A Systematic Literature Review of Blockchain Consensus Protocols

Sikho Luzipo[1] and Aurona Gerber[1,2](✉)

[1] University of Pretoria, Pretoria, South Africa
aurona.gerber@up.ac.za
[2] The Center for AI Research (CAIR), Pretoria, South Africa

Abstract. Blockchain is the underlying technology behind Bitcoin, the first digital currency, and due to the rapid growth of Bitcoin, there is significant interest in blockchain as the enabler of digital currencies due to the consensus distributed ledger model. The rise and the success of alternative cryptocurrencies such as Ethereum and Ripple has supported the development of blockchain technology, but the performance of blockchain applications has been documented as a significant obstacle for adoption. At the core of blockchain is a consensus protocol, which plays a key role in maintaining the safety, performance and efficiency of the blockchain network. Several consensus protocols exist, and the use of the right consensus protocol is crucial to ensure adequate performance of any blockchain application. However, there is a lack of documented overview studies even though there is agreement in the literature about the importance and understanding of blockchain consensus protocols. In this study, we adopt a systematic literature review (SLR) to investigate the current status of consensus protocols used for blockchain together with the identified limitations of these protocols. The results of this study include an overview of different consensus protocols as well as consensus protocol limitations and will be of value for any practitioner or scholar that is interested in blockchain applications.

Keywords: Blockchain technology · Consensus protocols · Challenges

1 Introduction

Since its emergence as the core underlying technology for Bitcoin in 2008 [31], blockchain technology has evolved from its use as a verification mechanism for cryptocurrencies to a broader field of applications. Blockchain's primary objective is to provide a transactional, distributed ledger functionality with the aim of eliminating the need for trusted intermediary third-parties [3]. This implies that with blockchain, applications that operate through the use of trusted intermediaries can now operate in a decentralized way without relying on intermediaries and achieve the same level of functionality and benefits [9].

Despite the well documented benefits of blockchain technology, its adoption is still very limited due to performance challenges. Many scholars associate these challenges

Published by Springer Nature Switzerland AG 2021
D. Dennehy et al. (Eds.): I3E 2021, LNCS 12896, pp. 580–595, 2021.
https://doi.org/10.1007/978-3-030-85447-8_48

to one of blockchain's key components namely the consensus protocol algorithm [6], the mechanism that allows blockchain to decentralize trust [23]. A consensus protocol ensures that all participants on the blockchain system reach an agreement with regards to the validity of transactions in the ledger [21]. In a blockchain network, consensus protocols fulfil the role that a single authority has in a centralized database or ledger.

According to Wu and Gao [41], consensus protocols have delayed the development and widespread adoption of blockchain technology. The reliability and efficiency of these consensus protocols remain a challenge [20]. Gramoli [18] emphasized that the issues experienced with existing blockchain consensus protocols maybe as a result of fundamental design flaws. The many different positions on consensus protocols motivated the need for this study, namely, to use literature to identify the different consensus protocols and protocol limitations.

Due to the increasing importance and popularity of blockchain technology together with consensus protocols, there is a need to understand the current consensus protocols used in blockchain technology applications and the limitations that are associated with them. To address this need, a systematic literature review (SLR) was conducted [24]. Section 2 provides background for this study, Sect. 3 describes the research method, Sect. 4 documents the findings and Sect. 5 concludes.

2 Background

According to Aste et al. [4], blockchain is better understood when viewed with two lenses. The first lens views blockchain as information and communications technology (ICT) that is aimed at recording ownership of assets and contractual agreements. This is because of the inherent characteristics of blockchain technology such as untemperability, immutability, transparency and traceability of information stored on the ledger [11]. The second lens views blockchain as an institutional technology aimed at decentralising structures that are aimed at governing economic decisions and people. Blockchain can be defined as a distributed data structure that is used to hold information shared among various members of the network [43].

Literature identified two challenges that are preventing widespread adoption of blockchain [39, 42, 45]. The first challenge, which has been the focus of many studies, is the scalability in terms of the efficiency and resilience of the consensus protocol. The second challenge affecting the adoption of blockchain technology is how to ensure the degree of transaction privacy that is a standard requirement in most real-world applications today. Both these challenges are linked to the consensus protocol which are the core of blockchain technology.

2.1 Blockchain Consensus Protocols

In a distributed ledger system, consensus represents a state that there is agreement among all the participants regarding the same data values [42]. Consensus is a procedure that allows participants in decentralized or distributed multi-agent platforms to arrive at a common agreement [35]. According to Zhao et al. [47], consensus has been a problem in distributed computing since the early 1980s.

To reach consensus in the network, each node needs to exchange information with other nodes. There may be some instances whereby some nodes will be down or offline and there will also be some malicious nodes with the intention of disrupting the consensus process [18]. These malicious nodes that behave arbitrarily are often referred to as Byzantine failures [38]. A consensus protocol that is Byzantine tolerant aims to guarantee the correctness of the network (blockchain system) by ensuring the order of the newly created blocks of transactions [18]. The design and the implementation of the consensus protocol needs to address how to deal with these problems [38].

In blockchain, new blocks are added by following a protocol that establishes consensus among the members of the network to confirm the validity of the new block [10]. A consensus protocol is defined as a set rules that guide the way users utilize their computing power to arrive at consensus to create new blocks [25]. It allows self-interested peers to reach agreements and make consistent decisions when faced with contradictory alternatives [28]. The stability of a blockchain system is directly determined by the effectiveness of the consensus protocol [45]. Ferdous et al. [14] described consensus protocol as the most crucial component in the design of a blockchain system as it determines its security and performance. As a result, a number of consensus protocols have been proposed. These range from new designs to modifications to some of the well-known consensus mechanisms in the distributed systems literature. Proof of Work (PoW) and Proof of Stake (PoS) are the two most widely used consensus protocols for blockchain [25]. According to Herlihy [19], the design of a consensus protocols should satisfy the following properties, *agreement* (all honest parties should agree on the block that was selected, no two correct processes should propose different blocks), *validity* (the selected block is valid), *termination* (all honest parties eventually decide on a block) and *integrity* (no parties should decide twice).

Even though there are many consensus protocols that have been proposed, Wu and Gao [41] argue that these have many shortcomings which are preventing blockchain from meeting the expected performance requirements of various applications. Leornados et al. [28] argued that the choice of a consensus protocol has a very critical role in the success of blockchain as it has an impact on the security and performance of a blockchain system.

3 SLR Research Method

In this study, a systematic literature review (SLR) was conducted to review the current consensus protocols used in blockchain technology. The SLR was based on Kitchenham's guidelines and includes three phases namely (1) planning, (2) conducting and (3) documenting the review. Each phase is described in the sections that follow and the process is depicted in Fig. 1.

3.1 Systematic Literature Review Planning

During the planning phase the rationale for the review and the research questions that will guide the review and review protocol are identified as described below.

The Purpose of a Systematic Literature Review: Altarawneh et al. [2] identified four categories of the reasons for conducting literature reviews which are describe, test, extend and critique previously published studies. This SLR aimed to identify the current consensus protocols and limitations of blockchain technology that have been mentioned in the literature, and the SLR is therefore descriptive.

Review Protocol: The review protocol is the written plan that is completed prior to the start of the SLR [24], which specifies conditions for the selection of primary studies as well as any boundaries that may apply [8]. The main components of a review protocol include the research questions that will guide the review, search strategy, the resources (databases) to be used, selection of the studies and quality assessment procedures. Table 1 presents the research questions that were proposed to guide this review.

Table 1. Research questions for the SLR

ID	Research question	Motivation
RQ1	What are the current consensus protocols that have been mentioned in the literature for different blockchain systems and how are they classified?	The purpose of this question is to provide information about the current consensus protocols that have been mentioned in the literature
RQ2	What are the limitations of the current consensus protocols?	The purpose of this question is to provide information about the limitations of blockchain consensus protocols that have been mentioned in the literature

The identified research questions are followed by the formulation of the search strategy to be used to find studies that will assist with answering the research questions. The search process involves the selection of digital libraries, defining the search terms, executing pilot search, refining the search term and the retrieval of initial list of primary studies from the literature databases (Table 5) based on the search string. To ensure comprehensive coverage of all the blockchain technology literature related to consensus protocols, the following search string was used: "Blockchain Consensus Protocols"

Table 2. Inclusion and exclusion criteria

Papers included	Papers excluded
• English peer reviewed studies published in conferences, workshops, symposiums and journals related to the research topic • Study contains discussion /analysis about a specific consensus protocol for blockchain technology (RQ1) • Study contains discussion/ analysis about the limitations or challenges of blockchain consensus protocols (RQ2)	• Papers which are not related to the research questions • Opinion pieces, viewpoints or purely anecdotal and short papers (poster) • Non-peer reviewed articles • Articles that only review blockchain technology

OR "Blockchain Protocols" OR "Blockchain Consensus Protocols" OR "Blockchain Protocols" OR "Blockchain Consensus Mechanism".

The source selection criteria are determined next, and Table 2 provides inclusion/exclusion criteria used to select relevant studies.

The quality assessment procedure is compiled to ensure the quality of the sources that will be included in the SLR, and the checklist for the current study is outlined Table 3.

Table 3. Quality assessment checklist (Adapted from [13])

• Are objectives of the study clearly defined?
• Are different types of blockchain consensus protocols clearly defined?
• Are the benefits/importance of consensus protocols clearly defined?
• Are the challenges of blockchain consensus protocols clearly defined?
• Does the study make a contribution to academia or the industry?
• Are the findings of the study clearly defined and supported by reporting results?

Data Extraction and Data Synthesis Strategy: The data extraction and data analysis

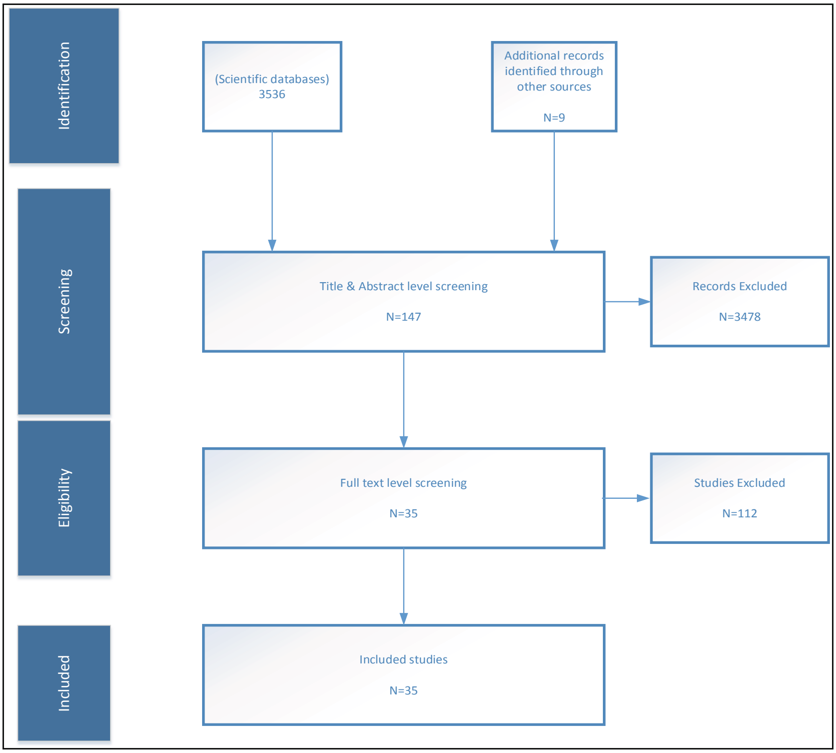

Fig. 1. SLR process

strategy are described in the next section. The strategy included that reference details of each of the relevant studies were recorded in Zotero (www.zotero.org), and notes and themes were identified. Narrative analysis and synthesis was adopted in order to identify the data related to the research questions.

3.2 Conducting the Review

During this phase the actual review is executed. The data extraction procedure involved four selection phases. The initial search resulted in a total of 3536 papers from the scientific databases as shown in Table 4. This was followed by selection by title and abstract reading. Due to the high number of the studies, only the first 200 relevant studies were reviewed from each of the databases as these were the most significant cited papers. In the end, there were 147 studies that met the inclusion criteria, and these were selected for full analysis and synthesis. These studies were then evaluated against the quality assessment checklist outlined in Table 3. A total of 35 papers remained at the end of this phase. The process is depicted in Fig. 1.

Table 4. Number of studies identified from the search databases

Database	Results	Search strategy	Search Date
ACM Digital library	166	Abstract and keywords	27-11-2020
IEEE Explore	2451	Abstract and keywords	28-11-2020
ScienceDirect	252	Abstract, title and keywords	11-12-2020
Springer Link	602	Abstract, title and keywords	11-12-2020
Ebsco	65	Abstract, title and keywords	11-12-2020
Total	**3536**		

3.3 Reporting the Review

During this phase the results of the review are documented. For the purpose of this paper the results and findings of this SLR are presented in the next section.

4 Findings: Blockchain Consensus Protocols

Thirty-five studies published between 2016 and 2021 were selected, and each study addressed one or both research questions. Among these, 20 papers were published in journals, 14 appeared in conference proceedings and one paper was extracted from a symposium. The number of papers by year publication is shown in Fig. 2.

4.1 Consensus Protocols Used in Blockchain Technology (RQ1)

Figure 2 provides a graphical representation of the current blockchain consensus protocols that have been identified in the SLR with a description presented in Table 5. In addition to all the protocols, three categories of consensus protocols were identified namely proof-based, voting-based and committee-based (hybrid) consensus protocols, which are briefly summarized in the remainder of this section.

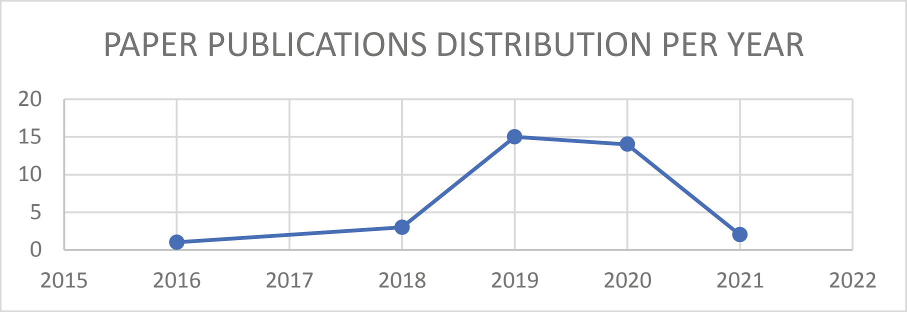

Fig. 2. Number of papers by year of publication

Table 5. Blockchain consensus protocols

Blockchain consensus classification	Reference
Permissioned consensus protocols; Permissionless consensus protocols	[29]
Public based consensus protocols; Alliance based consensus protocols	[47]
Leader based consensus protocols; Voting-based consensus protocols Committee + Voting based protocols; Fair accountant based protocols	[16]
Proof based; Capability based; Voting based; Compute Intensive-based	[7]
Proof based; Voting based	[22]
Quorum; Deterministic	[30]
Probabilistic finality; Absolute finality	[17, 46]
Leader-based; Voting based	[1]
Committee based; Sharding-based	[44]
Proof based; Voting based	[27, 34]
Incentivized consensus protocols; Non-incentivized consensus protocols	Bouraga (2021)
Classical consensus protocols; Elected leader consensus protocols Hybrid single committee consensus protocols; Hybrid multiple committee consensus protocols	Bano et al. (2019)

Proof-based consensus protocols are based on the idea that the node with sufficient proof will get the right to add the new block [27]. According to Wang et al. [40], each participant in proof-based consensus protocols has an attribute that is called the proof method. One of the main advantages of proof-based methods is that they guarantee consistency of under normal circumstances [27]. The most popular proof-based consensus protocol is proof of work (PoW) proposed by Nakamoto [31]. These protocols are mostly suited for public blockchains. Proof-based consensus protocols are also referred as 'leader-based consensus' [16] or 'competitive leader-based' [1]. Table 7 provides a list of some of the consensus protocols that fall in this category (Fig. 3).

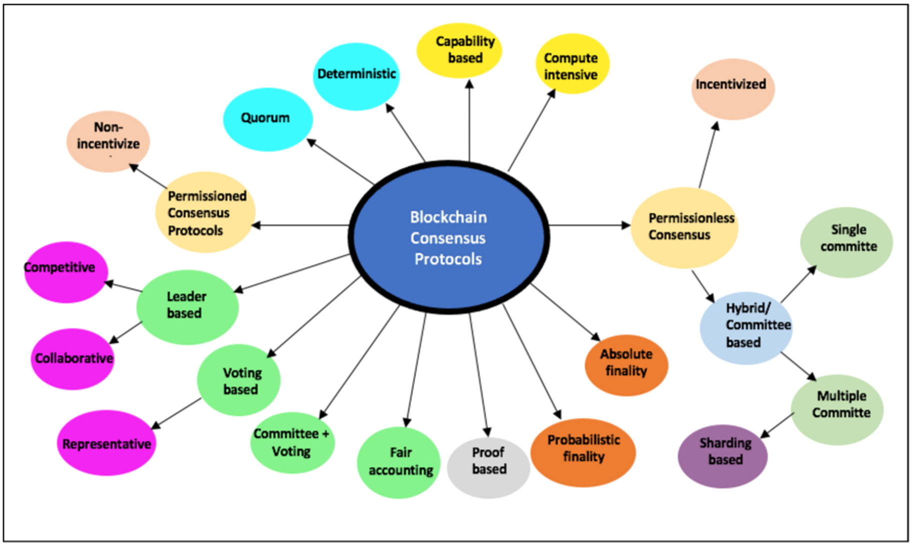

Fig. 3. Blockchain consensus protocols

Voting-based consensus protocols use a voting system to elect a node that is allowed to create a new block. In voting consensus protocols, nodes vote for the blocks they think are valid instead of competing [1]. For a node to append a block, a certain number of nodes must agree. If there are non-responsive nodes, the number of responsive nodes should exceed the non-responsive nodes for the voting consensus protocols to work. These types are mostly suited for use in private or consortium blockchains [34]. There are three stages [16] that must be followed for a block to be added in voting consensus protocols. In the first phase pre-prepare, the primary node that must send the block to other nodes (called replicas) verification. In the second phase, prepare, each replica sends back the verification results to all the other nodes. All replicas must confirm the new block. During the third phase, commit, each replica sends the verification result of the prepare stage to all other nodes again, and each node makes a final confirmation of the block according to the message received. Ismail and Materwala [21] classified voting consensus protocols into Bayzantine Fault Tolerant (BFT) based and Crash Fault Tolerant (CFT) based. A BFT based consensus ensures that the blockchain network will continue to operate even in the presence of malicious or failure nodes whereas a CFT based consensus prevents the system from failing when the node goes offline or crashes.

PBFT is one of the most popular BFT based consensus protocols used in blockchain. Altarawneh et al. [1] identified two broad categories of voting consensus protocols namely *representative* voting and *gossip* voting (not currently used in blockchain). In representative voting consensus protocols, a group of nodes are elected as representatives with the task of proposing new blocks. Some of the consensus protocols that fall in this category are listed in Table 7.

Committee-based (hybrid) consensus protocols have been proposed to address the imitations of single node consensus protocols where a committee rather than a single node is responsible for driving consensus. There are two types of committee-based consensus protocols namely single and multi-committee consensus protocols [29]. In single committee, the committee is responsible for managing transactions, while multiple committees act in parallel in order to improve the scalability of the blockchain network in multi-committee consensus protocols. The consensus process in single committees involves the following steps: committee formation, committee configuration and the actual consensus mechanism [6]. The consensus process for multi-committees comprises of committee topology, intra-committee configuration and the intra-committee consensus.

Table 6. Proof-based consensus protocols

Consensus protocols	How sufficient proof is achieved
Proof of Work (PoW)	Nodes are required to solve a puzzle with adjusted level of difficulty. The first node to solve the puzzle will get the right to append the new node in the current chain
Proof of stake	The node to append the next block on the blockchain is decided based on the size of the stake
Proof of elapsed time	In this type of consensus protocol, each node on the blockchain requests a wait-time. After all the nodes have received their wait-times, a timeout is set with scheduling and the node with the shortest wait-time wins the right to mine the new block
Proof of luck	In proof of luck, all the nodes are required to make their own blocks with different lucky numbers and add these to their chains. The chain with the most lucky numbers is chosen as the main one
Proof of space	In this consensus protocol, nodes are required to invest commit relevant disk space. A number of datasets called plots will be generated by proof of space protocol. The miner storing the most number of plots can mine a new block

Table 7. Voting-based consensus protocols

Consensus protocol	How consensus is achieved
Delegated Proof of Stake (DPoS)	DPoS works like a democracy, nodes in the network can register as voters in order to become shareholders and then have the right to vote for the block producers they want
Practical Byzantine Fault Tolerance (PBFT)	There is no leader required in PBFT. Instead, one node is considered as the primary and the others are regarded as replicas
Hotstuff	Hotstuff is considered as a leader variant of PBFT. Nodes communicate with each other via a leader resulting in a star communication network as compared to mesh communication network in PBFT
LibraBFT	LibraBFT is also a variant of PBFT consensus protocol. It makes improvements on Hotstuff with the introduction of a detailed specification and implementation of the Peacemaker mechanism
Delegated Byzantine Fault Tolerance (DBFT)	Consensus is achieved by selecting a group of nodes (representatives) through a vote. The selected nodes then use BFT consensus mechanism to reach a consensus and generate a new block
Federated Byzantine Agreement (FBA)	In FBA, any node can participate in the consensus process. All the participating nodes communicate with a group of nodes referred to as Unique Node List (UNL). A new transaction is added if 80% of the participating nodes agree
Raft CFT	In this consensus protocol, each node in the network is either a follower, candidate or leader. A leader is responsible for packaging all the new transactions received from the client and sends them to followers. Each block is replicated by the followers and acknowledgement sent to the leader. Once the leader receives confirmation from followers, it executes the transactions in the block and notifies the client

(*continued*)

Table 7. (*continued*)

Consensus protocol	How consensus is achieved
Federated CFT	In this type of consensus protocol, a leader and backup nodes are selected from a group of other nodes. The leader is responsible for validating and creating new blocks and the backup nodes are responsible for verifying the new blocks
Combined Delegated Proof of Stake and Byzantine Fault Tolerance (DPoS + BFT)	This consensus protocol uses DPoS to select the nodes to participate in the consensus process and then BFT to add the new transaction on the network

4.2 Challenges with the Current Blockchain Consensus Protocols (RQ2)

The most common challenges of blockchain consensus protocols that have been mentioned in the literature can be categorised under proof-based and voting-based and challenges that can happen on any of the two types (common attacks) as shown in Fig. 4. Table 8 list proof-based and voting-based protocol challenges, while Table 9 summarise the common attack challenges.

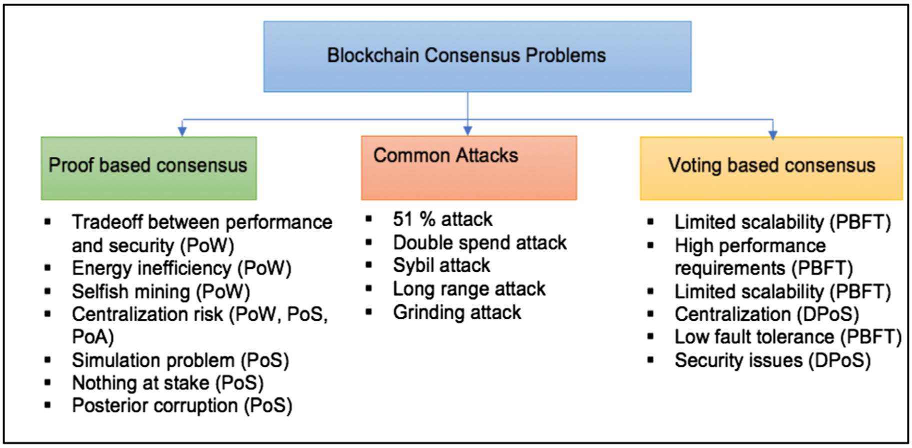
Blockchain Consensus Problems
Proof based consensus
Common Attacks
Voting based consensus
▪ Tradeoff between performance and security (PoW)
▪ Energy inefficiency (PoW)
▪ Selfish mining (PoW)
▪ Centralization risk (PoW, PoS, PoA)
▪ Simulation problem (PoS)
▪ Nothing at stake (PoS)
▪ Posterior corruption (PoS)
▪ 51 % attack
▪ Double spend attack
▪ Sybil attack
▪ Long range attack
▪ Grinding attack
▪ Limited scalability (PBFT)
▪ High performance requirements (PBFT)
▪ Limited scalability (PBFT)
▪ Centralization (DPoS)
▪ Low fault tolerance (PBFT)
▪ Security issues (DPoS)

Fig. 4. Blockchain consensus protocol challenges

Challenges associated with proof-based consensus protocols: One of the most popular proof-based consensus protocols is proof of work (PoW). The main criticism of PoW is that it consumes a lot of power [34] without generating anything useful [1]. These challenges have led to a number. of new consensus protocols with the aim of addressing these limitations, however, these new consensus protocols introduced their own challenges. For example, even though proof of stake (PoS) eliminated energy inefficiencies, it did it at the expense of decentralisation [5]. PoS has been criticized for its security

Table 8. Challenges associated with consensus protocols

Consensus protocols	Challenge	Reference
Proof-based consensus protocols	Tight trade-off between performance and security	[42]
	Energy inefficiency	[5, 42, 46]
	Vulnerability to selfish mining	[33, 42]
	Mining pools and centralization risk	[42]
	Costless simulation problem	[42]
	Nothing-at-stake problem	[29, 42]
	Vulnerability to the posterior corruption	[42]
	Vulnerability to the long-range attack	[29, 42]
	Vulnerability to the stake-grinding attack	[29, 42]
	Centralization risk	[5, 15, 42]
Voting-based consensus protocols	Limited scalability	[37, 40]
	High performance requirements	[46]
	Centralisation	[37]
	Low fault tolerance	[5]
	Security issues	[37, 40]

measures [32], nothing at stake problem [29] which leads to double spending [42]. Proof of burn (PoB) has been suggested as an alternative to PoW, however Sharma & Jain [36] argued that PoB wastes resources with no plan of recovering the money. Proof of Weight (PoWeight) is another alternative consensus protocol that has been proposed to address the weaknesses of PoS but has been criticized for not incentivizing nodes [36]. In proof-based consensus protocols, there is also a possibility of miners to mine in secrecy in order to create forks when they want to do so [33].

Challenges Associated with Voting-Based Consensus Protocols: One of the main issues with voting-based consensus protocols such as PBFT is scalability. The frequent network node communication generates high traffic overhead [26]. They are not suitable for networks with large number of nodes [40]. Another issue that has been raised with voting based consensus protocols is centralization due to reduction of the number of verification nodes [40]. PBFT assume a defined closed group therefore not suitable for open networks where anyone can join [22]. PBFT has also been criticized for its inability to identify and remove faulty nodes [27]. The security of DPoS has been criticized by [40], they argued that it has a weak defense against malicious nodes. Since the committee members control the creation of new blocks in DPoS, if these members become malicious other nodes will be unable to do anything [47].

Table 9. Common blockchain consensus protocol attacks

Attack type	Description
51% attack	This type of attack usually occurs when a node or group of nodes tries to take control of more than fifty percent of the blockchain network's proof method such as stake in case of PoS or computing power in case of PoW. Once an attacker takes over the control of the blockchain, they can engage in malicious activities such as double spending
Double spend attack	This type of an attack happens when a person tries to spend a specific amount that has already been spent on the blockchain [46]. This type of attack can be a result of an error or in the system or deliberate fraud
Sybil attack	In this form an attack, an adversary uses numerous forged identities in order to confuse the blockchain network [12]. Sybil attack is mostly common in public blockchains as the identities of the nodes is unknown
Long range attack	This attack happens when the adversary tries to produce new blocks before the current block. This attack becomes successful when the branch created by adversary gets longer than longer and overtakes the main chain
Grinding attack	In grinding attack, an adversary performs some computation in order to try manipulate the randomness in their favour [42]. The attacker tries to increase their chances of generating future blocks based on the information of the current block [30]

5 Conclusion

This study adopted a SLR to provide an overview of current consensus protocols used in blockchain technology and the challenges that have been mentioned in the literature for consensus protocols. The SLR was executed using five digital libraries and selecting 35 peer-reviewed articles published in either journals or conferences between 2016 and 2021 that adhere to the quality protocols. The findings of the SLR indicate there is no single common standard or framework for developing consensus protocols for blockchain technology, bit that a number of protocols exist that can be categorized as either proof-based, voting-based or committee-based/hybrid consensus protocols. Limitations are associated with either strategy namely proof-based or voting-based, as well as common attacks that impact both categories. Even though there is agreement in the literature about the importance of consensus protocols in blockchain, there is lack of documentation on how to design and develop effective consensus protocols to address the needs of specific blockchain technology applications. Even though new and improved consensus protocols are proposed to address limitations, they introduce their own set of limitations and challenges. The findings from this study could assist with an increased awareness of blockchain consensus protocols as well as their limitations.

References

1. Altarawneh, A., et al.: Buterin's scalability trilemma viewed through a state-change-based classification for common consensus algorithms. In: 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), pp. 0727–0736 (2020). https://doi.org/10.1109/CCWC47524.2020.9031204
2. Altarawneh, G., et al.: Synthesizing information systems knowledge: a typology of literature reviews. Inf. Manage. **52**(2), 183–199 (2015)
3. Andoni, M., et al.: Blockchain technology in the energy sector: a systematic review of challenges and opportunities. Renew. Sustain. Energy Rev. **100**, 143–174 (2019). https://doi.org/10.1016/j.rser.2018.10.014
4. Aste, T., et al.: Blockchain technologies: foreseeable impact on industry and society. Computer **50**(9), 18–28 (2017)
5. Bamakan, S.M.H., et al.: A survey of blockchain consensus algorithms performance evaluation criteria. Expert Syst. Appl. **154**, 113385 (2020)
6. Bano, S., et al.: SoK: consensus in the age of blockchains. In: Proceedings of the 1st ACM Conference on Advances in Financial Technologies, Zurich, Switzerland, pp. 183–198. Association for Computing Machinery (2019). https://doi.org/10.1145/3318041.3355458
7. Bodkhe, U., et al.: A survey on decentralized consensus mechanisms for cyber physical systems. IEEE Access **8**, 54371–54401 (2020)
8. Brereton, P., et al.: Lessons from applying the systematic literature review process within the software engineering domain. J. Syst. Softw. **80**(4), 571–583 (2007). https://doi.org/10.1016/j.jss.2006.07.009
9. Casado-Vara, R., et al.: How blockchain improves the supply chain: case study alimentary supply chain. Procedia Comput. Sci. **134**, 393–398 (2018). https://doi.org/10.1016/j.procs.2018.07.193
10. Cebe, M., et al.: Block4forensic: an integrated lightweight blockchain framework for forensics applications of connected vehicles. IEEE Commun. Mag. **56**(10), 50–57 (2018)
11. Chengfu, Y.: Research on autonomous and controllable high-performance consensus mechanism of blockchain. In: 2020 IEEE International Conference on Advances in Electrical Engineering and Computer Applications (AEECA), pp. 223–228 (2020). https://doi.org/10.1109/AEECA49918.2020.9213550
12. Deirmentzoglou, E., et al.: A survey on long-range attacks for proof of stake protocols. IEEE Access. **7**, 28712–28725 (2019). https://doi.org/10.1109/ACCESS.2019.2901858
13. Dybå, T., Dingsøyr, T.: Empirical studies of agile software development: a systematic review. Inf. Softw. Technol. **50**(9–10), 833–859 (2008). https://doi.org/10.1016/j.infsof.2008.01.006
14. Ferdous, M.S., et al.: Blockchain consensus algorithms: a survey. arXiv (2020)
15. Foti, M., et al.: Decentralized blockchain-based consensus for optimal power flow solutions. Appl. Energy **283**, 116100 (2021)
16. Fu, X., Wang, H., Shi, P.: A survey of Blockchain consensus algorithms: mechanism, design and applications. Sci. China Inf. Sci. **64**(2), 1–15 (2020). https://doi.org/10.1007/s11432-019-2790-1
17. Gao, S., et al.: T-PBFT: an EigenTrust-based practical Byzantine fault tolerance consensus algorithm. China Commun. **16**(12), 111–123 (2019). https://doi.org/10.23919/JCC.2019.12.008
18. Gramoli, V.: From blockchain consensus back to Byzantine consensus. Futur. Gener. Comput. Syst. **107**, 760–769 (2020). https://doi.org/10.1016/j.future.2017.09.023
19. Herlihy, M.: Blockchains from a distributed computing perspective. Commun. ACM **62**(2), 78–85 (2019)

20. Huang, C.-T., et al.: Consensus of whom? A spectrum of blockchain consensus protocols and new directions. In: 2019 IEEE International Smart Cities Conference (ISC2), pp. 1–8 (2019). https://doi.org/10.1109/ISC246665.2019.9071682
21. Ismail, L., Materwala, H.: A review of blockchain architecture and consensus protocols: use cases, challenges, and solutions. Symmetry **11**(10), 1198 (2019)
22. Jaroucheh, Z., et al.: SklCoin: toward a scalable proof-of-stake and collective signature based consensus protocol for strong consistency in blockchain. In: 2020 IEEE International Conference on Software Architecture Companion (ICSA-C), pp. 143–150. IEEE (2020)
23. Kim, D.-H., et al.: RSP consensus algorithm for blockchain. In: 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS), pp. 1–4. IEEE (2019)
24. Kitchenham, B., et al.: Systematic literature reviews in software engineering – a systematic literature review. Inf. Softw. Technol. **51**(1), 7–15 (2009). https://doi.org/10.1016/j.infsof.2008.09.009
25. Kokina, J., et al.: Blockchain: emergent industry adoption and implications for accounting. J. Emerging Technol. Account. **14**(2), 91–100 (2017)
26. Lao, L., et al.: G-PBFT: a location-based and scalable consensus protocol for IOT-Blockchain applications. In: 2020 IEEE International Parallel and Distributed Processing Symposium (IPDPS), pp. 664–673 IEEE (2020)
27. Lei, K., et al.: Reputation-based byzantine fault-tolerance for consortium blockchain. In: 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS), pp. 604–611 (2018). https://doi.org/10.1109/PADSW.2018.8644933
28. Leonardos, S., et al.: PREStO: a systematic framework for blockchain consensus protocols. IEEE Trans. Eng. Manage. **67**(4), 1028–1044 (2020)
29. Liu, Y., et al.: A fair selection protocol for committee-based permissionless blockchains. Comput. Secur. **91**, 101718 (2020)
30. Mackenzie, B., et al.: An assessment of blockchain consensus protocols for the Internet of Things. In: 2018 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC), pp. 183–190. IEEE (2018)
31. Nakamoto, S.: A peer-to-peer electronic cash system. Bitcoin, vol. 4 (2008). https://bitcoin.org/bitcoin.pdf
32. Nguyen, C.T., et al.: Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities. IEEE Access **7**, 85727–85745 (2019)
33. Niu, J., et al.: Incentive analysis of bitcoin-NG, revisited. Perform. Eval. **144**, 1–17 (2020)
34. Pahlajani, S., et al.: Survey on private blockchain consensus algorithms. In: 2019 1st International Conference on Innovations in Information and Communication Technology (ICIICT), Chennai, India, pp. 1–6. IEEE (2019). https://doi.org/10.1109/ICIICT1.2019.8741353
35. Panda, S.S., et al.: Study of blockchain based decentralized consensus algorithms. In: TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON), pp. 908–913 (2019). https://doi.org/10.1109/TENCON.2019.8929439
36. Sharma, K., Jain, D.: Consensus algorithms in blockchain technology: a survey. In: 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), pp. 1–7. IEEE (2019)
37. Vukolić, M.: The quest for scalable blockchain fabric: proof-of-work vs. BFT replication. In: Camenisch, J., Kesdoğan, D. (eds.) iNetSec 2015. LNCS, vol. 9591, pp. 112–125. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-39028-4_9
38. Wan, S., Li, M., Liu, G., Wang, C.: Recent advances in consensus protocols for blockchain: a survey. Wireless Netw. **26**(8), 5579–5593 (2019). https://doi.org/10.1007/s11276-019-02195-0
39. Wang, Q., et al.: A comparative study of blockchain consensus algorithms. In: Journal of Physics: Conference Series, p. 012007. IOP Publishing (2020)

40. Wang, Y., et al.: Study of blockchains's consensus mechanism based on credit. IEEE Access **7**, 10224–10231 (2019). https://doi.org/10.1109/ACCESS.2019.2891065
41. Wu, W., Gao, Z.: An improved blockchain consensus mechanism based on open business environment. In: IOP Conference Series: Earth and Environmental Science, p. 012043. IOP Publishing (2020)
42. Xiao, Y., et al.: A survey of distributed consensus protocols for blockchain networks. IEEE Commun. Surv. Tutor. **22**(2), 1432–1465 (2020). https://doi.org/10.1109/COMST.2020.2969706
43. Yli-Huumo, J., et al.: Where is current research on blockchain technology?—a systematic review. PLoS ONE **11**(10), e0163477 (2016). https://doi.org/10.1371/journal.pone.0163477
44. Zamani, M., et al.: RapidChain: scaling blockchain via full sharding. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto, Canada, pp. 931–948. Association for Computing Machinery (2018). https://doi.org/10.1145/3243734.3243853
45. Zhang, C., et al.: Overview of blockchain consensus mechanism. In: Proceedings of the 2020 2nd International Conference on Big Data Engineering, New York, NY, USA, pp. 7–12. Association for Computing Machinery (2020). https://doi.org/10.1145/3404512.3404522
46. Zhang, S., Lee, J.-H.: Analysis of the main consensus protocols of blockchain. ICT Express **6**(2), 93–97 (2020)
47. Zhao, W., et al.: On consensus in public blockchains. In: Proceedings of the 2019 International Conference on Blockchain Technology, New York, NY, USA, pp. 1–5. Association for Computing Machinery (2019). https://doi.org/10.1145/3320154.3320162