Implementing Smart Contracts in the Syndicated Loan Market: An Issue of Adoption

Merike Malan and Adriana Steyn
University of Pretoria

Abstract

Distributed ledger technology allows for data to be recorded, shared, and synchronized across multiple distributed data stores. This brought forth the idea of using this technology to build consensus. Implementing this technology within the Syndicated Loan Market through Smart Contracts allows for reduced manual labor and back-office workloads as well as the removal of reconciliation and corporate actions. As a result, counterparty risk and settlement times will be minimized, and performance and transparency for regular reporting will increase. However, an individual's embrace of this new technology will determine its successful implementation. To address this issue, this article examines the trust model, trust in technology drivers, and the revised unified theory of acceptance and use of the technology model to construct the trust and adoption of the technology model. This article culminates in guidelines for the implementation of Smart Contracts. Avenues for future work include the investigation of a multimotive information systems acceptance model.

Money has been the backbone of human society since the origins of human civilization. From its earliest form—barter—to its earliest form—barter—to the most recent cryptocurrencies, the concept of a medium of exchange has progressed from primitive to modern times.[1] The first ever cryptocurrency, Bitcoin, was introduced in 2009 as an obscure piece of code by a hacker operating under the pseudonym Satoshi Nakamoto.[2] With the

introduction of Bitcoin, a fundamental and untested concept was introduced simultaneously: the underlying distributed ledger known as Block-chain technology. Blockchain is an implementation of distributed ledger technology: a consensus of digital data that are replicated, shared, and synchronized across multiple locations with no third-party intermediaries.[3]

A vast number of use case opportunities for financial institutions and intermediaries, where distributed ledger technology can be beneficial, exist. The application of distributed ledger technology will differ, depending on the use case.[4]

The focus of this article is on the adoption and trust of distributed ledger technology in the capital market, specifically in the Syndicated Loan Market. Currently, no key factors influencing the adoption and trust of distributed ledger technology in the Syndicated Loan Market have been found. Thus, critical elements that shape the financial market to adopt and trust distributed ledger technology specifically within the Syndicated Loan Market are necessary.

SYNDICATED LOANS

Syndicated loans, which are loans where a group of lenders, typically financial institutions, offer funds jointly to a borrower, are structured, arranged, and administered by commercial or investment banks known as arrangers. Syndicated loans are made up jointly by a group of lending banks, also called syndicates.[5]

One technique that has been considered to reduce manual labor and back-office workloads and remove the need for reconciliation and corporate actions is Smart Contracts: a distributed ledger technology application.[6] Through implementing Smart Contracts, back-office functions are able to leverage the data collected across multiple parties as well as facilitate the exchange, signatures, and authentication of notary documents that is triggered by certain arrangement conditions,[7] providing a level of security and trust concerning arrangement conditions and their execution. The focus of this article underscores contributing factors relating to the adoption and trust of distributed ledger technology, specifically in the Syndicated Loan Market.

Due to the self-executing nature of Smart Contracts, the risk of relying on someone to follow through on commitments is eliminated. Smart Contracts eliminate unnecessary third-party intermediaries, minimizing counterparty risk and settlement times, as well as increasing contractual performance and transparency for regular reporting. Smart Contracts can lower the settlement time from 20 days to 6–10 days, resulting in an additional 6% growth in future demand.[8]

Smart Contracts are indeed a technology ahead of the law. The financial system has built trust among its customers for years through security and privacy; however, trust in distributed ledger technology has not yet been established.[10] For Smart Contracts to be binding in the future, to progress and grow, deep collaboration, adoption, and trust between all the Syndicated Loan parties and Smart Contracts are required.[4]

Research on information systems literature consists of many widely used technology acceptance theories. One of the major theories that is used to understand acceptance and/or adoption of new technologies is the unified theory of acceptance and use of technology (UTAUT) model.[12]

Unified Theory of Acceptance and Use of Technology

UTAUT helps institutions explain and predict the successful acceptance of technology. This is a valuable model to use when investigating the acceptance of technology, as well as factors such as demographics and experience which may influence individuals to accept and adopt new technologies.[12]

In investigating acceptance and adoption, it was noted that trust, or the lack thereof, in these technologies plays a fundamental part.[10] Trust must be placed in the technology for successful adoption. Trust is a major component that is necessary for human beings to interact, whether it be with one another or through technology.[13] Trust has the ability to influence an individual on whether or not to use technology.[14]

Revised UTAUT Model

Miller[11] identifies "trust" as one of the main barriers in adopting new technologies. McKnight *et al.*[12] suggest that there is a relationship between trust and technology adoption; hence,

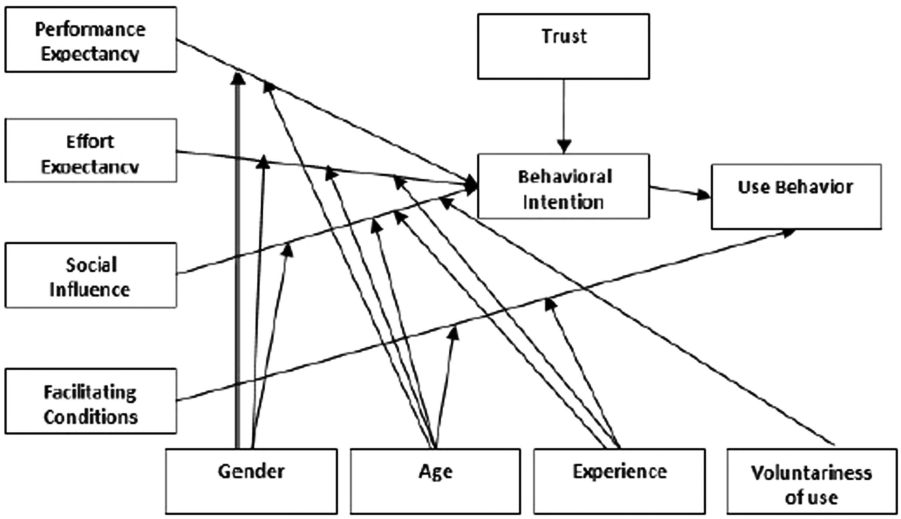

Figure 1. Revised UTAUT model.[14] This model combines the UTAUT model and trust as it was suggested that there is a relationship between trust and technology adoption.

a revised UTAUT model was designed where *trust* was taken as a main construct (see Figure 1).

Adding *trust* to the UTAUT model as a main construct has a direct impact on the "behavioral intention" of an individual to adopt new technologies.[11]

For the successful implementation of the distributed ledger technology in the capital market, especially in the Syndicated Loan Market, an individual's embrace (including acceptance, adoption, and trust) of this new technology had to be examined. To understand how trust can be built, trust as a construct needs to be understood first.

MATTER OF TRUST

The question has shifted from whether Smart Contracts can transform the Syndicated Loan Market to how the ecosystem can prepare for the future. The issue now faced was whether all the relevant stakeholders were willing to trust the technology innovation. Trust is a fundamental part of life and is necessary for interaction. Alharbi[13] reveals two distinct elements of trust in a virtual environment: human interaction and technological interaction.

Trust Through Technology

Contracts, in a traditional sense, rely on all relevant parties trusting one another to fulfil their side of the obligation. This relates to interpersonal trust that is associated with all the relevant parties. This interpersonal trust is often associated with collaboration, performance, and greater information sharing. Smart Contracts feature the same kind of agreement but eliminate the human aspect that replaces the need for trust between these parties, thus fulfilling the interpersonal trust measurements.[13]

Although distributed ledger technology is referred to as a trustless system,[3] it is important to remember that this refers to the trust that is placed in traditional trusted third parties such as banks, governments, and lawyers, to name a few, and not the trust placed in technology. Traditional contracts rely on peoples' trust in these trusted third parties.[14]

Trust can be seen as a main attribute when talking about distributed ledger and its applications, such as Smart Contracts. Rather than relying on trusted third parties, distributed ledger technology relies on a system of decentralized consensus. The architecture and structures of distributed ledger technology may result in the mitigation of our dependence on third parties.[14]

Distributed ledger technology builds trust between online peers through a trustworthy technology. This eliminates trust placed on people to deliver and focuses on building trust through cryptographic guarantees that ensure people delivering.[15] Trust is offered through Smart Contracts by means of a single source of truth given to all the participants.

Although trust can be built between online peers through a trustworthy platform, the

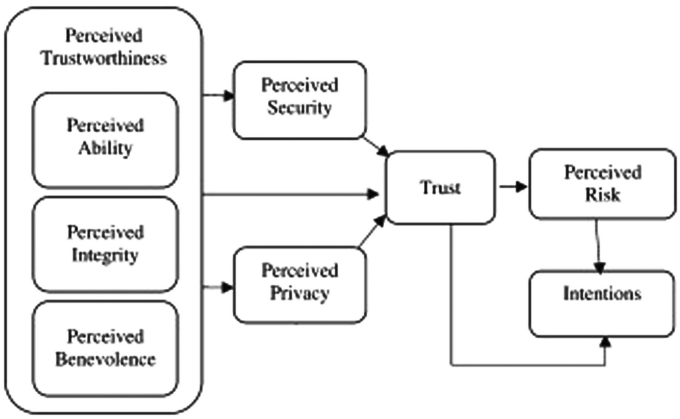

Figure 2. Model of trust.[13] This model illustrates three trust in people drivers that is used to build the foundation of trust.

success thereof not only relies on trusting the peers but also on trusting the technology. This refers to the second element of trust in a virtual environment, namely technology interaction. This not only shows that people and technology are intertwined when technology-mediated interactions occur but that it is also necessary to understand both trust through technology and trust in technology. This is due to the fact that humans interact with one another, peer-to-peer, as well as with the technology.[13]

Trust in Technology

Trust trough technology has been widely examined, but the effect of trust placed in technology has been generally absent. By focusing on trust placed in technology, a better understanding of the acceptance of technology, irrespective of the human aspect surrounding it, may be achieved.[16]

Research on interpersonal trust—trust in people—has led to three drivers of trust, namely ability, benevolence, and integrity.[16] Trust in people and trust in technology differ in the nature of the objective of dependence. According to Vance *et al.*,[17] trust in technology is "a belief that a specific technology has the attributes necessary to perform as expected in a given situation in which negative consequences are possible."

Venkatesh *et al.*[10] found that trust in people drivers[13] can be regarded as the dimensions of trustworthiness, building the foundation of trust. Although these drivers are recognized as the main drivers of trust in a virtual environment, lack of security and privacy can result in the reluctance of adoption of technology; thus, trust is established through safeguarding all information.[10] In this article, privacy and security refer to the trust that is built through technology as set out above.

Both security and privacy as well as the trustworthiness of technology have a direct effect on trust. For the perception of high security and privacy to exist, there must be a belief that the technology is trustworthy to perform reliably as expected. Thus, trust must be earned over time through the expected performance of technology.[10]

Technology interaction in a virtual environment involves risk. Trust is of paramount importance when risk is involved, as trust allows for participation in risky situations.[13] Perceived risk surrounding technology can ultimately be associated with the perception of security and privacy and the behavioral intention of a person.[10] This is illustrated through a model of trust that is shown in Figure 2.

Vance *et al.*[17] compared the three drivers of trust in people with trust in technology and found functionality, helpfulness, and reliability to be the common concepts.

Functionality relates to whether technology has all the necessary features to perform as expected, whereas helpfulness refers to the need to be helped if there is a problem using technology. Reliability depends on whether or not this technology will operate properly in a consistent manner.[17,18] Due to the fact that technology does not consist of a moral agency, trust in technology reflects the beliefs about its capability (or functionality) rather than its will or its motives.[17]

It is evident that the likelihood to adopt technology is higher if one trusts it, complementing adoption models. Trust in technology results in a deeper exploration, adoption, and repeated use of a particular technology.[13] For this paper, the trust model,[10] using trust in technology drivers, together with the revised UTAUT model,[11] is used to study trust and adoption of Smart Contracts (see Figure 3).

In Figure 3, the dependent variable is the behavioral intention of an individual. The relevant variables from both the trust model[10] and the revised UTAUT model[11] were extracted and

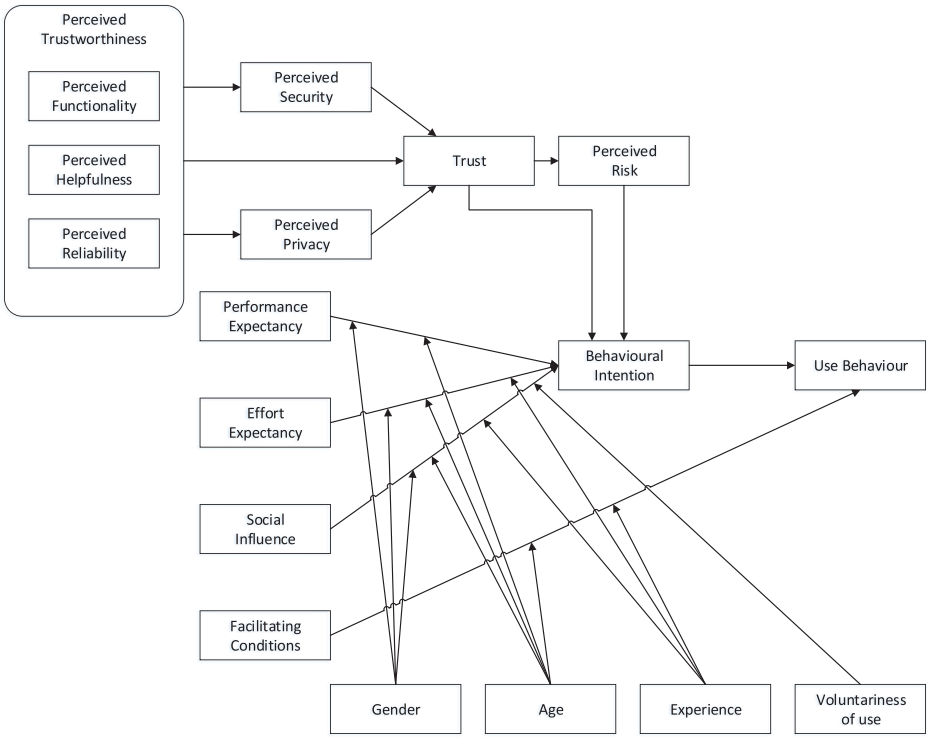

Figure 3. Trust and adoption of technology model. This model combines the trust model, trust in technology drivers, and the revised UTAUT model to construct the trust and adoption of technology model. This model illustrates how trust can be built to ultimately help to adopt a new technology.

merged. Mayer *et al.*[19] found that facilitating conditions directly link to the use behavior of an individual. The rest of the variables are mediated by the behavioral intention of an individual to use technology and are influenced by moderating variables (gender, age, experience, and voluntariness of use). The behavioral intention of an individual is influenced by trust and perceived risk.

By merging the trust model with the revised UTAUT model, an understanding of how one's trust in technology influences one's behavioral intention, overall acceptance, and adoption of technology can be achieved. Through this understanding, organizations can offer new opportunities to adapt processes to support trust and adoption.[20]

METHODOLOGY

This study used survey interviews to gather data that were analyzed using qualitative methods. Questions were formulated based on the trust and adoption of technology model constructed (see Figure 3). A thematic data analysis process was used to extract themes and patterns. This exposed a need to draw up guidelines on how the technology under discussion can be accepted, adopted, and trusted.

GENERAL SURVEY INFORMATION

Interviews were conducted with 20 participants. Three age groups were identified from a pragmatic and comparative point of view. The data were categorized according to the following age groups: 18–24, 25–34, and 35–44. In the data gathered, 10% of the participants fell in the 18–24 age group, 60% fell in the 25–34 age group, and 30% fell in the 35–44 age group.

The participants were highly unbalanced in terms of gender, age, experience, and voluntariness of use. This can be seen from the ages ranging from 18 to 44 with 60% of the participants being male and 40% being female. More than half of the participants worked in an information systems environment (60%) with employment duration ranging from less than three years to more than nine years.

The interview questions were designed in such a way that the data from individuals with and without distributed ledger technology or Smart Contract knowledge were collected. The dataset included participants with knowledge of distributed ledger technology (85%) in general and Smart Contracts (60%) in particular, as well as those without any knowledge of the distributed ledger technology (15%) in general and Smart Contracts (40%) in particular.

To compare the relationship between the main constructs and the moderating variables from the trust and adoption of technology model, an analysis was conducted by testing the statements that were identified in the literature. From the data, it was determined whether gender, age, experience, and voluntariness of use play a part in the behavioral intention to adopt distributed ledger technology in general and Smart Contracts in particular. It is important to note that the effect of experience could not be tested on most constructs as the concept of Smart Contracts is relatively new. For performance expectancy, effort expectancy, and social influence, this study found that gender and age have no significant effect on the relationship between these moderating variables and the behavioral intention to use Smart Contracts.

The differences in the relationship of the main constructs (performance expectancy, effort expectancy, social influence, and facilitating conditions) and the behavioral intention among these moderating variables were examined.

Performance Expectancy

All participants believed that if their performance would improve through using Smart Contracts, their intention to use Smart Contracts would be positive. This aligns with the statement made by Venkatesh *et al.*[10]

This study has found that there is a strong relation between the performance expectancy and the behavioral intention of the participant.

Effort Expectancy

A considerably lower effort was expected when using Smart Contracts than existing methods. Venkatesh *et al.*[10] state that effort expectancy has a positive influence on the behavioral intention of a participant. This can suggest that the easier a system is to use, the more likely it will be used, as outlined by one participant: "I expect this technology to be geared toward normal users who do not have technical skills." This provides strong empirical support relating to the seminal work of Venkatesh *et al.*[10]

In this study, effort expectancy pertains to the seminal statement made by Venkatesh *et al.*[10]

Social Influence

From the data analyzed, social influence has a positive influence on the behavioral intention to use Smart Contracts as suggested by Venkatesh *et al.*[10] Furthermore, it is evident that voluntariness of use negatively influenced the use of Smart Contracts. If Smart Contracts are required to be used within the work environment, the behavioral intention to use Smart Contracts will increase. This is evident from the following participant's answer: "I do not use it because in the environment in which I work are still reliant on a lot of paperwork. The industry had not evolved as yet to incorporate this type of technology into the process. At present, the only reason I will use this technology is if it becomes legislation."

In this study, strong agreement was found regarding the statement that social influence has a positive effect on the behavioral intention to use Smart Contracts.[10] Voluntariness of use negatively influenced the behavioral intention of the participants.

Facilitating Conditions

It was noted that although participants preferred to be trained in the overall concepts, setup, and use of Smart Contracts, the lack thereof did not influence their use behavior regarding Smart Contracts.

Venkatesh *et al.*[10] suggest that if the experience of a participant using Smart Contracts is agreeable, the participant will familiarize them with the technology, enhancing knowledge that will eventually reduce dependence on external support. Due to the nature of Smart Contracts being a new technology concept having been discussed only in theory, none of the participants had made use of it. However, the data analysis indicated that there were more participants that, irrespective of the availability to use Smart Contracts, said they would still make use of

Table 1. Trust and adoption guidelines for the implementation of Smart Contracts.

Trust
Step 1: Establish your audience • Identify internal and external stakeholders • Define all the roles and responsibilities • Are the intended goal and expectations clear?
Step 2: Shape the overall trustworthiness of Smart Contracts • Clear explanation of the functionality of Smart Contracts given • Is there a full, comprehensive set of explanatory notes (including the drawbacks and benefits of using Smart Contracts)? • Is there a good understanding of the intention of Smart Contracts?
Step 3: Discuss Security of Smart Contracts • Identify and document all security aspects of the current organizational methods and of Smart Contracts • Identify mitigation actions and owners
Step 4: Discuss the Privacy of Smart Contracts • Identify and document all privacy aspects of the current organizational methods and of Smart Contracts • Identify owners
Step 5: Risk Management • Identify all risks • Is it a risk or an opportunity? • Identify mitigation actions and owners

Accept
Step 1: Performance • Is there an understanding of how Smart Contracts will improve the overall performance of the organization and its day-to-day procedures?
Step 2: Effort • Is there an understanding of how Smart Contracts will improve the competitiveness the entire organization?
Step 3: Social Influence • Is there an understanding of the design and intention of Smart Contracts?
Step 4: Facilitating Conditions • Does the infrastructure support the use of Smart Contracts? • Identify and allocate technical support • Identify and allocate internal support

Adopt
Step 1: Strategic Alignment • Has strategic alignment been executed?
Step 2: Execution Plan • Establish execution plan

Smart Contracts if given the choice. This contradicts the statement of Venkatesh *et al.*[10]

Perceived Trustworthiness

Overall high perceived functionality (50%) and helpfulness (67%) were associated with Smart Contracts. However, more participants were undecided regarding the perceived reliability of Smart Contracts (33%). Reasons given for the perceived reliability include the fact that due to Smart Contracts being a new and growing technology, the environment and security features have not yet been tested: "I believe Smart Contracts have huge potential, however as it is

still new, lots of testing is required to ensure it is reliable and safe, thus in theory it is reliable, but because it has not been proved I cannot say with certainty that Smart Contracts are reliable."

As trustworthiness is measured through the three drivers set out above, overall high trustworthiness can be ascribed to Smart Contracts. The logic for this relationship is that the trust in Smart Contracts reflects the beliefs relating to their capability and functionality.

Perceived Privacy

A small majority of participants (55%) believe Smart Contracts are secure despite the fact that security issues have not been tested. Participants suggested that constant updates and strengthening of security is imperative as the lack thereof will result in their terminating all use of Smart Contracts: "I believe Smart Contracts are more secure than paper contracts; however, cybercrime is literally unstoppable and a further consideration should be given to the security of the information."

The majority of participants (60%) perceived Smart Contracts to protect personal information. However, one participant pointed out: "It can capture specific details of transactions without anyone knowing the parties involved. This is how it is intended to be used, but like any technology there might be concerns around how private it actually is."

Behavioral Intention

The recommendations conceptualized in this paper emphasize the trust, acceptance, and adoption of Smart Contracts. They range from shaping trustworthiness of Smart Contracts to enhance the performance and effort of business operations and processes.

However, adopting Smart Contracts will significantly change the entire organizational streamlining, requiring careful planning, and strategizing. In understanding the factors that influence the trust, acceptance, and adoption of technology, guidelines were formulated when implementing Smart Contracts (see Table 1).

Given these findings, it can be concluded that the research outcomes of this paper are instrumental in understanding how Smart Contracts impact the Syndicated Loan Market and in perceiving Smart Contracts as a trustworthy technology. Through understanding the factors that influence trust and the adoption of technology on behavioral intentions, markets and institutions can develop operational strategies that can foster positive acceptance and transition. This article provides a theoretical and practical contribution to the body of knowledge on the topic researched.

CONCLUSION

While there are still many questions that have to be answered, it has been found that building trust will lead to a higher likelihood to adopt technology. This research resulted in the trust and adoption of technology model. Trusting in a technology has been shown to result in a deeper exploration, adoption, and repeated use. An interesting find was the willingness to trust Smart Contracts despite the doubts about their reliability.

Through this understanding, this article provides guidelines to build an environment enabling this trust and adoption of Smart Contracts. These guidelines are not intended to be a set list of criteria, but rather general guidelines to ensure that all the parties are ready to implement Smart Contracts. Further investigation of a multimotive information systems acceptance model, together with software failure issues that may arise, is needed.

ACKNOWLEDGMENT

M. Malan would like to thank her supervisor, Dr. R. Steyn, for her invaluable contribution, feedback, and input, and those who took the time to partake in her interviews.

REFERENCES

1. L. J. Trautman and A. C. Harrell, "Bitcoin versus regulated payment systems: What gives?" *Cardozo Law Rev.*, 2016. [Online]. Available: https://ssrn.com/abstract=2730983 or http://dx.doi.org/10.2139/ssrn.2730983
2. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
3. J. Van Oerle and P. Lemmens, "Distributed ledger technology for the financial industry," White Paper, 2016.

4. "The future of financial infrastructure: An ambitious look at how blockchain can reshape financial services," World Econ. Forum, Cologny, Switzerland, 2016. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/no/Documents/financial-services/the-future-of-financial-infrastructure.pdf
5. L. Parker, "Ipreo and Symbiont to overhaul the $4.7 trillion global syndicated loans market," Brave New Coin, Auckland, New Zealand, 2016. [Online]. Available: https://bravenewcoin.com/news/ipreo-and-symbiont-to-overhaul-the-4-7-trillion-global-syndicated-loans-market/
6. B. Hughes, "Distributed ledger use cases in the financial industry," KuppingerCole Analysts, Wiesbaden, Germany, 2016. [Online]. Available: https://www.kuppingercole.com/blog/hughes/distributed-ledger-use-cases-in-the-financial-industry
7. S. A. Dennis, Syndicated Loans, *J. Finance Intermediation*, 2000. [Online]. Available: http://www.idealibrary.com
8. Capgemini Consulting, "Smart contracts in financial services: Getting from hype to reality," 2016. [Online]. Available: https://www.capgemini.com/resources/smart-contracts-in-financial-services-getting-from-hype-to-reality/
9. S. Yousafzai, J. Pallister, and G Foxall, "Multidimensional role of trust in internet banking adoption," *Serv. Ind. J.*, vol. 29, no. 5, pp. 591–605, 2009. [Online]. Available: https://www.researchgate.net/profile/Gordon_Foxall/publication/247523936_Multidimensional_role_of_trust_in_Internet_banking_adoption/links/09e4150a577607590d000000/Multidimensional-role-of-trust-in-Internet-banking-adoption.pdf
10. V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User acceptance of information technology: Toward a unified view," *MIS Quart.*, vol. 27, no. 3, pp. 425–478, 2003.
11. E. E. P. Miller, "Trust in people and trust in technology: Expanding interpersonal trust to technology-mediated interactions," Ph.D. dissertation, Dept. Psychol., Univ. South Florida, Tampa, FL, USA, 2015.
12. H. D. McKnight, M. Carter, J. B. Thatcher, and P. F. Clay, "Trust in a specific technology: An investigation of its components and measures," *ACM Trans. Manage. Inf. Syst.*, vol. 2, no. 2, pp. 12–32, 2011. [Online]. Available: https://dl.acm.org/citation.cfm?id = 1985353
13. S. T. Alharbi, "Trust and acceptance of cloud computing: A revised UTAUT model," in *Proc. Int. Conf. Comput. Sci. Comput. Intell.*, 2014, pp. 131–134.
14. D. Gefen, E. Karahanna, and D. W. Straub, "Trust and TAM in online shopping: An integrated model," *MIS Quart.*, vol. 27, no. 1, pp. 51–90, 2003.
15. M. Krause, "Implications for the developing world," Claremont McKenna College, Claremont, CA, USA, 2016. [Online]. Available: http://scholarship.claremont.edu/cmc_theses/1261
16. F. Mazzella and A. Sundararajan, "Entering the trust age," vol. 2, BlablaCar, Paris, France, 2016.
17. A. Vance, C. Elie-Dit-Cosaque, and D. W. Straub, "Examining trust in information technology artifacts: The effects of system quality and culture," *J. Manage. Inf. Syst.*, vol. 24, no. 4, pp. 73–100, 2008. [Online]. Available: http://www.tandfonline.com/doi/full/10.2753/MIS0742-1222240403
18. H. McKnight, M. Carter, and P. Clay, "Trust in technology: Development of a set of constructs and measures," in *Proc. Diffus. Interest Group Inf. Technol.*, 2009. [Online]. Available: http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1009&context=digit2009
19. R. C. Mayer, J. H. Davis, and F. D. Schoorman, "An integrative model of organizational trust," *Acad. Manage. Rev.*, vol. 20, no. 3, pp. 709–734, 1995. [Online]. Available: https://www.jstor.org/stable/258792
20. S. K. Lippert and M. A. Davis, "Conceptual model integrating trust into planned change activities to enhance technology adoption behavior," *J. Inf. Sci.*, vol. 32, no. 5, pp. 434–448, 2006.

Merike Malan joined Moyo Business Advisory as a Business Analyst in 2015, after completing her studies. Her current research interests include application programming interfaces, online payments, and digital currencies. She received the Master's degree in informatics from the University of Pretoria, Pretoria, South Africa, in 2019. Contact her at merike.malan@moyoafrica.co.za.

Adriana Steyn is currently a Lecturer with the University of Pretoria (UP), Pretoria, South Africa, after returning from industry, where she was an Information Manager for an international trading house. She focuses her research on ICT adoption for SMEs in developing contexts as well as innovative teaching technologies. She received the Ph.D. degree in entrepreneurship and ICT adoption focused on training entrepreneurs to effectively engage with technology. She is a recipient of UP Teaching Excellence Laureates' in 2019 as well as a recipient of Association of Information Systems' Award for Innovation in Teaching in 2018. Contact her at Riana.steyn@up.ac.za.