# Key characteristics to create optimized block chain consensus algorithms

J. Leo[1][0000-0003-1933-7298] and M.J. Hattingh[2][0000-0003-1121-8892]

University of Pretoria, Private Bag X20, Hatfield, 0028
joshualeslieleo@gmail.com, marie.hattingh@up.ac.za

**Abstract.** Blockchain is a fairly new technology and still in its infancy. As a result, many research papers are creating optimized consensus algorithms. Therefore, a need for key characteristics to create optimized blockchain consensus algorithms has been identified. This research paper presents the results of a systematic literature on identifying the main blockchain consensus algorithms and their associated advantages and disadvantages. Papers from four different databases were retrieved and after exclusion criteria were applied, 71 papers were ultimately included in the review. Results indicated that the five main consensus algorithms were Proof-of-Work (PoW), Proof-of-Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), and Delegated Proof-of-Stake. The results further indicated that efficiency was the main advantage of the PoS, PBFT, PoA and hybrid consensus algorithms. The main disadvantage was "energy wastage" and was attributed to the PoW algorithm. Security concerns were the main disadvantage of the PoS algorithm. These findings were used to present key characteristics that future researchers can have in mind when creating optimized blockchain consensus algorithms.

**Keywords:** Blockchain; Consensus Algorithm, Proof-of-Work (PoW); Proof-of-Stake (PoS)

## 1 Introduction

Satoshi Nakamoto first introduced blockchain technology when he developed Bitcoin in 2008 [1]. This technology allows for decentralization as a history of all the transactions are kept on each node on the network [2]. Any person with access to the network plays a role in maintaining the blockchain node. Blockchain has a strong advantage of being transparent as any party can acquire access to the transaction. Furthermore, other characteristics included security, immutability and transparency [3]. Due to these characteristics blockchain has played a disruptive role in major industries such as the supply chain, the medical industry, financial and energy industry [4]. In order for it to be carried out successfully in these industries, optimized blockchain consensus algorithms need to be utilized.

There have been a number of different consensus algorithms created. The most common ones being Proof-of-Work and Proof-of-Stake [5]. Both these algorithms come with their advantages and disadvantages. As a result, many new consensus algorithms are being created to deal with their shortcomings.

An initial scanning of research determined that numerous research papers were creating improved consensus algorithms. As a result, a gap in research was determined where it would be beneficial to have key characteristics that these new consensus algorithms should have. Therefore, this research paper proposes the following main research question: *What are the key characteristics to create optimized blockchain consensus algorithms?*

To determine the answers to the main research question the following sub-research questions need to be answered: (1) What are the main blockchain consensus algorithms? (2) What are the advantages of the main consensus algorithms found? , (3) What are the disadvantages of the main consensus algorithms found?

This systematic literature review will be structured as follows. Section 2 details the systematic review methodology. Section 3 and 4 presents the findings and discussion of the findings of the systematic literature respectively. Section 5 offers up future research whilst section 6 will conclude the study by summarizing the main findings.

## 2 Methodology

Blockchain technology is still in its infancy [22], as a result, the methodology proposed and utilized in this systematic literature review is designed specifically with the novel technology in mind. This research paper considers both qualitative and quantitative research. Both of these research types will be used as blockchain consortiums is exiting the Peak of Inflated Expectations and entering the Trough of Disillusionment in the Gartner Hype Cycle [23]. Its placement in the Gartner Hype Cycle means that there will be plenty of qualitative research into the topic but minimal quantitative research as there are not many applications for this type of research to be conducted on.

The process of selecting the research papers to be included in this systematic literature review was as follows:

1. The following keywords were initially inserted into the chosen databases: (block chain AND consensus algorithm) OR proof of work OR proof of stake. These keywords were selected as blockchain consensus algorithms is the core components of the research paper. Proof-of-Work and Proof-of-Stake were included in the search terms as they are two of the most popular blockchain consensus algorithms, therefore it would yield better results.
2. Blockchain technology was first introduced in a paper by Satoshi Nakamoto in 2008 [24]. Since it was introduced in 2008, the search filter data range for all the databases were from 2008-2020. The reasoning behind the source types that will be listed below is because formal research papers that have gone through a rigorous process to be published, is desired. The following is the filter parameters that were used for each database:

- Science Direct – source type: review articles and research articles
- IEEE – source type: journals and conferences
- Ebsco Host – source type: academic journals
- Emerald – source type: article

3. The following step is to select relevant research papers by reading through the title and abstract of the research paper. The paper will be included if the author mentions relevant research containing consensus algorithms in the title and abstract. The research paper must also be downloadable immediately for it to be included. The results can be seen in the "Title and Abstract".
4. The final step in selecting research papers to be included in the study will be analyzing the research papers to determine if it adheres to the following inclusion criteria:

- Advantages of blockchain consensus algorithms
- Disadvantages of blockchain consensus algorithms
- Future research of blockchain consensus algorithms

The process mentioned above resulted in 71 research papers being included in this study. Content analysis will be the chosen analysis technique.

## 3 Results – background

Analysis of the resultant papers indicated that 37 papers were based on qualitative research and 34 papers were based on quantitative research. Science Direct and IEEE databases produced 27 papers respectively followed by 11 papers from EBSCO Host and six papers from Emerald Insight.

In answering sub-research question one, results further indicated that **t**here was a total of 32 different blockchain consensus algorithms mentioned in the 71 articles that were included in the study. The four most common algorithms that the 71 included research papers mentioned, were Proof-of-Work (PoW), Proof-of-Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), and Delegated Proof-of-Stake (DPoS).

In answering the second sub-research question the main advantages of blockchain consensus algorithms were efficiency, scalability and security. Efficiency was the advantage that was mentioned in 72% of the papers. The second type of advantage, scalability was associated with the PoW, PoS, and DPoS having the advantage of scalability

Security as an advantage was associated with PoW and PBFT consensus algorithms [28],[29], [30].

In answering the sub-research questions, three findings indicated that "energy wastage" was mentioned in 35 papers as the most often occurring in the PoW and PoS algorithms. Security was identified as the biggest disadvantage of the PoS algorithm by seven papers [27], [31]–[36].

## 4 Discussion

The following sections discuss the findings in terms of the three sub-research questions posed in section 1.

### 4.1 S-RQ1 What are the main blockchain consensus algorithms?

According to the results in section 3, out of the 71 research papers considered, there were 33 different consensus algorithms that were identified. Of the 33 listed consensus algorithms, four of them were mentioned significantly more than the rest. These four algorithms included Proof-of-Work, Proof-of-Stake, Delegated Proof-of-Stake, and Practical Byzantine Fault Tolerance. This section will allow the reader to gain insights into how these consensus algorithms work. A stronger argument can be made for the advantages and disadvantages which will be further explored.

**Proof-of-Work.** Bitcoin uses the Proof-of-Work consensus algorithm [16]. This algorithm was included in 66 of the included research papers. Proof-of-Work is essentially nodes putting in a rigorous computational effort to keep the blockchain network secure [6], [37]. This consensus algorithm involves nodes on the network competing with each other to solve a cryptographic problem which is easily verifiable by other nodes on the network [6]. These nodes that are competing against each other are known as miners and the process of solving this cryptographic problem is known as mining. A miner's responsibility is to verify transactions, validate, create and add blocks to the chain[9]. This process of mining will be explained below.

Once a block is filled with transactions, the miner can initiate the verification process. The block contains a header that includes the hash pointer(the hash of the data of the previous block), the network difficulty, a timestamp, the version of the block, a list of the transactions that they think should be added to the network, and a nonce [6]. A nonce is a 4-byte adjustable number [32]. The miner must continuously change the nonce so that the outcome of the hash results in it is below the threshold that is set by the network difficulty level included in the header[6]. After the miner finds a hash that is below the threshold, the block will be propagated onto the blockchain network using flooding algorithms [38]. The other nodes on the network will verify this block by taking the nonce that was used for validation and will hash the block with the same cryptographic function used by the miner that proposed that the block is valid. If the resulting hash results in a value lower than the threshold, then the miner will deem the block to be valid. The majority of the nodes on the network must deem this block valid for it to be added onto the chain of the blockchain network [38]. If the block is successfully added to the chain, the miner will be rewarded with a certain amount of currency of the network, 12.5 coins in the Bitcoin context [39]. There are numerous miners mining blocks in parallel, as a result, multiple chains (known as forks) are created. The longest chain is deemed the most valid one as it required the majority of the network's computational power [40].

This process of mining has some advantages but result in more disadvantages according to the research papers analyzed. These advantages will be discussed in section 4.2. As a result of the disadvantages stemming from the proof-of-work consensus algorithm, there have been algorithms that have used Proof-of-Work as a building foundation but improvements have to be made

**Proof-of-Stake (PoS).** The proof-of-stake is an alternative consensus algorithm that was created to deal with the inefficiencies and disadvantages of Proof-of-Work [40]. According to the paper, *Analysis of the main consensus protocols of blockchain*, Ethereum is planning on moving away from Proof-of-Work and transitioning towards the proof-of-stake consensus algorithm [25]. 78,87% of the included research, either mentioned or elaborated on this algorithm.

This consensus algorithm involves validators that have the responsibility of ensuring transactions and blocks are authenticated and valid [9]. Stakeholders stake a certain amount to be considered to validated and add blocks to the chain. The stake is a certain amount of the digital currency that is stored in a vault to ensure that the validator does not carry out any malicious actions. This ensures that those who have staked more are less likely to carry out malicious actions as they will lose what they have staked [28]. The validator will be selected on a random selection basis with the validators staking more, having a higher chance of being selected as the one to validate the block [41]. The validator that is selected will ensure that the transactions in the block are valid. If the transactions are deemed to be valid, the validator will add the block onto the existing chain. They will then will be rewarded in transactions fees instead of coins as in the Proof-of-Work consensus algorithm [42].

The creation of this has resulted in some advantages such as the reduction of computational power required. Although there are benefits as a result of this algorithm, there are disadvantages that also occur. Further advantages and disadvantages of this consensus algorithm will be discussed further in section 4.3 Similar to Proof-of-Work, additional consensus algorithms use the foundation of proof-of-stake to create new and improved versions of this algorithm.

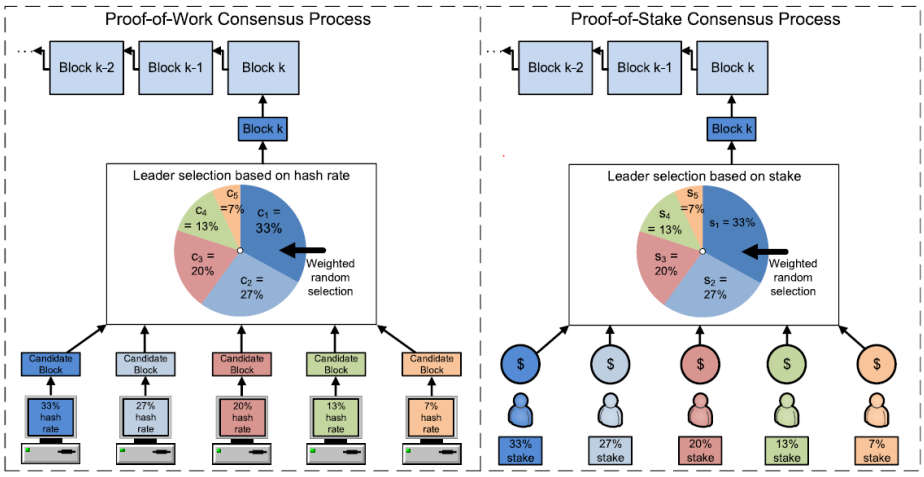


**Fig. 1.** Comparison of PoW vs PoS [60]

**Delegated Proof-of-Stake (DPoS).** Delegated Proof-of-Stake was mentioned in 12 of the research papers included in the study [17], [30], [37], [39], [41], [42], [48], [51], [52], [61], [62], [84]. This consensus algorithm according to the research paper, *Blockchain technology in the energy sector: A systematic review of challenges and opportunities*, is described as a stakeholder voting consensus scheme [40]. The stakeholders, the people that own coins, elect nodes(witnesses) to validate, authenticate and create blocks [40]. The witnesses that receive the greatest number of votes will be given the authorization to create blocks. They will take turns in validating the blocks [26]. If the witnesses do not adhere to their responsibilities the stakeholders have the ability to remove them as a witness and elect a different node. In return for creating these new blocks, the witnesses are awarded the associated fees. Nodes on the network are also able to elect delegates who determine the rules and protocols of the network [40].

**Practical Byzantine Fault Tolerance (pBFT).** Nodes in the blockchain network need to come to a consensus for a block to be added to the chain as discussed previously. There are times where nodes do not come to a consensus as a result of a block acting in a malicious manner or the communication between them is not successful. This causes a delay in the blocks being added to the chain. This is known as a Byzantine fault. A Byzantine Fault Tolerance system is one that allows a certain amount of these "malicious nodes" to be tolerated [40]. As a result, blocks can be added to the chain as per usual, without any delay being caused by these nodes.

The Practical Byzantine Fault Tolerance consensus algorithm is developed from the foundation of the Byzantine Fault Tolerance characteristic. It requires that 2/3 of the nodes of the network are to behave accordingly [40]. 26,76% of the included research papers mentioned this algorithm in its contents [3], [6], [25], [26], [28]–[30], [32], [38], [42]–[51].

Practical Byzantine Fault Tolerance two types of nodes, a primary node and secondary nodes (backup nodes). PBFT has five stages (note: m represents the maximum nodes that can be tolerated in the network) [25]:

1. Request: a block is created by the primary node and distributed on the network.
2. Prepare: a PRE-PARE message will be broadcasted by the primary node and the backup nodes need to verify this message.
3. Prepare: the backup nodes receive the PRE-PARE message and the block and then will broadcast the PREPARE message to the network. In order to move onto the next stage, the backup node must receive 2m + 1 of the same PREPARE message from the other backup nodes.
4. Commit: the nodes broadcast the COMMIT message to all nodes on the network. It also must wait for 2m+1 of the identical COMMIT message from the other blocks.
5. The primary node can then append the block to the network.

### 4.2 S-RQ2 What are the advantages of the main consensus algorithms found?

The advantages discussed in the research papers stemmed from the consensus algorithms that were mentioned in section 4.1. In this section, the advantages of efficiency,

security and scalability will be discussed and how they are achieved by the different blockchain consensus algorithms.

**Efficiency.** There are three different advantageous efficiencies identified namely efficiency as a general term, transaction throughput and energy efficiency. These three advantages that will be discussed and how they are obtained differently in the four consensus algorithms:

*Efficiency.* An advantage of the Proof-of-Stake consensus algorithm is increased efficiency. Four of the included research papers stated that Proof-of-Stake is efficient, but none of them provides a clear explanation on why they stated it was efficient [24], [35], [83], [56]. Efficient or efficiency is not an appropriate characteristic to describe Proof-of-Stake. It should rather be paired with another term to more accurately describe this consensus algorithm, for example, energy-efficient.

*Energy efficiency*. Seven of the research papers included stated that the benefit of Proof-of-Stake is its reduced power consumption or energy efficiency [25], [26], [32], [41], [52]–[54]. The way that this reduced power consumption is achieved, is by replacing the computational effort with a randomly weighted selection [31]. Instead of many nodes on the network competing to validate blocks, a node on the network is randomly chosen to become the validator. This eliminates the nodes needing to brute force the correct nonce thus reducing the computational power required as only one node is doing the work instead of all the nodes on the network.

Of the 71 research papers included in the analysis, 7,04% of them agreed that the implementation of the Practical Byzantine Fault Tolerance results in energy-efficiency benefits [25], [28]–[30], [46]. The key to its energy efficiency is by achieving consensus, and not solving complex mathematical problems like Proof-of-Work. However, the speed and scalability of the algorithm will be affected by the message overhead as the network grows in size [40].

*Transaction throughput.* The advantage of the Hybrid consensus algorithm is its high transaction throughput [55]. It is the combination of the Proof-of-Work and Byzantine Fault Tolerance consensus algorithms. It makes use of the Byzantine Fault Tolerance protocol to come to a consensus [55]. This results in increased energy efficiency as complex mathematical problems don't have to be solved.

**Scalability.** Delegated Proof-of-Stake as being scalable[25], [26]. Due to the voting scheme and the process to achieve consensus in Delegated Proof-of-Stake, this algorithm benefits from both increased efficiency and reduced energy wastage [26]. These 2 benefits will allow the application to be scalable with bigger networks.

Two papers deemed scalability as a benefit as a result of the Proof-of-Stake-consensus algorithm [25], [26]. This algorithm involves randomly selecting a validator to create and add a block to the chain. As there is only one agreement (picking the validator)

before adding the block to the chain, energy demand is decreased and the general efficiency increases. As stated in the text above, these benefits are a good indication that it will be able to handle a larger load as the network size increases and thus making it scalable.

The general consensus of scalability of the Proof-of-Work consensus algorithm in the analysed papers is inconsistent. Three papers identified it being scalable [25]–[27], whilst four papers deemed it not scalable [9], [50], [51], [56]. Based on the numbers above, Proof-of-Work is not scalable. All the reasons listed for good scalability above, have energy efficiency as a benefit. The results indicated 35 energy wastage as a disadvantage of the Proof-of-Work consensus algorithm.

**Security.** Practical Byzantine Fault Tolerance and Proof-of-Work having the advantage of security. Security in the Proof-of-Work algorithm is a result of including the hash pointer in the block [28]. As discussed in section 2, this hash pointer is what links blocks together. Any modification to a block will essentially change its hash and it will not match the one of the hash pointer [33].

Practical Byzantine Fault Tolerance is said to be secure by two of the analyzed papers. It was shown that it would tolerate a certain number of malicious and would ignore these nodes. The security is increased as malicious nodes have no say in the network.

### 4.3 S-RQ3 What are the disadvantages of the main consensus algorithms found?

This section will identify and elaborate on the common disadvantages identified of the main consensus algorithms as identified in section 4.1.

**Common disadvantages of Proof-of-Work.** Proof-of-Work is the consensus algorithm that Bitcoin uses in its blockchain architecture and it's the original consensus algorithm [53]. As a result of it being the original one, there are many disadvantages that included research papers have identified. The most common disadvantages experienced by Proof-of-Work is security issues, the wastage of energy, transaction throughput, and high latency.

The most common disadvantage of the Proof-of-Work consensus algorithm is that it is not energy efficient. As many as 49, (30%) of the included research papers, listed this as one of the disadvantages of the algorithm. The energy wastage occurs as many miners compete with each other to validate blocks. They compete with each other by solving complex mathematical problems by using brute force to determine the correct nonce that would solve these problems[57]. Brute forcing requires a lot of computational effort which leads to energy wastage[58]. This process of brute-forcing the correct nonce doesn't even guarantee that the miner will be the one chosen to validate the block and their effort could all in vain.

Transaction throughput is the number of transactions that can be processed in a certain time period [33]. Low transaction throughout was another recurring disadvantage

of the Proof-of-Work consensus algorithm. 8 of the research papers agreed on this disadvantage [55], [48], [16], [9], [56], [17], [33], [36]. The low throughput is a result of the creation and addition of blocks. As stated in section 1, miners validate and include transactions in a block. Once the block with the transaction is inserted into the chain, transactions have to wait for a number of additional blocks to be added to the chain before the transaction is confirmed [33]. The slow process of adding blocks to the chain delays the transaction confirmation and thus lowering the transaction throughput.

Seven out of the 71 research papers analyzed agreed that high latency was a recurring challenge of the Proof-of-Work consensus algorithm [28], [32], [33], [36], [50], [59], [60]. It is the period between a transaction and the time it takes for the transaction to be processed [32]. Block intervals are what determines the latency of a consensus algorithm[5]. The above text identified that it is a very slow process for blocks to be added to the chain in the Proof-of-Work consensus algorithm. This increases the block interval time and thus increasing the latency in the network.

49 or 30% of the research papers included in the research study, all had security issues as a disadvantage for the Proof-of-Work consensus algorithm[6], [16], [17], [25], [26], [28], [32]–[35], [39], [42], [43], [46], [48], [50], [51], [53], [55], [56], [58], [59], [61]–[72]. Security is one of the challenges as numerous attacks were developed to target and penetrate this consensus algorithm. Some of the attacks that were included in the included research paper are as follows:

- **51% attack** – Consensus algorithms are the core of blockchain technology. These algorithms involving using different mechanisms to come to a consensus that a block is valid and therefore able to be added to the chain. In the Proof-of-Work algorithm, a block can only be added to the chain if the majority of nodes in the network deem it is valid. To verify the validity of the block, miners need large amounts of computational power, also known as hashing power. This hashing power helps determine the performance of the specific miner. The 51% attack is when an organization or an entity is in control of the majority of the hashing power [17], [6]. As they have the majority of the hashing power, they are able to carry out the following actions [59]:
- Control if blocks get validated or not.
- The ability to exclude or modify the ordering of transactions.
- It also gives them the ability to prevent the confirmation of transactions.
- Proof-of-Work makes this attack difficult to carry out as an organization would need an enormous amount of hashing power which would not be feasible [5].
- **Double-spending** – the double-spending attack involves spending the same currency twice [6]. This can be carried out by taking a conflicting transaction from another branch and transferring the funds back to the attacker[6], [69].

Another way for this to happen is for an attacker to build up their chain [73]. This private chain will allow the attacker to remove records of their spending so they can use this currency later. When the two chains are merged, the trust will be destroyed as double-spending has occurred.

**Common disadvantages of Proof-of-Stake.** As described earlier in the research paper, Proof-of-Stake was designed to overcome the shortcomings of the Proof-of-Work consensus algorithm. Although it did achieve greater energy efficiency, some disadvantages followed this optimization. The common disadvantages of Proof-of-Stake is the threat of centralization, and the rich nodes having the ability to take advantage of the network. Both of these disadvantages all relate to the security of the consensus algorithm and it is the most common disadvantage identified in the research papers included in this study. Seven is the number of analyzed research papers that identified security as one of Proof-of-Stake's disadvantage [27], [31]–[36].

As security is the biggest disadvantage, this section aims to provide light on some of the attacks that were identified in the included research papers. This will be done by listing and explaining the most common attacks that would be possible on the Proof-of-Stake consensus algorithm.

There are three different types of long-range attacks: simple, posterior corruption and Stake Bleeding[6]. All three of these long-range attacks aim to do one thing, replace the existing chain with a new chain that begins from the Genesis block (the initial block. In this research article, we will only be discussing the Stake Bleeding attack.

As mentioned above, the Stake Bleeding attack occurs when another chain is created from a genesis block. Each new node is provided with the Genesis block [6]. This new chain becomes replaces the original one. A new node to the network always begins with the Genesis block. They try to build this chain up until it's longer or more valid than the valid chain. They are still a validator in the original chain, but when they get chosen to validate a block (become the slot leader), they skip their turn. This is called a Liveness Denial Attack [6]. Because of the mechanics of Proof-of-Stake, no block is generated in this phase. The attacker's stake does decrease as the process goes on, which makes it less likely that they will get chosen. At the same time, they begin validating and adding blocks to their own chain. The malicious validator also copies the transactions that occur on the main chain and includes them in their own chain. As they are validating transactions, they receive a stake that allows them to compete in the original chain. Once the chain outpaces the original one, they make one more stake to other validators and then publish this other branch.

Another security issue of the Proof-of-Stake is possible centralization. The following papers have identified this as a common security issue of the Proof-of-Stake consensus algorithm: [52], [62], [66], [68]. Nodes are selected to be validators by a weighted random selection process. The more a node stakes, the higher the probability that they will be selected as a validator. This means that the rich will get richer and centralization will start occurring as a small pool of rich nodes will always have a higher chance of becoming validators[52]. The "rich will get richer" is another disadvantage that was recurring in the research papers analyzed in section 4.3. There were a total of 6 papers agreeing upon this disadvantage of the Proof-of-Stake consensus algorithm [17], [27], [52], [55], [59], [62], [73].

## 5 Future work and implications for researchers

This systematic literature review provides a researcher with key characteristics to take into consideration when creating optimized blockchain consensus algorithms. It identified these characteristics to be security, scalability, and efficiency. As a result of the findings of this research paper, the following areas of research are proposed:

- Quantitative research into the scalability, security and efficiency of blockchain solutions on a larger scale.
- Quantitative research on how efficiency can affect the security and scalability of blockchain solutions.
- Quantitative research into the efficiency of blockchain consensus algorithms. A common pattern noticed in the analysed papers was that they relied on comparing the consensus algorithms to Proof-of-Work and logically deducing that it's more energy efficient. This may be the case, but statistical real-world evidence needs to be researched to determine the true energy consumption of a consensus algorithm

## 6 Conclusion

Blockchain will disrupt many industries and the core component of this technology is consensus algorithms. Currently, Proof-of-Work and Proof-of-Stake are two of the most popular algorithms, but they yield many disadvantages [52]. As a result, this systematic literature review identified the characteristics to create optimized blockchain consensus algorithms. These findings indicated that there were many different advantages and disadvantages for the different consensus algorithms. From these findings, key characteristics identified were scalability, security, and efficiency. It was determined that these three key characteristics are key to developing optimized solutions as they will have an effect on the real-world application. Due to the findings of this research paper, further research areas related to these characteristics were proposed.

## 7 References


1. I. Ali, M. Gervais, E. Ahene, and F. Li, “A blockchain-based certificateless public key signature scheme for vehicle-to-infrastructure communication in VANETs,” *J. Syst. Archit.*, vol. 99, p. 101636, Oct. 2019.
2. R. Azzi, R. K. Chamoun, and M. Sokhn, “The power of a blockchain-based supply chain,” *Comput. Ind. Eng.*, vol. 135, pp. 582–592, Sep. 2019.
3. W. Viriyasitavat and D. Hoonsopon, “Blockchain characteristics and consensus in modern business processes,” *J. Ind. Inf. Integr.*, vol. 13, pp. 32–39, Mar. 2019.
4. P. Scully and M. Höbig, “Exploring the impact of blockchain on digitized Supply Chain flows: A literature review,” in *2019 Sixth International Conference on Software Defined Systems (SDS)*, 2019, pp. 278–283.
5. I. G. A. K. Gemeliarana and R. F. Sari, “Evaluation of Proof of Work (POW) Blockchains Security Network on Selfish Mining,” in *2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, 2018, pp. 126–130.

6. E. Deirmentzoglou, G. Papakyriakopoulos, and C. Patsakis, “A Survey on Long-Range Attacks for Proof of Stake Protocols,” *IEEE Access*, vol. 7, pp. 28712–28725, 2019.
7. J. Leo, “The addition of blockchain to the supply chain to reduce the bullwhip effects.” 2019.
8. T. Aste, P. Tasca, and T. D. Matteo, “Blockchain Technologies: The Foreseeable Impact on Society and Industry,” *Computer*, vol. 50, no. 9, pp. 18–28, 2017.
9. S. S. Hazari and Q. H. Mahmoud, “A Parallel Proof of Work to Improve Transaction Speed and Scalability in Blockchain Systems,” in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, 2019, pp. 0916–0921.
10. B. K. Mohanta, D. Jena, S. S. Panda, and S. Sobhanayak, “Blockchain technology: A survey on applications and security privacy Challenges,” *Internet Things*, vol. 8, p. 100107, Dec. 2019.
11. C. Majaski, “Distributed Ledgers,” 2019. .
12. O. Belin, “The Difference Between Blockchain & Distributed Ledger Technology.” .
13. C. G. Schmidt and S. M. Wagner, “Blockchain and supply chain relations: A transaction cost theory perspective,” *J. Purch. Supply Manag.*, vol. 25, no. 4, p. 100552, Oct. 2019.
14. R. Agrawal, “Digital Signature from Blockchain context,” 25-May-2018. .
15. S. D, “How Digital Signature Work And Use In Blockchain,” 2019. .
16. X. Han, Y. Yuan, and F.-Y. Wang, “A Fair Blockchain Based on Proof of Credit,” *IEEE Trans. Comput. Soc. Syst.*, vol. 6, no. 5, pp. 922–931, Oct. 2019.
17. S. Sharkey and H. Tewari, “Alt-PoW: An Alternative Proof-of-Work Mechanism,” in *2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON)*, 2019, pp. 11–18.
18. S. J. Alsunaidi and F. A. Alhaidari, “A Survey of Consensus Algorithms for Blockchain Technology,” in *2019 International Conference on Computer and Information Sciences (ICCIS)*, 2019, pp. 1–6.
19. H. Zhao, “Hash Pointers and Data Structures,” 2018. .
20. H. Agrawal, “Different Types Of Blockchains In The Market and Why We Need Them,” *CoinSutra - Bitcoin Community*, 05-Dec-2017. [Online]. Available: https://coinsutra.com/different-types-blockchains/. [Accessed: 24-Sep-2019].
21. M. Andoni *et al.*, “Blockchain technology in the energy sector: A systematic review of challenges and opportunities,” *Renew. Sustain. Energy Rev.*, vol. 100, pp. 143–174, Feb. 2019.
22. Y. Wang, J. H. Han, and P. Beynon-Davies, “Understanding blockchain technology for future supply chains: a systematic literature review and research agenda,” *Supply Chain Manag. Int. J.*, vol. 24, no. 1, pp. 62–84, Jan. 2019.
23. M. Rimol, “Gartner 2019 Hype Cycle for Blockchain Business Shows Blockchain Will Have a Transformational Impact across Industries in Five to 10 Years,” 12-Sep-2019. .
24. [24] Q. Wen, Y. Gao, Z. Chen, and D. Wu, “A Blockchain-based Data Sharing Scheme in The Supply Chain by IIoT,” in *2019 IEEE International Conference on Industrial Cyber Physical Systems (ICPS)*, 2019, pp. 695–700.
25. S. Zhang and J.-H. Lee, “Analysis of the main consensus protocols of blockchain,” *ICT Express*, p. S240595951930164X, Aug. 2019.
26. F. Yang, W. Zhou, Q. Wu, R. Long, N. N. Xiong, and M. Zhou, “Delegated Proof of Stake With Downgrade: A Secure and Efficient Blockchain Consensus Algorithm With Downgrade Mechanism,” *IEEE Access*, vol. 7, pp. 118541–118555, 2019.
27. L. Chen, L. Xu, Z. Gao, Y. Lu, and W. Shi, “Protecting Early Stage Proof-of-Work Based Public Blockchain,” in *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*, 2018, pp. 122–127.
28. X. Wang *et al.*, “Survey on blockchain for Internet of Things,” *Comput. Commun.*, vol. 136, pp. 10–29, Feb. 2019.

29. Z. Liu, S. Tang, S. S. M. Chow, Z. Liu, and Y. Long, “Fork-free hybrid consensus with flexible Proof-of-Activity,” *Future Gener. Comput. Syst.*, vol. 96, pp. 515–524, Jul. 2019.
30. R. Azzi, R. K. Chamoun, and M. Sokhn, “The power of a blockchain-based supply chain,” *Comput. Ind. Eng.*, vol. 135, pp. 582–592, Sep. 2019.
31. V. Buterin, D. Reijsbergen, S. Leonardos, and G. Piliouras, “Incentives in Ethereum’s Hybrid Casper Protocol,” in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2019, pp. 236–244.
32. H. M. A. Aljassas and S. Sasi, “Performance Evaluation of Proof-of-Work and Collatz Conjecture Consensus Algorithms,” in *2019 2nd International Conference on Computer Applications Information Security (ICCAIS)*, 2019, pp. 1–6.
33. C. T. Nguyen, D. T. Hoang, D. N. Nguyen, D. Niyato, H. T. Nguyen, and E. Dutkiewicz, “Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities,” *IEEE Access*, vol. 7, pp. 85727–85745, 2019.
34. P. Gaži, A. Kiayias, and A. Russell, “Stake-Bleeding Attacks on Proof-of-Stake Blockchains,” in *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, 2018, pp. 85–92.
35. D. Rubel, “No Need to Ask: Creating Permissionless Blockchains of Metadata Records,” *Inf. Technol. Libr.*, vol. 38, no. 2, pp. 1–17, Jun. 2019.
36. P. Novotny *et al.*, “Permissioned blockchain technologies for academic publishing,” *Inf. Serv. Use*, vol. 38, no. 3, pp. 159–171, Jul. 2018.
37. A. Lipton, “Blockchains and distributed ledgers in retrospective and perspective,” *J. Risk Finance*, vol. 19, no. 1, pp. 4–25, Jan. 2018.
38. I. Makhdoom, M. Abolhasan, H. Abbas, and W. Ni, “Blockchain’s adoption in IoT: The challenges, and a way forward,” *J. Netw. Comput. Appl.*, vol. 125, pp. 251–279, Jan. 2019.
39. T. Chomsiri and K. Kongsup, “P Coin: High Speed Cryptocurrency Based on Random-Checkers Proof of Stake,” in *2018 Joint 10th International Conference on Soft Computing and Intelligent Systems (SCIS) and 19th International Symposium on Advanced Intelligent Systems (ISIS)*, 2018, pp. 524–529.
40. M. Andoni *et al.*, “Blockchain technology in the energy sector: A systematic review of challenges and opportunities,” *Renew. Sustain. Energy Rev.*, vol. 100, pp. 143–174, Feb. 2019.
41. J. Kang, Z. Xiong, D. Niyato, P. Wang, D. Ye, and D. I. Kim, “Incentivizing Consensus Propagation in Proof-of-Stake Based Consortium Blockchain Networks,” *IEEE Wirel. Commun. Lett.*, vol. 8, no. 1, pp. 157–160, Feb. 2019.
42. N. O. Nawari and S. Ravindran, “Blockchain and the built environment: Potentials and limitations,” *J. Build. Eng.*, vol. 25, p. 100832, Sep. 2019.
43. Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, “A survey on privacy protection in blockchain system,” *J. Netw. Comput. Appl.*, vol. 126, pp. 45–58, Jan. 2019.
44. X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, “A survey on the security of blockchain systems,” *Future Gener. Comput. Syst.*, p. S0167739X17318332, Aug. 2017.
45. H. Zheng, Q. Wu, J. Xie, Z. Guan, B. Qin, and Z. Gu, “An organization-friendly blockchain system,” *Comput. Secur.*, p. 101598, Aug. 2019.
46. A. Bugday, A. Ozsoy, S. M. Öztaner, and H. Sever, “Creating consensus group using online learning based reputation in blockchain networks,” *Pervasive Mob. Comput.*, vol. 59, p. 101056, Oct. 2019.
47. V. Gramoli, “From blockchain consensus back to Byzantine consensus,” *Future Gener. Comput. Syst.*, p. S0167739X17320095, Sep. 2017.
48. H. Tang, Y. Shi, and P. Dong, “Public blockchain evaluation using entropy and TOPSIS,” *Expert Syst. Appl.*, vol. 117, pp. 204–210, Mar. 2019.

49. G. He, W. Su, S. Gao, and J. Yue, “TD-Root: A trustworthy decentralized DNS root management architecture based on permissioned blockchain,” *Future Gener. Comput. Syst.*, vol. 102, pp. 912–924, Jan. 2020.
50. D. Tosh, S. Shetty, P. Foytik, C. Kamhoua, and L. Njilla, “CloudPoS: A Proof-of-Stake Consensus Design for Blockchain Integrated Cloud,” in *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, 2018, pp. 302–309.
51. J. Chen and S. Micali, “Algorand: A secure and efficient distributed ledger,” *Theor. Comput. Sci.*, vol. 777, pp. 155–183, Jul. 2019.
52. B. Lucas and R. V. Páez, “Consensus Algorithm for a Private Blockchain,” in *2019 IEEE 9th International Conference on Electronics Information and Emergency Communication (ICEIEC)*, 2019, pp. 264–271.
53. T. Xue, Y. Yuan, Z. Ahmed, K. Moniz, G. Cao, and C. Wang, “Proof of Contribution: A Modification of Proof of Work to Increase Mining Efficiency,” in *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*, 2018, vol. 01, pp. 636–644.
54. Q. Lyu, Y. Qi, X. Zhang, H. Liu, Q. Wang, and N. Zheng, “SBAC: A secure blockchain-based access control framework for information-centric networking,” *J. Netw. Comput. Appl.*, vol. 149, p. 102444, Jan. 2020.
55. B. Yu, J. Liu, S. Nepal, J. Yu, and P. Rimba, “Proof-of-QoS: QoS based blockchain consensus protocol,” *Comput. Secur.*, vol. 87, p. 101580, Nov. 2019.
56. S. R. Niya *et al.*, “Adaptation of Proof-of-Stake-based Blockchains for IoT Data Streams,” in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2019, pp. 15–16.
57. S. N. Mohanty *et al.*, “An efficient Lightweight integrated Blockchain (ELIB) model for IoT security and privacy,” *Future Gener. Comput. Syst.*, vol. 102, pp. 1027–1037, Jan. 2020.
58. G. Kumar, R. Saha, M. K. Rai, R. Thomas, and T.-H. Kim, “Proof-of-Work Consensus Approach in Blockchain Technology for Cloud and Fog Computing Using Maximization-Factorization Statistics,” *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6835–6842, Aug. 2019.
59. D. K. Tosh, S. Shetty, X. Liang, C. Kamhoua, and L. Njilla, “Consensus protocols for blockchain-based data provenance: Challenges and opportunities,” in *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)*, 2017, pp. 469–474.
60. I. Tarkhanov, D. Fomin-Nilov, and M. Fomin, “Application of public blockchain to control the immutability of data in online scientific periodicals,” *Libr. Hi Tech*, vol. 37, no. 4, pp. 829–844, Nov. 2019.
61. J. Sengupta, S. Ruj, and S. Das Bit, “A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT,” *J. Netw. Comput. Appl.*, vol. 149, p. 102481, Jan. 2020.
62. B. Shala, U. Trick, A. Lehmann, B. Ghita, and S. Shiaeles, “Novel trust consensus protocol and blockchain-based trust evaluation system for M2M application services,” *Internet Things*, vol. 7, p. 100058, Sep. 2019.
63. [63] S. Moin, A. Karim, Z. Safdar, K. Safdar, E. Ahmed, and M. Imran, “Securing IoTs in distributed blockchain: Analysis, requirements and open issues,” *Future Gener. Comput. Syst.*, vol. 100, pp. 325–343, Nov. 2019.
64. Z. Guan, X. Lu, N. Wang, J. Wu, X. Du, and M. Guizani, “Towards secure and efficient energy trading in IIoT-enabled energy internet: A blockchain approach,” *Future Gener. Comput. Syst.*, p. S0167739X19315018, Oct. 2019.
65. D. Puthal, S. P. Mohanty, P. Nanda, E. Kougianos, and G. Das, “Proof-of-Authentication for Scalable Blockchain in Resource-Constrained Distributed Systems,” in *2019 IEEE International Conference on Consumer Electronics (ICCE)*, 2019, pp. 1–5.

66. M. Borge, E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, and B. Ford, “Proof-of-Personhood: Redemocratizing Permissionless Cryptocurrencies,” in *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, 2017, pp. 23–26.
67. R. NAKAHARA and H. INABA, “Proposal of Fair Proof-of-Work System Based on Rating of User’s Computing Power,” in *2018 IEEE 7th Global Conference on Consumer Electronics (GCCE)*, 2018, pp. 746–748.
68. T. Ogawa, H. Kima, and N. Miyaho, “Proposal of Proof-of-Lucky-Id(PoL) to Solve the Problems of PoW and PoS,” in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2018, pp. 1212–1218.
69. R. Zhang and B. Preneel, “Lay Down the Common Metrics: Evaluating Proof-of-Work Consensus Protocols’ Security,” in *2019 IEEE Symposium on Security and Privacy (SP)*, 2019, pp. 175–192.
70. M. Ramkumar, “Executing large-scale processes in a blockchain,” *J. Cap. Mark. Stud.*, vol. 2, no. 2, pp. 106–120, Nov. 2018.
71. A. Baldominos and Y. Saez, “Coin.AI: A Proof-of-Useful-Work Scheme for Blockchain-Based Distributed Deep Learning,” *Entropy*, vol. 21, no. 8, pp. 723–723, Aug. 2019.
72. S. Park and H. Kim, “DAG-Based Distributed Ledger for Low-Latency Smart Grid Network,” *Energ. 19961073*, vol. 12, no. 18, p. 3570, Sep. 2019.
73. C.-N. Chou, Y.-J. Lin, R. Chen, H.-Y. Chang, I.-P. Tu, and S.-W. Liao, “Personalized Difficulty Adjustment for Countering the Double-Spending Attack in Proof-of-Work Consensus Protocols,” in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2018, pp. 1456–1462.
74. A. Ahl *et al.*, “Exploring blockchain for the energy transition: Opportunities and challenges based on a case study in Japan,” *Renew. Sustain. Energy Rev.*, vol. 117, p. 109488, Jan. 2020.
75. E. K. Wang, Z. Liang, C.-M. Chen, S. Kumari, and M. K. Khan, “PoRX: A reputation incentive scheme for blockchain consensus of IIoT,” *Future Gener. Comput. Syst.*, vol. 102, pp. 140–151, Jan. 2020.
76. T. Kerber, A. Kiayias, M. Kohlweiss, and V. Zikas, “Ouroboros Crypsinous: Privacy-Preserving Proof-of-Stake,” in *2019 IEEE Symposium on Security and Privacy (SP)*, 2019, pp. 157–174.
77. M. Król, A. Sonnino, M. Al-Bassam, A. Tasiopoulos, and I. Psaras, “Proof-of-Prestige: A Useful Work Reward System for Unverifiable Tasks,” in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2019, pp. 293–301.
78. D. Dhagarra, M. Goswami, P. R. S. Sarma, and A. Choudhury, “Big Data and blockchain supported conceptual model for enhanced healthcare coverage: The Indian context,” *Bus. Process Manag. J.*, p. BPMJ-06-2018-0164, Mar. 2019.
79. A. Lipton, “Blockchains and distributed ledgers in retrospective and perspective,” *J. Risk Finance*, vol. 19, no. 1, pp. 4–25, Jan. 2018.
80. S. E. Chang, Y.-C. Chen, and T.-C. Wu, “Exploring blockchain technology in international trade,” *Ind. Manag. Data Syst.*, vol. 119, no. 8, pp. 1712–1733, Jan. 2019.
81. Y. Kano and T. Nakajima, “A novel approach to solve a mining work centralization problem in blockchain technologies,” *Int. J. Pervasive Comput. Commun.*, vol. 14, no. 1, pp. 15–32, Apr. 2018.

82. I. Tarkhanov, D. Fomin-Nilov, and M. Fomin, “Application of public blockchain to control the immutability of data in online scientific periodicals,” *Libr. Hi Tech*, vol. 37, no. 4, pp. 829–844, Nov. 2019.
83. M. Ramkumar, “Executing large-scale processes in a blockchain,” *J. Cap. Mark. Stud.*, vol. 2, no. 2, pp. 106–120, Nov. 2018.
84. J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim, and J. Zhao, “Toward Secure Blockchain-Enabled Internet of Vehicles: Optimizing Consensus Management Using Reputation and Contract Theory,” *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2906–2920, Mar. 2019.
85. X. Sun, M. Sopek, Q. Wang, and P. Kulicki, “Towards Quantum-Secured Permissioned Blockchain: Signature, Consensus, and Logic,” *Entropy*, vol. 21, no. 9, pp. 887–887, Sep. 2019.
86. T. Ogawa, H. Kima, and N. Miyaho, “Proposal of Proof-of-Lucky-Id(PoL) to Solve the Problems of PoW and PoS,” in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2018, pp. 1212–1218.