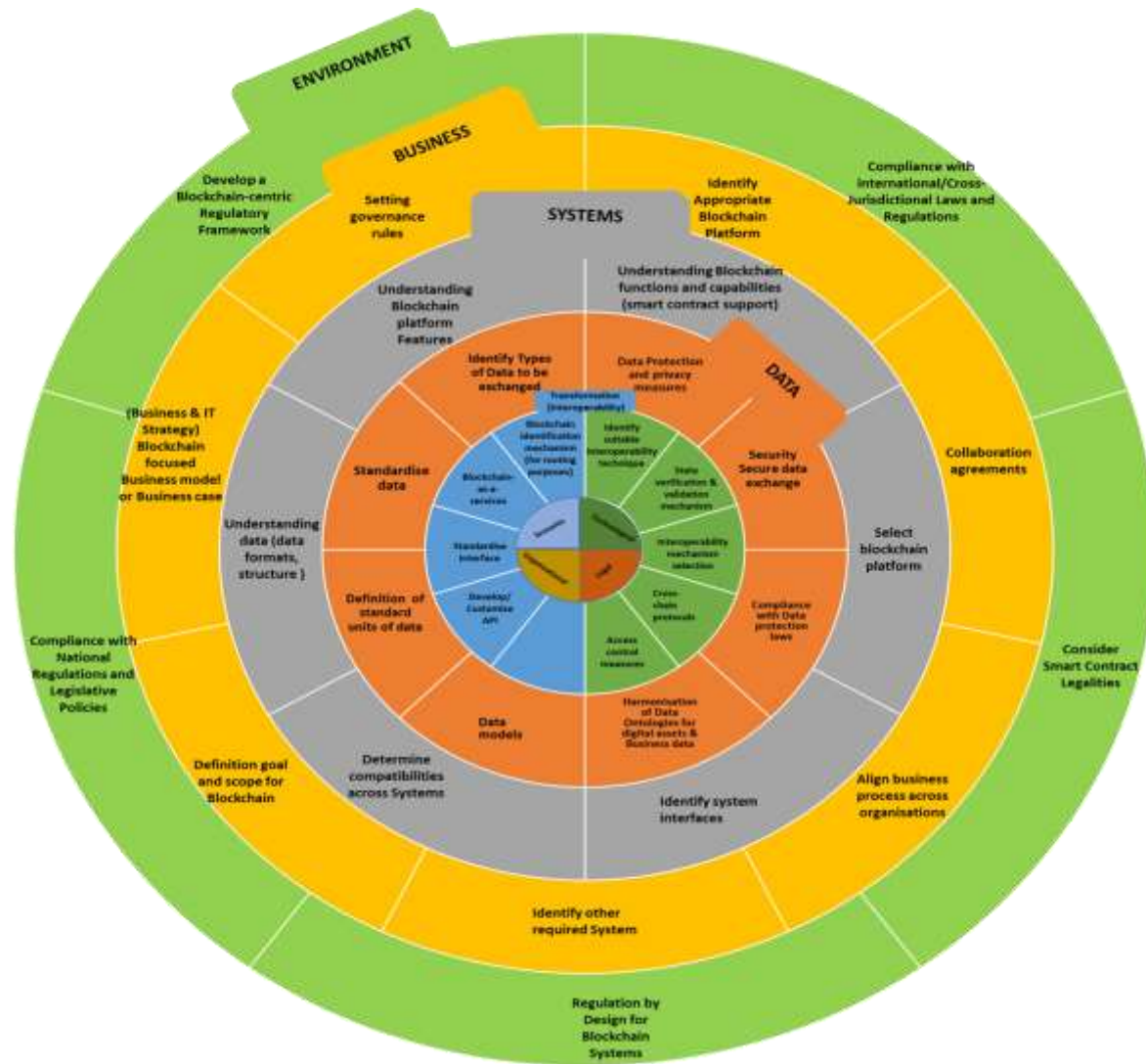


Figure 8-8 Overview of Proposed Enterprise Blockchain Interoperability (EBI) framework

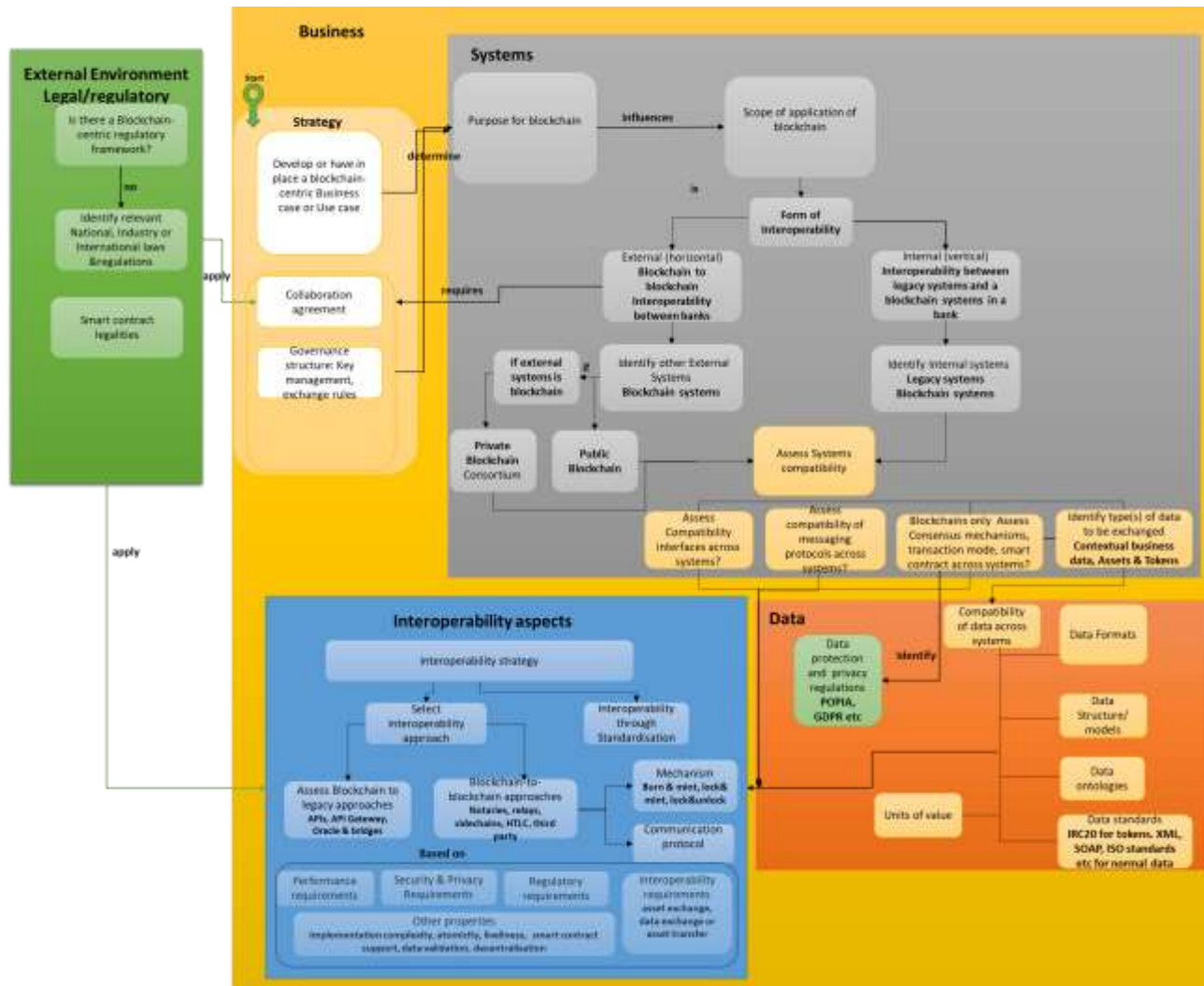


Figure 8-9 Enterprise Blockchain Interoperability Process Flow

Guidelines

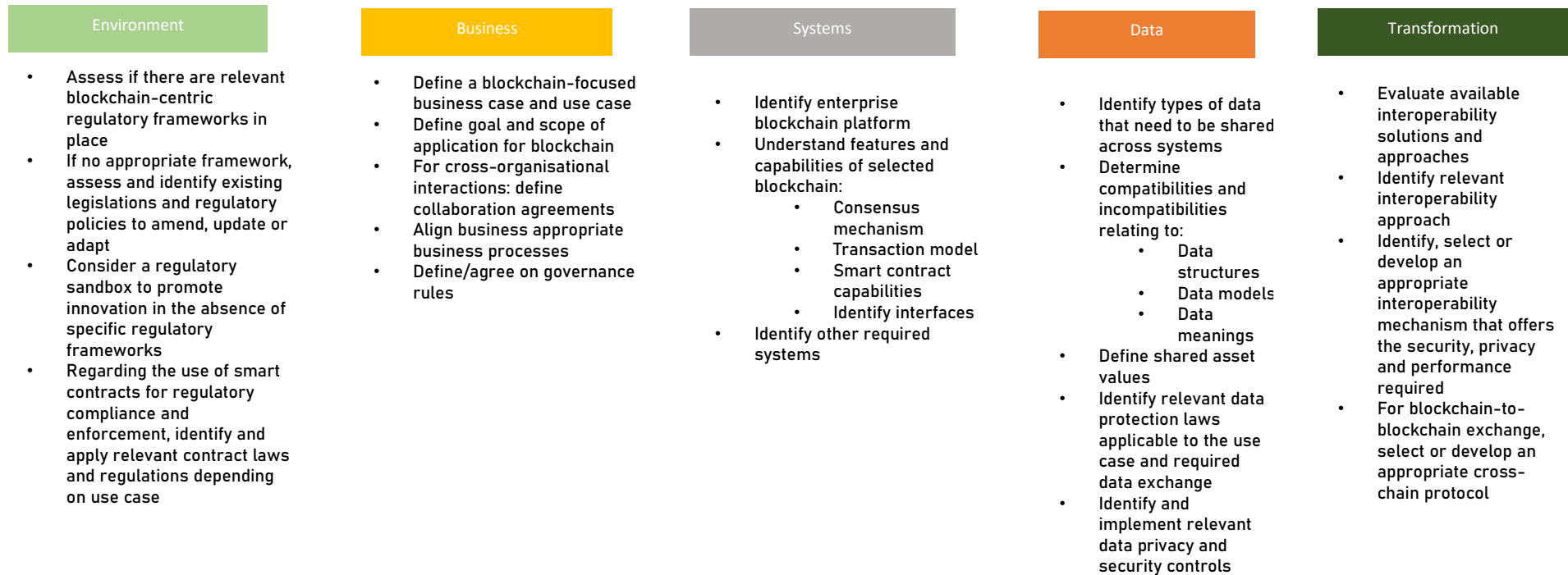


Figure 8-10 EBI Framework guidelines and considerations

8.3 CYCLE 2: FRAMEWORK DESIGN AND DEVELOPMENT BASED ON WEBINAR DATA

The current section presents the second iteration of the framework design and development phase. The main focus of the section is discussing the development of the framework based on the data collected from webinars. The discussion includes an outline of the data collection and analysis processes of the web seminars (webinars), presenting a brief introduction on webinars, the data collection process and data analysis, as well as the corresponding results. The section concludes with an enhanced framework, which includes additional elements resulting from the data collected from the webinars.

8.3.1 Overview of Webinars

Webinars are live seminars hosted over the internet, in which participants and facilitators communicate using shared virtual platforms that allow for voice and video recording (Gegenfurtner & Ebner, 2019). They are also interactive and usually include a chat function that enables participants to post questions and receive answers in real time (Buxton et al., 2012). Because webinars are hosted online, they can accommodate a large number of participants from different geographical locations and experiences and, thus, provide a rich source of information and insights.

Types of webinars

Webinars have different formats, depending on their purpose and target audience. These include educational and training webinars, interview webinars, panel discussion webinars, keynote speaker webinars, company case study or product webinars. Educational and training webinars are created to educate an audience about a particular topic. They usually support teaching and learning in distance learning and professional development (Gegenfurtner & Ebner, 2019). Interview webinars involve one-on-one or one-to-many interviews with subject matter experts, specialists or persons of interest in a particular field. They are intended to provide a platform where the interviewee can share insights and experiences with the audience. Panel discussion webinars involve a group of panel members who are typically experts. The panellists discuss a specific topic, and the

discussion is usually guided by the host. Similar to interview webinars, panel webinars provide insights and experience from experts, albeit from diverse viewpoints. In keynote webinars, a keynote speaker (who could be an expert) makes a presentation to the audience on a particular topic, while company case studies and product webinars are usually hosted by specific companies to present or market their products. This study used mainly panel, interview and case study type interviews.

8.3.2 Data Collection

The webinars employed in the study were identified through a search on the *YouTube* platform. *YouTube* is an online platform for hosting, sharing and viewing videos from different sources worldwide; it offers a large collection of videos, including the various types of webinars described above. The following search strings were used to search for the webinars. The string was constructed using the keywords: blockchain, interoperability and banking.

Search strings:

- Blockchain interoperability in banking
- Blockchain interoperability
- Blockchain in banking

Webinar screening and selection

The search strings were run on the *YouTube* platform to identify potential webinars. The resulting videos were screened for relevance based on their titles and by previewing the webinar introductions. Additional videos were identified via snowballing. *YouTube* enables snowballing by suggesting similar videos to the ones identified through the search strings. The process of selecting the relevant webinars to include in the study occurred thus: the videos identified through the search strings and snowballing were previewed on the platform. In this case, previewing refers to watching the video introductions on the platform to determine the relevance of the content to the objectives of the study. The relevant videos were downloaded using *YouTube* downloader software. Once the webinar videos were downloaded, the researcher watched each webinar to its end to confirm relevance and

select the final webinars to be included. The final webinars included for analysis were selected based on the inclusion/exclusion criteria shown in Table 8-5. The process of identifying potential webinars using the search keys and snowballing resulted in twenty-two webinars. Thirteen webinars were selected and included for analysis, as shown in Table 8-6. The webinars were downloaded as videos and then converted to voice (MP3 format) to reduce the size. The videos were then transcribed using the *Word 365* transcription service.

Table 8-5 Inclusion and exclusion criteria for webinars

Inclusion criteria	Exclusion criteria
Webinar focused on topic of blockchain interoperability in banking	Webinars do not discuss blockchain interoperability in banking
Webinar in English	Webinar not in English
Webinars discussing challenges, solutions and current work relating to blockchain in the banking sector	Webinars that promote specific products
	Webinars with duration of fewer than 20 minutes

Table 8-6 List of webinars included for analysis

Webinar number	Title
W1	A Business case for blockchain in enterprises
W2	Blockchains and Banks
W3	Blockchain into IP IBC Tendermints * CBDC session 12 DBDC interoperability
W4	Blockchain interoperability using IBC
W5	CBDCs designing for global access
W6	Global CBDC masterclass interoperability
W7	Inside Innovation Live 08 – CBDCs Ensuring global interoperability through collaboration Swift
W8	Inside Innovation Live 09 – Connecting blockchains Overcoming fragmentation in tokenised assets
W9	Interoperability amongst blockchains
W10	Interoperability across blockchains – FMSIG Mortgage Subgroup Update
W11	Layer 0: the future of blockchain interoperability
W12	The truth about blockchain interoperability
W13	Toward the success of enterprise blockchain

8.3.3 Data analysis

The use of webinars as a source of qualitative data is a relatively new approach in qualitative studies; as a result, very few studies have utilised this approach. Consequently, there is currently no widely accepted approach to analysing webinars. However, webinars are a form of multimedia or video data, which can include text, audio and video data. Video data have been used in various social science disciplines and medicine studies, resulting in the emergence of a variety of approaches to video analysis. (Knoblauch et al., 2014) consider video analysis to be the analysis of video recordings of social interactions. (Ramey et al., 2016) argue that videos offer multimodal forms of data (text, speech, gestures and interactions) that can be analysed. Therefore, a researcher should determine which unit of analysis to select for analysis. The selected unit of analysis and approach to the video analysis depends on the theoretical basis and the specific research questions being pursued (Derry et al., 2010). Accordingly, in some studies, the analysis of the various modalities of data might be required, while in others, only one form of data might be selected as a unit of analysis. The purpose of this study is not to understand and interpret the behavioural aspect of the people participating in the webinars but to obtain insights into issues relating to blockchain interoperability; therefore, gestures and interactions were not used as units of analysis. Rather, the analysis focused on the speech (what was said) in the webinars. Therefore, the data analysis process for the webinar data was conducted similarly to the process for the interview data analysis. The process entailed extracting the audio from the webinar recording by converting it to mp3 format and then transcribing the audio to text. The webinar transcriptions were then uploaded onto the *Atlas.ti* software for coding and analysis.

The analysis of the webinar data followed a deductive content analysis approach. The process involved three steps, which included preparation, organising and reporting. As suggested by Elo and Kyngäs (2008), the preparation step commenced by identifying the unit of analysis and reading through the transcripts to understand the data. According to (Polit & Beck, 2004), the unit of analysis can be a word or a theme. The units of analysis selected for this process are the themes identified from the analysis of the interviews, as elucidated in Chapter 7. The themes were used to code the webinar transcripts following a deductive coding approach. The deductive approach was adopted because of its suitability for testing an earlier theory in a different situation or for comparing categories at different times (Elo & Kyngäs, 2008). Furthermore, deductive content analysis is advantageous in

“cases where the researcher wishes to retest existing data in a new context” (Woods & Catanzaro, 1988) cited by (Elo & Kyngäs, 2008, p. 111). Therefore, taking a deductive approach would assist in testing and confirming the results identified from the interview analysis.

8.4 WEBINAR ANALYSIS RESULTS

The following discussion presents the findings obtained from the deductive content analysis of the webinars. As stated above, the deductive content analysis was informed by the codes and themes identified during the analysis of the interviews; as such, the following results are organised according to those themes.

8.4.1 Theme 1: Branch of blockchain interoperability

The current theme was introduced in Chapter 7 as referring to the different forms of interoperability that may concern blockchain technology in banking enterprises. The analysis of the webinars pointed to several types of interoperability enterprises might require for blockchain technology. This is exemplified in the quote from W1, in which it was stated that *“When enterprises want to use blockchain at scale, they’ll have to talk to each other. So then one blockchain will have to talk to another”*. This statement indicates that interoperability in the context of blockchain technology might refer to the notion of enabling communication between different blockchains. A similar idea was presented in W8: *“We’ve gotta, if we assume that there’s gonna be many different chains out there, right, how are we gonna actually kind of be able to to to link those together in a in a secure way?”* similarly, it was stated in W10 that, *“the proliferation of different and potentially siloed blockchains can serve as an impediment to the growth of blockchain usage. So today we’d like to underscore the importance of interoperability across blockchains”*.

The form of interoperability in which communication involves two or more different blockchains corresponds to the form identified as blockchain-to-blockchain interoperability in Chapter 7, Theme 1. According to W1, blockchain-to-blockchain interoperability may involve communication between a private blockchain and a public blockchain, as reflected in the following extract: *“The interoperability question, the private blockchain where the IP is critical to be protected, that is done with permission nodes inside the private blockchain and*

then when that interacts with the public blockchain, how do you tokenise? I would suggest that thinking about making sure that you have a private permission block, and then you have the bridge from the private to the public blockchain using some of these new interoperability advances". In addition, blockchain-to-blockchain interoperability in the context of the banking sector has been used to refer to interoperability between digital currencies, with a particular focus on CBDCs, as illustrated in the following quote from W5: *"It seems that interoperability has really come up the agenda both around, you know, current payment systems and infrastructures as well as with CBDC's. And actually that seems like it's going to be you know a kind foundational principle for CBDC's that we have to ensure interoperability".*

CBDCs are digital currencies developed by central banks. They differ from the other types of digital currencies, such as tokens and cryptocurrencies, which are created by private FinTech companies and are traded on public cryptocurrency exchanges. Because CBDCs are designed to replace or complement national fiat currencies, they have many additional requirements, which may vary depending on the purpose and type of CBDC. According to W6, enabling interoperability for CBDCs not only requires systems-focused interoperability but also requires interoperability from a user perspective. In W6, it was stated that *"we might need to started thinking about interoperability beyond that (systems Interoperability) to talk about interoperability from the perspective of persons being able to use his bank account and do credit transfer to an account which is which is denominated in the CBDC variant of the national currency and vice versa, and being able to access the CBDC account both from card as well as banking".* The concept of interoperability from a user perspective was not identified in the analysis of the interview data discussed earlier.

Furthermore, the webinar results show that interoperability between different blockchains can also be considered to refer to interoperability at the smart contract level. Interoperability at this level involves communication in which data is shared between programmable smart contracts located on different blockchain platforms. This is inferred from the following quote from W4: *"We have come up with a set of abstraction that we think capture what it means for blockchain to talk to one another to authenticate data packets from other blockchain such that applications which you might think of a smart contracts or modules on one blockchain can talk to application, smart contracts or module son anther blockchain and vice versa".* Webinar W9 corroborates this as follows: *"Another topic is also the integration and exchange*

of logic and tokens. So a lot of smart contracts are the business logic that has been automated as code so think of two different blockchain networks where the logic is stored in one certain way in one network and completely different in the other network. So that is also something that has to be translated like two languages so that they can communicate with each other”.

Another form of interoperability identified from the analysis concerns interoperability between blockchain systems and existing enterprise systems. However, it is worth mentioning that this form of interoperability was not identified or mentioned in the majority of the webinars. Only three webinars, W6, W12, and W13, referred to the need for interoperability between blockchain and existing systems. The presenters in W12 argued that the focus on interoperability should not be blockchain-to-blockchain interoperability alone, but interoperability between blockchain systems and existing enterprise systems should also be considered. For example, in W12, the presenters stated that *“what we want is an ideal way for doing interoperability [...] So what we are doing is enabling the ability to have interoperability with the existing enterprise systems with the blockchain systems. We are complementing all the different blockchains and we’re complementing how they interoperate, how they work with existing enterprise systems”*. The statement above was corroborated in W13; in which it was stated that *“you need to harness the enterprise blockchain for the incumbent. It needs to be built into the existing economic systems that we have. It needs to be built into the existing processes that the incumbent, the current participants in the market are already focusing or already have built the processes around”*. Similarly, in W6, it was discussed that facilitating blockchain-to-legacy interoperability may also be required, particularly in the context of CBDCs, ERP and accounting systems. In the case of CBDCs, it was stated that: *“we need to look at how does this effect within the overall national payment systems, the overall national payment systems consist of different systems. It consists of both systems which are used for wholesale payments which are used for supporting functioning of financial markets, [...]and these has (sic) different users, individuals, business and the government, and there a potentially different systems involved and CBDC is going to fit into this national system and have very important linkages with other systems.”* On the other hand, blockchain-to-legacy interoperability in the context of ERP and accounting systems is alluded to in the following quote from W6: *“But there is clear business-to-business implications also for interoperability, with particularly with respect to*

being able to share the data which is underpinning the commercial transaction. So there are integrations with the ERP systems, they have international accounting systems”.

The findings above regarding the types of interoperability required for blockchain systems in banking enterprises confirm the findings from the interviews, except for the concept of interoperability from the user perspective. The respective findings from the interview and webinar data agree regarding the main types of interoperability that should be considered in relation to blockchain interoperability in the banking context. However, there is a difference in terms of the perspective of blockchain-to-legacy interoperability. As mentioned earlier, the results from the webinar indicated an additional perspective of blockchain-to-legacy interoperability, which suggests that interoperability in CBDCs should include a user perspective in addition to the system perspective. Table 8-7 shows a comparative analysis of the findings obtained from the interviews and the webinars for the current theme.

Table 8-7 Comparison of key findings of interviews and webinars for Theme 1

Types of interoperability from Interviews	Types of interoperability from Webinars
1. Blockchain-to-blockchain interoperability	1. Blockchain-to-blockchain Interoperability
Sub-types: <ol style="list-style-type: none"> 1. Interoperability between different blockchain platforms 2. Interoperability between digital assets 3. Data interoperability (between different types of data formats) 4. Interoperability between smart contracts 	Sub-types: <ul style="list-style-type: none"> • Interoperability between blockchains (platforms in general) • Interoperability between digital assets (cryptocurrencies and tokens) • CBDC interoperability (CBDC to CBDC) • Interoperability at smart contract level
2. Blockchain-to-legacy interoperability	2. Blockchain-to-legacy interoperability
<ul style="list-style-type: none"> • Interoperability between blockchain systems and existing non-blockchain banking systems • Interoperability between blockchain based currencies (cryptocurrencies and/or CBDCs) and fiat currencies) 	<ul style="list-style-type: none"> • Interoperability between blockchain systems and existing non-blockchain banking systems e.g., ERP and accounting systems • Specifically highlighting interoperability between CBDCs • CBDCs includes user perspective interoperability which concerns interoperating CBDCs with current payment technologies that users use

8.4.2 Theme 2: Business perspective (business case)

The business perspective theme, as articulated in Chapter 7, concerns business considerations and aspects relating to enabling blockchain interoperability. The core idea of the theme is that the business case or use case for blockchain within the organisation determines the form of interoperability required and, thus, influences the choice of interoperability solution that is ultimately selected to enable interoperability.

Regarding the business aspects relating to blockchain interoperability, particularly the role of a use case / business case in influencing the choice of interoperability solution, the webinars indicate a different relationship between business cases or use cases and the

process of interoperability. Some webinars indicated that enabling blockchain interoperability might have certain business benefits but did not show how interoperability was influenced by the use case. For instance, in W12, it was reported that “*interoperability is the key to access other DLTS and other technologies, but also from a business perspective it gives new customers and new markets to transact with*”. Other webinars (W13) highlighted the need for enterprises to have a blockchain-centric business case, which makes economic sense, as illustrated by the following quote: “*And so technological wise the solution might be makes sense and blockchain technology can very well be used for that. But when it doesn’t make economic value, then the (sic) is very difficult to find an enterprise a business case behind*”. On the other hand, in W6, it was stated that one of the challenges relating to blockchain interoperability is the lack of business cases that support blockchain integration in organisations. It was argued in the webinar that organisations tend to disregard the importance of having a business case that supports blockchain interoperability. The argument is illustrated by the following quote: “*But I think we are underestimating is the lack of business case to invest in integration*”. The webinar went on to suggest that organisations should consider not only the technical aspects of interoperability but also the business aspects, as shown by the following quote: “*I think that’s an important element. Perhaps you’re underestimating that interoperability is not just about the technical infrastructure connectivity, but also the business rules behind it and then also the commercial model behind it*”.

Another business-related aspect of interoperability raised in some of the webinars relates to cross-organisational collaboration or interoperability. According to some of the webinars, cross-organisational collaboration can be achieved by leveraging blockchain technology and enabling interoperability between different blockchains across organisations. This was exemplified in W1, where it was stated: “*Think of whether the emphasis will be on primarily internal applications of blockchain [...] such as in the manufacturing setting an inter organisational application might make sense versus an inter-organisational setting [...] once you start thinking about inter organisational applications, you need cooperation whereas in an internal application you have more ability to use hierarchy.*” In addition, the webinars show that enabling interoperability between blockchains in cross-organisational collaboration requires organisations to consider several aspects, such as governance models, approaches and rules. In w13, it was stated that “*we often say blockchain is the*

network for trust and trust building it still need a certain kind of governance and rules that are defining how the trade and how the collaboration on the network on the enterprise solution is working". In addition, the webinars have further explained that establishing inter-organisational applications may require the collaborating organisations to agree on ways to encourage participation and protect the privacy of the data shared across organisational boundaries. W1 suggested that for *"inter organisational applications you need to create some form of incentive for collaboration as well as privacy protection"*. It was further stated in the webinar that incentives should be considered because *"to join in that blockchain into organisations applications are harder because you have to develop you know cooperation you have to decide governance of that into organisation blockchain"*.

The findings above from the webinars correlate with the findings from the systematic literature reviews and interviews in terms of the need to consider business aspects of interoperability. The webinar findings confirm the need for organisations to consider having a blockchain-centric and interoperability-centric business case to support blockchain interoperability. In addition, the webinars support the findings from the systematic literature review regarding the importance of considering the appropriate governance models and rules to facilitate cross-organisational interoperability or collaboration.

8.4.3 Theme 3: Legal and regulatory compliance

Regarding legal and regulatory issues relating to blockchain interoperability, the majority of the webinars did not provide any discussion on the relationship between legal and regulatory compliance and interoperability. Most of the webinars discussed legal and regulatory issues concerning blockchain technology overall, but no particular attention was given to regulatory considerations about blockchain interoperability. Nevertheless, some webinars highlighted the importance of regulation in driving the adoption and development of blockchain technology in organisations. For instance, in W2, it was suggested that *"one should not underestimate, particularly when talking about blockchain the importance of the legal framework. And it's true, I think, around the world that there are many feature of the legal framework, particularly as they apply to payments and cross border payments that weren't designed for blockchain. And it will be important for jurisdictions to think through these problems to consider amendments to legal frameworks that will accommodate the specific features of blockchain"*. Similar views were echoed in W12 where it was stated that *"the third*

important feature which I think is a key takeaway is that international cooperation and regulation is essential”.

The few webinars that referred to regulation in the context of blockchain interoperability reiterated the findings from the interviews, which suggested a need for the financial sector and other sectors using blockchain technology to review and amend current regulatory frameworks for blockchain technology. This view is represented in the following quote from W7, in response to a question asked in the webinar regarding hurdles that should be addressed to *“ensure interoperability from a legal framework perspective as opposed to a technical perspective”*. The quote suggests that regulators should relook and revise existing regulations to accommodate blockchain technology:

“That’s definitively one of the, I don’t want to called problems, but challenges that we’re facing. it’s kind of like a hen egg because you know, a lot of the things that are already into regulation obviously look at the status quo of things. And now if you’re if you’re venturing out into like new technologies, you really need to re-visit a lot of the this that have already been put down on paper.”

In another webinar (W8), several legal and regulatory considerations were suggested for blockchain interoperability concerning asset transfers (atomic swaps). Specifically, it is suggested that considerations should be made regarding who is liable in the case of loss during asset transfer processes. The presenters in W8 suggested that organisations have to *“think across legal operation compliance considerations... what is the liability model when you are doing for example lock and mint, yes in an interoperability model versus burn and mint, is it liability of protocol? Is it liability of user?”* It was further suggested that banking enterprises should consider the risks associated with exchanging digital assets across multiple chains. This is exemplified in the following quote: *“And how different models lead to different surfaces of risks, how we can manage and monitor them, so I think when you believe the world is multi chain you can’t ignore the surface area of risk.”*

Table 8-8 Comparison of key findings of interviews and webinars for Theme 3

Legal and regulatory findings from interviews	Legal and regulatory findings from webinars
1. Recommend development of new laws and regulations where necessary	1. Recommend amendment to existing legal and regulatory frameworks to cater for blockchain systems
2. Recommend amendments to existing laws to accommodate blockchain systems	2. Determine legal liability model for assets transfers
3. Recommend identification and selection of current laws and regulations that are applicable to blockchain systems Focusing on data privacy and protection laws Anti-money laundering and financial crime prevention laws	

8.4.4 Theme 4: Interoperability techniques

The analysis of the webinars revealed a number of techniques that can be applied to facilitate interoperability between blockchains and between blockchains and legacy systems.

Some webinars highlighted the use of protocols as a means to enable interoperability between different blockchain systems. For example, W3 discussed the use of a protocol referred to as the IBC protocol to enable the exchange of messages across blockchain systems: *“IBC is a reliable, ordered and authenticated protocol for relaying arbitrary messages between independent distribute[d] ledgers, so again pointing to this concept of a layer 0 proving interoperability and communication between different layer one distributed ledger networks”*. Similarly, W4 referred to using a cross-chain protocol as an alternative to bridges. The webinar states that *“the same protocol IBC intends to serve the same role in the ecosystem of many blockchains, it’s a protocol which different blockchain can implement, and modules on those blockchains can elect to speak and then use to talk to each other without any necessary case by case, you know, pairing or bridges between these*

two blockchains". The quote reiterates the role of protocols in facilitating interoperability and also suggests that bridges can also enable interoperability between blockchain systems.

The suggestion of using bridges to enable blockchain interoperability was supported in W9, where it was stated that *"you can bridge, you can create a bridge that's also something that we'll see across these different blockchain"*. However, W8 alluded that bridges as tools for enabling interoperability have poor security, as shown by the following quote: *"The question of interoperability really comes into play, if we assume that there gonna be many different chains out there, right, how are we gonna actually kind of be able to link those together in a secure way. You know the kind of situation with bridges and other things that happened"*.

Other techniques suggested in the webinars include techniques that use APIs to connect different blockchain systems and also to enable blockchain-to-legacy communication. In W8, it was suggested that *"you can have one to one API which connect the two"*. The webinars suggested sidechains and oracles as other techniques that could be utilised. For example, W8 suggested that *"you can have side chain or a blockchain in between which to talk to both, you can have an oracle of network which is what was used as part of this experiment where you don't rely on that centralised party for that Merkle root verification"*. Correspondingly, sidechains are discussed in W9, where they were referred to as cross chains. W9 stated that *"cross-chains helps like we understood so far it helps in enabling the exchange of value and information between various networks so that data from main chain to the cross chains or the side chains can be seamlessly interpreted between these chains which always go and connect to the main chain, or sometimes you can also choose to create a completely separate china out of it which the parent chain"*.

In addition to the techniques identified above, some webinars, W5 and W6, mentioned interlinking as a technique that could be used, particularly in the case of blockchain systems facilitating CBDC payments. Webinar W5 suggested three main approaches to interlinking, as shown in the following quote: *"There is (sic) three ways to achieve a link, it [is] either through a single access point, through technical bilateral links or through a hub and spoke which is really using a common hub, a common platform which is connecting different systems"*. W6, on the other hand, stated that *"there are different arrays which are possible, one is, in interlinkage where you interlink the systems and somehow exchange the message and handle the clearing. You could have one central system to which everybody connects,*

then you can have across membership which is basically about that one institution participates in multiple scheme or multiple systems and in that way you are able to bridge them”.

The findings above corroborate the findings obtained from the analysis of the interviews and the literature, except for the interlinking technique suggested in the webinars. Table 8-9 below shows a comparative summary of the findings from the webinars and interviews relating to the different techniques for enabling blockchain interoperability.

Table 8-9 Comparison of key findings of interviews and webinars for Theme 4

Interoperability techniques from interviews	Interoperability techniques from webinars
1. APIs <ul style="list-style-type: none"> • Blockchain-to-blockchain interoperability • For Blockchain-to-legacy interoperability 2. Oracles <ol style="list-style-type: none"> 1. Blockchain-to-legacy interoperability 	1. APIs <ul style="list-style-type: none"> • Blockchain-to-blockchain interoperability • For Blockchain-to-legacy interoperability 2. Oracles Blockchain-to-legacy interoperability
3. Bridges <ol style="list-style-type: none"> 2. Blockchain-to-blockchain interoperability 	3. Bridges <ol style="list-style-type: none"> 3. Blockchain-to-blockchain interoperability
4. Protocols <ol style="list-style-type: none"> 4. Blockchain-to-blockchain interoperability 	4. Protocols <ol style="list-style-type: none"> 5. Blockchain-to-blockchain interoperability
	5. Interlinking Blockchain-to-blockchain interoperability (context of CBDCs)

8.4.5 Theme 5: Properties of Interoperability Techniques

Concerning the properties and features the interoperability techniques/mechanisms should have to provide efficient interoperability, the webinars identified some key properties that should be considered when selecting interoperability mechanisms. However, the webinars also posited that the features were not universal and that varying mechanisms offer different features, which may be suitable in some cases and not in other cases. W8 stated “*there is*

a right answer to that, it depends on the trust assumption between the two systems and what level of resilience you are looking at”.

The first property relates to the security or trust property of the interoperability mechanism and the communicating systems. W10 highlighted security as the biggest concern and consideration for enabling blockchain interoperability. They argued that because different blockchains have different security models, connecting a secure blockchain to one with much lower security compromised the security of both systems. This is implied in the following quote from W10: *“if you’re connecting to a blockchain that’s weak, you will assume the weakness of that blockchain and this is one of the biggest concerns within information security circles”*. Furthermore, the webinars indicated that the security or trust property can be used to determine when and which mechanisms to apply. For example, in W8, it was stated that selecting the mechanism/technique to use is *“it’s all about what trust assumptions are required between those two chains, if both your chains are very highly trusted then maybe your trust assumption are lower and API s more cost effective, faster way of operating”*. This quote implies that APIs are a reliable solution to use when the communication system are secure and trustworthy. A similar statement was made regarding sidechains: *“side chains primarily is suited for applications where there’s are low level security threats”* (W9).

The other feature or property identified from the webinars relates to provenance, which refers to the process that determines the history of a data product, starting from its original sources (Simmhan et al., 2005). In the context of blockchain interoperability, provenance means that the receiving blockchain should be able to validate and verify the received data. W8 stated that in cases where provenance was required, oracles can be used to facilitate interoperability: *“Whereas if you want to have a model where there’s a decentralised network which guarantees the provenance of message and the merkle route across the network. Then maybe an oracle based network which is used in this design is more appropriate.”*

In addition, the webinars mentioned throughput as another characteristic that should be considered when selecting an interoperability solution or mechanism. Throughput in this context implies the number of transactions that can be processed/transferred in a second. W9 mentioned that *“if you want higher throughput while also creating a more secure system, we can use multi chains or parallel chains”*.

Table 8-10 Comparison of key findings of interviews and webinars for Theme 5

Characteristics of interoperability mechanism from interviews	Characteristics of interoperability mechanism from webinars
<ol style="list-style-type: none"> 1. Mechanism should ensure the security and privacy of data 2. Should not compromise the security of underlying blockchains 	<ol style="list-style-type: none"> 1. Mechanism to ensure security and privacy of data
	<ol style="list-style-type: none"> 2. Provenance of data <ul style="list-style-type: none"> • Mechanism should ensure/provide a means to validate and verify data

8.4.6 Theme 6: Data

The findings from the webinars regarding data indicated that organisations seeking to interoperate their systems with blockchain systems have to consider the type of data to be shared and the method and approach of exchanging the data. This was highlighted in W13: *“When they want to exchange the data through the blockchain, then you know they (sic) typical way to [to] is each company puts their data on the blockchain [...] they put the rules of how, what kind of information can be exchanged, how they exchange, some backup rules”*.

The webinars identified primary forms of data that may be exchanged by enabling blockchain interoperability. The data from the webinars indicated that enabling interoperability between blockchain systems and other enterprise systems was required mainly to facilitate the exchange of two forms of data: digital assets and arbitrary messages (data). For example, W4 explained that *“users have their assets and data locked up in different silos at different blockchain, we need a way to connect it to allow this Cambrian explosion of blockchain and protocol to flourish [...] such that people can try out and experiment with different ideas but still allow users to move their assets and data around as new blockchains and protocols are developed with better rules”*.

In the webinars, digital assets mainly denoted digital currencies and tokenised assets, whereby digital currencies represent native currencies used as incentives on the various blockchain systems or refer to central bank digital currencies. This distinction of digital currencies is deduced from the following quote extracted from W7: *“We wanna have, you know, instant and frictionless payments and that to be really smooth whether it’s with a CBDC or whether it’s with some other form of digital currency”*.

Conversely, tokenised assets represent digital forms of real-life assets stored on the blockchain. Tokenised assets may also require to be exchanged across different systems as alluded to in the following quote from W1: *“I think there are also some issues with tokenisation, particularly when you don’t have native tokens inside a blockchain, but when you have assets outside the blockchain, real assets which are being tokenised and then introduced into the blockchain for transacting between the various network nodes”*.

Other issues raised in the webinars regarding data, included issues around governance of data, privacy issues and data formats. In W1, it was stated that when data is shared across different blockchain systems, decisions have to be made regarding the governance of that data. Specifically, W1 suggested that decisions have to be made regarding *“who is going to control what data is seen, by who”*. A similar statement was made in W13 regarding the importance of considering the privacy and ownership aspects of the data shared across blockchain systems. W13 stated that *“aspects of privacy and data ownership are also quite important and probably more relevant, so speaking of our customers, we wanted to ensure their privacy and their sovereignty, there the decision to share the data to whom they were sharing and when”*. Regarding data formats, the W5 indicated that *“if you want to build some interoperability or single system, and each country has different rules when it come to data sharing, that might be challenging to overcome [...] and having some minimum data standards to ensure that if you are paying form one CBDC country network to another you have the data required in the beneficiary network, because they may have different requirements”*. This implies the need for banking organisations to agree on data formats used during interoperability, particularly where the data will be shared across organisational or national boundaries.

The findings discussed above relate to the types of data banking organisations may be required to exchange across blockchain systems and the privacy requirements that should

be fulfilled align with the findings from the literature and interviews. In addition, the webinars highlighted data governance as an additional aspect that should be considered, particularly when multiple organisations are involved. However, the webinars did not provide sufficient detail regarding how the privacy and security requirements should be met.

Table 8-11 Comparison of key findings of interviews and webinars for Theme 6

Data aspects from interviews	Data aspects from webinars
3. Types of data identified <ul style="list-style-type: none"> • Contextual business data • Digital assets (cryptocurrencies, CBDCs and digital assets) 	2. Types of data identified <ul style="list-style-type: none"> • Arbitrary data • Digital assets (e.g., cryptocurrencies, including CBDCs and tokenised assets)
2. Data privacy and security <ul style="list-style-type: none"> • Identify relevant data privacy laws and regulations • Implement privacy and security measures and control 	3. Data privacy and security <ul style="list-style-type: none"> • Identifying and developing measure to ensure the privacy and security of shared data
3. Data standardisation <ul style="list-style-type: none"> • Standardised data formats 	3. Data standardisation <ul style="list-style-type: none"> • Standardised data formats • Standardised data ontologies
	4. Data governance in cross-organisational interoperability scenarios <ul style="list-style-type: none"> • Who controls what data are shared and how its shared and protected

8.4.7 Interoperability through standardisation

The standardisation of data across heterogeneous systems has been widely reported as a prominent aspect in many studies on interoperability. Similarly, the systematic literature reviews and the results from the interview data indicated the standardisation of data formats as a fundamental requirement for enabling blockchain interoperability. The analysis of the

webinars corroborated the above-mentioned findings and showed how standards can enable interoperability in blockchain systems.

The webinars demonstrated different ways standardisation enables data interoperability (semantic interoperability) across blockchain systems. For example, W4 discussed an approach in which data packets are standardised across smart contracts and modules on different blockchain systems. They suggest the approach can enable *“people writing contracts on different or modules on different blockchains and the interchange. Can standardise on certain packet formats for certain tasks like sending tokens, collateralising, stable coins, making cross contract calls, voting and governance systems, that sort of thing”*. Conversely, W3 alluded to the concept of using standardised ontologies for digital assets to enable the exchange of the assets between heterogeneous blockchains, as reflected in the following quote: *“...we’re working on is basically a standards based. Ontology of digital currencies that will help to sort of define these sort of interrupt technical interoperability points, points of contact and so on”*. As a testament to the idea that standardisation is important to enabling blockchain interoperability, W5 also highlighted ongoing work in developing standards for interoperability focusing on standardising data representations, storage and exchange, alluded to in the quote stating: *“Standardisation body that is working on creating an interoperability standard for blockchain where they try to build something based on the semantics of how you store data, how you name them and how you could share them?”*.

Furthermore, the webinars suggested that existing standards should be amended to accommodate digital assets shared on the blockchains. W2 stated that *“they actually amended the standard to provide for more comprehensive coverage of crypto assets”*. Similarly, in W9, it was stated that *“if there are things that already work really well, then we should look to reuse them. And that was, you know, one of the reasons in the solution for example uses ISO 2082 as the common language for payments, because everybody's been really heavily invested in it”*. Hence, organisations should consider re-using and customising existing standards to accommodate new forms of data sharing over blockchain systems.

Table 8-12 Comparison of key findings of interviews and webinars for Theme 7

Standardisation issues from interviews	Data aspects from webinars
<ol style="list-style-type: none"> 1. Develop new standards for blockchain systems 2. Standardisation of data formats 3. Standardised interfaces 	<ol style="list-style-type: none"> 1. Standardisation of data formats 2. Standardised data ontologies 3. Re-use and customisation of existing data standards

8.5 INSIGHTS FROM WEBINAR DATA

Overall, the findings from the webinar data analysis confirmed the findings obtained from the earlier analysis of the interview data and the findings from the systematic literature reviews. However, some additional insights can be drawn from the webinar results. One of the key insights pertains to data governance. The webinars indicated that organisations involved in cross-organisational interactions involving blockchain technology should agree on the rules governing what data is shared, who controls what data, and who is responsible for handling the security and privacy of the shared data. Another key consideration raised in the webinars concerned legal accountability. It was suggested in the webinars that organisations should consider and select an accountability model relevant to the needs of the organisations involved in a blockchain-enabled cross-organisation collaboration. It was further suggested that in selecting the relevant model, organisations should consider the risks associated with the selected model.

The findings regarding the need for governance rules in cross-organisational collaborations are in line with the existing literature on inter-organisational collaboration. Van den Broek and van Veenstra (2015) assert that in data collaboration arrangements where data is shared across multiple organisations, governance structures are often required to mitigate risks relating to sharing data across organisational boundaries. Developing the required

governance structures calls for organisations to decide jointly to establish “data protocols and data exchanges and reporting mechanisms” (Bertot & Choi, 2013). Furthermore, (Van den Broek & van Veenstra, 2015) agree with the webinar findings on the need to identify an appropriate governance model. The authors further state that organisations involved in a data collaboration arrangement must decide collectively on the governance model to use. Organisations can opt for traditional governance models that enable data control to remain with the respective organisations or a model in which data is controlled by a dominant organisation. The selection of the model can also be based on the type of coordination mechanisms required, such as contracts, trust-based, data quality or the dominant partner being in charge of the coordination (Van den Broek & van Veenstra, 2015).

In the context of blockchain technology, organisations may select models that balance the decentralised features of blockchain with the traditional central governance models used in organisations. The World Economic Forum (2020) proposed models: the business governance model and the operational governance model. The business governance model “includes the formation of a legal person or an agreement between various members” and requires well-defined legal frameworks and compatible governance models across organisations. The legal framework should include rules to determine “who is the owner of the network and data, who is the processor and responsible for the information, who controls the information, and which jurisdiction are disputes applied and who owns and manage[s] the shared infrastructure” (World Economic Forum, 2020). The operational model concerns establishing standards and information security measures using blockchain and focuses on defining the rules governing how new participants join the network and how and by whom they are approved. It also includes defining standards and rules for data exchange and storage considering legal requirements (World Economic Forum, 2020).

The insights from the webinars and the additional information from the literature discussed above were used to identify the following elements included in the proposed framework. Table 8-13 highlights the additional framework elements, as suggested in the webinars. The Legal (environment) component of the framework was updated to include the accountability model, as illustrated in the revised framework shown in Figure 8-11. The new element is indicated with an asterisk (*). The other suggestions were not added to the architectural component framework in Figure 8-11 but were included in the guidelines in Figure 8-12.

Table 8-13 Additional elements obtained from the webinars

Element	Framework component updated
<p>Selection of governance model</p> <p>Considerations to make:</p> <ul style="list-style-type: none"> • Determine the required level of centralisation or decentralisation of model • Determine rules for joining (incentives or no incentives) • Determine rules for data ownership, data exchange • Determine accountability model 	<p>Business Component and Legal component</p>

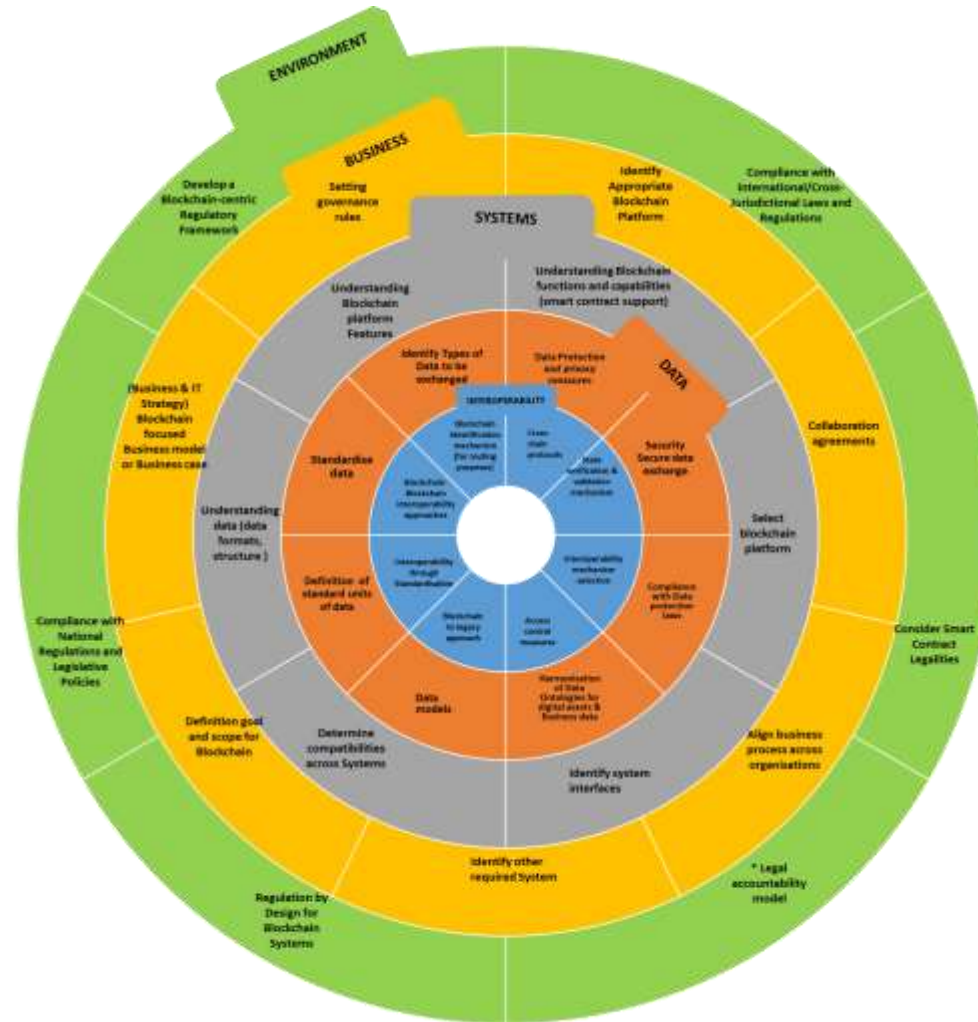


Figure 8-11 The EBI architectural component framework revised from webinar data

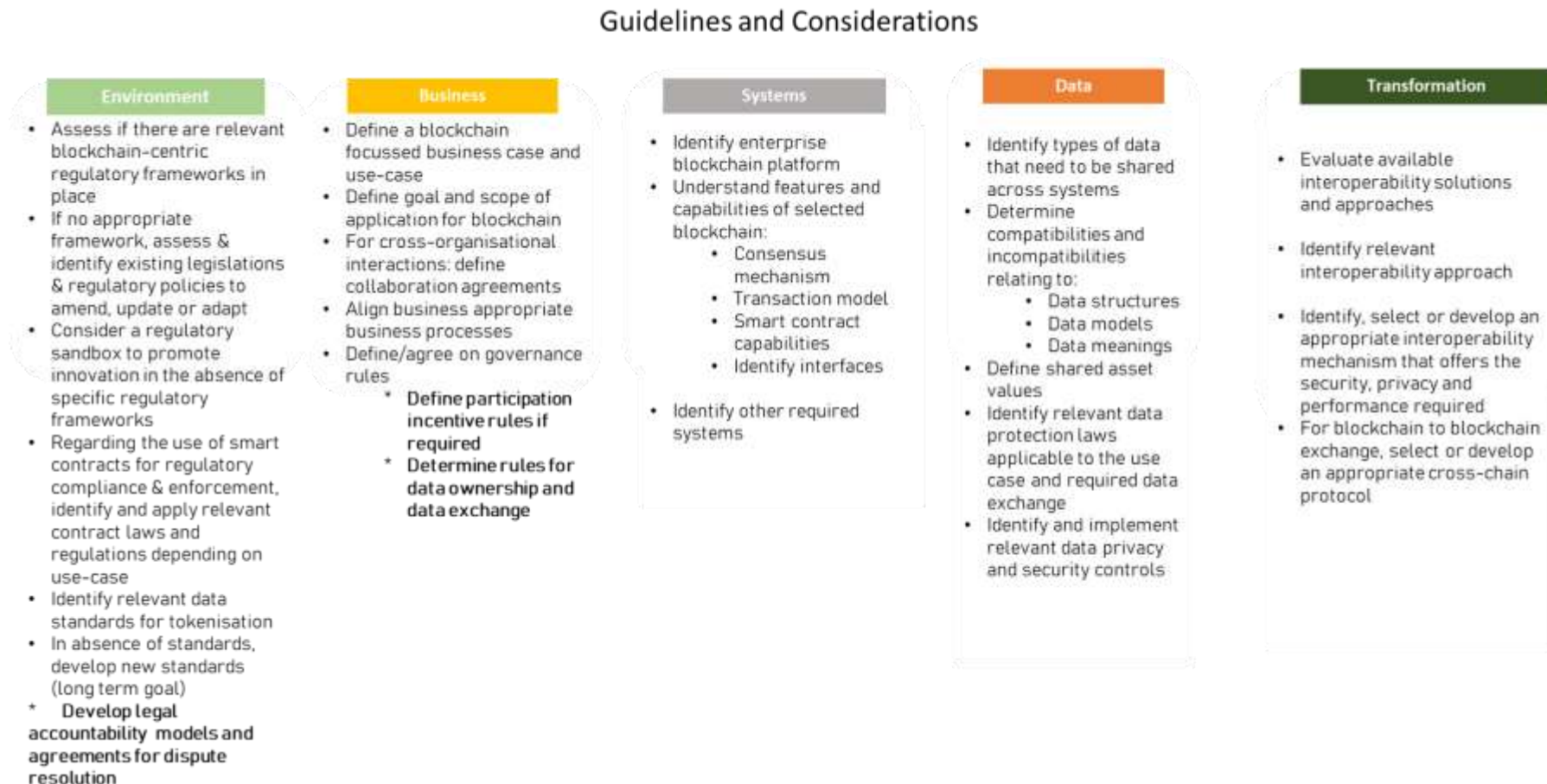


Figure 8-12 Revised guidelines and considerations per webinar data

8.6 EXPLANATION OF FRAMEWORK

8.6.1 Framework Components

The Enterprise blockchain interoperability framework (EBI) consists of five main components (see Figure 8-8). The first component denotes the external environment representing the banking industry overall, as well as the regulatory environment, which influences how banking institutions operate. The environment provides inputs in the form of regulatory policies, which are, in turn, used to guide internal business processes and decisions. The external environment specifically indicates that enterprises must consider regulatory issues relating to blockchain interoperability. This includes defining blockchain-centric regulatory frameworks as well as short-term considerations to identify the appropriate regulations and regulatory considerations that must be accounted for to enable blockchain interoperability in enterprise settings. The second component represents the business aspects informing how the blockchain interoperability process should be handled within the business. In particular, the business component represents the business considerations and guidelines concerning interoperating blockchain technology into the business. A systems component is included within the business component, representing the ICT systems used in the organisation and the associated system considerations regarding blockchain interoperability in the organisation. The next component is the data component. The data component signifies all the data-related aspects organisations must consider for interoperating blockchain technology with other systems. The interoperability component shows the technical considerations for interoperability, which include consideration of the interoperability approach, the interoperability mechanism, the communication protocol and privacy, security considerations and other technical aspects related to enabling the efficient exchange of data between blockchain systems and other systems.

The blockchain interoperability process flow framework in Figure 8-9 includes the components outlined in Section 8.3.1 and illustrates how the respective components interrelate. In addition, the framework outlines the interoperability process steps banking enterprises should follow to facilitate blockchain interoperability.

The first step concerns the business component. In this step, an organisation is required to define a blockchain-centric business case or identify a specific business goal for adopting blockchain technology. The business case and use case play a fundamental role in guiding the decisions an organisation can make during the interoperation process. A clearly defined business case and use case for blockchain determine the scope of the application of the technology within the organisation. That is, they determine where within the business the technology is used, what it is used for, and thereby determine what other systems it would interact with and, consequently, what interactions are required and how that would be achieved.

In essence, the business component influences the systems component. Specifically, through the business case and use case, an organisation can identify the type of blockchain suited for the case, other systems involved and whether the selected blockchain is interoperated with internal systems of the organisation or externally, across organisational boundaries. For an internal case, the organisation has to identify existing systems required to exchange data with the new blockchain systems. These systems could be existing legacy systems, such as core banking systems, ERP, payment systems or other blockchain systems. Alternatively, external interoperation may be required when two organisations are involved in a strategic collaboration, which is enabled through blockchain technology. This could be the case, for example, in interbank settlement arrangements. Achieving external interoperability may require the involved institutions to have a blockchain-centric collaboration agreement in place to outline the business processes to be aligned, the types of blockchain systems involved, the data to be shared, governance rules, the degree of centralisation or decentralisation required, and incentive rules, if any. The collaboration agreements are guided by the appropriate contractual laws or regulations emanating from the environment.

After identifying the systems, the organisation needs to identify the data to be shared. The data considerations form part of the data component. Regarding the data component, the organisation must identify the type of data to be shared across systems, understand how the data is stored and formatted as regards each system, and identify any incompatibilities that may hinder interoperability. The data component and its associated steps are influenced by the external regulatory environment, which requires organisations to comply with data privacy and protection regulations. Therefore, organisations have to comply with the relevant

data protection laws to guide decisions regarding what data are exchanged and how that data are exchanged. Once the data have been identified, the next step is to determine appropriate ways of exchanging the data across the identified systems. The process of selecting the appropriate ways to exchange the data is represented by the interoperability component.

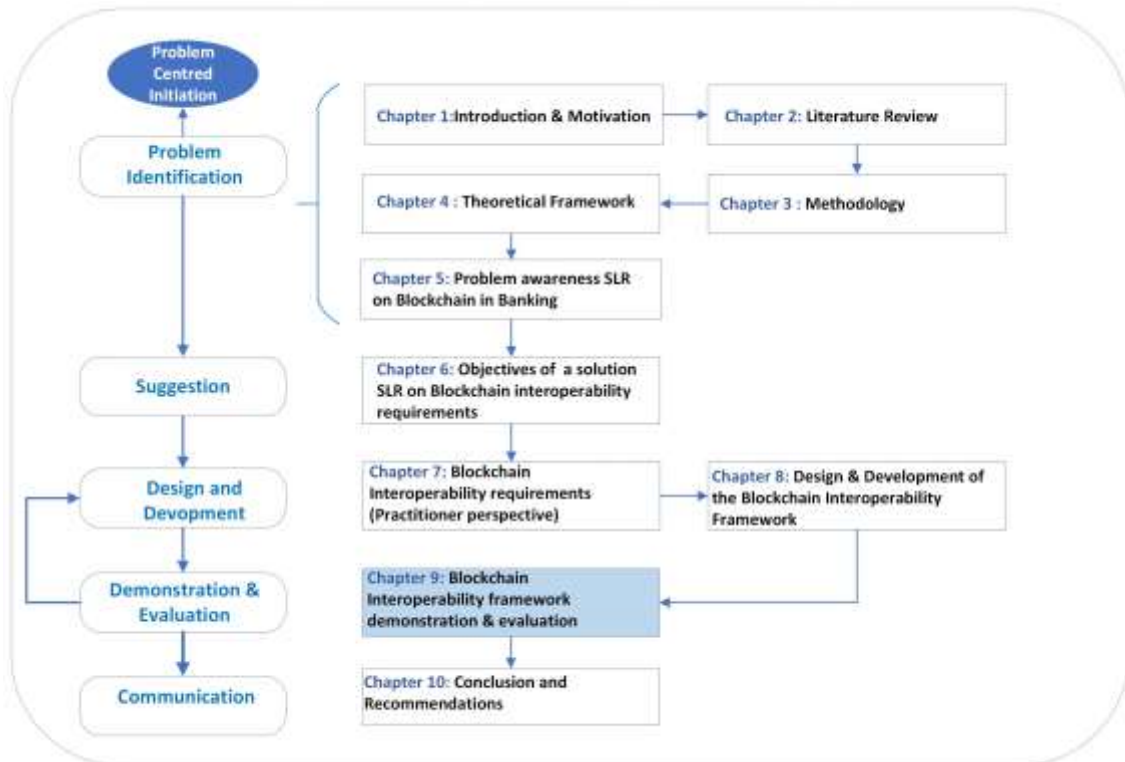
The interoperability component represents aspects relating to the technical means used to enable interoperability. The component encompasses processes to determine the appropriate interoperability solution for the type of interoperability required. The process requires organisations to identify the interoperability mechanisms. This process requires institutions to familiarise themselves with existing mechanisms and understand the available options in terms of their capabilities, strengths and weaknesses. For blockchain-to-blockchain interoperability, the process involves understanding the capabilities, benefits and limitations of available mechanisms, such as third-party solutions, notaries, and sidechains, juxtaposed with developing a custom mechanism. On the other hand, for blockchain-to-legacy, the process would involve comparing the capabilities, benefits and weaknesses of mechanisms, including APIs, oracles, blockchain services and middleware solutions. In addition, the component includes considerations for selecting or developing an appropriate cross-chain communication protocol to facilitate the data exchange between different blockchain platforms. Furthermore, decisions regarding security and privacy measures and how they are implemented, as well as decisions relating to how the data exchange is validated and verified, are included in the component.

8.7 SUMMARY

Chapter 8 narrated the process that was followed to construct the proposed EBI framework. The chapter demonstrated how the System theory elements were applied to conceptualise the framework. The chapter further discussed details of the two cycles of development that were followed. Specifically, it explained how the findings from the interviews and systematic literature reviews were conceptualised to construct the framework in cycle 1. The chapter further explained the findings from the deductive content analysis of webinars and how they were applied in the construction of the framework as part of cycle 2. The chapter concluded with an explanation of the proposed framework.

CHAPTER 9

9 DEMONSTRATION AND EVALUATION



9.1 INTRODUCTION

Chapter 9 presents the methods adopted to demonstrate and evaluate the proposed EBI framework. The chapter commences with an overview of artefact evaluations in design science research and an overview of the evaluation approach used to evaluate the EBI framework. The chapter presents two evaluation approaches: Using an illustrative scenario to demonstrate the applicability of the framework, followed by the application of expert evaluation (expert interview) of the framework.

9.2 ARTEFACT EVALUATION IN DESIGN SCIENCE RESEARCH

Design science research consists of two core activities: the construction (build) activity and the evaluation activity. Conducting evaluations is vital to producing rigorous design science research (March & Smith, 1995) and can assist in providing feedback for further development of artefacts (Venable et al., 2016). Evaluations in DSR focus on the evaluation

of two main design science research outputs: design artefacts (March & Smith, 1995) and design theories, which are identified as upper-level types of artefacts (Gregor & Hevner, 2013). Generally, the key purpose of evaluation in design science is to determine how well an artefact solves a contextual problem (Peppers et al., 2007). However, evaluations in design science research also serve various other purposes. Venable et al. (2012) outlined five purposes for evaluation in DSR: 1) evaluate a design artefact's utility and efficacy (or lack of) for achieving its goal; 2) evaluate formal knowledge about the artefact's utility for achieving its goals; 3) evaluate a designed artefact or formalised knowledge about it in comparison to other designed artefacts' ability to achieve a similar purpose; 4) evaluate a designed artefact or formalised knowledge about it for side effects or undesirable consequences of its use; and 5) evaluate a designed artefact formatively to identify weaknesses and areas of improvement for an artefact under development. "Regardless of the purpose of evaluation, artefacts should be "evaluated based on criteria derived from the requirements of the context in which the artefact will be implemented" (Coetzee, 2019, p. 291). Exemplary comprehensive evaluation criteria were proposed by (March & Smith, 1995), i.e., the evaluation criteria are based on the type of artefact being evaluated. Other scholars have also provided some criteria for evaluating design artefacts (Aier & Fischer, 2011; Rosemann & Vessey, 2008). The criteria put forward by Aier and Fischer (2011) are specifically for evaluating design theories, while that by Rosemann and Vessey (2008) are designed to evaluate the applicability of design science outputs. This study adopted the criteria proposed by (Prat et al., 2014), shown in Figure 9-3.

Evaluating design science artefacts can follow different strategies and methods, depending on the type of artefact and the functional purpose of the artefact being evaluated (Venable et al., 2016). Venable (2006) classified DSR evaluation approaches into two primary categories: artificial and naturalistic evaluation. Artificial evaluation evaluates an artefact in a contrived manner, and naturalistic evaluation appraises the performance of an artefact in its real context or setting and using real users. (Pries-Heje et al., 2008). Evaluations have also been categorised based on when they are conducted. For example, Pries-Heje et al. (2008) categorised evaluation strategies based on two dimensions: ex-ante vs post-ante and naturalistic vs artificial. Ex-ante evaluates artefacts before they are developed and ex-post after development.

Artificial evaluation methods include laboratory and field experiments, simulations, criteria-based analysis, theoretical arguments, and mathematical proofs. Naturalistic methods include case studies, field studies, surveys, ethnography, phenomenology, hermeneutic methods, and action research. Similarly, Peffers et al. (2012) provide a broader taxonomy of evaluation methods, which includes logical argument, expert evaluation, technical experiments, subject-based experiments, action research, prototypes, case studies and illustrative scenarios. Venable et al. (2012) propose an evaluation method selection framework, which highlights some of the appropriate methods that can be used in different evaluation strategies (see Figure 9-1).

DSR evaluation method selection	Ex-ante	Ex-Post
Naturalistic	Action research Focus groups	Action research Case study Focus groups Ethnography Phenomenology Surveys (qualitative and quantitative)
Artificial	Mathematical or logical proof Criteria based evaluation Lab experiment Computer simulation	Mathematical or logical proof Lab experiments Role-playing simulation Computer simulation Field experiments

Figure 9-1 Evaluation method selection framework (adapted from Venable et al., 2012)

According to Pries-Heje et al. (2008) and Venable et al. (2012), the selection of the appropriate evaluation strategy, method and corresponding evaluation criteria should be guided by the type of artefact and the purpose of the evaluation. Where relevant, the researcher can leverage strengths from multiple evaluation methods that combine artificial and naturalistic evaluation as well as positivist and interpretive evaluation methods to provide a more pluralist view of the research.

9.2.1 The Evaluation Approach in This Study

In this study, the evaluation strategy followed the artificial *ex-post* evaluation strategy conducted in two phases (demonstration and evaluation phases) to assess the proposed blockchain interoperability framework. Artificial evaluations have been used in several DSR studies to evaluate various forms of DSR artefacts. Artificial evaluations can either be empirical or non-empirical, with the empirical approach bringing the benefit of scientific reliability through its improved repeatability and protection against falsifiability (Baskerville et al., 2015). The evaluation strategy used in this study is considered artificial because it does not include all three realities of "a real organisation, on real tasks and real users" defined by (Venable, 2006); rather, the framework was evaluated using real users (experts) and illustrative scenarios but not in a real organisational setting. The artificial strategy was selected due to the sensitivity of the banking context regarding innovations and new projects. Blockchain technology is still a relatively new technology in the banking sector; consequently, the majority of banks engaging in blockchain projects are still very secretive to protect intellectual property and maintain a competitive advantage over their counterparts. For this reason, the researcher could not access a real organisation and specific tasks to facilitate the evaluation; hence, the selection of the artificial evaluation strategy. However, the researcher believes that the one-on-one interview with blockchain experts from the sector brought contextual experience and insights to assist in evaluating the framework.

The methods applied for evaluation were expert evaluations and realistic illustrative scenarios. Expert evaluations and realistic illustrative scenarios are some of the evaluation methods used in IS studies to evaluate frameworks (Peffer et al., 2012). "Expert evaluations are assessments of an artefact by one or more experts" (Peffer et al., 2012, p. 5). Conversely, illustrative scenarios are the "application of an artefact to a synthetic or real-world situation aimed at illustrating suitability or utility of the artefact" (Peffer et al., 2012, p. 5). Figure 9-2 provides a summary of the evaluation approach applied in the current study, drawing from the evaluation method selection framework (Venable et al., 2012) and the framework for evaluation in design science (FEDS) (Venable et al., 2016).

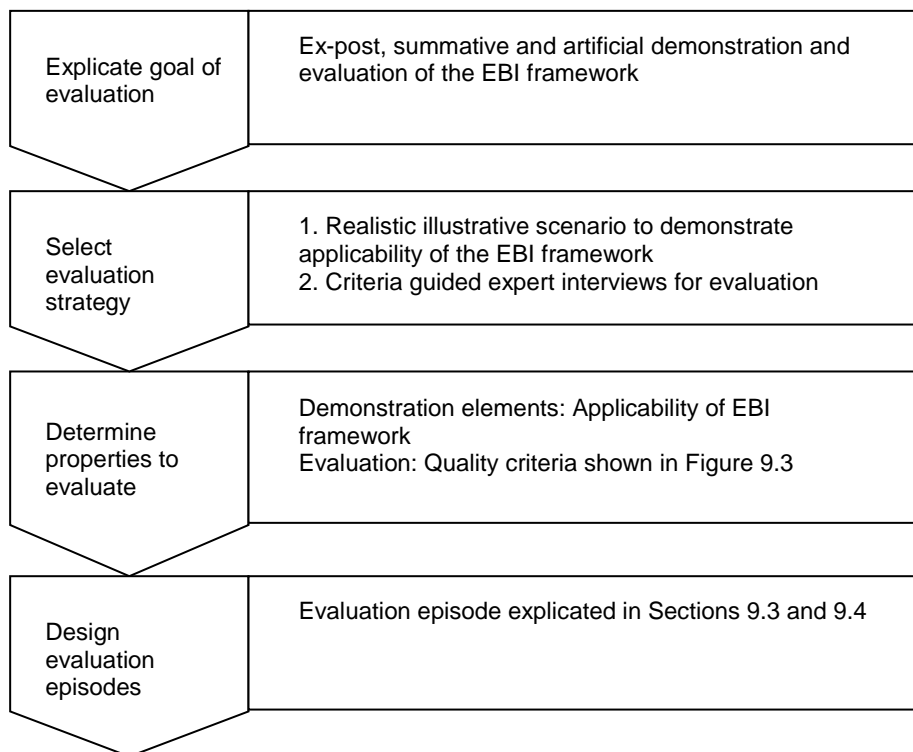


Figure 9-2 Summary of evaluation methods used to evaluate the EBI Framework in this study

In this study, the type of expert evaluation used was one-on-one expert interviews. The researcher selected one-on-one expert interviews over alternatives like focus groups and the Delphi techniques because the interviews have the advantage of generating more data from each interviewee compared to the alternatives, and the resultant data are not influenced by group opinions, as is the case with focus groups and the Delphi technique (Elmer et al., 2010). One-on-one interviews were also selected because they did not require all participants to be available simultaneously, which encouraged participation and simplified scheduling. The expert evaluations were operationalised using the evaluation criterion by (Prat et al., 2014) (shown in Figure 9-3). Not all criteria applied to the evaluation adopted strategy; only the highlighted criteria were selected. The criteria were used to guide the formulation of questions for the expert interview questionnaire (see APPENDIX B).

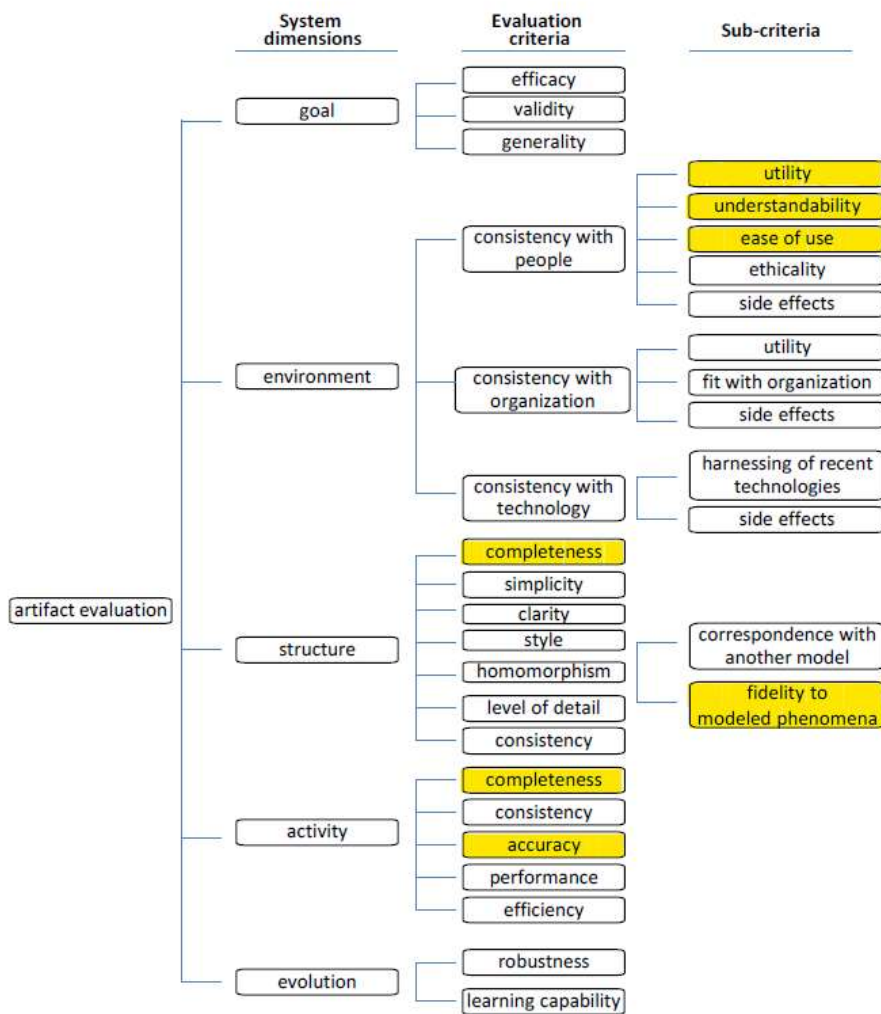


Figure 9-3 Hierarchy of criteria of IS artefact evaluation (adapted from Prat et al.,2014)

Scenario-based evaluations are techniques focusing on using scenarios to reflect on user experiences or assess the applicability of a system (Lampasona et al., 2014). Scenario-based evaluations are effective in evaluating various IS and IT artefacts, software architecture (Babar & Gorton, 2004), human–computer interaction (Varsaluoma, 2009), and document access control systems (Clausner et al., 2011). Scenario-based testing is a scenario-based evaluation technique typically used in software testing to evaluate software artefacts. The scenario-based testing approach evaluates artefacts using scenarios, which are "hypothetical stories used to help a person think through a complex problem" (Cem Kaner, 2003). Scenarios are brief descriptions of concrete, realistic situations (Kim, 2012) representing how an application will function (Nyakundi et al., 2023). Scenarios can be case

stories, case simulations, hypothetical scenarios, tasks or situation scenarios. In scenario-based testing, the tester assumes the role of the end-user and identifies realistic scenarios or use cases which can be applied to the systems or artefacts.

Scenario-based testing has the advantage of enabling the evaluation of specific system features and also allows for evaluation focusing on contextual user interactions. In addition, scenarios have the potential to reduce the effort and expense associated with more immersive approaches, such as field studies and ethnography, because scenarios allow for the focus to be on specific points of evaluation. Scenarios can allow for broader test coverage by enabling testing to be conducted on all parts of functionalities of the system under evaluation with a measurable objective (Mirza et al., 2021). This study borrows from the scenario-based testing approach to demonstrate the applicability or functionality of the proposed EBI framework.

9.3 DEMONSTRATION OF THE EBI FRAMEWORK USING AN ILLUSTRATIVE SCENARIO

This section explicates the application of the EBI framework to a realistic banking use case scenario involving the interoperability of blockchain (DLTs) to a real-time gross settlement (RTGS) system. The use case was informed by evidence from real-life projects, such as Project Khoka 1 by the South African Reserve Bank, Project Meridian by the Bank of England and an industry project between Accenture, R3 Consortium and SAP, which focused on integrating RTGS with blockchain ledgers. The following discussion provides an overview of the aforementioned projects.

9.3.1 Overview of Project Khoka

Project Khoka was a collaborative project between the South African Reserve Bank and a consortium of seven retail banks in South Africa. The main purpose of the project was to develop a proof of concept wholesale payments system for interbank settlements by leveraging blockchain technology. The scope of Project Khoka was to create a "distributed ledger between participating banks for a wholesale payment system, backed by central-bank deposits, allowing participating banks to pledge, redeem and track balances of the tokenised rand on the ledger" (South African Reserve Bank, 2018, p. 22). Specifically, the

project was undertaken to demonstrate real-time wholesale payment clearing and settlement on a distributed ledger.

In South Africa, wholesale payments clearing and settlements between banks are typically facilitated by the SAMOS system. The SAMOS system is a South African real-time gross settlement system. The SAMOS system is provided by the SARB and connected to various banks, clearing systems and operators, as depicted in Figure 9-4. Project Khoka simulated SAMOS functions on a distributed ledger to understand how SAMOS processes could operate on the distributed ledger. However, according to the SARB, there is currently no intention to overhaul SAMOS and replace it with DLTs; rather, the SARB intends to integrate DLTs with the existing SAMOS systems. However, the challenge with an arrangement in which DLTs co-exist with the existing SAMOS system is that this arrangement introduces implementation challenges and complexities related to interoperability and enabling these two systems to communicate with each other and other legacy systems (South African Reserve Bank, 2018).



Figure 9-4 Overview of the RTGS payment process for the SAMOS systems (adapted from South African Reserve Bank, 2018)

9.3.2 Overview of Project Meridian

Project Meridian was an experimental effort by the Bank of England and the Bank of International Settlement's Innovation Hub in London, which explored the interlinking of digital asset ledger (DLTs) with RTGS systems. The primary purpose of Project Meridian was to "develop functionality that facilitates synchronised settlement for digital assets using central bank money" (Bank of England, 2023, p. 3). The project involved integrating a DLT with secure RTGS and other centralised systems using open-standard application programming interfaces (APIs). The project enables synchronised settlements of assets through a synchronisation operator, which coordinates the conditional settlement between an RTGS system and a payment or asset ledger or DLT. The linkage between the RTGS and the DLT represents several actors that are linked, consisting of the RTGS operator (central bank), the other asset ledger, the transaction counterparties (end users) and the financial institutions providing services to end users (see Figure 9-5 below).

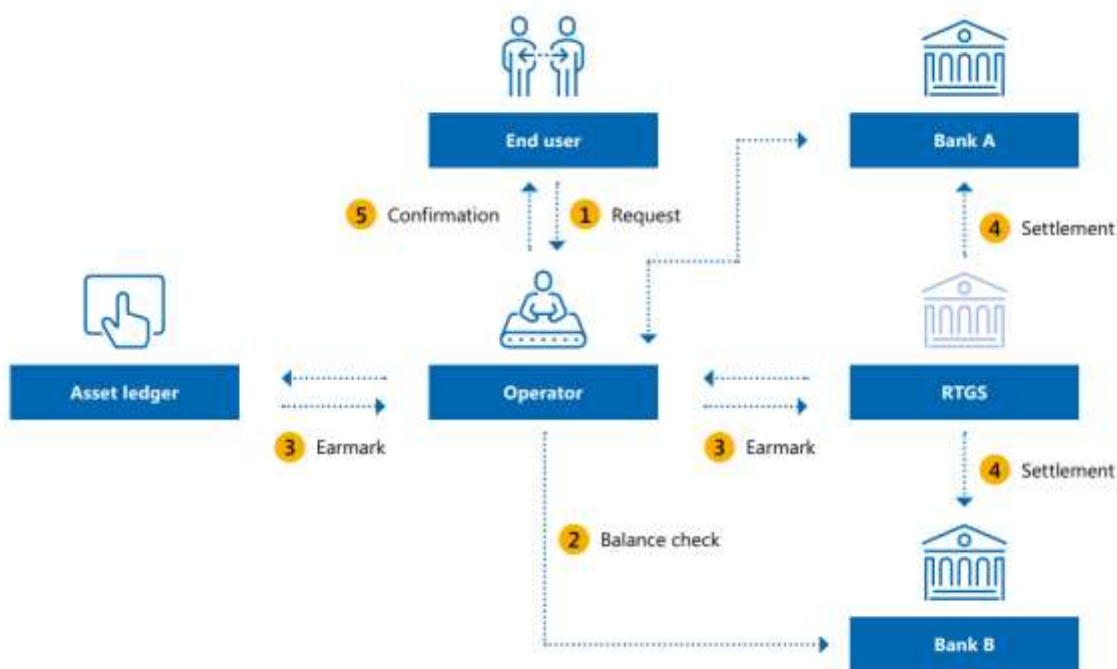


Figure 9-5 Illustrative real-life example showing the integration of RTGS with blockchain (adapted from Bank of England, 2023)

9.3.3 Overview of the industry RTGS to DLT integration project by Accenture, R3 and SAP

The Accenture, R3 consortium and SAP project presented a proof of concept demonstrating how the RTGS system functionality can be augmented by integrating with DLTs (R3, 2021). Figure 9-6 illustrates their proposed blockchain integration with RTGS. In their proposed solution, the RTGS owned by the central bank is connected to two commercial banks: Commercial Bank 1 and Commercial Bank 2. The RTGS is integrated with a *Corda* blockchain node (C.node) using a SAP DLT payment adapter as the integration mechanism. The commercial banks also have the *Corda* blockchain integrated with their legacy payment hubs to enable token-based payments between the commercial banks.

SAP-Corda blockchain integration - example Showing SAP Payment Engine role in intermediation and control

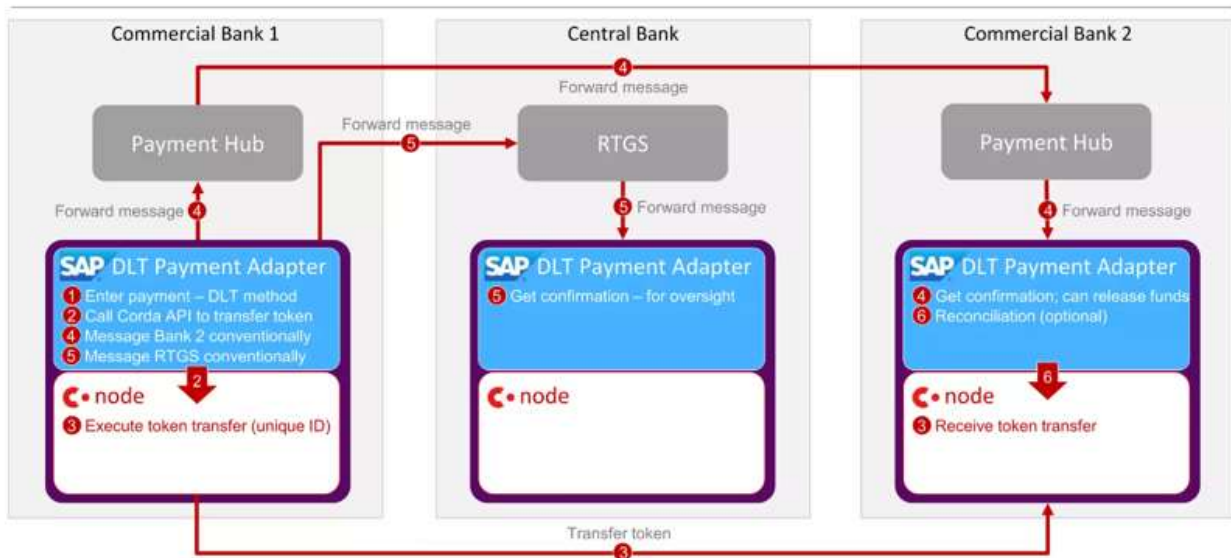


Figure 9-6 Example Illustration of a real-life project scenario for RTGS to blockchain integration(adapted from R3, 2021)

The researcher drew insights from the example projects to create a test scenario demonstrating how the EBI framework would guide the process of enabling interoperability between an RTGS system and a blockchain system. The key information identified from the three illustrative examples is as follows. First, the example project indicates that the purpose of linking blockchain to RTGS is to enable token payments. Second, the examples include

similar key participants, which include the central bank as RTGS host and commercial banks. Another insight is that linking the blockchain to the RTGS also requires linking the blockchain to the commercial banks. These insights were extrapolated to design a narrative test scenario shown in Figure 9-7. The scenario was created for a hypothetical central bank named Skybank.

The following discussion demonstrates how the proposed EBI framework could be applied to assist Skybank in addressing the interoperability challenges between its RTGS system and blockchain systems. The demonstration is based on the narrative scenario created by drawing relevant information from real-life projects. The scenario focuses on the central bank context.

The emergence of *Bitcoin* and many other cryptocurrencies has sparked the emergence of new token-based financial ecosystems. For example, cryptocurrency exchanges that enable the exchange of tokens are now developing organically. These ecosystems are challenging the status quo by providing cost-effective transactions. To ensure their competitive stance in this space, central banks globally are exploring ways to leverage blockchain technology to accommodate these new payment tokens and enhance payment settlements.

Skybank, like all other central banks, wants to leverage blockchain technology to enhance its payment settlement processes. The bank has conducted a feasibility study, and a decision was taken to adopt and integrate *Corda* blockchain technology to support its existing RTGS system. The bank identified the *Corda* blockchain as their blockchain of choice because Skybank does not want to replace the existing RTGS system with blockchain but wants to keep the existing RTGS system and still leverage the benefits offered by blockchain technology.

By integrating blockchain into RTGS, Skybank hopes to enable commercial banks to settle secure and confidential payments using tokenised currency for interbank settlements. To achieve this, the bank has specified the following objectives: 1) To enable payments in tokenised form of the national currency between the central bank and the national commercial banks. 2) To integrate the selected *Corda* blockchain with the existing RTGS to enable the reconciliation of payments between the RTGS and the *Corda* blockchain. 3) To link blockchain-enabled banks to facilitate token-based payments between the banks.

However, it is still unclear how to manage the process of linking with the conventional RTGS to provide a blockchain-enabled RTGS. To address this, the bank has tasked its IT department to manage the project. The IT project team has adopted the EBI framework to guide them through the process.

Figure 9-7 Banking scenario: Enabling RTGS to blockchain interoperability

Example technical specification based on extracts from SWIFT RTGS connectivity requirements

This label aims to ensure that RTGS Application providers meet well-defined requirements related to SWIFT standards, messaging, and connectivity. SWIFT certification is frequently listed as a requirement in RFPs for financial applications.

The following requirements are stipulated for RTGS system providers.

1. Messaging

- FIN protocol

The application must support the FIN protocol (for example, message validation) application must be able to generate the correct FIN header, body, and trailer blocks

- *InterAct Store-and-Forward* protocol

FileAct (optional) *FileAct* can be used by the RTGS application for a variety of flows to send files securely, including the following:

- Ad-hoc or scheduled (such as end-of-day) automated reports to participants (for example, transaction overviews, audit logs, transaction copies)
- Information exchange with ancillary systems
- Regulatory reporting

2. Direct Connectivity Requirements

For direct connectivity, the vendor application must integrate with *Alliance Access*. A business application that does not connect directly to *Alliance* cannot be considered for a SWIFT Certified Application label. The direct connection from the business application to *Alliance Access* can be achieved using one or more of the *Alliance Access* adapters

- *MQ Host Adapter* (MQHA) • *Automated File Transfer* (AFT) • *SOAP Host Adapter*

3. Data Integration

Available formats: Flat file in XML or TXT format

4. User Interface

The application must have a manual entry, display, and repair capability for the MTs and the MXs listed in Standards on page 11.

- Message entry: The application must make it possible for a user to input manually or modify the MT and MX messages by offering normalised fields for input (independent of the underlying syntax and business meaning).
- Message repair: The application must validate the user data input at field level and must flag any invalid entry, prompting the user to correct the input. This includes but is not limited to flagging mandatory fields.

Figure 9-8 Technical specification example for the RTGS

Example technical specification based on extracts from *Corda*

1. Network overview

- Nodes, communicating using *AMQP/1.0* over *TLS*. Nodes use a relational database for data storage.
- A permissioning service that automates the process of provisioning *TLS* certificates.
- A network map service that publishes information about nodes on the network. • One or more notary services. A notary may itself be distributed over multiple nodes.
- A *Corda* network consists of the following components: • Nodes, communicating using *AMQP/1.0* over *TLS*. Nodes use a relational database for data storage

2. Message delivery

- Identity and the permissioning service Unlike *Bitcoin* and *Ethereum*, *Corda* is designed for semi-private networks in which admission requires obtaining an identity signed by a root authority. This assumption is pervasive – the flow API provides messaging in terms of identities, with routing and delivery to underlying nodes being handled automatically. There is no global broadcast at any point.

3. Serialisation, sessioning, deduplication and signing

- All messages are encoded using a compact binary format. Each message has a *UUID* set in an *AMQP* header, which is used as a deduplication key, thus accidentally redelivered messages will be ignored. Messages may also have an associated organising 64-bit session ID. Note that this is distinct from the *AMQP* notion of a session. Sessions can be long-lived and persist across node restarts and network outages. They exist to group messages that are part of a flow, described in more detail below.

4. Data model

- Transaction structure States are the atomic unit of information in *Corda*.
- Transactions consist of the following components:
- Input references: These are (hash, output index) pairs that point to the states a transaction is consuming.
- Output: states Each state specifies the notary for the new state, the contract(s) that define its allowed transition functions and, finally, the data itself.
- Attachments: Transactions specify an ordered list of zip file hashes. Each zip file may contain code, data, certificates or supporting documentation for the transaction.
- Contract: code has access to the contents of the attachments when checking the transaction for validity.
- Commands: There may be multiple allowed output states from any given input state.

Figure 9-9 Technical specification example for *Corda*

9.3.4 Application of EBI Framework to Assist the Skybank in Its Case for Enabling Blockchain to RTSG Interoperability (Scenario 1)

This section elucidates how the proposed EBI framework can be applied to the banking scenario described above. The framework provides general technology agnostic guidelines and considerations that banking organisations can follow when addressing blockchain interoperability. However, the reader should note that the framework does not provide any guidance regarding how organisations can select the blockchain system. The assumption is that organisations required to integrate blockchain technology within their operations will have already made a strategic decision to select a specific blockchain. Furthermore, as stated before, the framework is designed to be technology agnostic to accommodate the many variations in technological choices that may present in different blockchain use cases and organisational settings. Therefore, specific technologies mentioned in the following discussions are only examples used for the scenario.

EBI Step 1: *Is there a blockchain-centric business case / use case in place?*

This step requires the project team first to identify and understand the business case for blockchain in the organisation. A suitable business case or use case for blockchain technology is important because it maps out the intended purpose of blockchain and also has a bearing on the goal of enabling interoperability and, therefore, influences the choice of interoperability approach taken in terms of the costs and operational requirements.

Application to banking scenario

The banking scenario has a clear use case defined for blockchain in the bank, and that is to “augment and support payment settlement services of the current RTGSs system”. The use case also indicates the goal for blockchain in the bank. This goal relates to supporting the RTGS processes using a tokenised national currency to settle payments between the central bank and commercial banks and between commercial banks.

EBI Step 2: *Determine the scope of application of blockchain and required scope of interoperability required*

This step of the EBI framework requires the project team to understand the scope of the application of blockchain. The scope of the application can be guided by the purpose and goal of the blockchain identified in Step 1. Determining the scope of the application encompasses identifying business processes in which the technology will be used. It may also include identifying existing systems used in those processes. The scope of application determines the scope of interoperability. In the EBI framework, the scope of interoperability refers to several aspects. It refers to whether interoperability is required internally (what is typically referred to as vertical interoperability), which implies interoperating different systems within one organisation. Alternatively, it refers to external interoperability (horizontal interoperability), which involves the interoperability of systems across organisational boundaries. In addition, the scope of interoperability in EBI refers to the two forms of interoperability: legacy-to-blockchain interoperability or blockchain-to-blockchain interoperability.

Application to the banking scenario

Therefore, applying Step 2 of EBI to the scenario would require the project team to consider the scope of interoperability required from the above-stated perspectives. This would involve identifying the internal and external systems involved in the process. For example, in the scenario, the team would have to identify the process, the systems involved, and whether those systems are internal or external to the organisation. The process of identifying the scope of interoperability could be undertaken for the scenario as follows:

Task 1: Identifying scope of application of blockchain

From the scenario, the scope of application of blockchain is deduced from the purpose defined in Step 1, namely to “support existing RTGS functions of enabling payment settlement between the Skybank (central bank) and the blockchain enable commercial banks”. From the defined purpose, the team can identify the form of interoperability required.

Types of interoperability identified from the banking scenario:

- The bank intends to interoperate an existing RTGS system with a blockchain system. The RTGS is a legacy system that belongs to the central bank. Therefore, the team can conclude that connecting the two systems would constitute a vertical, legacy-to-blockchain type of interoperability. In this case, the interoperability process will take place in one organisation. The organisation can be the central bank / Reserve Bank or the commercial bank. This implies that for vertical internal interoperability, each bank would have full control of the integration process within its context. Therefore, the interoperability process will be centralised.
- Conventional RTGS settlements involve cross-organisational payments between the central bank and commercial banks, as shown in the narrative scenario. This implies that integrating blockchain technology with the RTGS would also be required to support this process. From this, the project team can identify an additional scope of interoperability that should be considered, i.e., the external interoperability (horizontal interoperability) of blockchains between the central bank and commercial banks or between blockchain systems across the commercial banks.

However, it should be noted that though only two forms of interoperability are identified from the example banking scenario, other forms of interoperability may be required, depending on other use cases. Table 9-1 provides a summary of possible forms of interoperability that may be required for different banking use cases.

Table 9-1 Possible types of interoperability in banking organisations

Type of interoperability	Scope	Description
Blockchain-to-legacy	Internal/vertical	Interoperability between a blockchain and a legacy system conducted in one organisation
Blockchain-to-legacy	External/horizontal	Interoperability between a blockchain and a legacy system between two or more organisations
Blockchain-to-blockchain	Internal/vertical	Interoperability between blockchain systems within a single organisation
	External/horizontal	Interoperability between blockchain systems across two or more organisations

EBI Step 3: *Identify systems for which interoperability is required*

This step entails identifying the respective systems that would need to be interoperated to meet the interoperability objective of the selected use case. The process of identifying the systems is based on the scope of interoperability identified in the previous step. This means identifying all the systems to be integrated and interoperated for each form of interoperability required. All the systems requiring integration with the blockchain within the organisation have to be identified to enable internal (vertical interoperability). In the external case, the organisation has to identify internal systems as well as external systems to be integrated. The types of systems identified depend on the use case and goal of interoperability.

Application to the banking scenario

The internal scope of application in the context of the banking scenario should include the RTGS system and the selected blockchain system. According to the scenario, Skybank selected the *Corda* blockchain as their blockchain of choice. Therefore, the team would also identify the selected blockchain system as the *Corda* blockchain. The other system would then be the RTGS system, which is a legacy type of system.

Regarding the external scope, interoperability is required between the blockchain systems between the central bank and the commercial banks. In this scenario, both the central bank and the commercial banks use the same *Corda* blockchain. Therefore, for this banking scenario, external interoperability is required within the same *Corda* network.

However, in some cases, different banks may opt for different blockchain systems, as evidenced by current central bank projects. For instance, some central banks selected the *Corda* blockchain (Monetary Authority of Singapore, 2017a; Payments Canada et al., 2017) as their preferred blockchain choice, while others have opted for alternatives such as the *Hyperledger Fabric* blockchain (Monetary Authority of Singapore, 2017a) and *Quorum* blockchain (South African Reserve Bank, 2018). Table 9-2 provides an overview of typical blockchains used in banking use cases.

Table 9-2 Overview of blockchain systems used by the banking sector

Blockchain Platform	Example Use Cases
Corda	Interbank real time gross settlements (Monetary Authority of Singapore, 2017a)
Hyperledger blockchains (Fabric, Aroha, Besu)	Retail payments (National Bank of Cambodia, 2020) CDCB (retail and domestic payments) (Central Bank of Norway, 2023)
Quorum	Interbank payment settlements (South African Reserve Bank, 2018)
Enterprise Ethereum	Project i2i Blockchain payments (Consensys, 2019)
IBM blockchain	Bond issuance (Thailand, 2018)

EBI Step 4: Assess compatibility across systems

Step 4 of the EBI framework involves assessing the compatibility of the systems that need to be interoperated. The purpose of the assessment is to determine differences and similarities in terms of the communication protocols, messaging formats, data structures and interfaces. For blockchain-to-blockchain interoperability, this assessment can be extended to include an evaluation of the consensus mechanism and the transaction models.

Application to banking scenario

In the context of the scenario above, the project team would have to determine the compatibility between the RTGS and the selected *Corda* blockchain. The team should review the respective technical specification documents for both the RTGS and the *Corda* systems to identify the protocols used, the data formats and standards, and the types of interfaces each system uses.

By illustration, the technical specification extracts were used as the specification for the RTGS system. The extracts are from the RTGS-Swift guidelines (Swift, 2017, p. 7), which SWIFT provides to central banks as criteria regarding the technical elements required for connectivity of RTGS systems to the SWIFT system. The guidelines “ensure that RTGS application providers meet well-defined requirements related to SWIFT standards, messaging, and connectivity” (Swift, 2017, p. 7). Swift provides a secure payment channel

and messaging standards enabling banks globally to settle payments between different parties. The SWIFT standards are the *de facto* connectivity standards used by the global banking industry to facilitate the settlement of payments within nations and across borders. Therefore, the assumption is that most RTGS systems comply with the SWIFT connectivity requirements and, thus, use the same data formats, standards and protocols required for SWIFT connectivity.

Using the example specifications as a reference point from which to determine the compatibility of the identified systems, the team would be able to compare the systems in terms of their data models, protocols and interfaces.

- **Checking protocol compatibility:** For example, from the RTGS and *Corda* technical specifications, the team would be able to identify that the RTGS system and the *Corda* blockchain used different messaging protocols. For example, the RTGS uses the FIN and *InterAct Store-and-Forward* protocols to facilitate message delivery, whereas the *Corda* messaging protocol is the *AMQP/1.0 7*.
- **Checking data compatibility:** This involves identifying the types of data each system uses. Typically, blockchain systems may be required to store and exchange any of the following three types of data: arbitrary data, cryptocurrencies and tokenised assets. In this example scenario, the systems are expected to exchange normal business data and tokenised currency. Once the data is identified, the team can identify the data formats and standards supported by the two systems. For instance, in the banking scenario, the team would identify that the RTGS supports XML and TXT data formats, whereas *Corda* does not support TXT and XML but, instead, uses state transactions formatted as *Advanced Message Queuing Protocol (AMQP)* data.
- **Checking interface compatibility:** Regarding the types of interfaces used, the team would be able to determine that the RTGS uses the *MQ Host Adapter (MQHA)*, *Automated File Transfer (AFT)*, and *SOAP Host Adapter* as its interfaces while the *Corda* blockchain relies on APIs and the AMQP protocol.
- **Assess data standards:** This step involves evaluating differences and commonalities in the data representations adopted by each system. Understanding how the data are represented in each system is paramount to ensuring that the value

of the asset or currency is consistent across systems. Furthermore, understanding compatibilities between the data standards can assist in determining whether or not to select a standardisation-focused approach to interoperability or to adopt a mediated approach. Example standards used for RTGS systems include the MT standard and the newer ISO20022 messaging standards for payments (Swift, 2017). On the other hand, *Corda* uses the JAVA standards to represent common business data (Brown et al., 2016).

In the case of external interoperability between blockchain systems across the banks, a compatibility test would not be required because the banks are using the same *Corda* blockchain. However, if the banks were using different blockchain systems, compatibility checks would be required, in which the data formats and types, interfaces, protocols, consensus mechanism, and transaction models and speeds of the different blockchains are evaluated and compared.

EBI Step 5: *Selecting an interoperability approach*

The next step in the EBI process flow is determining the appropriate interoperability solution or approach. The selected approach can be either a mediated or standardisation approach. In this study, a mediated approach is regarded as an approach in which interoperability is enabled through a technological mechanism linking the communicating systems. Alternatively, a standardised approach involves using shared and open standardised interfaces, protocols and data models to enable interoperability.

The selection of the interoperability approach is informed by choices made in the previous steps. Specifically, the choice of interoperability approach depends on the type of interoperability selected (i.e., legacy-to-blockchain or blockchain-to-blockchain) and the scope of interoperability (vertical or horizontal). In addition, the type of data that needs to be exchanged also contributes to the choice of approach selected. Some approaches may be appropriate for the exchange of digital assets, others are relevant to the exchange of business data, and other approaches may accommodate both types of data.

In addition, the process involves other considerations, including regulatory requirements, security, privacy, performance considerations, and the availability of suitable open and common standards. Determining the appropriate approach requires an awareness of

existing approaches and mechanisms and also an understanding of the capabilities and limitations of the various approaches.

Sub-step 1: Identify potential approaches based on the type of interoperability required. Thus, if the type of interoperability is blockchain-to-legacy interoperability, the relevant approaches would be those that can enable this form of interoperability; the same applies in the case of blockchain-to-blockchain interoperability, in which only approaches enabling this type of interoperability would be considered. The approach selected is also influenced by the findings on the compatibilities assessments. If the systems share standard data formats, interfaces and protocols, the standardisation approach can be taken. On the other hand, if there are inconsistencies, the mediated approach can be selected.

The example compatibilities assessment from the Skybank scenario indicated incompatibilities in terms of the data formats, interfaces and messaging protocols of the RTGS and the *Corda* blockchain. The incompatibilities indicate that the two systems do not share common communication and data standards. In the absence of relevant standards, a standardised approach may not be suitable. The team would then have the option to select a mediated approach. For example, mediated approaches that enable blockchain-to-legacy interoperability include APIs, oracles, and bridges, whereas notaries, sidechains and relays are some of the approaches that can facilitate blockchain-to-blockchain interoperability.

Sub-step 2: This step requires the potential approaches identified in Sub-step 1 to be further assessed and selected based on predetermined security, privacy and performance requirements, where possible. Different approaches provide varying levels of security and privacy; therefore, it is important to understand these variations and select the appropriate solution. Furthermore, possible regulatory requirements governing data exchange processes might also need to be considered. However, it should be noted that the security and privacy requirements would vary depending on the use case and business context.

For instance, in the Skybank scenario, two types of interoperability were identified. The first is the vertical legacy-to-blockchain interoperability to enable the exchange of both normal business data and tokenised assets between the RTGS and *Corda* blockchain. The second form is the horizontal blockchain-to-blockchain interoperability between the *Corda* blockchains between banks. In each case, the team would have to evaluate the available interoperability approaches to determine whether or not they support the transfer of arbitrary

business data and the tokenised currency, as required for the use case. An example of an assessment of the approaches based on the type of data they support is shown in Table 9-3 below.

Table 9-3 Example assessment of interoperability approaches based on the type of data they support

Potential interoperability approach	Support normal/arbitrary data	Type of interoperability supported
APIs	Support normal data and digital assets	Legacy-to-blockchain
Oracles	Support normal data and digital assets	Legacy-to-blockchain
Third-party	Supported	Legacy-to-blockchain Blockchain-to-blockchain
Sidechains	Support data exchange, asset transfer and asset exchange (Monika & Bhatia, 2020b)	Blockchain-to-blockchain
Relays	Support data exchange, asset transfer and asset exchange (Buterin, 2016)	Blockchain-to-blockchain
Notaries	Support data and asset transfer and exchange (Pang, 2020)	Blockchain-to-blockchain
Bridges	Support data transfer, asset transfer and asset exchange (Bhatia, 2020)	Blockchain-to-legacy Blockchain-to-blockchain
Hash Time locks	Support asset exchange but not data or asset transfer	Blockchain-to-blockchain
Blockchain routers	Support transfer of data and assets	Blockchain-to-blockchain
Smart contracts	Support data and asset exchange and transfer	Blockchain-to-blockchain

From the example assessment above, it is evident that some of the potential approaches can be used to exchange both normal business data and assets; some only support asset

exchanges, not transfers, and others only support arbitrary data exchanges. For example, with legacy-to-blockchain interoperability, three potential approaches can be used, i.e., APIs, oracles and bridges. In terms of enabling blockchain-to-blockchain interoperability, the approaches supporting both data and asset transfer include sidechains, relays, notaries and bridges, while the Hash time lock contracts are not suitable in this case because they do not support the required arbitrary data exchange and only support data exchange and not data transfer.

The next step requires the team to evaluate the options identified above against the desired security and privacy requirements. RTGS supports transactions involving large sums of money and, therefore, requires strong security measures to ensure that the transactions are secure and payments are atomic and final. Security measures such as strong encryption techniques, secure communication channels and authentication protocols are typically used to safeguard the integrity of the transactions. The security requirements have a bearing on the interoperability approach selected and imply that the team should select an approach that would not compromise the security of the RTGS system.

The approaches can be evaluated for suitability using the security capability assessment shown in Table 9-4. Regarding legacy-to-blockchain interoperability, the team would be able to determine that APIs are a better solution than oracles and bridges to provide the required security measures of authentication and encryption between the RTGS and the selected *Corda* blockchain. APIs, particularly private APIs used with one organisation, are more secure than public APIs, oracles and bridges.

However, in the case of blockchain-to-blockchain interoperability across organisations, approaches such as notaries, hash time locks, bridges, side chains and blockchain routers can be used. Nevertheless, the team would have to select an approach that provides a balance in trade-offs between the required support for real-time, high-volume transactions privacy and security requirements and implementation complexity to meet the high security and privacy and performance requirements for banking transactions. For example, drawing from the performance comparison of the various solutions shown in Table 9-5, the team might exclude the HTLC-based solutions because they do not offer the required asset transfer functionality, even though HTLC provides strong security measures. Alternatives like notaries, sidechains and relays offer the requisite support for the transfer of the

tokenised currency, as required for the scenario; however, the team might have to select an acceptable trade-off between security, performance and the level of implementation complexity. For instance, for the Skybank scenario, multiple notary solutions can be selected because they provide high security compared to the single notary and have medium implementation complexity compared to the relays and sidechains alternatives.

Table 9-4 Simple example of security and performance assessment of the interoperability approaches

Approach	Security capabilities (authentication, validations, encryption)	Limitations
APIs	<ul style="list-style-type: none"> • Some APIs offer authentication and access control mechanism (Sakho et al., 2019) • APIs and API gateways support encryption (Sakho et al., 2019) 	Vulnerable to security breaches that can compromise the confidentiality of the data (Sakho et al., 2019)
Oracles	<ul style="list-style-type: none"> • Require additional access control, identification and registration services (Al-Breiki et al., 2020) • Most support Public Key Encryption, Certificates (Ezzat et al., 2022) 	Introduce single point of failure if centralised (Hassan et al., 2023) Do not provide data verification mechanisms (Hassan et al., 2023)

Table 9-5 Comparative assessment of cross-chain approaches (adapted from Mao et al., 2023)

Approach	Types of data supported	Security	Transaction speeds	Implementation complexity	Multi-currency Smart contracts	Atomicity / finality of transaction
Sidechains/ relays	Support asset exchange and transfer Support arbitrary data	Low	Slow	Difficult, high complexity	Difficult	Supported through Merkle proofs
Hash time locking	Supports asset exchange and not data or asset transfer	Medium	Medium	Easy, low complexity	Not supported	Provide using Hash time locks
Notaries	Support asset exchange and transfer Support arbitrary data	Low	Slow	Medium complexity	Difficult	Provide through trust notary
Bridges	Support data exchange and asset exchange and transfer	Very low for trust Medium for trustless		Trusted easy low complexity Trustless high complexity	Trustless difficult	

Other measures that can be used to select an interoperability approach include the performance/transaction processing speed, atomicity and settlement finality requirements. In addition to the requirements above, other factors, such as ensuring that the interoperability mechanisms/solutions comply with legal and regulatory statutes, such as those governing the storage of data, should be considered. Possible regulations relevant to the example scenario are provided in Table 9-6.

Table 9-6 Regulations that impact interoperability in the banking sector in the South African context

Type of regulation	Regulation	Description
Data protection law	Protection of Private Information Act 4 of 2013 (POPIA)	Aims to protect the personal information processed by private and public institutions in South Africa
Payments-related regulations	R National Payments Systems Act (NPS Act78 or 1998)	Governs the administration, management, supervision of payment clearing and settlement systems
Anti-corruption laws	Anti-Money Laundering and Know-Your-Customer regulation through Prevention and	FICA is a regulatory framework that provide measures for certain businesses to mitigate

	Combatting of Corrupt activities (POCA) Act of 2004	money laundering and terrorist funding risks.
Data governance regulations	Basel 3 regulations	Basel 3 regulation are international regulations that active international banks have to comply with. The Basel 3 regulations aim to enhance the regulation, supervision and risk management of banks

In addition, for external blockchain-to-blockchain interoperability cases, considerations include the development of collaboration agreements, governance structures, accountability, and risk models. For example, in the illustrative scenario case, the banks may agree on a centralised governance model in which the central bank determines the rules of participation and the rules for the exchange. However, in some instances, a distributed governance model may be preferred. Alternatively, collaborating organisations may opt for an on-chain governance model, which leverages blockchain technology and smart contracts to enforce collaboration rules and policies.

Enabling blockchain interoperability for asset transfer and asset exchange requires the selection and use of an appropriate and common cross-chain messaging protocol. Cross-chain communication protocols define a set of rules that govern how messages are exchanged between blockchain systems. This implies that organisational teams need to be aware of the available protocols, their feature and capabilities. The evaluation of the EBI framework using the RTGS-to-blockchain scenario for internal (vertical) and external interoperability is demonstrated in Figure 9-10.

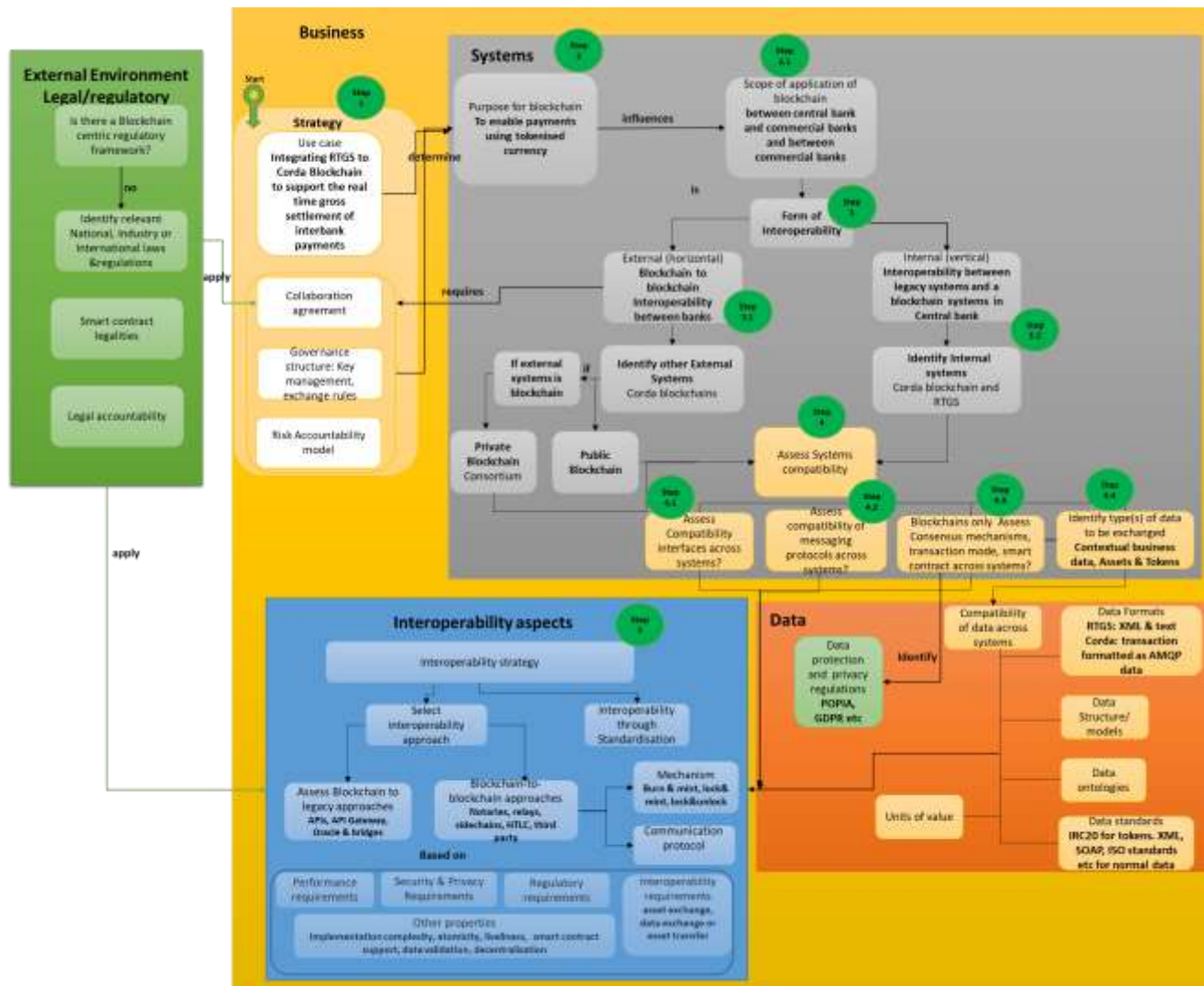


Figure 9-10 Flow diagram representing the EBI framework application to the RTGS-to-Blockchain scenario for Skybank

9.4 EVALUATION OF THE EBI FRAMEWORK USING EXPERT INTERVIEWS

This section discusses the evaluation of the proposed EBI framework. For the evaluation, structured, expert interviews were conducted with three blockchain experts from the banking sector. Expert interviews are an empirical method used to evaluate artefacts and have the benefit of being effective in collecting users' opinions and views about the use and value of artefacts (Johannesson et al., 2021). The discussion below presents the interview process and the results of the evaluation obtained from the interviews.

9.4.1 Interview Process

The interview process entailed 30-minute interviews with the selected participants. The interviews were guided by an interview guide, which included qualitative and quantitative questions (see APPENDIX B). Before the interview sessions, a copy of the proposed framework and a brief description of the framework were sent to each participant to afford the participants sufficient time to familiarise themselves and review the framework.

The sample of participants was selected using the convenience sampling approach, which involved contacting the same participants who had been interviewed as part of the data collection process conducted as part of the design and development phase. These participants were preferred over new participants because they had previous knowledge of the topic under discussion (Trevelyan & Robinson, 2015). Three of the thirteen participants who had participated in the previous interviews were available for participation in the evaluation process. A brief description of each participant is provide in Table 9-7.

Table 9-7 Description of participating experts

Role	Years of Experience	Experience in blockchain/DLTs and banking
DLT Research Group Leader	7	Blockchain Regulatory Technology
Systems Architect	5	Banking Payment systems Regulation
Software Engineer	7	Banking Blockchain Regulatory Technology

The three participants were interviewed during one-on-one sessions conducted using online conference platforms. The interview sessions were guided by an interview questionnaire comprising sections categorised under the evaluation criteria adapted from (Prat et al., 2014), as explained in Section 9.2.1 above. The first section of the questionnaire comprised questions relating to the participant demographics, depicted in Table 9-7 above. The next section comprised the questions designed to evaluate the framework. This section was deconstructed into four subsections. Sub-section A comprised questions relating to the utility of the framework, Sub-section B included questions on the completeness of the framework, and Sub-section C consisted of questions to evaluate the usability of the framework. Sub-section D focused on the relevance of the framework, and lastly, Sub-section E included questions that aimed to evaluate the framework against other frameworks the participants might have used. The results of the interviews are presented in the next section.

9.4.2 Evaluation results from the analysis of expert interviews

This section discusses the findings obtained from the analysis of the interviews. The results are presented per the five main criteria on which the interview questions were based. For each of the criteria, the results of the analysis are as follows:

Reviewers' experience in blockchain: 66 % of the participants had experience working in the banking sector, while 33% did not work in the banking sector but in the banking regulatory field. In terms of specific skills and experience in blockchain technology, 100% of the participants indicated they had experience working with permissioned (private) blockchains and smart contracts but no technical experience in cryptocurrencies or permissionless blockchains.

Utility:

1. *In your view, how applicable is the framework to the banking context in South Africa?*

The reviewers agreed that the framework is applicable to guiding blockchain interoperability activities in the banking sector. One reviewer stated that because the “*framework is general, and it's not imposing any technologies, it can be applied to many scenarios in banking*”. Another participant stated “*I think the framework is relevant and applicable to the banking context.*”

2. *How do you see the framework being applied by organisations looking to deploy blockchain solutions in the sector?*

The participants indicated that the framework provided a good starting point from which banks can think about blockchain interoperability. One of the Respondents stated “*I can see this framework being used to complement other tools that we normally use to handle integration of new systems. It brings an additional perspective on what we can think about when we are thinking blockchain integration*”. Another reviewer stated, “*I can see how the framework would work for individual banking institutions and at domestic level, but I think for a cross border, it may not cater for all the complexities of cross border arrangements.*”

3. *In your view, how effective would the framework be in assisting banking organisations to address blockchain interoperability issues?*

In terms of the effectiveness of the framework, there was consensus among the reviewers that assessing the effectiveness of the framework is a bit difficult without having utilised the framework in a real integration process. However, the reviewers stated that at face value, they assess the framework to be effective because the framework is not one-dimensional but includes different perspectives. The participant stated that this is because “*Blockchain technology is still very new, and has not matured yet... and so there are, still many things that we are still figuring out about the technology, which I think, that um [...] may be added later on to improve the framework. You know we are all still trying to figure this technology out, so, other issues we may learn about in the process so we can't really say exactly to what extent the framework is effective*”.

4. *Does the framework provide sufficient/adequate guidance to organisations regarding how to handle or address interoperating blockchain technology? If No, Do you have any suggestions or recommendation on how we can improve the utility of the framework?*

There is consensus among the experts that the framework covers the necessary aspects that should be considered; however, some of the reviewers indicated that in terms of utility, the main framework was too detailed. The participant suggested: “*Reduce the details in the high-level framework, maybe only include the core elements because the details are already included in the process flow and guidelines*”. This was supported by another participant, who stated: “*Try and simplify the overview of the framework, it contains too much information which makes a bit difficult to follow, but the process flow and the guideline makes sense to me*”.

Completeness

5. *In your view, does the framework adequately cover all the relevant and critical aspects on blockchain interoperability in the banking sector inasfar as the following areas are concerned, business, legal, data and technical?*

Regarding the completeness of the framework regarding the business, legal, data and technical aspects, one of the participants suggested resources the researcher should explore for more contextual information concerning the regulatory aspects. The participants stated: *“The framework looks great. Please have a look at the MiCA to see how the EU approach, categorise and make a distinction as to whether something is a currency, or it fits another case, this is where a lot of regulatory ambiguity has often stemmed. This is purely for you to get more context as I feel the framework is sound and covers all the aspects and positioning of this technology”*.

Usability

Concerning the usability of the framework, the reviewers were asked three questions in which they had to select one option from the Likert scale. The options ranged from very easy, easy, slightly difficult and difficult. The purpose of the question was to establish how easy it was to understand and use the framework. In response, all the reviewers indicated the process flow and the guidelines provided were very easy to understand and use; however, as stated above, they suggested that the overview of the framework was too detailed and should be simplified.

Relevance

Two questions were posed to assess the relevance of the proposed framework to the blockchain interoperability domain. The first question sought to determine the reviewers' opinions regarding the relevance of the framework to blockchain interoperability in general, and the second question focused on the relevance of the framework in relation to blockchain interoperability frameworks. In response to the first question, the reviewers indicated they found the framework to be very relevant to the blockchain interoperability domain. Regarding the second question, the reviewers rated the framework relevant. One reviewer stated that he rated framework relevant as opposed to very relevant because *“I feel that the framework is generic in the sense that it can work in many instances, not only the banking sector. I also like the fact that it is not focused on one use case, like for example just CBDCs, because I feel that would limit its applicability, but because it is general it can be used in many use cases in the banking sector”*.

Benchmarking

Regarding the benchmarking questions, the reviewers responded that they did not know of any or had not used any blockchain interoperability frameworks because they had not engaged in any blockchain projects requiring integration with existing legacy systems. The reviewers stated this was because most projects on blockchain were still in experimental stages and had not yet reached production levels.

The experts validated the proposed EBI framework by highlighting that the framework was sufficiently comprehensive to provide support for blockchain interoperability initiatives in the banking sector. They also indicated the framework was easy to understand and follow, with particular reference to the usability of the process flow and the guidelines provided (see Chapter 8). However, the experts suggested that the high-level framework should be simplified, although they did not specify details on how the framework should be simplified. To address this concern, the researcher updated the framework by including only components and removing activities/actions included in the earlier versions of the component architectural framework. The simplified version of the high-level framework is shown in Figure 9-11 below.

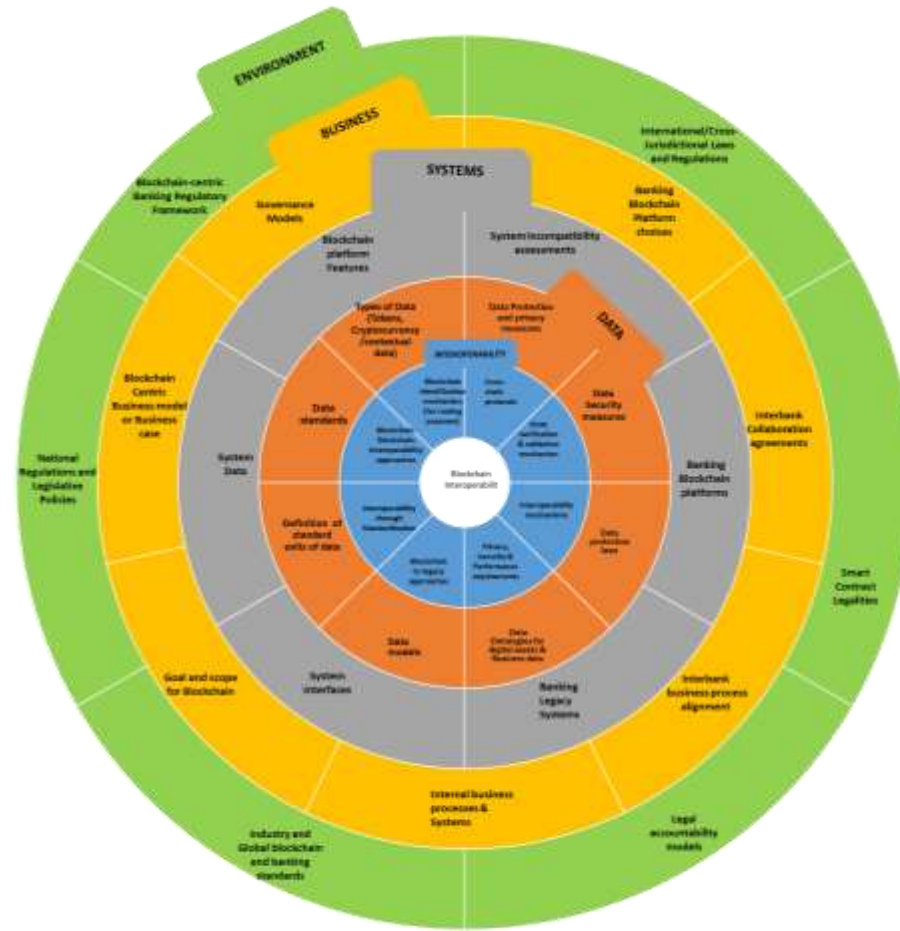


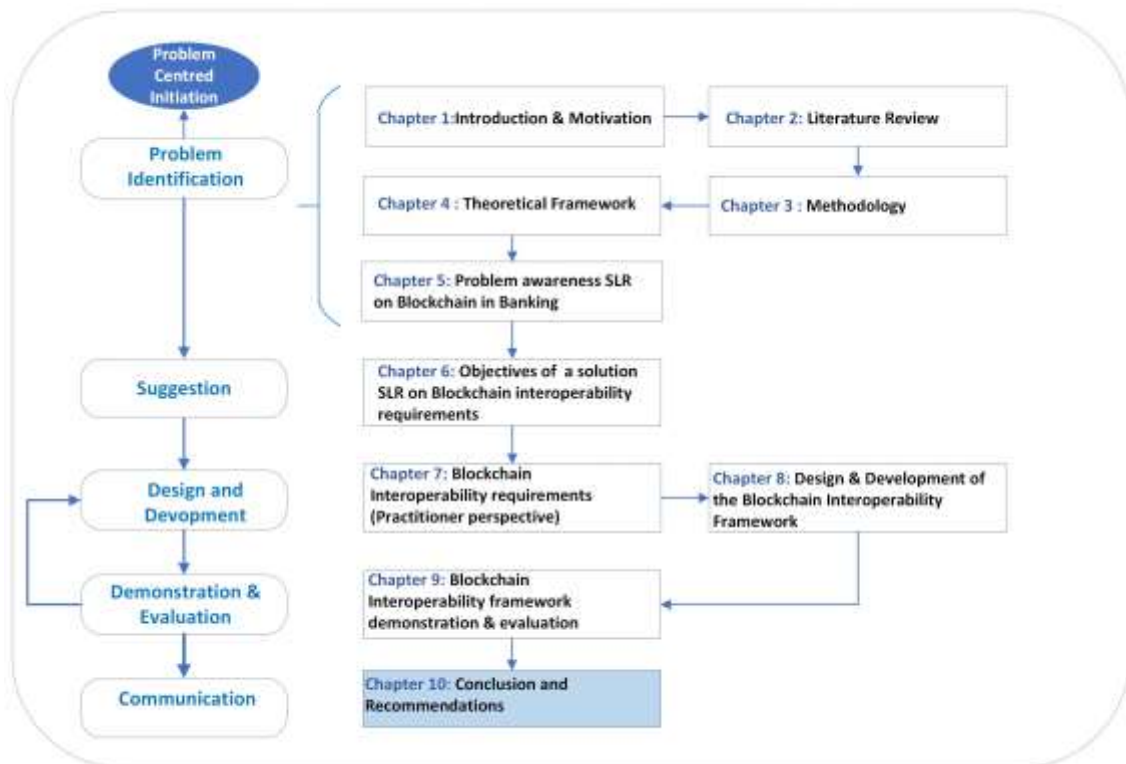
Figure 9-11 Simplified EBI framework

9.5 SUMMARY

This chapter explored the demonstration and evaluation of the proposed EBI framework. The chapter demonstrated the applicability of the framework using an illustrative scenario based on real-life banking use cases. In addition, the chapter presented the results of the framework evaluation by blockchain experts. The chapter also presented the simplified version of the EBI framework, as suggested by the experts. The next chapter concludes the study and presents recommendations for future research.

CHAPTER 10

10 CONCLUSION AND EVALUATION OF THE RESEARCH STUDY



10.1 INTRODUCTION

The current chapter concludes this study by presenting an overview of the key findings in relation to the research questions outlined for the study. The chapter includes a discussion of the various contributions of this study and also presents a reflection on the methodological approach adopted. The chapter concludes with recommendations for future research.

The main purpose of this study was to investigate how blockchain interoperability in banking organisations can be implemented to address the challenge of lack of interoperability between blockchain systems and other traditional systems. An enterprise blockchain interoperability (EBI) framework was proposed to guide organisations regarding the considerations and processes that should be followed to enable blockchain interoperability.

A pragmatic design science research approach was followed to construct and evaluate the framework to achieve the study's goal. The construction of the framework drew from the systems theory and was informed by data collected using systematic literature reviews,

interviews with 13 blockchain experts, and webinars. The study was operationalised through the following research questions.

Main research question:

- *How can a blockchain interoperability framework be conceptualised to guide the process of implementing blockchain interoperability in the banking sector?*

Sub-research questions:

SRQ1: *What are the use cases, challenges, and considerations for blockchain implementation in the banking sector?*

SRQ2: *What are the requirements for enabling blockchain interoperability?*

SRQ3: *What are the critical elements required to formulate a blockchain interoperability framework?*

SRQ4: *How can a blockchain interoperability framework be developed?*

SRQ5: *How can the developed framework be evaluated?*

10.2 ADDRESSING RESEARCH QUESTIONS

This section presents a summary of the key findings concerning each of the sub-research questions and demonstrates how answering these questions addresses the main research question.

SRQ1: What are the use cases, challenges, and considerations for blockchain implementation in the banking sector?

This question was addressed through a systematic literature review which was presented in Chapter 5. The findings of the review indicated that the banking sector was embracing blockchain technology despite reports that the technology was intended to challenge the role of banks as intermediators in the payment space. The results indicated the banking sector was involved in various experimentation efforts to explore the use of blockchain technology to address inefficiencies of various payment systems. Specifically, it was found

that blockchain technology use cases in the sector encompassed its use in cross-border and remittance payment processes (Bank of Canada & Monetary Authority of Singapore, 2019), inter-bank settlements (Payments Canada et al., 2017), and security settlements (Monetary Authority of Singapore, 2017b). An additional area of application identified in the literature related to the use of blockchain in developing central bank digital currencies to facilitate retail and wholesale payments.

Results relating to the challenges for blockchain implementation in the sector indicated three main challenges inhibiting the effective implementation of blockchain in the sector. The results showed that the banking sector was encountering drawbacks concerning the scalability and performance capabilities of blockchain platforms. The identified challenge was that most of the blockchain platforms were incapable of handling the required transaction loads and speeds that current methods could achieve. Challenges regarding the lack of appropriate blockchain-centric legal and regulatory frameworks were highlighted as an additional obstacle to the implementation of blockchain technology in the sector. The results further indicated the lack of interoperability between blockchain systems and between blockchain systems and other traditional systems as a critical impediment to the implementation of blockchain in the sector. The lack of interoperability was found to be a key inhibitor of the mass adoption of the technology because organisations could not share transactions and data seamlessly across the various systems, as required and, as a result, they could not fully leverage the benefits of adopting the technology. The latter challenge formed the basis of this study.

Regarding the factors to consider for blockchain implementation in the sector, the findings showed that there are technological, organisational and environmental considerations that should be allowed for when dealing with blockchain implementation. The key technological considerations identified included selecting an appropriate blockchain platform, data privacy and security, scalability, and resilience. Other technological considerations related to the compatibility of legacy systems with emerging blockchain systems. Key organisational considerations related to the governance of blockchain systems in organisations. The findings indicated that organisations needed to develop new governance models that provide a balance between the traditional governance models used in banking organisations, with decentralised governance models typical to blockchain systems.

Concerning environmental considerations, the results show that banking organisations implementing blockchain-centric solutions should consider the legal and regulatory implications of the technology. Specifically, the results showed that new blockchain-centric regulatory frameworks should be developed to address the regulatory issues with the technology.

SRQ2: What are the requirements for enabling blockchain interoperability?

The purpose of this research question was to assist the researcher in identifying and understanding the different requirements that should be met to enable blockchain interoperability. The question was operationalised through a systematic literature review study discussed in detail in Chapter 6. The systematic literature review leveraged the interoperability levels of the European interoperability framework to categorise the requirements into technical and semantic interoperability requirements, organisational interoperability requirements, and legal interoperability requirements.

The findings relating to the technical and semantic requirements showed that ensuring the security and privacy of stored data, as well as data in transit, is a critical requirement for blockchain interoperability in the banking sector. In particular, the results indicated that the interoperability approach or mechanism used should not compromise the security of the connected systems; it should be fault-tolerant and provide access control and authentication capabilities to ensure the confidentiality of the exchanged data. Another identified technical requirement concerned the identification of blockchain systems: The findings indicated that blockchain systems were required to be identifiable for routing and verification purposes. For semantic interoperability, the key requirement concerned the standardisation of data formats. The findings indicated that data formats used on the blockchains should be standardised to enable all participants in the data exchange to verify the reliability of the information and for the communicating parties to have a shared understanding of the data. In terms of the requirements needed to enable organisational interoperability, the findings highlighted three requirements that should be fulfilled. The first requirement was that organisations should have a shared collaborative blockchain-centric business model in place. The second requirement was that organisations engaged in collaborative arrangements involving blockchain technology should establish a trust mechanism, such as

smart contracts, to orchestrate cross-organisational business processes and enforce contractual obligations. The other requirement was that governance models between collaborating organisations should be compatible to ensure interoperability between these organisations.

For legal interoperability, the findings showed that facilitating legal interoperability requires blockchain systems and parties involved in transactions on blockchain platforms to be distinguishable to ensure compliance with domestic and national regulations, such as know-your-customer and anti-money laundering regulations. In addition, the findings emphasised the need for compliance with domestic and cross-jurisdictional regulations. Specifically, the finding indicated that the interoperability mechanisms and smart contracts used to enable blockchain interoperability should be designed to anticipate jurisdictional variations and include policies and legal controls to address the jurisdictional uncertainties.

SRQ3: What are the critical elements required to formulate a blockchain interoperability framework?

This question was addressed by data collected from interviews with thirteen blockchain experts and thirteen webinars on blockchain interoperability and interoperability in banking. The main findings concerning this question (see Chapter 7), indicated that a blockchain interoperability solution or framework should accommodate different forms of interoperability that might be required in organisational contexts. In this regard, two forms of interoperability were identified: blockchain-to-blockchain interoperability and blockchain-to-legacy interoperability. The study revealed that both forms can include aspects relating to the legal, organisation, technical and semantic interoperability levels.

Concerning the organisational or business elements, the findings emphasised the need for a blockchain-centric business case or use case. The findings show that a clear business case is an important element of an interoperability framework because it outlines the goal for blockchain, thus influencing the choice of system involved and the form of interoperability required. Other business elements include collaboration agreements, risk and accountability models and governance models for interoperability between and across organisations.

In addition, the results indicated that a blockchain interoperability framework or solution for the banking sector should include legal and regulatory elements representing all the legal statutes and regulations that govern the storage and exchange of data. The findings revealed that regulatory elements have a direct bearing on the choices in the approach and mechanisms selected to facilitate the required interoperability. For instance, the data protection and privacy regulations were shown to influence the data privacy and security requirements for the interoperability approach or mechanism.

The results further indicated that data-related elements and interoperability elements should also be included in the framework. The data elements represent all the data-related requirements and considerations, such as the type of data to be exchanged and how the data is formatted and represented on each system. The interoperability elements represent the possible interoperability approaches, the selection of an interoperability mechanism and related considerations.

SRQ4: How can a blockchain interoperability framework be developed?

A blockchain interoperability framework (EBI) was developed to guide banking organisations through the process of implementing blockchain interoperability to address the question above. The developed EBI framework was conceptualised by mapping the findings from Chapters 5, 6 and 7 to system theory elements, as explained in Chapter 8. The framework included five main components: the environmental, business, systems, data, and interoperability components. The framework is represented in three forms: the high-level architectural component framework (Figure 8-8), the process flow (Figure 8-9), and the guidelines (Figure 8-10).

SRQ5: How can the developed framework be evaluated?

The EBI framework was demonstrated by utilising an illustrative scenario based on real banking use cases involving interoperating RTGS systems with blockchain technology to support settlements of transactions. The results of this process showed that the framework

applies to guiding decisions on blockchain interoperability in banking. The framework was also evaluated by a sample of blockchain experts. The findings showed that the experts believed the framework applied and was useful for addressing blockchain interoperability in the sector and in general. The findings further indicated that the framework was sufficiently comprehensive and could be applied to many use-case scenarios in banking. The component framework was updated as suggested by the experts and resulted in the EBI component framework shown in Figure 9-11.

10.3 EVALUATING THE RESEARCH CONTRIBUTION

10.3.1 Practical Contribution

This study developed a comprehensive framework to guide the process of enabling blockchain interoperability in the banking sector. At the time of publication of this thesis, the researcher was unaware of any comprehensive blockchain interoperability framework addressing the technical, organisational and legal perspectives on blockchain interoperability. Studies have focused predominantly on blockchain interoperability from a technical perspective, particularly focusing on public (permissionless) blockchains; however, this study also contributes to the understanding of how organisations can interoperate permissioned blockchains with existing legacy systems in organisational settings. Therefore, the proposed framework can be used as a guide and reference point for blockchain practitioners and organisations to guide the decisions regarding the process of interoperating blockchain technology with existing organisational processes.

The proposed framework includes an architectural component framework, a process flow and a set of guidelines and considerations. The process flow and guidelines provide practical guidance to inform the process practitioners can follow to determine the relevant technical, business and regulatory aspects required to implement blockchain interoperability.

10.3.2 Theoretical Contribution

This study's contribution to the body of knowledge is fourfold. First, the study contributes by extending the body of knowledge on blockchain interoperability in the main, as well as understanding the nuances of blockchain interoperability in banking organisations. This aspect is particularly important because the field of blockchain and blockchain interoperability is still in its nascent stage. Therefore, this study provides other scholars and practitioners with a starting point from which further studies on blockchain interoperability can be explored.

Second, the study contributed by providing a holistic interrogation of blockchain interoperability that surpasses the typical technological focus of current studies. This study explored blockchain from technical, semantic, organisational and legal views, which are not covered by existing studies on the topic of blockchain interoperability. The third theoretical contribution of this study is demonstrating the suitability of general systems theory in understanding blockchain interoperability. The general systems theory informed the development of the framework.

Lastly, the study provided the proposed blockchain interoperability framework as a contribution to the body of knowledge on blockchain interoperability. Prior studies on blockchain and blockchain interoperability highlight the complexities of enabling blockchain interoperability and suggest the need for an interoperability framework to guide organisations. This study responded by providing the EBI framework.

10.3.3 Methodological Contribution

The study contributed methodologically by triangulating data collected through traditional and uncommon data collection methods. This study augmented the results obtained from the interviews by using webinars. Webinars are an atypical data collection method; however, their application in this study revealed that webinars could be an effective supplementary data collection method for enabling researchers to collect data from subjects inaccessible through traditional methods and for new research areas, which might have a limited number of experienced participants. In this study, webinars enabled the researcher to draw insights

from international banking and blockchain professionals who could not be reached through traditional data collection methods. Such access was particularly important because the topic of blockchain interoperability was still relatively new; as such, access to experienced blockchain experts is limited. Thus, leveraging webinars contributed to corroborating the results obtained from the local experts. Using webinars in this study laid the foundation for other researchers to explore such use of webinars to complement traditional methods of collecting data, particularly for investigating emerging topics with constrained populations.

In addition, this study elucidates how the DSRM (Peffer et al., 2007) can be utilised to interrogate a nascent topic such as blockchain interoperability. Furthermore, the study can be a reference point for other DSR researchers on how to apply the DSRM to develop and evaluate a framework artefact such as the EBI framework proposed in this study.

10.4 LIMITATIONS OF THE STUDY

The study had several limitations, as listed below:

- As mentioned earlier, blockchain experts are generally scarce because the topic is still in its infancy, and most organisations are still experimenting with the technology. As a result, the researcher could not access many participants. Consequently, the study relied on insights from only thirteen blockchain experts. However, the thirteen participants had diverse blockchain- and banking-related experiences, which enabled them to provide an in-depth understanding of the blockchain interoperability topic. As the technology matures, researchers can extend this study by including more participants.
- Due to the reasons stated in the bullet point above, the evaluation was undertaken with three experts. In addition, the evaluation strategy followed to evaluate the framework was artificial, even though scenarios based on real-life use cases and real-life users (experts) were used. Future evaluations can be undertaken with real users, real tasks and in a real organisational context.

10.5 DIRECTIONS FOR FUTURE RESEARCH

From the findings of this study, the following recommendations for future studies are made:

- This study is one of a few studies interrogating the topic of blockchain interoperability from organisational and legal perspectives. However, the study does not provide an exhaustive exploration of these aspects. Therefore, future studies could extend this study by exploring the aforementioned aspects further.
- Future studies could also explore governance issues relating to decentralised blockchain systems in organisational settings. The findings of the study showed that organisations using blockchain technology for collaboration should determine the appropriate governance models, risk models and accountability models. The details of how organisations could select these models were outside the scope of this research and thus were not provided. Therefore, the researcher recommends that future studies should investigate the various governance and risk models that can be used for blockchain-centric use cases spanning multiple organisations and jurisdictions.
- The findings of this study further indicated a need for new blockchain-centric regulatory frameworks to be developed. Future research studies should consider investigating how such new frameworks can be developed to regulate the storage and exchange of data on blockchain systems, guide smart contract legalities, and regulate crypto assets and tokens.
- Security and privacy-related concerns were highlighted as essential requirements for enabling blockchain interoperability. However, studies investigating such security and privacy requirements in the blockchain interoperability context are scarce. Accordingly, the researcher recommends that future studies examine security and privacy challenges related to blockchain interoperability in more detail.

- This study demonstrated and evaluated the EBI framework for banking use cases. Future studies might enhance the EBI framework by applying and evaluating the framework in other organisational contexts.
- The findings also indicated that data standards were required to simplify the process of interoperating blockchain systems. Upcoming studies could seek to understand standardisation in the context of blockchain interoperability by exploring how crypto assets and tokens can be standardised and how different standards for blockchain technology can be developed.

10.6 CONCLUDING SUMMARY

In conclusion, this study aimed to address the blockchain interoperability challenges banking organisations face when considering the adoption of blockchain technology to optimise their business processes. The blockchain interoperability challenge refers to the lack of interoperability between different blockchain systems, which inhibits these blockchain systems from seamlessly exchanging data with other blockchains and legacy systems. Enabling blockchain interoperability is a complex process, and the absence of appropriate tools, models, and frameworks to guide organisations on how to manage blockchain interoperability further complicates this process. As a result, organisations are unable to reap the full benefits of the technology.

This study conceptualised an interoperability framework called the EBI framework to address this lack. The EBI framework consists of an architectural component framework, a process flow and a set of guidelines and considerations. The framework provides banking organisations with guidance on how to implement blockchain interoperability. The framework achieves this by highlighting key steps and considerations in implementing blockchain interoperability.

The proposed Enterprise blockchain interoperability (EBI) framework was developed following a design science approach proposed by (Peffer et al., 2007). The study used a methodological triangulation approach for data collection, including systematic literature

reviews, expert interviews and webinars. General systems theory was adopted as the main theoretical lens through which the framework was conceptualised.

The key findings indicated that to enable blockchain interoperability in banking organisations, some key elements should be considered. Organisations must have a specific blockchain use case in place and understand the scope of the application of the adopted blockchain. In addition, organisations must understand the systems needed for interoperation. The study also revealed that data standards, formats and structures are essential elements to consider. Furthermore, the findings revealed that regulatory compliance and ensuring security and privacy are critical for enabling blockchain interoperability in banking. The above-stated elements were identified as elements that could inform the interoperability approach that is ultimately selected.

In summary, the overall aim and objective of the research were achieved by developing and evaluating a blockchain interoperability framework that can be utilised to guide the process of implementing blockchain interoperability in the banking sector.

11 REFERENCES

- Abebe, E., Behl, D., Govindarajan, C., Hu, Y., Karunamoorthy, D., Novotny, P., Pandit, V., Ramakrishna, V., & Vecchiola, C. (2019a). *Enabling Enterprise Blockchain Interoperability with Trusted Data Transfer (Industry Track)* Proceedings of the 20th International Middleware Conference Industrial Track, Davis, CA, USA. <https://doi.org/10.1145/3366626.3368129>
- Abu-elezz, I., Hassan, A., Nazeemudeen, A., Househ, M., & Abd-alrazaq, A. (2020). The benefits and threats of blockchain technology in healthcare: A scoping review. *International Journal of Medical Informatics*, 142, 104246. <https://doi.org/10.1016/j.ijmedinf.2020.104246>
- Adams, K. M. (2012). Systems theory: a formal construct for understanding systems. *International Journal of System of Systems Engineering*, 3(3-4), 209-224. <https://doi.org/10.1504/IJSSE.2012.052684>
- Adams, K. M., Hester, P. T., Bradley, J. M., Meyers, T. J., & Keating, C. B. (2014). Systems theory as the foundation for understanding systems. *Systems Engineering*, 17(1), 112-123. <https://doi.org/10.1002/sys.21255>
- Adams, R. J., Smart, P., & Huff, A. S. (2017). Shades of grey: guidelines for working with the grey literature in systematic reviews for management and organizational studies. *International Journal of Management Reviews*, 19(4), 432-454. <https://doi.org/10.1111/ijmr.12102>
- Adomavicius, G., Bockstedt, J. C., Gupta, A., & Kauffman, R. J. (2008). Making sense of technology trends in the information technology landscape: A design science approach. *Mis Quarterly*, 779-809.
- Agostinho, C., & Jardim-Goncalves, R. (2015). Sustaining interoperability of networked liquid-sensing enterprises: A complex systems perspective. *Annual Reviews in Control*, 39, 128-143. <https://doi.org/10.1016/j.arcontrol.2015.03.012>
- Aier, S., & Fischer, C. (2011). Criteria of progress for information systems design theories. *Information Systems and e-Business Management*, 9(1), 133-172. <https://doi.org/10.1007/s10257-010-0130-8>
- Al-Breiki, H., Rehman, M. H. U., Salah, K., & Svetinovic, D. (2020). Trustworthy Blockchain Oracles: Review, Comparison, and Open Research Challenges. *IEEE Access*, 8, 85675-85685. <https://doi.org/10.1109/ACCESS.2020.2992698>
- Al-Jabri, I. M., & Sohail, M. S. (2012). Mobile banking adoption: Application of diffusion of innovation theory. *Journal of Electronic Commerce Research*, 13(4), 379-391. <https://ssrn.com/abstract=2523623>

- Al-Jaroodi, J., & Mohamed, N. (2019, January). Industrial applications of blockchain. In *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 0550-0555). IEEE. <https://doi.org/10.1109/CCWC.2019.8666530>
- Al-Rakhami, M., & Al-Mashari, M. (2022). Interoperability approaches of blockchain technology for supply chain systems. *Business Process Management Journal*(ahead-of-print). <https://doi.org/10.1108/BPMJ-04-2022-0207>
- Albrecht, S., Reichert, S., Schmid, J., Strüker, J., Neumann, D., & Fridgen, G. (2018). Dynamics of blockchain implementation-a case study from the energy sector. Proceedings of the 51st Hawaii International Conference on System Sciences. <http://hdl.handle.net/10125/50334>
- Aliyu, A. A., Singhry, I. M., Adamu, H. A. R. U. N. A., & AbuBakar, M. A. M. (2015, December). Ontology, epistemology and axiology in quantitative and qualitative research: Elucidation of the research philosophical misconception. In *Proceedings of the Academic Conference: Mediterranean Publications & Research International on New Direction and Uncommon* (Vol. 2, No. 1, pp. 1054-1068).
- Alvi, M. (2016). *A manual for selecting sampling techniques in research*. University of Karachi, Iqra University. <https://mpr.a.ub.uni-muenchen.de/id/eprint/70218>
- Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., McCallum, P., & Peacock, A. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renewable and Sustainable Energy Reviews*, 100, 143-174. <https://doi.org/10.1016/j.rser.2018.10.014>
- Angus, D., Rintel, S., & Wiles, J. (2013). Making sense of big text: a visual-first approach for analysing text data using Leximancer and Discursis. *International Journal of Social Research Methodology*, 16(3), 261-267. <https://doi.org/10.1080/13645579.2013.774186>
- Ansari, S. (2004). *Teaching note: Systems theory and management control*. <https://faculty.darden.virginia.edu/ansaris>
- Antwi, S. K., & Hamza, K. (2015). Qualitative and quantitative research paradigms in business research: A philosophical reflection. *European journal of business and management*, 7(3), 217-225. <https://www.iiste.org>
- Aras, S. T., & Kulkarni, V. (2017). Blockchain and its applications—a detailed survey. *International Journal of Computer Applications*, 180(3), 29-35. <https://doi.org/10.5120/ijca2017915994>
- Asiamah, N., Mensah, H., & Oteng-Abayie, E. F. (2017). General, target, and accessible population: Demystifying the concepts for effective sampling. *The Qualitative Report*, 22(6), 1607-1621. <https://doi.org/10.46743/2160-3715/2017.2674>
- ATHENA, D. (2005). Framework for the establishment and management methodology, version 1.0, ATHENA IP. *Interoperability Research for Networked Enterprises Applications and Software*.

- Awa, H. O., Ukoha, O., & Emecheta, B. C. (2016). Using TOE theoretical framework to study the adoption of ERP solution. *Cogent Business & Management*, 3(1), 1196571.
- Babar, M. A., & Gorton, I. (2004, November). Comparison of scenario-based software architecture evaluation methods. In *11th Asia-Pacific software engineering conference* (pp. 600-607). IEEE. <https://doi.org/10.1109/APSEC.2004.38>
- Bandara, H. D., Xu, X., & Weber, I. (2020, July). Patterns for blockchain data migration. In *Proceedings of the European Conference on Pattern Languages of Programs 2020* (pp. 1-19). <https://doi.org/10.1145/3424771.3424796>
- Bank of England, B. o. I. S. I. H. (2023). *Project Meridian: Simplifying transactions through innovation*. <https://www.bis.org/publ/othp63.pdf>
- Bank of Canada. (2018). *Securities Settlement Using Distributed Ledger Technologies (Project Jasper Phase 3)*.
- Bank of Canada, & Monetary Authority of Singapore. (2019). Jasper – Ubin Design Paper: Enabling Cross-Border High Value Transfer Using Distributed Ledger Technologies (Ubin phase 4). <https://www.mas.gov.sg/-/media/MAS/ProjectUbin/Jasper-Ubin-Design-Paper.pdf>
- Bank of Thailand. (2018). *Project Inthanon Phase 1: An application of Distributed Ledger Technology for a Decentralised Real Time Gross Settlement system using Wholesale Central Bank Digital Currency*. https://cdn.crowdfundinsider.com/wp-content/uploads/2019/05/Bank-of-Thailand-CBDC-Inthanon_Phase1_Report.pdf
- Banouar, O., & Raghay, S. (2016). Interoperability of information systems through ontologies: State of art. *International Journal of Computer Science and Information Security*, 14(8), 392. <https://sites.google.com/site/ijcsis/>
- Baskerville, R., Baiyere, A., Gregor, S., Hevner, A., & Rossi, M. (2018). Design science research contributions: Finding a balance between artifact and theory. *Journal of the Association for Information systems*, 19(5), 3. <https://aisel.aisnet.org/jais/vol19/iss5/3/>
- Bauer, J. M., & Schneider, V. (2007). Governance: Prospects of Complexity Theory in Revisiting System Theory.
- Beck, R., Müller-Bloch, C., & King, J. L. (2018). Governance in the blockchain economy: A framework and research agenda. *Journal of the Association for Information systems*, 19(10), 1020-1034. <https://doi.org/10.17705/1jais.00518>
- Bedin, A. R. C., Capretz, M., & Mir, S. (2021). Blockchain for Collaborative Businesses. *Mobile Networks and Applications*, 26(1), 277-284. <https://doi.org/10.1007/s11036-020-01649-6>
- Belchior, R., Riley, L., Hardjono, T., Vasconcelos, A., & Correia, M. (2022). Do You Need a Distributed Ledger Technology Interoperability Solution? *Distributed Ledger Technology: Research and Practice*, 2(1). <https://doi.org/10.1145/3564532>

- Belchior, R., Vasconcelos, A., Correia, M., & Hardjono, T. (2022). Hermes: Fault-tolerant middleware for blockchain interoperability. *Future Generation Computer Systems*, 129, 236-251. <https://doi.org/10.1016/j.future.2021.11.004>
- Belchior, R., Vasconcelos, A., Guerreiro, S., & Correia, M. (2021a). A survey on blockchain interoperability: Past, present, and future trends. *ACM Computing Surveys (CSUR)*, 54(8), 1-41. <https://doi.org/10.1145/3471140>
- Belchior, R., Vasconcelos, A., Guerreiro, S., & Correia, M. (2021b). A Survey on Blockchain Interoperability: Past, Present, and Future Trends [Article]. *Acm Computing Surveys*, 54(8), Article 168. <https://doi.org/10.1145/3471140>
- Bellavista, P., Esposito, C., Foschini, L., Giannelli, C., Mazzocca, N., & Montanari, R. (2021). Interoperable blockchains for highly-integrated supply chains in collaborative manufacturing [Article]. *Sensors*, 21(15), Article 4955. <https://doi.org/10.3390/s21154955>
- Bendassolli, P. F. (2013). Theory building in qualitative research: Reconsidering the problem of induction. In *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research* (Vol. 14, No. 1). <https://doi.org/10.17169/fqs-14.1.1851>
- Beniiche, A. (2020). A study of blockchain oracles. *arXiv preprint arXiv:2004.07140*.
- Benos, E., Garratt, R., & Gurrola-Perez, P. (2019). The economics of distributed ledger technology for securities settlement. *Ledger*, 4, 129-156. <https://doi.org/doi10.5195/LEDGER.2019.144>
- Berg, C. (2022). Interoperability as a critical design choice for central bank digital currencies. *Available at SSRN*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4205405
- Berger, B., Huber, S., & Pfeifhofer, S. (2020). OraclesLink: An architecture for secure oracle usage. In *2020 Second International Conference on Blockchain Computing and Applications (BCCA)* (pp. 66-72). IEEE. <https://doi.org/10.1109/BCCA50787.2020.9274455>
- Bernard, T. J., & Ritti, R. R. (1990). The Role of Theory in Scientific Research. In K. L. Kempf (Ed.), *Measurement Issues in Criminology* (pp. 1-20). Springer New York. https://doi.org/10.1007/978-1-4613-9009-1_1
- Berre, A. J., Elvesæter, B., Figay, N., Guglielmina, C., Johnsen, S. G., Karlsen, D., Knothe, T., & Lippe, S. (2007). The ATHENA Interoperability Framework. Enterprise Interoperability II, London. https://link.springer.com/chapter/10.1007/978-1-84628-858-6_62
- Bertot, J. C., & Choi, H. (2013). *Big data and e-government: issues, policies, and recommendations* Proceedings of the 14th Annual International Conference on Digital Government Research, Quebec, Canada. <https://doi.org/10.1145/2479724.2479730>

- Besançon, L., Da Silva, C. F., & Ghodous, P. (2019, May). Towards blockchain interoperability: Improving video games data exchange. In *2019 IEEE international conference on blockchain and cryptocurrency (ICBC)* (pp. 81-85). IEEE. <https://doi.org/10.1109/BLOC.2019.8751347>
- Bhaskaran, K., Ilfrich, P., Liffman, D., Vecchiola, C., Jayachandran, P., Kumar, A., ... & Suen, C. H. (2018, April). Double-blind consent-driven data sharing on blockchain. In *2018 IEEE international conference on cloud engineering (IC2E)* (pp. 385-391). IEEE. <https://doi.org/10.1109/IC2E.2018.00073>
- Bhatia, R. (2020, October). Interoperability solutions for blockchain. In *2020 international conference on smart technologies in computing, electrical and electronics (ICSTCEE)* (pp. 381-385). IEEE. <https://doi.org/10.1109/ICSTCEE49637.2020.9277054>
- Bhutta, M. N. M., Khwaja, A. A., Nadeem, A., Ahmad, H. F., Khan, M. K., Hanif, M. A., Song, H., Alshamari, M., & Cao, Y. (2021). A survey on blockchain technology: Evolution, architecture and security. *IEEE Access*, *9*, 61048-61073. <https://doi.org/A Survey on Blockchain Technology: Evolution, Architecture and Security>
- Biesta, G. (2010). Pragmatism and the philosophical foundations of mixed methods research. *Sage handbook of mixed methods in social and behavioral research*, *2*, 95-118. <https://dx.doi.org/10.4135/9781506335193.n4>
- Biswas, S., Sharif, K., Li, F., Latif, Z., Kanhere, S. S., & Mohanty, S. P. (2020). Interoperability and synchronization management of blockchain-based decentralized e-health systems. *IEEE Transactions on Engineering Management*, *67*(4), 1363-1376.
- Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives*, *29*(2), 213-238. <https://doi.org/10.1257/jep.29.2.213>
- Boman, J., Currie, G., MacDonald, R., Miller-Young, J., Yeo, M., & Zettel, S. (2017). Overview of Decoding across the Disciplines. *New Directions for Teaching and Learning*, *2017*(150), 13-18.
- Borkowski, M., Sigwart, M., Frauenthaler, P., Hukkinen, T., & Schulte, S. (2019). Dextt: Deterministic Cross-Blockchain Token Transfers [Article]. *IEEE Access*, *7*, 111030-111042. <https://doi.org/10.1109/access.2019.2934707>
- Braun, V., & Clarke, V. (2006). *Using thematic analysis in psychology* (Vol. 3).
- Braun, V., & Clarke, V. (2012). *Thematic analysis*. American Psychological Association.
- Bridgen, S. (2017). Using systems theory to understand the identity of academic advising: A case study. *NACADA Journal*, *37*(2), 9-20.

- Brown, R. G., Carlyle, J., Grigg, I., & Hearn, M. (2016). Corda: an introduction. *R3 CEV, August, 1(15)*, 14.
- Brunnermeier, M. K., James, H., & Landau, J.-P. (2019). *The digitalization of money*. https://www.nber.org/system/files/working_papers/w26300/w26300.pdf
- Burns, T., Cosgrove, J., & Doyle, F. (2019). A Review of Interoperability Standards for Industry 4.0. *Procedia Manufacturing, 38*, 646-653. <https://doi.org/10.1016/j.promfg.2020.01.083>
- Buterin, V. (2016). Chain interoperability. *R3 Research Paper, 9*. <https://allquantor.at/blockchainbib/pdf/buterin2016chain.pdf>
- Buxton, E. C., Burns, E. C., & De Muth, J. E. (2012). Professional development webinars for pharmacists. *American journal of pharmaceutical education, 76(8)*, 155.
- Byrne, D. (2021). A worked example of Braun and Clarke's approach to reflexive thematic analysis. *Quality & Quantity*. <https://doi.org/10.1007/s11135-021-01182-y>
- Caldarelli, G. (2020). Understanding the blockchain oracle problem: A call for action. *Information, 11(11)*, 509. <https://doi.org/10.3390/info11110509>
- Cali, U., Sebastian-Cardenas, D. J., Saha, S., Chandler, S., Gourisetti, S. N. G., Hughes, T., ... & Tillman, L. C. (2022, April). Standardization of smart contracts for energy markets and operation. In *2022 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)* (pp. 1-5). IEEE. <https://doi.org/10.1109/ISGT50606.2022.9817542>
- Campbell-Verduyn, M. (2018). Bitcoin, crypto-coins, and global anti-money laundering governance. *Crime, Law and Social Change, 69(2)*, 283-305. <https://link.springer.com/article/10.1007/s10611-017-9756-5>
- Capocasale, V., & Perboli, G. (2022). Standardizing Smart Contracts. *IEEE Access, 10*, 91203-91212. <https://doi.org/10.1109/ACCESS.2022.3202550>
- Carminati, B., Ferrari, E., & Rondanini, C. (2018, October). Blockchain as a platform for secure inter-organizational business processes. In *2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC)* (pp. 122-129). IEEE. <https://doi.org/10.1109/CIC.2018.00027>
- Caron, F. (2018). The evolving payments landscape: Technological innovation in payment systems. *It Professional, 20(2)*, 53-61. <https://ieeexplore-ieee-org.uplib.idm.oclc.org/stamp/stamp.jsp?tp=&arnumber=8338026>
- Cem Kaner, J. (2003). *An introduction to scenario testing* In Lecture Notes, Center for Software Testing Education and Research, Florida Institute of Technology, <http://www.testingeducation.org/a/scenario2.pdf>
- Central Bank of Norway. (2023). *PROJECT: Experimental test of CBDC*. <https://www.norges-bank.no/en/topics/financial-stability/cbdc>

- Chapman, J., Garratt, R., Hendry, S., McCormack, A., & McMahon, W. (2017). Project Jasper: Are distributed wholesale payment systems feasible yet. *Financial System*, 59. <https://www.bankofcanada.ca/wp-content/uploads/2017/06/fsr-june2017.pdf#page=59>
- Chapurlat, V., & Daclin, N. (2012). System interoperability: definition and proposition of interface model in MBSE Context. *IFAC Proceedings Volumes*, 45(6), 1523-1528. <https://doi.org/10.3182/20120523-3-RO-2023.00174>
- Chau, P. Y., & Tam, K. Y. (1997). Factors affecting the adoption of open systems: an exploratory study. *MIS quarterly*, 21(1), 1-24. <https://doi.org/10.2307/249740>
- Chen, D., & Daclin, N. (2006, January). Framework for enterprise interoperability. In *Interoperability for Enterprise Software and Applications: Proceedings of the Workshops and the Doctorial Symposium of the Second IFAC/IFIP I-ESA International Conference: EI2N, WSI, IS-TSPQ 2006* (pp. 77-88). London, UK: ISTE.
- Chen, D., Doumeingts, G., & Vernadat, F. (2008). Architectures for enterprise integration and interoperability: Past, present and future. *Computers in Industry*, 59(7), 647-659. <https://doi.org/10.1016/j.compind.2007.12.016>
- Chen, S., Goel, T., Qiu, H., & Shim, I. (2022). CBDCs in emerging market economies. *BIS Papers*. <https://dx.doi.org/10.2139/ssrn.4085690>
- Chikere, C. C., & Nwoka, J. (2015). The systems theory of management in modern day organizations-A study of Aldgate congress resort limited Port Harcourt. *International Journal of Scientific and Research Publications*, 5(9), 1-7. <http://www.ijsrp.org>
- Cibangu, S. K. (2010). Paradigms, methodologies, and methods. *Library & information science research*, 32(3), 177-178. <https://doi.org/10.1016/j.lisr.2010.03.006>
- Cicchetti, D., & Rogosch, F. A. (1996). Equifinality and multifinality in developmental psychopathology. *Development and psychopathology*, 8(4), 597-600. <https://doi.org/10.1017/S0954579400007318>
- Clausner, C., Pletschacher, S., & Antonacopoulos, A. (2011, September). Scenario driven in-depth performance evaluation of document layout analysis methods. In *2011 International Conference on Document Analysis and Recognition* (pp. 1404-1408). IEEE. <https://doi.org/10.1109/ICDAR.2011.282>
- Clohessy, T., Acton, T., & Rogers, N. (2019). Blockchain adoption: technological, organisational and environmental considerations. In *Business transformation through blockchain* (pp. 47-76). Springer. <https://doi.org/10.1007/978-3-319-98911-2>
- Coetzee, R. (2019). Towards designing an artefact evaluation strategy for human factors engineering: a lean implementation model case study. *South African Journal of Industrial Engineering*, 30(3), 289-303. <https://hdl.handle.net/10520/EJC-1bf8857a48>

- Committee on Payments and Market Infrastructures. (2018). *Cross-border retail payments*.
<https://www.bis.org/cpmi/publ/d173.pdf>
- Consensys. (2019). *Project i2i: Blockchain Case Study for Payments in the Philippines*.
<https://consensys.io/blockchain-use-cases/finance/project-i2i>
- Cooper, H. M. (1988). Organizing knowledge syntheses: A taxonomy of literature reviews.
Knowledge in society, 1(1), 104.
- Cresswell, J. (2014). *Research design*. Sage publications Thousand Oaks.
- Creswell, J. (2009). *Research Design: Qualitative, Quantitative, and Mixed-Method Approaches*. In (3 ed.). Sage Publication.
- Creswell, J. W. (2013). *Qualitative inquiry and research design: Choosing among five approaches* (Vol. 3). Sage publications.
- Crotty, M. (1998). *The foundations of social research: Meaning and perspective in the research process*. Sage.
- Cruz-Jesus, F., Pinheiro, A., & Oliveira, T. (2019). Understanding CRM adoption stages: empirical analysis building on the TOE framework. *Computers in Industry*, 109, 1-13. <https://doi.org/10.1108/02635571111161262>
- Dagher, G. G., Adhikari, C. L., & Enderson, T. (2017). Towards secure interoperability between heterogeneous blockchains using smart contracts. *Future Technologies Conference (FTC)*, Vol. 2017, pp. 73-81.
- Das, K. (2019). The role and impact of ICT in improving the quality of education: An overview. *International Journal of Innovative Studies in Sociology and Humanities*, 4(6), 97-103.
<https://ijish.org/storage/Volume4/Issue6/IJISSH-040611.pdf>
- Davies, J., Welch, J., Milward, D., & Harris, S. (2020). A formal, scalable approach to semantic interoperability. *Science of Computer Programming*, 192, 102426.
<https://doi.org/10.1016/j.scico.2020.102426>
- De Angelis, S., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., & Sassone, V. (2018). PBFT vs proof-of-authority: Applying the CAP theorem to permissioned blockchain. In *CEUR workshop proceedings* (Vol. 2058). CEUR-WS.
- De Filippi, P. (2016). The interplay between decentralization and privacy: the case of blockchain technologies. *Journal of Peer Production*, Issue(7), 0-18.
<https://ssrn.com/abstract=2852689>
- Denzin, N. (2010). Moments, Mixed Methods, and Paradigm Dialogs. *Qualitative Inquiry*, 16(6), 419-427. <https://doi-org.uplib.idm.oclc.org/10.1177/1077800410364608>
- Denzin, N. K., & Lincoln, Y. S. (2018). *The Sage handbook of qualitative research*. In: Sage publications.

- Derry, S. J., Pea, R. D., Barron, B., Engle, R. A., Erickson, F., Goldman, R., Hall, R., Koschmann, T., Lemke, J. L., & Sherin, M. G. (2010). Conducting video research in the learning sciences: Guidance on selection, analysis, technology, and ethics. *The journal of the learning sciences*, 19(1), 3-53. <https://doi.org/10.1080/10508400903452884>
- Deshpande, A., Stewart, K., Lepetit, L., & Gunashekar, S. (2017). *Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards* (Overview report The British Standards Institution (BSI), Issue.
- Dib, O., Brousmiche, K.-L., Durand, A., Thea, E., & Hamida, E. B. (2018). Consortium blockchains: Overview, applications and challenges. *Int. J. Adv. Telecommun*, 11(1), 51-64. <https://cognizium.io/uploads/resources>
- Dimitrov, I., & Gigov, R. (2020). Exploring Interoperability of Blockchain Technology and the Possibility of Collaboration with the Existing Information Systems of the Enterprises. *3rd International Conference on High Technology for Sustainable Development, HiTech 2020 - Proceedings*, (pp. 1-4). IEEE.
- Doyle, L., Brady, A.-M., & Byrne, G. (2009). An overview of mixed methods research. *Journal of Research in Nursing*, 14(2), 175-185. <https://doi.org/10.1177/1744987108093962>
- Drover, G., & Shragge, E. (1977). General systems theory and social work education: A critique. *Canadian Journal of Social Work Education/Revue canadienne d'éducation en service social*, 28-39. <https://www.jstor.org/stable/41668794>
- Dubois, A., & Gadde, L.-E. (2002). Systematic combining: an abductive approach to case research. *Journal of Business Research*, 55(7), 553-560. [https://doi.org/10.1016/S0148-2963\(00\)00195-8](https://doi.org/10.1016/S0148-2963(00)00195-8)
- Ducq, Y., Chen, D., & Doumeingts, G. (2012). A contribution of system theory to sustainable enterprise interoperability science base. *Computers in Industry*, 63(8), 844-857. <https://doi.org/10.1016/j.compind.2012.08.005>
- Duque, G. G., & Torres, J. D. Z. (2020). Enhancing E-Commerce through Blockchain (DLTs): The Regulatory Paradox for Digital Governance. *Global Jurist*, 20(2). <https://doi.org/doi:10.1515/gj-2019-0049>
- Dybå, T., & Dingsøyr, T. (2008). Strength of evidence in systematic reviews in software engineering. Proceedings of the Second ACM-IEEE International Symposium on Empirical software engineering and measurement, (pp. 178-187)
- Ekwonwune, E. N., Egwuonwu, D. U., Elebri, L. C., & Uka, K. K. (2016). ICT as an instrument of enhanced banking system. *Journal of Computer and Communications*, 5(1), 53-60. <https://doi.org/10.4236/jcc.2017.51005>
- Elmer, F., Seifert, I., Kreibich, H., & Thieken, A. H. (2010). A Delphi method expert survey to derive standards for flood damage data collection. *Risk analysis: An international journal*, 30(1), 107-124. <https://doi.org/10.1111/j.1539-6924.2009.01325.x>

- Elo, S., & Kyngäs, H. (2008). The qualitative content analysis process. *Journal of Advanced Nursing*, 62(1), 107-115.
<https://doi.org/10.1111/j.1365-648.2007.04569.x>
- Elsayed, A. H., & Nasir, M. A. (2022). Central bank digital currencies: An agenda for future research. *Research in International Business and Finance*, 62, 101736.
<https://doi.org/10.1016/j.ribaf.2022.101736>
- European Central Bank, & Bank of Japan. (2018). *Project Stella Phase 2: Securities Settlement Systems: delivery vs payment in a distributed ledger environment*.
https://www.ecb.europa.eu/pub/pdf/other/stella_project_report_march_2018.pdf
- European Central Bank, & Bank of Japan. (2020). *Project Stella Phase 4: Balancing confidentiality and auditability in a distributed ledger environment*.
https://www.boj.or.jp/announcements/release_2020/data/rel200212a1.pdf
- European Commission. (2017). *European Interoperability Framework (EIF)*.
https://ec.europa.eu/isa2/eif_en/
- European Commission. (2020). *Study on Blockchains: Legal, governance and interoperability aspects*.
- Ezzat, S. K., Saleh, Y. N. M., & Abdel-Hamid, A. A. (2022). Blockchain Oracles: State-of-the-Art and Research Directions. *IEEE Access*, 10, 67551-67572.
<https://doi.org/10.1109/ACCESS.2022.3184726>
- Farshidi, S., Jansen, S., España, S., & Verkleij, J. (2020). Decision support for blockchain platform selection: Three industry case studies. *IEEE Transactions on Engineering Management*, 67(4), 1109-1128. <https://doi.org/10.1109/TEM.2019.2956897>
- Fischer, H. R. (2001). Abductive Reasoning as a Way of Worldmaking. *Foundations of Science*, 6(4), 361-383. <https://doi.org/10.1023/A:1011671106610>
- Folorunso, O., Vincent, R. O., Adekoya, A. F., & Ogunde, A. O. (2010). Diffusion of innovation in social networking sites among university students. *International journal of computer science and security*, 4(3), 361-372.
<https://www.researchgate.net/publication/46093467>
- Foster, K., Blakstad, S., Gazi, S., & Bos, M. (2021). Digital currencies and CBDC impacts on least developed countries (LDCs). *The Dialogue on Global Digital Finance Governance Paper Series*.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3871301
- Frizzo-Barker, J., Chow-White, P. A., Adams, P. R., Mentanko, J., Ha, D., & Green, S. (2020). Blockchain as a disruptive technology for business: A systematic review. *International Journal of Information Management*, 51, 102029.
<https://doi.org/10.1016/j.ijinfomgt.2019.10.014>
- Funmi, A., Rosemary, F., Paula, K., & Darelle Van, G. (2013). A Review of Interoperability Standards in E-health and Imperatives for their Adoption in Africa. *South African*

Computer Journal, 0(50). Retrieved 5/5/2022/, from
<https://doaj.org/article/b536132c416a4c1da5b783961692c3abc>

- Gajjar, N. (2013). Ethical consideration in research. *International Journal for Research in Education*, 2(7), 8-15. https://www.raijmr.com/ijre/wp-content/uploads/2017/11/IJRE_2013_vol02_issue_07_02.pdf
- Gao, Z., Li, H., Xiao, K., & Wang, Q. (2020). Cross-chain oracle based data migration mechanism in heterogeneous blockchains. In *2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS)* (pp. 1263-1268). IEEE. <https://doi.org/10.1109/ICDCS47774.2020.00162>
- Garousi, V., Felderer, M., & Mäntylä, M. V. (2019). Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. *Information and Software Technology*, 106, 101-121. <https://doi.org/10.1016/j.infsof.2018.09.006>
- Geerts, G. L. (2011). A design science research methodology and its application to accounting information systems research. *International Journal of Accounting Information Systems*, 12(2), 142-151. <https://doi.org/10.1016/j.accinf.2011.02.004>
- Gegenfurtner, A., & Ebner, C. (2019). Webinars in higher education and professional training: A meta-analysis and systematic review of randomized controlled trials. *Educational Research Review*, 28, 100293.
- Geiger, D., Rosemann, M., & Felt, E. (2011a). Crowdsourcing information systems—a systems theory perspective. <https://aisel.aisnet.org/acis2011/33>
- Geiger, D., Rosemann, M., & Felt, E. (2011b). *Crowdsourcing information systems—a systems theory perspective* ACIS 2011 Proceedings, <https://aisel.aisnet.org/acis2011/33>
- Gerber, A., Kotze, P., & Van der Merwe, A. (2015). *Design Science Research as Research Approach in Doctoral Studies* Twenty-first Americas Conference on Information Systems, Puerto Rico. http://www.cair.org.za/sites/default/files/2019-08/Paper_2_0.pdf
- Ghaemi, S., Rouhani, S., Belchior, R., Cruz, R. S., Khazaei, H., & Musilek, P. (2021). A pub-sub architecture to promote blockchain interoperability. *arXiv preprint arXiv:2101.12331*. <https://doi.org/10.48550/arXiv.2101.12331>
- Ghosh, B. C., Ramakrishna, V., Govindarajan, C., Behl, D., Karunamoorthy, D., Abebe, E., & Chakraborty, S. (2021, 3-6 May 2021). Decentralized Cross-Network Identity Management for Blockchain Interoperation. 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC),
- Gill, P., Stewart, K., Treasure, E., & Chadwick, B. (2008). Methods of data collection in qualitative research: interviews and focus groups. *British Dental Journal*, 204(6), 291-295. <https://doi.org/10.1038/bdj.2008.192>

- Gioia, D. A., & Pitre, E. (1990). Multiparadigm perspectives on theory building. *Academy of management review*, 15(4), 584-602. <http://www.jstor.org/stable/258683>
- Goldkuhl, G. (2008, December 14). What kind of pragmatism in information systems research. AIS SIG Prag inaugural meeting,
- Goldkuhl, G. (2011). Design research in search for a paradigm: Pragmatism is the answer. European Design Science Symposium,
- Goles, T., & Hirschheim, R. (2000). The paradigm is dead, the paradigm is dead...long live the paradigm: the legacy of Burrell and Morgan. *Omega*, 28(3), 249-268. [https://doi.org/10.1016/S0305-0483\(99\)00042-0](https://doi.org/10.1016/S0305-0483(99)00042-0)
- Governatori, G., Idelberger, F., Milosevic, Z., Riveret, R., Sartor, G., & Xu, X. (2018). On legal contracts, imperative and declarative smart contracts, and blockchain systems. *Artificial Intelligence and Law*, 26(4), 377-409. <https://doi.org/10.1007/s10506-018-9223-3>
- Gregor, S. (2006). The nature of theory in information systems. *MIS quarterly*, 611-642. <https://doi.org/10.2307/25148742>
- Gregor, S., & Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. *MIS quarterly*, 337-355. <https://www.jstor.org/stable/43825912>
- Gregory, R., & Muntermann, J. (2011). Theorizing in design science research: inductive versus deductive approaches. *ICIS 2011 Proceedings*.
- Guba, E. G., & Lincoln, Y. S. (1994). Competing paradigms in qualitative research. In *Handbook of qualitative research* (Vol. 2, pp. 105-117). Thousand Oaks.
- Guédria, W., & Naudet, Y. (2014, 2014//). Extending the Ontology of Enterprise Interoperability (OoEI) Using Enterprise-as-System Concepts. Enterprise Interoperability VI, Cham.
- Guo, H., Liu, Y., & Nault, B. R. (2020). *Provisioning Interoperable Disaster Management Systems: Integrated, Unified, and Federated Approaches*. SSRN.
- Guo, H., & Yu, X. (2022). A survey on blockchain technology and its security. *Blockchain: Research and Applications*, 3(2), 100067. <https://doi.org/10.1016/j.bcra.2022.100067>
- Guo, Y., & Liang, C. (2016). Blockchain application and outlook in the banking industry. *Financial Innovation*, 2(1), 24. <https://doi.org/10.1186/s40854-016-0034-9>
- Habbershon, T. G., Williams, M., & MacMillan, I. C. (2003). A unified systems perspective of family firm performance. *Journal of Business Venturing*, 18(4), 451-465. [https://doi.org/10.1016/S0883-9026\(03\)00053-3](https://doi.org/10.1016/S0883-9026(03)00053-3)
- Haig, B. D. (2008). Scientific method, abduction, and clinical reasoning. *Journal of Clinical Psychology*, 64(9), 1013-1018. <https://doi.org/10.1002/jclp.20505>

- Ham, J., Lee, J.-N., Kim, D., & Choi, B. (2015). *Open innovation maturity model for the government: An open system perspective* Thirty Sixth International Conference on Information Systems, Fort Worth <https://core.ac.uk/download/pdf/301367394.pdf>
- Han, X., Yuan, Y., & Wang, F.-Y. (2019). *A blockchain-based framework for central bank digital currency* 2019 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), Zhengzhou, China.
- Hardjono, T., Lipton, A., & Pentland, A. (2019). Toward an interoperability architecture for blockchain autonomous systems. *IEEE Transactions on Engineering Management*, 67(4), 1298-1309. <https://doi.org/10.1109/TEM.2019.2920154>
- Hardjono, T., Lipton, A., & Pentland, A. (2020). Toward an Interoperability Architecture for Blockchain Autonomous Systems [Article]. *IEEE Transactions on Engineering Management*, 67(4), 1298-1309, Article 8743548. <https://doi.org/10.1109/TEM.2019.2920154>
- Hassan, A., Makhdoom, I., Iqbal, W., Ahmad, A., & Raza, A. (2023). From trust to truth: Advancements in mitigating the Blockchain Oracle problem. *Journal of Network and Computer Applications*, 217, 103672. <https://doi.org/10.1016/j.jnca.2023.103672>
- Haugum, T., Hoff, B., Alsadi, M., & Li, J. (2022b). *Security and Privacy Challenges in Blockchain Interoperability - A Multivocal Literature Review* Proceedings of the International Conference on Evaluation and Assessment in Software Engineering 2022, Gothenburg, Sweden. <https://doi-org.uplib.idm.oclc.org/10.1145/3530019.3531345>
- Hayes, B. K., Heit, E., & Swendsen, H. (2010). Inductive reasoning. *Wiley interdisciplinary reviews: Cognitive science*, 1(2), 278-292. <https://doi.org/10.1002/wcs.44>
- Hegnauer, T. (2019). Design and development of a blockchain interoperability API. *Zürich, Switzerland, February*.
- Herlihy, M. (2018). *Atomic Cross-Chain Swaps* Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing, Egham, United Kingdom. <https://doi.org/10.1145/3212734.3212736>
- Herold, D. M., Saberi, S., Kouhizadeh, M., & Wilde, S. (2022). Categorizing transaction costs outcomes under uncertainty: a blockchain perspective for government organizations. *Journal of Global Operations and Strategic Sourcing*, 15(3), 431-448. <https://doi.org/10.1108/JGOSS-09-2021-0066>
- Herrada, J., & Lawson, A. N. (2022). Fit-for-Purpose Payment System Interoperability: A Framework. *FEDS Notes*(2022-07), 14-12. <https://doi.org//10.17016/2380-7172.3136>
- Hesse-Biber, S. (2015). Mixed Methods Research: The “Thing-ness” Problem. *Qualitative Health Research*, 25(6), 775-788. <https://doi.org/10.1177/1049732315580558>
- Hevner, A. R. (2007). A three cycle view of design science research. *Scandinavian journal of information systems*, 19(2), 4. <http://aisel.aisnet.org/sjis/vol19/iss2/4>

- Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS quarterly*, 75-105. <https://www.jstor.org/stable/25148625>
- Hewett, N., van Gogh, M., & Pawczuk, L. (2020). *Inclusive Deployment of Blockchain for Supply Chains: Part 6 – A Framework for Blockchain Interoperability*. <https://www.weforum.org/whitepapers/inclusive-deployment-of-blockchain-for-supply-chains-part-6-a-framework-for-blockchain-interoperability>
- Higgins, J. P., Altman, D. G., Gøtzsche, P. C., Jüni, P., Moher, D., Oxman, A. D., Savović, J., Schulz, K. F., Weeks, L., & Sterne, J. A. (2011). The Cochrane Collaboration's tool for assessing risk of bias in randomised trials. *Bmj*, 343. <https://doi.org/10.1136/bmj.d5928>
- Hirschheim, R., & Klein, H. K. (1989). Four paradigms of information systems development. *Communications of the ACM*, 32(10), 1199-1216. <https://doi.org/10.1145/67933.67937>
- Hitarshi, B. (2020). *Enterprise Integration and Interoperability of Blockchain*. <https://www.networkcomputing.com/author/hitarshi-buch>
- Hodapp, D., & Hanelt, A. (2022). Interoperability in the era of digital innovation: An information systems research agenda. *Journal of Information Technology*, 37(4), 407-427. <https://doi.org/10.1177/02683962211064304>
- Hong Kong Monetary Authority, & Bank of Thailand. (2018). *Inthanon-LionRock Leveraging Distributed Ledger Technology to Increase Efficiency in Cross-Border Payments*. https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/Report_on_Project_Inthanon-LionRock.pdf
- Hosseini, M., & Dixon, B. E. (2016). Chapter 8 - Syntactic Interoperability and the Role of Standards. In B. E. Dixon (Ed.), *Health Information Exchange* (pp. 123-136). Academic <https://doi.org/10.1016/B978-0-12-803135-3.00008-6>
- Hovorka, D. (2009). Design Science Research: A call for a pragmatic perspective. Proceedings of SIGPrag Workshop, Sprouts Working Papers on Information Systems, 322. https://aisel.aisnet.org/sprouts_all/322
- Huber, R., D'Onofrio, C., Devaraju, A., Klump, J., Loescher, H. W., Kindermann, S., Guru, S., Grant, M., Morris, B., Wyborn, L., Evans, B., Goldfarb, D., Genazzio, M. A., Ren, X., Magagna, B., Thiemann, H., & Stocker, M. (2021). Integrating data and analysis technologies within leading environmental research infrastructures: Challenges and approaches. *Ecological Informatics*, 61, 101245. <https://doi.org/10.1016/j.ecoinf.2021.101245>
- Hughes, L., Dwivedi, Y. K., Misra, S. K., Rana, N. P., Raghavan, V., & Akella, V. (2019). Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. *International Journal of Information Management*, 49, 114-129. <https://doi.org/10.1016/j.ijinfomgt.2019.02.005>
- Hurley, P. J. (2000). *A concise introduction to logic* (7th ed.). Wadsworth Pub.

- Hutchinson, G. S., & Oltedal, S. (2014). Five theories in social work.
- Hyde, K. F. (2000). Recognising deductive processes in qualitative research. *Qualitative market research*, 3(2), 82-89. <https://doi.org/10.1108/13522750010322089>
- Hyoungh Seok, S. (2019). Reasoning processes in clinical reasoning: from the perspective of cognitive psychology. *Korean Journal of Medical Education*, 31(4), 299-308. <https://doi.org/10.3946/kjme.2019.140>
- Ide, N., & Pustejovsky, J. (2010). What does interoperability mean, anyway? Toward an operational definition of interoperability for language technology. Proceedings of the Second International Conference on Global Interoperability for Language Resources. Hong Kong, China.
- IEEE Computer Society. (1991). IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries. In *IEEE Std 610* (pp. 1-217).
- ISO/IEC International Standard. (2011). ISO/IEC 13066-1:2011. Information technology - Interoperability with assistive technology(AT) --Part1:Requirements and recommendations for interoperability.
- Jaccard, J., & Jacoby, J. (2010). *Theory construction and model-building skills : a practical guide for social scientists*. Guilford Press.
- Janiszewski, C., & van Osselaer, S. M. (2022). Abductive theory construction. *Journal of Consumer Psychology*, 32(1), 175-193. <https://doi.org/10.1002/jcpy.1280>
- Javaid, M., Haleem, A., Singh, R. P., Suman, R., & Khan, S. (2022). A review of Blockchain Technology applications for financial services. *BenchCouncil Transactions on Benchmarks, Standards and Evaluations*, 2(3), 100073. <https://doi.org/10.1016/j.tbench.2022.100073>
- Jin, H., Dai, X., & Xiao, J. (2018, July). Towards a novel architecture for enabling interoperability amongst multiple blockchains. In *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)* (pp. 1203-1211). IEEE. <https://doi.org/10.1109/ICDCS.2018.00120>
- Joffe, H. (2012). Thematic analysis. *Qualitative research methods in mental health and psychotherapy*, 1, 210-223.
- Johannesson, P., Perjons, E., Johannesson, P., & Perjons, E. (2021). Evaluate artefact. *An introduction to design science*, 141-152. https://doi.org/10.1007/978-3-030-78132-3_9
- Johnson, R. A., Kast, F. E., & Rosenzweig, J. E. (1964). Systems Theory and Management. *Management Science*, 10(2), 367-384. <http://www.jstor.org/stable/2627306>
- Johnson, S., Robinson, P., & Brainard, J. (2019). Sidechains and interoperability. *arXiv preprint arXiv:1903.04077*. <https://arxiv.org/pdf/1903.04077.pdf>

- Juels, A., Kosba, A., & Shi, E. (2016, October 2016). The ring of gyges: Investigating the future of criminal smart contracts. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security,
- Jung, H., & Jeong, D. (2021). Blockchain implementation method for interoperability between CDBC's [Article]. *Future Internet*, 13(5), Article 133. <https://doi.org/10.3390/fi13050133>
- Karaarslan, E., & Konacaklı, E. (2020). Data storage in the decentralized world: Blockchain and derivatives. *arXiv preprint arXiv:2012.10253*. <https://arxiv.org/ftp/arxiv/papers/2012/2012.10253.pdf>
- Kast, F. E., & Rosenzweig, J. E. (1972). General systems theory: Applications for organization and management. *Academy of management journal*, 15(4), 447-465. <https://www.jstor.org/stable/26815585>
- Katehakis, D. G., Kouroubali, A., & Fundulaki, I. (2018). Towards the Development of a National eHealth Interoperability Framework to Address Public Health Challenges in Greece. SWH@ ISWC.
- Katrakazas, P., Pasiadis, K., Bibas, A., & Koutsouris, D. (2020). A General Systems Theory Approach in Public Hearing Health: Lessons Learned From a Systematic Review of General Systems Theory in Healthcare. *IEEE Access*, 8, 53018-53033. <https://doi.org/10.1109/ACCESS.2020.2981160>
- Katz, D., & Kahn, R. L. (1978). Organizations and the system concept. *Classics of organization theory*, 80(480), 27.
- Kaushik, V., & Walsh, C. A. (2019). Pragmatism as a research paradigm and its implications for social work research. *Social Sciences*, 8(9), 255. <https://doi.org/10.3390/socsci8090255>
- Kelemen, M., & Rumens, N. (2012). Pragmatism and heterodoxy in organization research: Going beyond the quantitative/qualitative divide. *International Journal of Organizational Analysis*. <http://www.emeraldinsight.com/1934-8835.htm>
- Kelly, L. M., & Cordeiro, M. (2020). Three principles of pragmatism for research on organizational processes. *Methodological Innovations*, 13(2), 205979912093724. <https://doi.org/10.1177/2059799120937242>
- Khan, S., Amin, M. B., Azar, A. T., & Aslam, S. (2021). Towards Interoperable Blockchains: A Survey on the Role of Smart Contracts in Blockchain Interoperability [Article]. *IEEE Access*, 9, 116672-116691. <https://doi.org/10.1109/ACCESS.2021.3106384>
- Kim, J. (2012). Scenarios in information seeking and information retrieval research: A methodological application and discussion. *Library & Information Science Research*, 34(4), 300-307. <https://doi.org/10.1016/j.lisr.2012.04.002>
- Kitchenham, B. (2004). *Procedures for performing systematic reviews* (TR/SE-0401). (Keele University Technical Report, Issue.

https://www.researchgate.net/publication/228756057_Procedures_for_Performing_Systematic_Reviews?

- Knoblauch, H., Tuma, R., & Schnettler, B. (2014). Video analysis and videography. In U. Flick (Ed.), *The SAGE handbook of qualitative data analysis* (pp. 435-449). SAGE. <https://books.google.co.za/>
- Koens, T., & Poll, E. (2019). Assessing interoperability solutions for distributed ledgers. *Pervasive and Mobile Computing*, 59, 101079. <https://doi.org/10.1016/j.pmcj.2019.101079>
- Kotey, S. D., Tchao, E. T., Ahmed, A. R., Agbemenu, A. S., Nunoo-Mensah, H., Sikora, A., Welte, D., & Keelson, E. (2023). Blockchain interoperability: the state of heterogenous blockchain-to-blockchain communication. *IET Communications*, 17(8), 891-914.
- Kothari, C. R. (2004). *Research methodology: Methods and techniques*. New Age International.
- Kouroubali, A., & Katehakis, D. G. (2019). The new European interoperability framework as a facilitator of digital transformation for citizen empowerment. *Journal of Biomedical Informatics*, 94, 103166. <https://doi.org/10.1016/j.jbi.2019.103166>
- Kshetri, N. (2021). The Economics of Central Bank Digital Currency [Computing's Economics]. *Computer*, 54(6), 53-58. <https://doi.org/10.1109/MC.2021.3070091>
- Kuechler, W., & Vaishnavi, V. (2012). A Framework for Theory Development in Design Science Research: Multiple Perspectives. *Journal of the Association of Information Systems*, 13, 395-423. <https://doi.org/10.17705/1jais.00300>
- Lai, C.-H., & Huili Lin, S. (2017). Systems Theory. In *The international encyclopedia of organizational communication* (pp. 1-18). John Wiley & Sons. <https://doi.org/10.1002/9781118955567.wbieoc203>
- Lakhani, K., & Iansiti, M. (2017). The truth about blockchain. *Harvard Business Review*, 95(1), 119-127. <https://hbr.org/2017/01/the-truth-about-blockchain>
- Lampasona, C., Diebold, P., Eckhardt, J., & Schneider, R. (2014, September). Evaluation in practice: artifact-based requirements engineering and scenarios in smart mobility domains. In *Proceedings of the 8th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement* (pp. 1-8).
- Larios-Hernández, G. J. (2017). Blockchain entrepreneurship opportunity in the practices of the unbanked. *Business Horizons*, 60(6), 865-874. <https://doi.org/10.1016/j.bushor.2017.07.012>
- Lehmann, M. (2019). Who Owns Bitcoin: Private Law Facing the Blockchain. *Minn. JL Sci. & Tech.*, 21, 93. <https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1474&context=mjlst>

- Lehne, M., Sass, J., Essenwanger, A., Schepers, J., & Thun, S. (2019). Why digital medicine depends on interoperability. *NPJ digital medicine*, 2(1), 1-5. <https://www.nature.com/articles/s41746-019-0158-1>
- Lemrabet, Y., Bigand, M., Clin, D., Benkeltoum, N., & Bourey, J.-P. (2010). *Model driven interoperability in practice: preliminary evidences and issues from an industrial project* Proceedings of the First International Workshop on Model-Driven Interoperability, Oslo, Norway. <https://doi-org.uplib.idm.oclc.org/10.1145/1866272.1866274>
- Levin-Rozalis, M. (2004). Searching for the Unknowable: A Process of Detection — Abductive Research Generated by Projective Techniques. *International Journal of Qualitative Methods*, 3(2), 1-18. <https://doi.org/10.1177/160940690400300201>
- Li, D., Wong, W. E., & Guo, J. (2020, January). A survey on blockchain for enterprise using hyperledger fabric and composer. In *2019 6th International Conference on Dependable Systems and Their Applications (DSA)* (pp. 71-80). IEEE. <https://doi.org/10.1109/DSA.2019.00017>
- Li, Z., Barenji, A. V., & Huang, G. Q. (2018). Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform. *Robotics and Computer-Integrated Manufacturing*, 54, 133-144. <https://doi.org/10.1016/j.rcim.2018.05.011>
- Liberati, A., Altman, D. G., Tetzlaff, J., Mulrow, C., Gøtzsche, P. C., Ioannidis, J. P., Clarke, M., Devereaux, P. J., Kleijnen, J., & Moher, D. (2009). The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: explanation and elaboration. *Journal of clinical epidemiology*, 62(10), e1-e34. <https://doi.org/10.1016/j.jclinepi.2009.06.006>
- Lima, C. (2018). Developing Open and Interoperable DLT/Blockchain Standards [Standards]. *Computer*, 51(11), 106-111. <https://doi.org/10.1109/MC.2018.2876184>
- Lin, S., Kong, Y., Nie, S., Xie, W., & Du, J. (2021, 29-30 May 2021). Research on Cross-chain Technology of Blockchain. 2021 6th International Conference on Smart Grid and Electrical Automation (ICSGEA),
- Lipton, A., & Hardjono, T. (2022). Blockchain Intra- and Interoperability. In *Springer Series in Supply Chain Management* (Vol. 13, pp. 1-30).
- Liu, S., Mu, T., Xu, S., & He, G. (2022). *Research on cross-chain method based on distributed Digital Identity* The 2022 4th International Conference on Blockchain Technology, Shanghai, China. <https://doi.org/uplib.idm.oclc.org/10.1145/3532640.3532649>
- Liu, Z., Xiang, Y., Shi, J., Gao, P., Wang, H., Xiao, X., Wen, B., & Hu, Y.-C. (2019). *HyperService: Interoperability and Programmability Across Heterogeneous Blockchains* Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, London, United Kingdom. <https://doi-org.uplib.idm.oclc.org/10.1145/3319535.3355503>

- Lohachab, A., Garg, S., Kang, B., Amin, M. B., Lee, J., Chen, S., & Xu, X. (2021). Towards Interconnected Blockchains: A Comprehensive Review of the Role of Interoperability among Disparate Blockchains. *ACM Comput. Surv.*, *54*(7), Article 135. <https://doi.org/10.1145/3460287>
- Lom, M., & Pribyl, O. (2021). Smart city model based on systems theory. *International Journal of Information Management*, *56*, 102092. <https://doi.org/10.1016/j.ijinfomgt.2020.102092>
- Loutas, N., Kamateri, E., & Tarabanis, K. (2011, November). A semantic interoperability framework for cloud platform as a service. In *2011 IEEE Third International Conference on Cloud Computing Technology and Science* (pp. 280-287). IEEE. <https://doi.org/10.1109/CloudCom.2011.45>
- Low, C., Chen, Y., & Wu, M. (2011). Understanding the determinants of cloud computing adoption. *Industrial management & data systems*, *111*(7), 1006-1023. <https://doi.org/10.1108/026355711111161262>
- Lu, S., Pei, J., Zhao, R., Yu, X., Zhang, X., Li, J., & Yang, G. (2023). CCIO: A Cross-Chain Interoperability Approach for Consortium Blockchains Based on Oracle. *Sensors*, *23*(4), 1864. <https://www.mdpi.com/1424-8220/23/4/1864>
- Lukka, K., & Modell, S. (2010). Validation in interpretive management accounting research. *Accounting, Organizations and Society*, *35*(4), 462-477. <https://doi.org/10.1016/j.aos.2009.10.004>
- Lyytinen, K., & Damsgaard, J. (2001). What's wrong with the diffusion of innovation theory? The case of a complex and networked technology. In *Diffusing Software Product and Process Innovations: IFIP TC8 WG8. 6 Fourth Working Conference on Diffusing Software Product and Process Innovations April 7–10, 2001, Banff, Canada 4* (pp. 173-190). Springer US. https://doi.org/10.1007/978-0-387-35404-0_19
- Mahood, Q., Van Eerd, D., & Irvin, E. (2014). Searching for grey literature for systematic reviews: challenges and benefits. *Research Synthesis Methods*, *5*(3), 221-234. <https://doi.org/10.1002/jrsm.1106>
- March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems*, *15*(4), 251-266. [https://doi.org/10.1016/0167-9236\(94\)00041-2](https://doi.org/10.1016/0167-9236(94)00041-2)
- Marczyk, G., DeMatteo, D., & Festinger, D. (2005). *Essentials of research design and methodology*. John Wiley & sons, Inc.
- Mele, C., Pels, J., & Polese, F. (2010). A brief review of systems theories and their managerial applications. *Service science*, *2*(1-2), 126-135. <https://ssrn.com/abstract=2003159>
- Melnikovas, A. (2018). Towards an explicit research methodology: Adapting research onion model for futures studies. *Journal of Futures Studies*, *23*(2), 29-44. [https://doi.org/10.6531/JFS.201812_23\(2\).0003](https://doi.org/10.6531/JFS.201812_23(2).0003)

- Mending, J., Weber, I., Aalst, W. V. D., Brocke, J. V., Cabanillas, C., Daniel, F., Debois, S., Ciccio, C. D., Dumas, M., & Dustdar, S. (2018). Blockchains for business process management-challenges and opportunities. *ACM Transactions on Management Information Systems (TMIS)*, 9(1), 1-16.
<https://doi.org/10.1145/3183367>
- Merriam, S. B., & Tisdell, E. J. (2016). *Qualitative research : a guide to design and implementation* (Fourth edition. ed.). John Wiley & Sons. <https://books.google.com>
- Miller, R. L., & Brewer, J. D. (2003). *The AZ of social research: A dictionary of key social science research concepts*. Sage.
- Millett, B. (1998). Understanding organisations: the dominance of systems theory. *International Journal of Organisational Behaviour*, 1(1), 1-12.
<https://www.researchgate.net/profile/Bruce-Millett-2/publication/228691593>
- Mirza, A. M., Khan, M. N. A., Wagan, R. A., Laghari, M. B., Ashraf, M., Akram, M., & Bilal, M. (2021). ContextDrive: Towards a Functional Scenario-Based Testing Framework for Context-Aware Applications. *IEEE Access*, 9, 80478-80490.
<https://doi.org/10.1109/ACCESS.2021.3084887>
- Mishi, S., Sibanda, K., & Tsegaye, A. (2016). Industry concentration and risk taking: Evidence from the South African banking sector. *African Review of Economics and Finance*, 8(2), 113-135. <https://www.ajol.info/index.php/aref/article/view/162158>
- Mohamed Shaffril, H. A., Samsuddin, S. F., & Abu Samah, A. (2021). The ABC of systematic literature review: the basic methodological guidance for beginners. *Quality & Quantity*, 55, 1319-1346. <https://doi.org/10.1007/s11135-020-01059-6>
- Mohanty, D., Anand, D., Aljahdali, H. M., & Santos Gracia, V. (2022). Blockchain Interoperability: Towards a Sustainable Payment System. *Sustainability*, 14(2), 913.
<https://doi.org/10.3390/su14020913>
- Monetary Authority of Singapore. (2017a). *Re-imagining Interbank Real-Time Gross Settlement System Using Distributed Ledger Technologies (Project Ubin Phase 2)*. <https://www.mas.gov.sg/-/media/MAS/ProjectUbin/Project-Ubin-Phase-2-Reimagining-RTGS.pdf>
- Monetary Authority of Singapore. (2017b). *SDG on Distributed Ledger (Project Ubin Phase 1)*. <https://www.mas.gov.sg/-/media/MAS/ProjectUbin/Project-Ubin--SGD-on-Distributed-Ledger.pdf>
- Monetary Authority of Singapore, & Bank of Canada. (2019). *Jasper – Ubin Design Paper Enabling Cross-Border High Value Transfer Using Distributed Ledger Technologies*. <https://www.mas.gov.sg/-/media/Jasper-Ubin-Design-Paper.pdf>
- Monika, R. & Bhatia, R. (2020, 9-10 Oct. 2020). Interoperability solutions for blockchain. Proceedings of the International Conference on Smart Technologies in Computing, Electrical and Electronics, ICSTCEE 2020, (pp. 381-385). IEEE.
<https://doi.org/10.1109/ICSTCEE49637.2020.9277054>

- Monrat, A. A., Schelén, O., & Andersson, K. (2020, December). Performance evaluation of permissioned blockchain platforms. In *2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)* (pp. 1-8). IEEE. <https://doi.org/10.1109/CSDE50874.2020.9411380>
- Moon, M. D. (2019). Triangulation: A method to increase validity, reliability, and legitimation in clinical research. *Journal of emergency nursing*, *45*(1), 103-105. <https://doi.org/10.1016/j.jen.2018.11.004>
- Morabito, V. (2017). *Business innovation through blockchain*. <https://doi.org/10.1007/978-3-319-48478-5>
- Morales-Resendiz, R., Ponce, J., Picardo, P., Velasco, A., Chen, B., Sanz, L., Guiborg, G., Segendorff, B., Vasquez, J. L., & Arroyo, J. (2021). Implementing a retail CBDC: Lessons learned and key insights. *Latin American Journal of Central Banking*, *2*(1), 100022. <https://doi.org/10.1016/j.latcb.2021.100022>
- Moreno, S. M. d. B. M., & Seigneur, J.-M. (2022). *Enabling KYC and AML verification in DeFi services* Actes de conférence, Zug, Switzerland. <https://archive-ouverte.unige.ch/unige:165553>
- Morgan, D. L. (2007). Paradigms lost and pragmatism regained: Methodological implications of combining qualitative and quantitative methods. *Journal of Mixed Methods Research*, *1*(1), 48-76. <https://doi.org/10.1177%2F2345678906292462>
- Morgan, D. L. (2014). Pragmatism as a paradigm for social research. *Qualitative inquiry*, *20*(8), 1045-1053. <https://doi.org/10.1177%2F1077800413513733>
- Moyano, J. P., & Ross, O. (2017). KYC optimization using distributed ledger technology. *Business & Information Systems Engineering*, *59*(6), 411-423. <https://doi.org/10.1007/s12599-017-0504-2>
- Mueller, B., & Urbach, N. (2017). Understanding the why, what, and how of theories in IS research. *Communications of the Association for Information Systems*, *41*, 349-388. <http://aisel.aisnet.org/cais/vol41/iss1/17>
- Mwansa, G. (2015). *Exploring the development of a framework for agile methodologies to promote the adoption and use of cloud computing services in South Africa* http://uir.unisa.ac.za/bitstream/handle/10500/21159/thesis_mwansa_g.pdf
- Nadahalli, T., Khabbazian, M., & Wattenhofer, R. (2022, May). Grief-free Atomic Swaps. In *2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (pp. 1-9). IEEE. <https://doi.org/10.1109/ICBC54727.2022.9805490>
- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, 21260. www.bitcoin.org/pdf4
- Nakamoto, S. (2009). Bitcoin: A peer-to-peer electronic cash system Bitcoin: A Peer-to-Peer Electronic Cash System. *Bitcoin. org*. Disponible en <https://bitcoin.org/en/bitcoin-paper>.

- National Bank of Cambodia. (2020). *Project Bakong: Next Generation Payment System*.
<https://bakong.nbc.org.kh>
- Naudet, Y., Latour, T., Guedria, W., & Chen, D. (2010). Towards a systemic formalisation of interoperability. *Computers in Industry*, 61(2), 176-185.
<https://doi.org/10.1016/j.compind.2009.10.014>
- Nazarov, S., Shukla, P., Erwin, A., & Rajput, A. (2020). Bridging the Governance Gap: Interoperability for blockchain and legacy systems. *World Economic Forum whitepaper*. <https://www.weforum.org/whitepapers/bridging-the-governance-gap-interoperability-for-blockchain-and-legacy-systems>
- Ndlovu, K., Mars, M., & Scott, R. E. (2021). Interoperability frameworks linking mHealth applications to electronic record systems. *BMC Health Services Research*, 21(1), 459. <https://doi.org/10.1186/s12913-021-06473-6>
- Nguyen, G.-T., & Kim, K. (2018). A Survey about Consensus Algorithms Used in Blockchain. *Journal of Information Processing Systems*, 14(1).
<https://doi.org/10.3745/JIPS.01.0024>
- Nier, E. W. (2009). *Financial stability frameworks and the role of central banks: lessons from the crisis*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1378882
- Nightingale, A. (2009). A guide to systematic literature reviews. *Surgery (Oxford)*, 27(9), 381-384. <https://doi.org/10.1016/j.mpsur.2009.07.005>
- Nissl, M., Sallinger, E., Schulte, S., & Borkowski, M. (2021, August). Towards cross-blockchain smart contracts. In *2021 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS)* (pp. 85-94). IEEE.
<https://doi.org/10.1109/DAPPS52256.2021.00015>
- Niya, S. R., Dordevic, D., & Stiller, B. (2021, May). Itrade: a blockchain-based, self-sovereign, and scalable marketplace for iot data streams. In *2021 IFIP/IEEE International Symposium on Integrated Network Management (IM)* (pp. 530-536). IEEE.
- Noble, H., & Heale, R. (2019). Triangulation in research, with examples. *Evidence Based Nursing*, 22(3), 67-68. <https://doi.org/10.1136/ebnurs-2019-103145>
- Nodehi, T., Zutshi, A., Grilo, A., & Rizvanovic, B. (2022). EBDF: The enterprise blockchain design framework and its application to an e-Procurement ecosystem. *Computers & Industrial Engineering*, 171, 108360. <https://doi.org/10.1016/j.cie.2022.108360>
- Novakouski, M., & Lewis, G. A. (2012). *Interoperability in the e-Government Context*.
<https://apps.dtic.mil/sti/citations/ADA611103>
- Nyakundi, N. B. N., Reynolds, S. M., & Reza, H. (2023, 18-20 May 2023). Scenario-Based Approach to Systematically Derive Test Cases for Systems. 2023 IEEE International Conference on Electro Information Technology (eIT),

- Offermann, P., Levina, O., Schönherr, M., & Bub, U. (2009). Outline of a design science research process. Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology,
- Okoli, C. (2015). A guide to conducting a standalone systematic literature review. *Communications of the Association for Information Systems*, 37. <https://hal.science/hal-01574600/>
- Okoli, C., & Schabram, K. (2010). A guide to conducting a systematic literature review of information systems research.
- Oliveira, T., & Martins, M. F. (2010, September 2010). Information technology adoption models at firm level: review of literature. The European Conference on Information Systems Management,
- Onwuegbuzie, A. J., & Collins, K. M. (2007). A typology of mixed methods sampling designs in social science research. *Qualitative report*, 12(2), 281-316. <http://www.nova.edu/ssss/QR/QR12-2/onwuegbuzie2.pdf>
- Orlikowski, W. J., & Baroudi, J. J. (1991). Studying information technology in organizations: Research approaches and assumptions. *Information systems research*, 2(1), 1-28.
- Oyedele, A., Owolabi, H. A., Oyedele, L. O., & Olawale, O. A. (2020). Big data innovation and diffusion in projects teams: Towards a conflict prevention culture. *Developments in the Built Environment*, 3, 100016. <https://doi.org/10.1016/j.dibe.2020.100016>
- Ozili, P. K. (2022). Central bank digital currency in Nigeria: opportunities and risks. In *The New Digital Era: Digitalisation, Emerging Risks and Opportunities* (Vol. 109, pp. 125-133). Emerald Publishing Limited. https://mpra.ub.uni-muenchen.de/110291/1/MPRA_paper_110291.pdf
- Paez, A. (2017). Gray literature: An important resource in systematic reviews. *Journal of Evidence-Based Medicine*, 10(3), 233-240.
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., & Brennan, S. E. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *Bmj*, 372. <https://doi.org/10.1136/bmj.n71>
- Panetta, F. (2018). *21st century cash: Central banking, technological innovation and digital currencies* (40). (Do we need central bank digital currency, Issue. https://www.suerf.org/docx/f_504c296f8eb5fd521e744da4e8371f28_3251_suerf.pdf
- Pang, Y. (2020). A New Consensus Protocol for Blockchain Interoperability Architecture. *IEEE Access*, 8, 153719-153730. <https://doi.org/10.1109/ACCESS.2020.3017549>
- Paradis, E., O'Brien, B., Nimmon, L., Bandiera, G., & Martimianakis, M. A. (2016). Design: Selection of data collection methods. *Journal of graduate medical education*, 8(2), 263-264. <https://doi.org/10.4300/JGME-D-16-00098.1>

- Parino, F., Beiró, M. G., & Gauvin, L. (2018). Analysis of the Bitcoin blockchain: socio-economic factors behind the adoption. *EPJ Data Science*, 7(1), 38. <https://link.springer.com/article/10.1140/epjds/s13688-018-0170-8>
- Park, Y. S., Konge, L., & Artino Jr, A. R. (2020). The positivism paradigm of research. *Academic Medicine*, 95(5), 690-694. <https://doi.org/10.1097/ACM.000000000000309>
- Pasdar, A., Lee, Y. C., & Dong, Z. (2023). Connect API with Blockchain: A Survey on Blockchain Oracle Implementation. *ACM Comput. Surv.*, 55(10), Article 208. <https://doi.org/10.1145/3567582>
- Patel, H., & Connolly, R. (2007). Factors influencing technology adoption: A review. *Information Management in the Networked Economy: Issues & Solutions*, 416-431.
- Pather, S., & Remenyi, D. (2005). Some of the philosophical issues underpinning research in information systems-from positivism to critical realism: reviewed article. *South African Computer Journal*, 2005(35), 76-83. <https://hdl.handle.net/10520/EJC27994>
- Patton, M. Q. (2002). *Qualitative research & evaluation methods*. sage.
- Payments Canada, Bank of Canada, & R3. (2017). A Canadian Experiment with Distributed Ledger Technology for Domestic Interbank Payments Settlement (Project Jasper). https://www.payments.ca/sites/default/files/29-Sep-17/jasper_report_eng.pdf
- Peppers, K., Rothenberger, M., Tuunanen, T., & Vaezi, R. (2012). Design Science Research Evaluation. *Design Science Research in Information Systems. Advances in Theory and Practice*, Berlin, Heidelberg.
- Peppers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of management information systems*, 24(3), 45-77. <https://doi.org/10.2753/MIS0742-1222240302>
- Peirce, C. S. (1974). *Collected papers of charles sanders peirce* (Vol. 5). Harvard University Press. <https://books.google.co.za/>
- Peslak, A., Ceccucci, W., & Sendall, P. (2010). An empirical study of social networking behavior using diffusion of innovation theory. Conference on Applied Information Systems Research (CONISAR), Nashville, Tennessee.
- Peters, G. W., & Panayi, E. (2016). Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. In *Banking beyond banks and money* (pp. 239-278). Springer.
- Pillai, B., Biswas, K., Hou, Z., & Muthukkumarasamy, V. (2022). Level of conceptual interoperability model for blockchain based systems. IEEE International Conference on Blockchain and Cryptocurrency Crosschain Workshop, ICBC-CROSS 2022,

- Pillai, B., Biswas, K., Hóu, Z., & Muthukkumarasamy, V. (2021). Burn-to-Claim: An asset transfer protocol for blockchain interoperability. *Computer Networks*, 200, 108495. <https://doi.org/10.1016/j.comnet.2021.108495>
- Pillai, B., Biswas, K., & Muthukkumarasamy, V. (2020). Cross-chain interoperability among blockchain-based systems using transactions [Article]. *Knowledge Engineering Review*, Article e23. <https://doi.org/10.1017/S0269888920000314>
- Pillai, B., Hóu, Z., Biswas, K., Bui, V., & Muthukkumarasamy, V. (2023). *Blockchain Interoperability: Performance and Security Trade-Offs* Proceedings of the 20th ACM Conference on Embedded Networked Sensor Systems, Boston, Massachusetts. <https://doi.org/10.1145/3560905.3568176>
- Pocher, N., & Veneris, A. (2021). Privacy and transparency in cbdcs: A regulation-by-design aml/cft scheme. *CFT Scheme (January 3, 2021)*. <https://dx.doi.org/10.2139/ssrn.3759144>
- Pokharna, S. S. (2013). Exploration of General Systems Theory (GST) and Jainism may provide new frontiers of knowledge and evolution. *Syntropy*, 2, 243-279. https://www.jainfoundation.in/JAINLIBRARY/books/GST_and_Jainism_269185_ST D.pdf
- Polit, D. F., & Beck, C. T. (2004). *Nursing research: Principles and methods*. Lippincott Williams & Wilkins.
- Prat, N., Comyn-Wattiau, I., & Akoka, J. (2014). *Artifact evaluation in information systems design-science research—a holistic view* Pacific Asia Conference on Information Systems (PACIS), <http://aisel.aisnet.org/pacis2014>
- Prewett, K. W., Prescott, G. L., & Phillips, K. (2020). Blockchain adoption is inevitable—Barriers and risks remain. *Journal of Corporate accounting & finance*, 31(2), 21-28.
- Pries-Heje, J., Baskerville, R., & Venable, J. (2008). Strategies for Design Science Research Evaluation. In *Conference Proceedings, 16th European Conference on Information Systems*. National University of Ireland.
- Qasse, I. A., Abu Talib, M., & Nasir, Q. (2019). Inter blockchain communication: A survey. Proceedings of the ArabWIC 6th Annual International Conference Research Track,
- R3. (2021). *Integrating Token-Based Payments into Existing Payment Systems*. <https://r3.com/blog/integrating-token-based-payments-into-existing-payment-systems-with-a-plug-and-play-approach>
- Ramey, K. E., Champion, D. N., Dyer, E. B., Keifert, D. T., Krist, C., Meyerhoff, P., Villanosa, K., & Hilppö, J. (2016). Qualitative analysis of video data: Standards and heuristics. In. Singapore: International Society of the Learning Sciences. <https://repository.isls.org/handle/1/370>
- Rajasekaran, A. S., Azees, M., & Al-Turjman, F. (2022). A comprehensive survey on blockchain technology. *Sustainable Energy Technologies and Assessments*, 52, 102039. <https://doi.org/10.1016/j.seta.2022.102039>

- Raphael Auer, Philipp Haene, & Henry Holden. (2021). *Multi-CBDC arrangements and the future of cross-border payments (No. 115)*. <http://www.bis.org>
- Reegu, F. A., Abas, H., Gulzar, Y., Xin, Q., Alwan, A. A., Jabbari, A., Sonkamble, R. G., & Dziauddin, R. A. (2023). Blockchain-Based Framework for Interoperable Electronic Health Records for an Improved Healthcare System. *Sustainability*, 15(8), 6337.
- Reegu, F. A., Abas, H., Hakami, Z., Tiwari, S., Akmam, R., Muda, I., Almashqbeh, H. A., & Jain, R. (2022). Systematic Assessment of the Interoperability Requirements and Challenges of Secure Blockchain-Based Electronic Health Records [Article]. *Security and Communication Networks*, 2022, Article 1953723. <https://doi.org/10.1155/2022/1953723>
- Rehman, A. A., & Alharthi, K. (2016). An introduction to research paradigms. *International Journal of Educational Investigations*, 3(8), 51-59. <http://www.ijeionline.com/>
- Reiter, B. (2017). Theory and methodology of exploratory social science research. *International Journal of Science and Research Methodology*, 5(4), 129. http://scholarcommons.usf.edu/gia_facpub/132
- Rella, L. (2019). Blockchain technologies and remittances: from financial inclusion to correspondent banking. *Frontiers in Blockchain*, 2, 14. <https://doi.org/10.3389/fbloc.2019.00014>
- Ren, K., Ho, N. M., Loghin, D., Nguyen, T. T., Ooi, B. C., Ta, Q. T., & Zhu, F. (2023). Interoperability in Blockchain: A Survey. *IEEE Transactions on Knowledge and Data Engineering*, 1-20. <https://doi.org/10.1109/TKDE.2023.3275220>
- Ren, M., Yin, Z., Ma, F., Xu, Z., Jiang, Y., Sun, C., Li, H., & Cai, Y. (2021). *Empirical evaluation of smart contract testing: what is the best choice?* Proceedings of the 30th ACM SIGSOFT International Symposium on Software Testing and Analysis, Virtual, Denmark. <https://doi.org/10.1145/3460319.3464837>
- Renduchintala, T., Alfauri, H., Yang, Z., Pietro, R. D., & Jain, R. (2022). A survey of blockchain applications in the fintech sector. *Journal of Open Innovation: Technology, Market, and Complexity*, 8(4), 185. <https://doi.org/10.3390/joitmc8040185>
- Rezaei, R., Chiew, T. K., & Lee, S. P. (2014). A review on E-business Interoperability Frameworks. *Journal of Systems and Software*, 93, 199-216. <https://doi.org/10.1016/j.jss.2014.02.004>
- Rezaei, R., Chiew, T. K., Lee, S. P., & Shams Aliee, Z. (2014). Interoperability evaluation models: A systematic review. *Computers in Industry*, 65(1), 1-23. <https://doi.org/10.1016/j.compind.2013.09.001>
- Robinson, P. (2021). Survey of crosschain communications protocols. *Computer Networks*, 200, 108488. <https://doi.org/10.1016/j.comnet.2021.108488>
- Rogers, E. M. (1995). *Diffusion of innovations*. Free Press.

- Rosemann, M., & Vessey, I. (2008). Toward Improving the Relevance of Information Systems Research to Practice: The Role of Applicability Checks. *MIS Quarterly*, 32(1), 1-22. <https://doi.org/10.2307/25148826>
- Rosli, K., Yeow, P. H., & Siew, E.-G. (2012). Factors influencing audit technology acceptance by audit firms: A new I-TOE adoption framework. *Journal of Accounting and Auditing*, 2012, 1. <https://doi.org/10.5171/2012.876814>
- Rosner, M. T., & Kang, A. (2015). Understanding and regulating twenty-first century payment systems: The ripple case study. *Mich. L. Rev.*, 114(4), 649-681. <https://repository.law.umich.edu/mlr/vol114/iss4/4>
- Saheb, T., & Mamaghani, F. H. (2021). Exploring the barriers and organizational values of blockchain adoption in the banking industry. *The Journal of High Technology Management Research*, 32(2), 100417. <https://doi.org/10.1016/j.hitech.2021.100417>
- Sakho, S., Jianbiao, Z., Essaf, F., & Badiss, K. (2019, December). Improving banking transactions using blockchain technology. In *2019 IEEE 5th International Conference on Computer and Communications (ICCC)* (pp. 1258-1263). IEEE. <https://doi.org/10.1109/ICCC47050.2019.9064344>
- Saudi Central Bank, C. b. o. U. (2019). *Project Aber: Joint Digital Currency and Distributed Ledger project*. https://www.sama.gov.sa/en-US/News/Documents/Project_Aber_report-EN.pdf
- Saunders, M., Lewis, P., Thornhill, A., & Bristow, A. (2015). *Understanding research philosophies and approaches: Research methods for business students*. Harlow: Pearson Education, England.
- Schaffers, H. (2018, 2018//). The Relevance of Blockchain for Collaborative Networked Organizations. *Collaborative Networks of Cognitive Systems*, Cham.
- Scheid, E. J., Hegnauer, T., Rodrigues, B., & Stiller, B. (2019, October). Bifröst: a modular blockchain interoperability API. In *2019 IEEE 44th Conference on Local Computer Networks (LCN)* (pp. 332-339). IEEE.
- Scholl, H. J., Kubicek, H., & Cimander, R. (2011, 2011//). Interoperability, Enterprise Architectures, and IT Governance in Government. *Electronic Government*, Berlin, Heidelberg.
- Schulte, S., Sigwart, M., Frauenthaler, P., & Borkowski, M. (2019a). Towards Blockchain Interoperability. In *Lecture Notes in Business Information Processing* (Vol. 361, pp. 3-10).
- Schulte, S., Sigwart, M., Frauenthaler, P., & Borkowski, M. (2019). Towards blockchain interoperability. In *Business Process Management: Blockchain and Central and Eastern Europe Forum: BPM 2019 Blockchain and CEE Forum, Vienna, Austria, September 1–6, 2019, Proceedings 17* (pp. 3-10). Springer International Publishing.

- Schwartz-Shea, P., & Yanow, D. (2012). *Interpretive research design: concepts and processes*. Routledge. <https://ebookcentral-proquest-com.uplib.idm.oclc.org/lib/pretoria-ebooks/detail.action?docID=957663>
- Scott, S., & McGuire, J. (2017). Using Diffusion of Innovation Theory to Promote Universally Designed College Instruction. *International Journal of Teaching and Learning in Higher Education*, 29(1), 119-128. <http://www.isetl.org/ijtlhe>
- Scott, W. R., & Davis, G. (2015). *Organizations and organizing: Rational, natural and open systems perspectives*. Routledge.
- Sedlmeir, J., Lautenschlager, J., Fridgen, G., & Urbach, N. (2022). The transparency challenge of blockchain in organizations. *Electronic Markets*, 32(3), 1779-1794. <https://doi.org/10.1007/s12525-022-00536-0>
- Sekaran, U., & Bougie, R. (2016). *Research methods for business: A skill building approach*. John Wiley & Sons. <https://books.google.com>
- Senthilkumar, D. (2020). Cross-industry use of Blockchain technology and opportunities for the future: Blockchain technology and artificial intelligence. In *Cross-Industry Use of Blockchain Technology and Opportunities for the Future* (pp. 64-79). IGI Global. <https://doi.org/DOI: 10.4018/978-1-7998-3632-2.ch004>
- Shadab, N., Cody, T., Salado, A., & Beling, P. (2022, 25-28 April 2022). Closed Systems Paradigm for Intelligent Systems. 2022 IEEE International Systems Conference (SysCon), (pp. 1-8). IEEE.
- Shbair, W., Steichen, M., & François, J. (2018, April 2018). Blockchain orchestration and experimentation framework: A case study of KYC. IEEE/IFIP Man2Block 2018 - IEEE/IFIP Network Operations and Management Symposium, Taipei, Taiwa.
- Sheather, G. (1968). A TOPOLOGY OF GENERAL SYSTEMS THEORY. *Ekistics*, 26(153), 173-178. <http://www.jstor.org/stable/43616763>
- Sheth, A. P. (1999). Changing focus on interoperability in information systems: from system, syntax, structure to semantics. In *Interoperating geographic information systems* (pp. 5-29). Springer.
- Sheth, H., & Dattani, J. (2019). Overview of blockchain technology. *Asian Journal For Convergence In Technology (AJCT) ISSN-2350-1146*. <https://asianssr.org/index.php/ajct/article/view/728>
- Siew, E.-G., Rosli, K., & Yeow, P. H. (2020). Organizational and environmental influences in the adoption of computer-assisted audit tools and techniques (CAATTs) by audit firms in Malaysia. *International Journal of Accounting Information Systems*, 36, 100445. <https://www.sciencedirect.com/science/article/pii/S1467089518300411>
- Sigwart, M., Frauenthaler, P., Spanring, C., Sober, M., & Schulte, S. (2021, 15-17 Nov. 2021). *Decentralized Cross-Blockchain Asset Transfers. 2021 Third International Conference on Blockchain Computing and Applications (BCCA)*, Electr. Network.

- Sigwart, M., Frauenthaler, P., Spanring, C., Sober, M., & Schulte, S. (2021, November). Decentralized cross-blockchain asset transfers. In *2021 Third International Conference on Blockchain Computing and Applications (BCCA)* (pp. 34-41). IEEE.
- Simmhan, Y. L., Plale, B., & Gannon, D. (2005). A survey of data provenance in e-science. *SIGMOD Rec.*, *34*(3), 31–36. <https://doi.org/10.1145/1084805.1084812>
- Singh, A., Click, K., Parizi, R. M., Zhang, Q., Dehghantanha, A., & Choo, K.-K. R. (2020). Sidechain technologies in blockchain networks: An examination and state-of-the-art review. *Journal of Network and Computer Applications*, *149*, 102471. <https://doi.org/10.1016/j.jnca.2019.102471>
- Soares, D., & Amaral, L. (2014, April). Reflections on the concept of interoperability in information systems. In *16th International Conference on Enterprise Information Systems* (Vol. 2, pp. 331-339). SCITEPRESS.
- Sober, M., Sigwart, M., Frauenthaler, P., Spanring, C., Kobelt, M., & Schulte, S. (2022). *Dataset: Decentralized Cross-Blockchain Asset Transfers with Transfer Confirmation* Zenodo. <https://doi.org/http://dx.doi.org/10.5281/ZENODO.6394522>
- Solidity. (2022). *Solidity Programming Language*. Retrieved 10/05/2023 from <https://soliditylang.org>
- Soni, A., & Duggal, R. (2014). Reducing risk in KYC (know your customer) for large Indian banks using big data analytics. *International Journal of Computer Applications*, *97*(9). <https://doi.org/10.5120/17039-7347>
- Sonkamble, R. G., Phansalkar, S. P., Potdar, V. M., & Bongale, A. M. (2021). Survey of Interoperability in Electronic Health Records Management and Proposed Blockchain Based Framework: MyBlockEHR. *IEEE Access*, *9*, 158367-158401. <https://doi.org/10.1109/ACCESS.2021.3129284>
- South African Reserve Bank. (2018). *Project Khoka: Exploring the use of distributed ledger technology for interbank payments settlement in South Africa*. <https://www.resbank.co.za>
- Stewart, D., & Klein, S. (2016). The use of theory in research. *International journal of clinical pharmacy*, *38*(3), 615-619. <https://doi.org/10.1007/s11096-015-0216-y>
- Straub, D. W., Ang, S., & Evaristo, R. (1994). Normative standards for IS research. *SIGMIS Database*, *25*(1), 21–34. <https://doi.org/10.1145/188423.188429>
- Sun, Y., Yi, L., Duan, L., & Wang, W. (2022, 10-16 July 2022). A Decentralized Cross-Chain Service Protocol based on Notary Schemes and Hash-Locking. 2022 IEEE International Conference on Services Computing (SCC),
- Surujnath, R. (2017). Off the chain: A guide to blockchain derivatives markets and the implications on systemic risk. *Fordham J. Corp. & Fin. L.*, *22*, 257. <https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1440&context=jcfl>

- Sveriges Riksbank. (2017). *The Riksbank's E-krona Project*.
https://www.riksbank.se/globalassets/media/rapporter/e-krona/2017/rapport_ekrona_uppdaterad_170920_eng.pdf
- Swan, M. (2017). Anticipating the economic benefits of blockchain. *Technology innovation management review*, 7(10), 6-13. <https://doi.org/10.22215/TIMREVIEW%2F1109>
- Swift. (2017). *Certified application RTGS label criteria 2017*. <https://www.swift.com/swift-resource/21461>
- Tan, E., Mahula, S., & Crompvoets, J. (2022). Blockchain governance in the public sector: A conceptual framework for public management. *Government Information Quarterly*, 39(1), 101625. <https://doi.org/10.1016/j.giq.2021.101625>
- Tapscott, D., & Tapscott, A. (2017). How blockchain will change organizations. *MIT Sloan Management Review*, 58(2), 10. <http://mitsmr.com/2gblHrl>
- Tashakkori, A., Teddlie, C., & Teddlie, C. B. (1998). *Mixed methodology: Combining qualitative and quantitative approaches* (Vol. 46). sage.
- Thailand, B. o. (2018). *Project DLT Scripless Bond: Investing in Thailand's future Transforming the securities markets infrastructure with blockchain*. B. o. Thailand. <https://www.bot.or.th/English/DebtSecurities/Documents/DLT%20Scripless%20Bond.pdf>
- Themistocleous, M., Rupino da Cunha, P., Tabakis, E., & Papadaki, M. (2023). Towards cross-border CBDC interoperability: insights from a multivocal literature review. *Journal of Enterprise Information Management*, 36(5), 1296-1318. <https://doi.org/10.1108/JEIM-11-2022-0411>
- Thompson, A. (1996). Political pragmatism and educational inquiry. *Philosophy of Education*, 425-434. <https://d1wqtxts1xzle7.cloudfront.net/31796740>
- Tiong, W. N., & Sim, A. F. S. F. (2020). Web-based Seminar - New Source of Qualitative Study: Data Collection during the Pandemic of COVID-19. *SEISENSE Journal of Management*, 3(6), 50-64. <https://doi.org/10.33215/sjom.v3i6.477>
- Tornatzky, L. G., Fleischer, M., & Chakrabarti, A. K. (1990). *Processes of technological innovation*. Lexington books.
- Trevelyan, E. G., & Robinson, P. N. (2015). Delphi methodology in health research: how to do it? *European Journal of Integrative Medicine*, 7(4), 423-428. <https://doi.org/10.1016/j.eujim.2015.07.002>
- Tsagkani, C. (2005). Inter-organizational collaboration on the process layer. Proceedings of the IFIP/ACM SIGAPP INTEROP-ESA Conference,
- Underwood, S. (2016). Blockchain beyond bitcoin. <http://web.a.ebscohost.com.uplib.idm.oclc.org>

- Upmeier zu Belzen, A., Engelschalt, P., & Krüger, D. (2021). Modeling as Scientific Reasoning—The Role of Abductive Reasoning for Modeling Competence. *Education Sciences*, 11(9), 495. <https://www.mdpi.com/2227-7102/11/9/495>
- Vaishnavi, V., & Kuechler, W. (2004). *Design research in information systems*. <https://www.desrist.org/design-research-in-information-systems>
- Vaishnavi, V., & Kuechler, W. (2008). *Design science research methods and patterns : innovating information and communication technology*. Auerbach Publications. <https://doi.org/10.1201/9781420059335>
- Van den Broek, T., & van Veenstra, A. F. (2015). Modes of Governance in Inter-Organizational Data Collaborations. In *ECIS 2015 Completed Research Papers* (pp. 0-12).
- Van der Merwe, A., Gerber, A., & Smuts, H. (2019, July). Guidelines for conducting design science research in information systems. In *Annual Conference of the Southern African Computer Lecturers' Association* (pp. 163-178). Cham: Springer International Publishing.
- Van der Veer, H., & Wiles, A. (2008). Achieving technical interoperability. *European telecommunications standards institute*. <https://portal.etsi.org/CTI/Downloads/ETSIApproach/IOP%20whitepaper%20Edition%203%20final.pdf>
- Van der Veer, H., & Wiles, A. (2018). ETSI White paper No. 3 Achieving Technical Interoperability—The ETSI Approach. *European Telecommunications Standards Institute (ETSI): Sophia Antipolis, France*. http://www.etsi.org/website/document/whitepapers/wp3_iop_final.pdf
- Van Lier, B., & Hardjono, T. (2011a). A Systems Theoretical Approach to Interoperability of Information. *Systemic Practice and Action Research*, 24(5), 479-497. <https://doi.org/10.1007/s11213-011-9197-5>
- Van Lier, B., & Hardjono, T. (2011b). A Systems Theoretical Approach to Interoperability of Information. *Systemic Practice and Action Research*, 24(5), 479. <https://doi.org/10.1007/s11213-011-9197-5>
- Varsaluoma, J. (2009). Scenarios in the heuristic evaluation of mobile devices: emphasizing the context of use. In *Human Centered Design: First International Conference, HCD 2009, Held as Part of HCI International 2009, San Diego, CA, USA, July 19-24, 2009 Proceedings 1* (pp. 332-341). Springer Berlin Heidelberg.
- Venable, J. (2006). A framework for design science research activities. In *Emerging Trends and Challenges in Information Technology Management: Proceedings of the 2006 Information Resource Management Association Conference* (pp. 184-187). Idea Group Publishing.
- Venable, J., Pries-Heje, J., & Baskerville, R. (2012). A Comprehensive Framework for Evaluation in Design Science Research. *Design Science Research in Information Systems. Advances in Theory and Practice*, Berlin, Heidelberg.

- Venable, J., Pries-Heje, J., & Baskerville, R. (2016). FEDS: a framework for evaluation in design science research. *European journal of information systems*, 25(1), 77-89. <https://link.springer.com/article/10.1057/ejis.2014.36>
- Vernadat, F. B. (2010). Technical, semantic and organizational issues of enterprise interoperability and networking. *Annual Reviews in Control*, 34(1), 139-144. <https://doi.org/10.1016/j.arcontrol.2010.02.009>
- Viriyasitavat, W., Bi, Z., & Hoonsopon, D. (2022). Blockchain technologies for interoperation of business processes in smart supply chains. *Journal of Industrial Information Integration*, 26, 100326, Article 100326. <https://doi.org/10.1016/j.jii.2022.100326>
- Vo, L.-C. (2012). Pragmatist perspective on knowledge and knowledge management in organizations. *International Business Research*, 5(9), 78. <https://doi.org/10.5539/ibr.v5n9p78>
- Vocal Philosopher. (2018). *The pragmatic theory of truth: A defense and reconciliation*. Retrieved 16/5/2022/ from <http://www.vocal-philosopher.com/pragmatic-truth#:~:text=Bertrand>
- vom Brocke, J., Hevner, A., & Maedche, A. (2020). Introduction to design science research. In *Design Science Research. Cases* (pp. 1-13). Springer. http://dx.doi.org/10.1007/978-3-030-46781-4_1
- Von Bertalanffy, L. (1972). The history and status of general systems theory. *Academy of management journal*, 15(4), 407-426. <https://doi.org/10.5465/255139>
- Walton, D. (2013). *Abductive Reasoning*. University of Alabama Press. <http://site.ebrary.com/id/10869313>
<https://public.ebookcentral.proquest.com/choice/publicfullrecord.aspx?p=1687320>
- Wang, G., Wang, Q., & Chen, S. (2023). Exploring Blockchains Interoperability: A Systematic Survey. *ACM Comput. Surv.* <https://doi.org/10.1145/3582882>
- Wang, H., Ma, S., Dai, H.-N., Imran, M., & Wang, T. (2020). Blockchain-based data privacy management with Nudge theory in open banking. *Future Generation Computer Systems*, 110, 812-823. <https://doi.org/10.1016/j.future.2019.09.010>
- Wang, Y., Han Jeong, H., & Beynon-Davies, P. (2019). Understanding blockchain technology for future supply chains: a systematic literature review and research agenda. *Supply Chain Management: An International Journal*, 24(1), 62-84. <https://doi.org/10.1108/SCM-03-2018-0148>
- Weber, R. H. (2014). *Legal interoperability as a tool for combatting fragmentation* (Canadian Electronic Library,, Issue. <https://policycommons.net/artifacts/1205649/legal-interoperability-as-a-tool-for-combatting-fragmentation/1758760/>
- Weber, S. (2010). Design science research: Paradigm or approach? <https://aisel.aisnet.org/amcis2010/214>

- Weichhart, G. (2014, 2014//). Requirements for Supporting Enterprise Interoperability in Dynamic Environments. *Enterprise Interoperability VI*, Cham.
- Weichhart, G., Guédria, W., & Naudet, Y. (2016). Supporting interoperability in complex adaptive enterprise systems: A domain specific language approach. *Data & Knowledge Engineering*, 105, 90-106. <https://doi.org/10.1016/j.datak.2016.04.001>
- Weichhart, G., & Naudet, Y. (2014). Ontology of enterprise interoperability extended for complex adaptive systems. On the Move to Meaningful Internet Systems: OTM 2014 Workshops: Confederated International Workshops: OTM Academy, OTM Industry Case Studies Program, C&TC, EI2N, INBAST, ISDE, META4eS, MSC and OnToContent 2014, Amantea, Italy, October 27-31, 2014. Proceedings,
- Weigand, H., Johannesson, P., & Andersson, B. (2021). An artifact ontology for design science research. *Data & Knowledge Engineering*, 133, 101878. <https://doi.org/10.1016/j.datak.2021.101878>
- Whitman, L. E., & Panetto, H. (2006). The missing link: Culture and language barriers to interoperability. *Annual Reviews in Control*, 30(2), 233-241. <https://doi.org/10.1016/j.arcontrol.2006.09.008>
- Wiatt, R. G. C. M. A. C. P. A. (2019). FROM THE MAINFRAME TO THE BLOCKCHAIN. *Strategic Finance*, 100(7), 26-35. <https://www.proquest.com/docview/2288590796>
- Wilkie, A., & Smith, S. S. (2021). Blockchain: Speed, Efficiency, Decreased Costs, and Technical Challenges. In H. K. Baker, E. Nikbakht, & S. S. Smith (Eds.), *The Emerald Handbook of Blockchain for Business* (pp. 157-170). Emerald Publishing Limited. <https://doi.org/10.1108/978-1-83982-198-120211014>
- Williams, C. (2007). Research methods. *Journal of Business & Economics Research (JBER)*, 5(3). <https://doi.org/> <https://doi.org/10.19030/jber.v5i3.2532>
- Wipro. (2023). *Blockchain: what it means for your enterprise integration strategy?* <https://www.wipro.com/applications/blockchain-what-it-means-for-your-enterprise-integration-strategy>
- Wisniewski, T. P., Polasik, M., Kotkowski, R., & Moro, A. (2021). Switching from cash to cashless payments during the COVID-19 pandemic and beyond. Available at SSRN 3794790. <https://ssrn.com/abstract=3794790>
- Woiceshyn, J., & Daellenbach, U. (2018). Evaluating inductive vs deductive research in management studies. *Qualitative Research in Organizations and Management: An International Journal*, 13(2), 183-195. <https://doi.org/10.1108/QROM-06-2017-1538>
- Woods, N. F., & Catanzaro, M. (1988). Nursing research: Theory and practice. (No Title).
- World Bank Group. (2020). *Blockchain Interoperability*. <https://documents1.worldbank.org/curated/en/373781615365676101/pdf/Blockchain-Interoperability.pdf>

- World Bank Group. (2021). *Interoperability in Fast Payment Systems* (World Bank Fast Payments Toolkit, Issue).
- World Economic Forum. (2020). *Redesigning Trust: Blockchain Deployment Toolkit*. <https://widgets.weforum.org/blockchain-toolkit/index.html>
- Wüst, K., & Gervais, A. (2018). Do you need a blockchain?. In *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)* (pp. 45-54). IEEE. <https://doi.org/10.1109/CVCBT.2018.00011>
- Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A survey of distributed consensus protocols for blockchain networks. *IEEE communications surveys & tutorials*, *22*(2), 1432-1465. <https://doi.org/10.1109/COMST.2020.2969706>
- Xie, J., Tang, H., Huang, T., Yu, F. R., Xie, R., Liu, J., & Liu, Y. (2019). A survey of blockchain technology applied to smart cities: Research issues and challenges. *IEEE communications surveys & tutorials*, *21*(3), 2794-2830. <https://doi.org/10.1109/COMST.2019.2899617>
- Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019a). *Blockchain technology overview*. <https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf>
- Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019b). *Blockchain technology overview* (arXiv preprint arXiv:1906.11078, Issue. <https://arxiv.org/abs/1906.11078>
- Yang, F., Zhou, W., Wu, Q., Long, R., Xiong, N. N., & Zhou, M. (2019). Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism. *IEEE Access*, *7*, 118541-118555. <https://doi.org/10.1109/ACCESS.2019.2935149>
- Yin, R., Yan, Z., Liang, X., Xie, H., & Wan, Z. (2023). A survey on privacy preservation techniques for blockchain interoperability. *Journal of Systems Architecture*, *140*, 102892. <https://doi.org/10.1016/j.sysarc.2023.102892>
- Yin, R. K. (2017). *Case study research and applications: Design and methods*. Sage publications.
- Yoo, Y., Boland Jr, R. J., Lyytinen, K., & Majchrzak, A. (2012). Organizing for innovation in the digitized world. *Organization science*, *23*(5), 1398-1408. <http://dx.doi.org/10.1287/orsc.1120.0771>
- Yunis, M., Tarhini, A., & Kassar, A. (2018). The role of ICT and innovation in enhancing organizational performance: The catalysing effect of corporate entrepreneurship. *Journal of Business Research*, *88*, 344-356. <https://doi.org/10.1016/j.jbusres.2017.12.030>
- Yvonne Feilzer, M. (2010). Doing mixed methods research pragmatically: Implications for the rediscovery of pragmatism as a research paradigm. *Journal of Mixed Methods Research*, *4*(1), 6-16. <https://doi.org/10.1177/1558689809349691>

- Zachariadis, M., Hileman, G., & Scott, S. V. (2019). Governance and control in distributed ledgers: Understanding the challenges facing blockchain technology in financial services. *Information and Organization*, 29(2), 105-117. <https://doi.org/10.1016/j.infoandorg.2019.03.001>
- Zetsche, D. A., Anker-Sørensen, L., Passador, M. L., & Wehrli, A. (2022). DLT-based enhancement of cross-border payment efficiency—a legal and regulatory perspective [Article]. *Law and Financial Markets Review*. <https://doi.org/10.1080/17521440.2022.2065809>
- Zhang, L., Hang, L., Jin, W., & Kim, D. (2021). Interoperable multi-blockchain platform based on integrated REST APIs for reliable tourism management [Article]. *Electronics (Switzerland)*, 10(23), Article 2990. <https://doi.org/10.3390/electronics10232990>
- Zhang, M., Qu, Q., Ning, L., Fan, J., & Yang, R. (2022 Dec 17-19). An Effective and Reliable Cross-Blockchain Data Migration Approach. *Lecture Notes in Computer Science. 22nd International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT 2021)*, Sun Yat Sen Univ, Guangzhou, People's Republic of China.
- Zhang, S., & Hou, C. (2021). Model of decentralized cross-chain energy trading for power systems. *Global Energy Interconnection*, 4(3), 324-334. <https://doi.org/10.1016/j.gloi.2021.07.006>
- Zhang, X. (2020). *Opportunities, Challenges and Promotion Countermeasures of Central Bank Digital Currency 2020* Management Science Informatization and Economic Innovation Development Conference (MSIEID), Guangzhou, China.
- Zhang, X., Yu, P., Yan, J., & Spil, I. T. A. (2015). Using diffusion of innovation theory to understand the factors impacting patient acceptance and use of consumer e-health innovations: a case study in a primary care clinic. *BMC Health Services Research*, 15(1), 71. <https://doi.org/10.1186/s12913-015-0726-2>
- Zheng, Z., Xie, S., Dai, H.-N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, 14(4), 352-375. <https://doi.org/10.1504/IJWGS.2018.095647>
- Zhu, K., Kraemer, K. L., & Xu, S. (2006). The process of innovation assimilation by firms in different countries: a technology diffusion perspective on e-business. *Management Science*, 52(10), 1557-1576. <https://doi.org/10.1287/mnsc.1050.0487>
- Žukauskas, P., Vveinhardt, J., & Andriukaitienė, R. (2018). Philosophy and paradigm of scientific research. *Management Culture and Corporate Social Responsibility*, 121(13), 506-518.

APPENDIX A

ETHICS APPROVALS



Faculty of Engineering, Built Environment and Information Technology

Fakulteit Ingenieurswese, Bou-omgewing en
Inligtingtegnologie / Lefapha la Boetšenere,
Tikologo ya Kago le Theknolothi ya Tshedimošo

4 July 2022

Reference number: EBIT/165/2022

Miss SS Mafike
Department: Informatics
University of Pretoria
Pretoria
0083

Dear Miss SS Mafike,

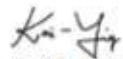
FACULTY COMMITTEE FOR RESEARCH ETHICS AND INTEGRITY

Your recent application to the EBIT Research Ethics Committee refers.

Approval is granted for the application with reference number that appears above.

1. This means that the research project entitled "Towards an interoperability framework for blockchain in the banking sector" has been approved as submitted. It is important to note what approval implies. This is expanded on in the points that follow.
2. This approval does not imply that the researcher, student or lecturer is relieved of any accountability in terms of the Code of Ethics for Scholarly Activities of the University of Pretoria, or the Policy and Procedures for Responsible Research of the University of Pretoria. These documents are available on the website of the EBIT Research Ethics Committee.
3. If action is taken beyond the approved application, approval is withdrawn automatically.
4. According to the regulations, any relevant problem arising from the study or research methodology as well as any amendments or changes, must be brought to the attention of the EBIT Research Ethics Office.
5. The Committee must be notified on completion of the project.

The Committee wishes you every success with the research project.



Prof K.-Y. Chan

Chair: Faculty Committee for Research Ethics and Integrity
FACULTY OF ENGINEERING, BUILT ENVIRONMENT AND INFORMATION TECHNOLOGY



Faculty of Engineering, Built Environment and Information Technology

Fakulteit Ingenieurswese, Bou-omgewing en
Inligtingtegnologie / Lefapha la Boetšhenere,
Tikologo ya Kago le Theknolotši ya Tshedimošo

29 November 2023

Reference number: EBIT/280/2023

Miss SS Mafike
Department: Informatics
University of Pretoria
Pretoria
0083

Dear Miss SS Mafike,

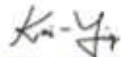
FACULTY COMMITTEE FOR RESEARCH ETHICS AND INTEGRITY

Your recent application to the EBIT Research Ethics Committee refers.

Approval is granted for the application with reference number that appears above.

1. This means that the research project entitled "Towards an interoperability framework for blockchain in the banking sector" has been approved as submitted. It is important to note what approval implies. This is expanded on in the points that follow.
2. This approval does not imply that the researcher, student or lecturer is relieved of any accountability in terms of the Code of Ethics for Scholarly Activities of the University of Pretoria, or the Policy and Procedures for Responsible Research of the University of Pretoria. These documents are available on the website of the EBIT Research Ethics Committee.
3. If action is taken beyond the approved application, approval is withdrawn automatically.
4. According to the regulations, any relevant problem arising from the study or research methodology as well as any amendments or changes, must be brought to the attention of the EBIT Research Ethics Office.
5. The Committee must be notified on completion of the project.

The Committee wishes you every success with the research project.



Prof K.-Y. Chan

Chair: Faculty Committee for Research Ethics and Integrity

FACULTY OF ENGINEERING, BUILT ENVIRONMENT AND INFORMATION TECHNOLOGY

APPENDIX B

CONSENT FORMS AND INTERVIEW GUIDES

INFORMED CONSENT FORM (Form for research participant's permission)

1. Project information

1.1 Title of research project: Towards an interoperability framework for blockchain in the banking sector

1.2 Researcher details: Senate Mafike, senatemafike@gmail.com and 0738862896

1.3 Research study description

This study aims to develop and evaluate a framework to address the blockchain interoperability challenge faced by banking organizations looking to adopt the blockchain technology in their operations. The framework will act as a guide for the banking sector on how to interoperate their existing systems with emerging blockchain systems. The research will also contribute to the advancement of blockchain and blockchain interoperability research.

- **The main research question is:** *How can a blockchain interoperability framework be developed to contribute to the effective communication between blockchain systems and the existing non-blockchain systems within the banking sector?*

Your role as a participant in this research

You will participate in two phases of this research. The first phase will be a semi-structured interview in which you will be asked questions relating to blockchain technology and blockchain interoperability. The interviews will be conducted in English. The sessions should last no more than 1 hour. The interviews will be recorded and the researcher may take additional notes.

The second phase will come at a later stage when the framework has been developed and is evaluated. In this phase, your participation will be requested to evaluate the framework through a questionnaire that will be provided later.

Potential risks to participants

There are no risks or negative consequences for participating in or choosing not to participate in this study.

Your participation in this study is purely voluntary and there will be no penalty should you choose not to participate.

No private information will be collected about you as a participant.

To protect your identity, a pseudo-name will be used in place of your name in any publications or presentations relating to this study. And none of the responses you give can be traced back to you.

The information you share will be treated as confidential and will be used only for the purposes of this study.

The notes from the interviews will be scanned to an appropriate digital format and the original paper notes destroyed. The scanned notes and the interview recording will be encrypted and stored securely on a cloud storage for no more than 5 years.

2. Informed consent (to be completed by the participant)

2.1 I, _____ hereby voluntarily grant my permission for participation in the project as explained to me by the researcher Senate Mafike.

2.2 The nature, objective, possible safety and health implications have been explained to me and I understand them.

2.3 I hereby give consent for the session to be voice recorded.

2.4 I understand my right to choose whether to participate in the project and that the information furnished will be handled confidentially. I am aware that the results of the investigation may be used for the purposes of publication.

2.4 Upon signature of this form, the participant will be provided with a copy.

Signed: _____ Date: _____

Researcher: _____ Date: _____

INTERVIEW GUIDE 1

Towards an Enterprise Blockchain Interoperability Framework

Participant's experience with blockchain technology

Which industry do you work in? _____

What is your job role? _____

Years of experience working with blockchain?

- Less than 1 year
- 1 - 3 years
- 3.5 -5 years
- 6-10 years
- more than 10 years

What type of blockchains (private, public or consortium) and platforms have you worked on?

Blockchain type

- Private
- Public
- Consortium

Platform _____

Technologies/applications

- Smart contracts
- DApps
- DeFi
- Payments
- Cross-chain technology

Other: _____

Blockchain Interoperability

1. What do you understand by blockchain interoperability?
2. What internal organizational, technical and external challenges have you encountered with regards to interoperating and integrating blockchain with other blockchains or non-blockchain legacy systems?
3. What type of legacy systems have you attempted to or have successfully interoperated and integrated with blockchain?
4. From your experience, what is the nature/type of the data that needs to be shared between the non blockchain systems and the blockchain or between blockchain systems?
5. What interfaces or integration approaches did you use to connect blockchain to the legacy systems or to other blockchain? And why?
6. Which tools, methods and/or approaches have you applied in interoperating blockchain with other systems?
7. Are there any challenges/limitations with the approaches you have used to interoperate blockchain with legacy systems?

8. What key considerations would you suggest should be taken into account when interoperating blockchain with non blockchain systems?
9. If you were to select a framework to assist organizations on how to achieve blockchain interoperability, what key components and features would you want this framework to have?
10. Are there any further suggestions you would make in relation to how blockchain interoperability can be achieved in organizations?

THANK YOU!!

INFORMED CONSENT FORM (Evaluation Phase) (Form for research participant's permission)

1. Project information

1.1 Title of the research project: Towards an Interoperability Framework for Blockchain in the Banking Sector

1.2 Researcher details: Senate Mafike, senatemafike@gmail.com and 0738862896

1.3 Research study description

This study aims to develop and evaluate a framework to address the blockchain interoperability challenges faced by banking organizations looking to adopt blockchain technology in their operations. The framework will guide the banking sector on how to interoperate their existing systems with emerging blockchain systems. The research will also contribute to the advancement of blockchain and blockchain interoperability research.

- **The main research question is:** *How can a blockchain interoperability framework be developed and evaluated to contribute to the effective communication between blockchain systems and the existing non-blockchain systems within the banking sector?*

Your role as a participant in this research

Your participation in this study will involve you reviewing the Interoperability framework that will be sent to you. You will also be provided with a survey questionnaire which you will be requested to complete as part of the evaluation process. The questionnaire will be online and you will be furnished with the link to the questionnaire once you have agreed to participate and signed the consent form.

Potential risks to participants

There are no risks or negative consequences for participating in or choosing not to participate in this study.

Your participation in this study is purely voluntary and there will be no penalty should you choose not to participate.

No private information will be collected about you as a participant.

To protect your identity, a pseudo-name will be used in place of your name in any publications or presentations relating to this study. And none of the responses you give can be traced back to you.

The information you share will be treated as confidential and will be used only for the purposes of this study.

The responses will be encrypted and stored securely on cloud storage for no more than 10 years.

2. Informed consent (to be completed by the participant)

2.1 I, _____ hereby voluntarily grant my permission to participate in the project as explained to me by the researcher Senate Mafike.

2.2 The nature, objective, possible safety, and health implications have been explained to me and I understand them.

2.3 I understand my right to choose whether to participate in the project and that the information furnished will be handled confidentially. I am aware that the results of the investigation may be used for the purposes of publication.

2.4 Upon signature of this form, the participant will be provided with a copy.

Signed: _____ Date: _____

Researcher: _____ Date: _____

INTERVIEW GUIDE 2

FRAMEWORK EVALUATION MIXED INTERVIEW QUESTIONNAIRE

PARTICIPANT DEMOGRAPHICS

1. What is your current job role?
2. How many years of experience do you have working with blockchain or DLTs?
3. Which blockchain areas do you have experience working in:

Smart contracts

Permissioned Blockchains

DeFi

Permissionless

Blockchains

NFTs

Cryptocurrencies

Blockchain/Crypto regulations

FRAMEWORK EVALUATION CRITERIA

A. Utility

1. In your view how applicable is the framework to the banking context in South Africa?

Not

Slightly

Applicable

Totally

Applicable

Applicable

Applicable

2. How do you see the framework being applied by organisations looking to deploy blockchain solutions in the sector?
3. In your view, how effective would the framework be in assisting banking organisations to address blockchain interoperability issues?

Not Effective **Slightly Effective** **Effective** **Totally Effective**

4. Does the framework provide sufficient/adequate guidance to organisations regarding how to handle or address interoperating blockchain technology?

Yes	No
-----	----

if No,

Do you have any suggestions or recommendation on how we can improve the utility of the framework?

B. Completeness

1. In your view does the framework adequately cover all the relevant and critical aspects on blockchain interoperability in the banking sector in as far as the following areas are concerned?

- a. Business related aspects

Yes	No
-----	----

- b. Legal and regulatory aspects

Yes	No
-----	----
- c. Technical aspects

Yes	No
-----	----
- d. Data related aspects

Yes	No
-----	----
- e. Other aspects

Yes	No
-----	----

If No, what additional aspects would you suggest and what considerations?

C. Usability

1. How easy is it to understand the framework?

Difficult **Slightly** **Easy** **Very easy**

Difficult

2. In your view, how easy is it to use and apply the framework?

Difficult **Slightly** **Easy** **Very easy**
Difficult

3. To what extent is the framework usable (easy to use)?

Difficult **Slightly** **Easy** **Very easy**
Difficult

APPENDIX C

TRANSCRIPT EXAMPLE

Unknown Speaker 1:50

I'm trying to come up with framework for organization to guide how they can integrate the blockchain, and I am focusing on blockchain in banking sectors

Unknown Speaker 2:03

with whatever systems that are the sole focus was mainly on the banking sector because from leading in terms of the last as in the South African Reserve Bank of Canada nearly dying in terms of blockchain initiatives like locally.

Unknown Speaker 2:21

So that's why I focused on the banking sector. So they get all the information they're hoping that in fact, I just want us to discuss that via from your experience from central bank so true to where you are now without even saying the names could look like cut off all these paths. So to say, what is your experience in working within the banking sector? Where which areas do you think would benefit from blockchain and how would you suggest process to be followed what would be the things that we need to think about in you know in building this framework?

Unknown Speaker 3:06

Well

Unknown Speaker 3:08

yeah

Unknown Speaker 3:42

Okay so can you briefly tell us a bit about unpack about your experience what in banking what were you working on not in details, they got compromised and you know,

Unknown Speaker 3:56

confidentiality organization, but in general, what from your experience? What have you been working on in the banking sector? What roles have you occupied and so on?

Unknown Speaker 4:10

Okay.

Respondent 4:15

It's all yours. It's a lot.

Yeah, I've been working in payments for about 16 years now. And it's been different roles. And starting off as a technician, later moved to a more professional roles in payments I've worked on international payments, domestic payments, card, electronic funds transfer, mobile money, Blockchain, now I just do mostly advisory work.

Respondent 5:16

So it's pretty much all things payments FinTech payments, anything payment let me put it that.

Speaker 1 5:28

So yes you are the right guy to talk to.

Respondent 5:32

So blockchain Yeah. Blockchain. Yeah, I think when I left Lesotho there was still a bit of uncertainty as to exactly what is this thing? what or where

We should we be worried about it because I was in the regulatory space.

But now I'm on more on the commercial side of things. So there was a big of worry in terms of what is this thing. remember blockchain

Respondent 6:06

Blockchain is a technology but the one thing that became predominant and well known was Bitcoin. .. so in the financial services sector so it was initially seen as a threat because the suggestion was to bypass the banking system.so the regulators were cautious, including one they didn't know what it was, they didn't understand it, and they couldn't put

their pulse on it So if you don't know what's going on, you cannot regulate regulate effectively.

Respondent 6:45

But different markets mature at different paces, you did say that's why maybe the South African reserve bank took initiative to learn. and try to come up with a regulatory framework. but generally globally even in SA there is still regulatory uncertainty around this thing as a technology.

Unknown Speaker 7:10

Yeah.

Unknown Speaker 7:12

Yeah. It's

Respondent 7:16

it's one of those things.

The way regulation works is that you don't want to disrupt the innovation process. Yeah, you need to wait for some time to see anything come to fruition. So you'll know if it's gonna be of any concern. If it's worth wasting time on then you need to establish at what point you need to step in without stifling the innovation process

Respondent 7:57

So the that's the state at which we are at, that why I feel the Reserve Bank is in today that's why part of coming up with that project Khokha and into the that's why part of them come up with that project whole days, just to even considering building their own digital currency to explore

Unknown Speaker 8:16

It's what everyone is doing. JP Morgan is one of the major institutions were also spearheading this initiatives. China has tried coming up with their own digital currencies. other markets are Yeah, my guess is trying to adopt it to flee Inflation. Yeah, problems. But at the end of the day, it's still in its infancy with huge regulatory uncertainty.

Unknown Speaker 8:47

Yeah, maybe call it something you're studying today, you may have been picked up a lot of back and forth in the US where companies are being brought before the law, and even that process is still uncertain, because I think they call it regulation by enforcement, where you don't really have a list of rules and regulations that people participating in blockchain should follow. But at the back of that, you feel like something needs to be done because companies are busy going bankrupt and crashing with people's money.

Unknown Speaker 9:34

So everyone is sort of sitting on a fence.

Speaker

Yeah, but sitting on the fence, but at the same time still trying to see what they can like experiment in a way. right?

Respondent 9:58

Yeah, you have one side with people experimenting. People come up with all sorts of use cases, some fail and some are still sustainable and working today. Yeah, you have governments on one end, also trying to learn as quickly as possible. So they know illegally where their stance is.

Unknown Speaker 10:20

So

Unknown Speaker 10:22

okay, so continue. No, no. ask

Unknown Speaker 10:26

I was saying so, um, from all these experimentation, are we within the South African context or not just South African even maybe they SADC that area? Or even Africa in general? It's just mostly experimentation, you would say or is there any? Are there any initiatives internally that are going on? Looking at how this technology can be used?

Unknown Speaker 10:51

There are a lot of chips going on? A lot.

Unknown Speaker 10:55

Yeah. Everyone is interested in right now? Yes. They're

Unknown Speaker 11:03

learning curve trees. It's a fairly complex space. So one on one end, there is the learning curve, There's a skills gap, understanding of the technology itself.

Unknown Speaker 11:26

And

Unknown Speaker 11:28

trying to figure out ways to make it interoperable with our current ways because you can drop what you're doing today because this blockchain and replace it entirely. Yes. So there is that going on? And also one of the key things been being able to, to make a decision when it's applicable, and when it's not, it's not a silver bullet that you can do absolutely anything with.

Unknown Speaker 12:06

And it's not just about money or currencies. There are a lot of use cases in in the financial services sector, that you can enforce using Blockchain.

Unknown Speaker 12:21

And

Unknown Speaker 12:24

so talking about you mentioned a lot of important things that didn't give Atlanta workouts or no, you mentioned one, we need to, it's not a silver bullet, right. So you can just apply it everywhere in anyhow. How is that decision, like the choice to say, Okay, now we're applying what informs that that choice to say we are applying it in this area, but not in that area, in another area, called the blood process, generally get into the thing, Tim? What are the things that they consider to say, Okay, we are going to choose to apply it say in in cross border payments, or in whatever area, other areas else wherever they they're applying, but what what informs but what do they consider to say, Okay, we will apply it in this area and not in another area.

Respondent 13:14

Um, it's usually the business case at. What do you think you're trying to achieve?

And the key question is always or the

the require they the key thing to consider is whether there will be money involved or not. If you're using it as a way of transacting or not, you can apply use blockchain without any touching money. As an example, yeah. People use it for supply chain to enforce contracts with smart contracts, to electronically exchange things like securities, that you can physically but they're just a representation of money, without them being the actual money, just two parties have an agreement, you want to put that in electronic form. So, you look at the business case, you look at the value that can be derived from it. You test the regulatory aspect around it.

Respondents 14:27

Then you see how you want to manage it. This has been something what they call a consensus mechanism, just the way blockchain is driven, security driven, validation driven.

So

those mechanisms that you use, will even dictate which platform will be ideal for you. And one of the consideration are the Technological performance, how much data you are working with, blockchain doesn't work with huge amounts of data

Respondent 15:09

On the regulation, again, when you're using this distributed Ledgers, because it's transparent, in a sense that Everyone shares everything from day one.

Respondent 15:22

Whenever changes are done, everyone knows.

But the problem of that is you can step on the regulatory toes because it depends on what kind of information or trading that should decide if you're gonna go blockchain or not. What your in country laws say. You don't want to cross any legal boundaries. Expose, retain information, when and how, how? Yeah, if it's going to be shared across the entire network.

Is it in applicable case? Are we allowed to do so.

Unknown Speaker 16:06

Yeah.

Respondent 16:08

Yeah, because confidentiality is one thing. It's more strong is strong on the security side, but everyone who participates gets to know everything that's happening.

Unknown Speaker 16:22

So privacy issues?

Respondent 16:24

privacy issues, you need to think about what are the laws say if people be playing with people's personal information as an example, as part of a business case?

Is it something that I can share on the on a blockchain platform? So that its a ledger that's shared by everyone in everyone knows all changes that happened there? they are preview to Every piece of information that goes on

Unknown Speaker 16:55

Hmm.

Unknown Speaker 16:58

Then, okay, so then you can decide. So in terms of the you mentioned the issue of , testing, the regulatory space is one of the considerations or even now you're speaking to that, or, you know, you need to also look holy, whatever it is that whatever choices or decisions that you're taking have to be within their regulatory space? Or how do you how do you know, we don't you don't break any laws? So, so far from, from your experience, what what considerations like what what within the South African context that you work in?

What legal

considerations would need to be made? Like what laws for instance, would would apply? You know, do they apply even to as in the existing regulatory law policies and the laws that are they? Do they even apply in the way that they are to blockchain? Or if somehow you have to choose and pick on this one? I think I cannot. So how is that? Because there's no regulation. Right. What we're working with now is what is the and what has been designed for other types of systems? So now this regulations? Pat, do we apply the regulations that are there somehow? Or Correct? What happens in that space?

Respondent 18:19

Yeah, it's you have to pick and choose, you have to be selective, and it often becomes difficult to know if you're heading the right way. I'll give you an example. If you're we speak of the POPI act today.

Respondent 18:33

It's not a blockchain blockchain, no rule, or law. Yes. But you know, if you're dealing with personal information, you're obliged by law. It's not gonna say there are exceptions, because now you're on the blockchain. And whenever you are obliged, by law, to say, you need to have someone consent to the their information, you need to make certain attestations that you will only use it for the purposes for which it was requested or gathered, and it's going to be stored securely and all these things.

But it's not a blockchain law is a law that exists for you as an entity in operation. So the line, the the line, because the lines become blurred, you need to be at all times be sure where

when you're about to cross them when not to cross them,

then there's the legal aspect of it. To say, if something doesn't go well, then potentially you risk a litigation, not because this is blockchain because it could have breached certain laws in the country that govern other aspects of financial services.

Respondent 19:58

And there's also the issue of data residency its a huge thing in banks today that certain pieces of information are required within the national borders and cannot or may not exist outside. And blockchain is borderless by design. and yet, you hop onto that space, it sort of becomes borderless. Remember, I said it can bypass institutions, because it's an open forum, you don't have jurisdiction.

Respondent 20:34

So you need to think carefully about your business case to say, what are the elements of this business that I'm trying to realise. what laws today Currently, govern, this line of business outside blockchain? If I was to put it onto the on to the blockchain platform which of these laws would I potentially temper with?

Unknown Speaker 20:55

Hmm.

Unknown Speaker 20:59

So where would I find details regarding these loans for somebody who is me, being a student, let's say I'm outside the financial services sector, but I need I need to, because for this framework to work, like you're right, rightly saying, I need to consider all these laws, right? That work in that space. So how do I access those laws to say, okay, these are the laws that would apply in terms of protection of certain financial information and so on, as you're mentioning, how do I access that those laws or what laws would those be?

Respondent 21:35

Look at the South African Reserve Bank website, they should have an NPS Act there. They should have papers pertaining to blockchain. On this Swift website, they do have a

articles on blockchain there, IBM should also have something on blockchain because they big within this space.

Unknown Speaker 22:01

And I found some frameworks on Udemy.

Unknown Speaker 22:07

Or Udemy. Yeah, there are people just

Unknown Speaker 22:11

Udemy like, yeah, of course. Plus.

Unknown Speaker 22:15

Yeah. Don't look at it as you are going to portray the

Unknown Speaker 22:20

information. They have lots of.

Unknown Speaker 22:23

Okay, practitioners? Yes, is.

Unknown Speaker 22:28

Okay.

Unknown Speaker 22:30

All right. So

Unknown Speaker 22:33

I'm the enforcement of this

Unknown Speaker 22:37

in the regulated space, so how do you enforce it and thinking of blockchain, I could have nearly the smart contracts and, you know, the others have suggested What a smart

contract can then be used to set some of the rules to govern, or to even implement some of these legal and regulatory requirements. From your experience. Do you think that would be the case? Or how if not, then how else would enforcement be done?

Respondent 23:06

Its again done on a use case basis, there are public blockchains and then there are private blockchains. Private blockchains are usually more protected. You can control who participates.

Unknown Speaker 23:25

And you can at least set some rules of conduct around rules to say, Who are the members, you know, who joins and who participate. But as a public people come in and off as they see fit? A lot of private institutions choose Private options, then not everything is a smart contract. Again, it depends on which platform you're using.

It also depends on the rules that you're gonna embed on your solute blockchain solution, if it's gonna be smart, contract driven or not.

Unknown Speaker 24:05

limitations of smart contracts is that they have to be simple because it's just a code that you execute. That is true.

execute some of the clauses that you will have one a legal contract that a typical legal contract can be 10 pieces, you're not going to have that on the blockchain, its probably going to be a few lines of code that have to meet a certain condition for them to execute.

Unknown Speaker 24:33

So, there is that thing as well there where i always say not everything can be applicable, some works just fine. You know, you have two conditions and whatever you want to put in your smart contract, it is just a block of code when certain conditions are met.

Unknown Speaker 24:52

You will predefined or say if case one is true, then do

With this case,

Unknown Speaker 25:02

you know, the contract is made, it will always execute if those terms are made, but not every scenario fits that.

Unknown Speaker 25:10

Because in a real world, lawyers will go into paragraphs to explain conditions. so not everything fits into that brackets.

Unknown Speaker 25:20

Right, good. Yeah. Yeah. Yeah, if I say on a Monday, execute this task, it will do it. Straightforward.

Unknown Speaker 25:34

But even now, you have to include human elements considerations. It becomes difficult to act on So again the smart contracts won't work everywhere. Not every blockchain is smart contract driven, just like not every piece of blockchain is designed for cryptocurrencies. Yes. Some just use, for instance, supply chain to just track.

Unknown Speaker 26:06

Source of certain goods, ascertain that maybe they were counterfeit or they were sourced fraudulently, all the standards and regulations that would need to be followed, were adhered to, that they went through the proper channels and eventually reached the correct end right destination.

Unknown Speaker 26:38

So in a way, it's so yes, we can enforce some, as you said, some of the legal and regulatory things on on contract smart contracts. But in most cases that will still need to be supported by or that smart contract will be supporting the traditional contracts, because they because they're more detailed.

Responded

They're more details. But there's also the issue of if a contractor is not honoured in one way or another.

Depending on your location where you are, can it be enforceable in a court of law if you're supposed to follow it?

Unknown Speaker 27:27 say, I'm not happy with how this thing transpired. I think they should take a legal course on will it be live recognized.?

Unknown Speaker 27:37

Yeah.

Unknown Speaker 27:40

So the cost in the cost of running these platforms themselves, once you embark on the chain,

they tend to be

resource intensive, lots of power. They use up a lot of electricity. The managed through huge data centres that are not

it's either the you'll be burning money funds for energy, or there are not sustainable in the era where we are trying to move towards green energy,

be sustainable, not utilise fossil fuels and all these things, but then you have be more energy efficient, and then have this type of technology that requires so much compute power, some of the blockchain mining Bitcoin mining data centers, for instance, today, the can consume a lot of electricity

Unknown Speaker 28:49

Or when, at any point in the mix, the cost of you doing business expensive, because if you support the infrastructure financially, would your business case make sense? Yeah, something you'd be in because you want some business value out.

Unknown Speaker 29:14

So another consideration?

Unknown Speaker 29:17

Yeah, it's another consideration. It can be extremely difficult for business executives to rationalize going this route, because you need to demonstrate the value that will be derived from

Unknown Speaker 29:32

Hmm, it's one thing to do it, but does it make business sense? Yeah. So in terms of investment,

Unknown Speaker 29:42

into infrastructure,

Unknown Speaker 29:45

or using existing infrastructure, or do they also have to make additional investments towards you know, getting more new infrastructure or about to accommodate this blockchains or can they use what is already there

respondent

well you can use what is already there, AWS and Microsoft already offer blockchain in a sense and IBM does the same. some people are already building data centres and have their own servers, its nothing new they are using the same thing but its the code the resides on them is what's different. b

But they are not most efficient way of doing in some respects, even the cost of hosting a blockchain solution maybe more expensive than even the financial projections you have for any business idea you thought you would benefit from.

speaker

so for integrating them with what is already there, what are you guys using and why that. what is the process there?

Respondent

we have things they call oracles, not to be confused with oracle databases. it just a tool or way to integrate the distributed peer to peer network which is blockchain and our traditional networks. so its largely encryption-driven that's the one thing you need to be on top of and know very well. but there are ways to integrate. there are technology services and there are people who specialise in that, they call it on chain and off chain. Off chain being what we are used to today and on chain being what runs on the blockchain. and you can have tools that plugs in the two.

speaker

are those working? dont they have some limitations of their own?

respondent

they do have their own limitations. as i said they can run big data sets like we do in traditional industries today. so we have a billion use cases for blockchain that would be a no brainer to hop onto , but we also equally have limitations that they cannot support everything we do today. but you can still integrate, yu need to understand the rules, you need to understand the security around it, you need to understand how we manage things like encryption, hashing it all back to your data structures in second year again . What type of information do you pass, how is it encrypted and how does everyone relate, because blockchain is a peer to peer network which means you have a network of interconnected computers which you all participate in validating transactions so its almost like you all vote for something to happen. and if one is of then it fails. that is why i said it has privacy issues because now you have interconnected computers and everyone knows exactly what is happening at every stage. so so the way it changes things, is that it

changes the way we handle our approach to systems design and security. so if you try to integrate the two, then obviously there are trade-off. but again its another use case where we have smart individual who have said lets forget blockchain challenges, we are going to design services where the two worlds meet. a case in point are the stable coins when a token is pegged to existing currency which means you have a smart contract which can read a commodity systems there to keep track of the fluctuations of the exchange rates at all times and inform the nodes on the blockchain real time

speaker

so you mention that we have things like oracles. I am assuming APIs. and like you are saying there are certain tradeoff

Respondent

yes so ...everyone has their own approach to that, they can use APIs or oracles for integration.

Speaker

so from integrating normal technologies, are there any frameworks that the banking sector uses to guide that process and what are the elements of focus in those frameworks?

?

Respondent

remember i said these thing largely start form outside, and when they start you let them do whatever they do then you bring into your world and you check what impact it will have. so you will think about if i do this today, and we already have banking regulations. let me give an example. if i decide that from now on i want to use stable coins to handle some overseas transactions, as opposed to following the normal payment process the rule of

thumb would be i am transferring money, and the rules at the bank would be to check if we have money or liquidity to back it with, to say if i say on the blockchain i have 10000 dollar to i actually have 10000 dollars, cos that 10000 dollar has to exist somewhere that the rule .and whatever activity the blockchain there is it reconcilable with the bank. can i show it in my books, can i do accounting on it to show what happened out there and can it be reported on adequately, here the finances or can i put some financials on that, or do i need to report to some entity internally and operationally speaking to say do we have reporting lines, can it be auditable, can it be checked and traced, does it still follow the necessary authorisation and approval processes that we have today. even if you are doing it outside (on blockchain) it still need to conform to your business as usual. so we need to consider auditability, reporting, and being able to account for things around it. managing risk around it , we have risk management frameworks in business.. so which element can you apply to this new thing now. and if the reserve bank is involved then you need to consider what it that you need to report to then.. i think the most important thing with financial services is the protection of consumer welfare, for instance today you have money in a bank, and so the bank has an obligation to protect it.. the same goes for blockchain.