 doi:10.20944/preprints202211.0085.v1

Review

Evolution of Blockchains based on the Architecture and Consensus Algorithms used on Blockchains

Kalenga Muteba Arcel [1], Kinsgley Ogudo [1] and Espoir Bondo [2,*]

[1] Department of Electrical & Electronics Engineering Technology University of Johannesburg, Johannesburg, South Africa; kingsleyo@uj.ac.za (K.O.)
[2] Engineering Research and Development Paris, France1
*Correspondence: arcelkaleng@gmail.com (K.M.A.) Tel: +27817259801 ; espoirbondo@bondaf.com (E.B.)

Abstract: Blockchain technology has gotten much interest recently from academics, industry, and governments worldwide. It is regarded as a technical innovation that can disrupt various application fields affecting many aspects of our lives. Cryptocurrencies are a public blockchain application's success story that sparked extensive research and development. Scalability, energy consumption, and security, on the other hand, remain significant challenges. With low throughput, high transaction delay, and high energy consumption, most cryptocurrencies are experiencing low-efficiency difficulties. The scalability issue with public Blockchains is preventing organizations and sectors from receiving effective solutions. As a result, it is critical to bridge the gap and develop new frameworks that connect Blockchain with those goals. This paper examines the evolution of blockchain architecture and consensus protocols, provides a retrospective analysis, discusses the rationale for the various architectures and protocols' change, and captures the assumptions supporting their development and contributions to collaborative application development. However, existing research on consensus algorithms is insufficient. The features of the algorithms are discussed insufficiently in those papers, and some prominent blockchain consensus methods are not examined in terms of their scopes. The study's findings are delivered in tabular formats, allowing for a clear representation of these algorithms. We discovered in our investigation that scalability is a result of many parameters such; transaction throughput, number of nodes, storage, block size, high communication, latency, cost. Furthermore, Due to its off-chain data storage and smaller block size, PoF is much more scalable than PoS and PoW, and Because PoA is a hybrid of PoW and PoC, it does not necessitate a large number of computational resources. As a result, it has a higher throughput than PoW. PoPF entails ranking all participating nodes and appointing n accountants to compete for adding new blocks. This article addresses the need by analyzing a wide range of consensus algorithms using a complete taxonomy of attributes and delving into the consequences of several still-present flaws in consensus algorithms.

Keywords: blockchain; throughput; consensus; energy consumption; scalability; security

1. Introduction

A blockchain application is a decentralized application that runs on a peer-to-peer network. Data integrity, accountability, secrecy, availability, and transparency are all enabled by the mechanisms used to store and validate blockchain network data. Blockchain pioneered a new method of constructing an immutable distributed ledger for data storage. Depending on the consensus process utilized. [1] Most network participants complete and validate the transactions, removing the need for a middleman. The transactions are organized into blocks to achieve immutability, chained together using a cryptographic hash.

While various forms of consensus algorithms have arisen, a recent shortage of research provides a current review of existing consensus algorithms and their critical criteria for classification. Addressing concerns with their architectural approach is critical for developing new techniques or improving existing consensus algorithms as a foundation for

 doi:10.20944/preprints202211.0085.v1

more efficient blockchains. In addition, due to the increasing number of nodes, blockchain systems are encountering issues such as scalability, energy consumption, and security. When it comes to energy usage and scalability, security and privacy are frequently sacrificed.[2]

The following are the objectives of this paper: present a timeline of the growth of blockchain platforms and an evaluation of consensus algorithms. We conducted a high-level overview of the most recent research on the scalability of public blockchains. The schematic literature review began with a deep investigation into the scalability issue in major public blockchain applications to identify the impacts of blockchain technology adoption in areas and fields other than cryptocurrency, after which potential factors associated with challenges in transaction throughput, energy consumption, the number of nodes, latency, storage, and so on were explored and tracked. All scalability-related components were thoroughly examined and linked to the public blockchain consensus mechanism. 1. We give a high-level overview of the blockchain layers, including transaction execution and data flow, similar to all blockchain systems. 2. In the blockchain literature, we present a taxonomy, classification, and comparison of the various consensus protocols. 3. We describe the scalability features of each architecture and the security approaches used. 4. We give a critical examination of the various challenges in blockchain technology and the potential solutions proposed to address these issues.

2. Literature review

T Multiple research projects have been dedicated to evaluating and analyzing the existing Blockchain consensus protocols; this session will look at previously-published papers related to Blockchain consensus. The analysis of more than 100 top cryptocurrencies belonging to different categories of consensus algorithms was analyzed by Md Sadek, Mohammad Jabed, A. Hoque, and Alan Colman. Their study presented the gap using a comprehensive classification of properties and examined the implications of specific aspects of consensus algorithms that are still prevalent in detail. They developed a decision tree that can be used to evaluate consensus algorithms under various criteria [3].

Moreover, Visconti, A.; Rao, U.P.; Shah, K.A.; Zanolini, L.; Lepore, C.; Ceria, M.;.developed a review of consensus protocols, examining a new protocol called pure PoS and comparing them with PoW, PoS, and the Pure PoS based on throughput and scalability. Also discussed were cryptography and blockchain technology. CAP theorem has been used to analyze performance and show performance comparisons [4]. Z.; Niyato, D.; Wang, P.; Wen, Wang, W.; Hoang, D.T.; Hu, P.; Xiong Y.; Kim, DI. These researchers examined both the design aspects of distributed consensus system design and the incentive mechanism design of incentivized consensus protocols in the context of a typical blockchain network before comparing those two perspectives. By utilizing game theory, they discussed self-organizing strategies used by individual nodes in blockchain networks. Also highlighted were emerging blockchain applications [5].

L. Ismail and H. Materwala presented a table mapping blockchain architectures to corresponding platforms. They also established a classification system for mainstream consensus protocols and compared them. A comprehensive analysis of various current blockchain challenges was conducted, and possible remedies were presented. Future directions for developing an energy-efficient and scalable blockchain architecture and protocols have been suggested [6].

Y. Xiao, N. Zhang, W. Lou, and Y.T. Hou reviewed major blockchain consensus protocols. Their review included analytical results for the classical fault tolerance theory and key terminology. It then defined five key components of every blockchain network: block proposal, Validation, finalization, an incentive component, and information dissemination. Based on these components, some of the most prominent blockchain consensus protocols were examined and compared. Their findings gave them a better understanding of the strengths, applicability, and limitations of fault tolerance, scalability, and drawbacks in terms of fault tolerance, scalability, and downsides. Many of these protocols were still

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 4 November 2022 doi:10.20944/preprints202211.0085.v1

in development and subject to significant revisions when they were published [7]. [8],[9],[10],[11],[12],[13], and [14] are also included. In terms of energy consumption, scalability, security, and throughput metrics, they revised and presented a Hybrid PoW-BFT, PoS, DPoS, PoA, PoET, PoTS, Proof of Reputation (PoR, Ripple protocol).

2.1. Background of blockchain

The blockchain architecture comprises four layers: infrastructure, platform, distributed computing, and application. Infrastructure includes nodes, storage, and network facilities required to run the Blockchain. Nodes are members of the network. Nodes in a blockchain network usually fall into three categories: superficial nodes (otherwise known as light nodes), full nodes, and mining nodes. A simple node only sends and receives transactions in the network and does not store a copy of the ledger, nor do they validate any transactions, whereas full nodes do. Mine nodes (also known as block generators) generate new blocks in mining. [1]. In addition to the storage layer, the platform layer serves to facilitate remote procedure calls (RPCs), web application programming interfaces (APIs), and Representational State Transfer APIs (REST) for communication between the network and the server. An overview of blockchain technology is shown in Table 1.

Table 1. Blockchain layers.

Application Layer	Distributed Computing Layer
Digital asset transaction, Smart contracts	Consensus protocols, security, Transaction
Platform Layer	Infrastructure Layer
Web API, RPC, REST API	Network, Storage, Nodes

2.2.1. Types of blockchains

Public, private, hybrid, and consortium are the four different subtypes of blockchain technology [15,16].

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 4 November 2022 doi:10.20944/preprints202211.0085.v1

Table 2. Types of Blockchains.

Types of Blockchain Technology	
Name of Blockchain	**Description**
Public Blockchain	Public blockchains, also called trustless blockchains, or permissionless blockchains, are open networks that let anybody take part in the consensus procedure that blockchains use to validate transactions and data. They are dispersed among numerous unidentified parties and are totally decentralized.
Private Blockchain	Private blockchains, also known as permissioned blockchains, are private networks in which only pre-approved parties can connect and take part in consensus and data validation, occasionally as consortium members. They differ from permissionless blockchains in that they are distributed among known participants rather than anonymous ones, making them partially decentralized. Although they are viable, tokens and digital assets are not as common as in permissionless contexts.
Federated Blockchain	A Federated Blockchain, also known as a Consortium Blockchain. However, there is a dividing line between the two. There is no single entity that influences a Federated Blockchain network.
Hybrid Blockchain	A hybrid blockchain combines public and private blockchains. This implies that some processes are kept private while others are made public.

2.2.2. Consensus algorithms

Table 3. Common Consensus algorithms.

Category	Consensus algorithm
Proof-based algorithm or Validation Based	Proof of work
	Proof of stake
	Proof of burn
	Delegated proof of stake
	Proof of elapsed time
	Proof of publication
	Proof of excellence
	Proof of activity
	Proof of authority
	Proof of importance
	Proof of play
Voting-Proof-based algorithm or	Stellar consensus protocol
	Proof of vote
	Distributed byzantine fault tolerance 2.0
	Ripple consensus protocol
	Fast
Authentication Based	Proof of authentication
	Proof of previous transaction
	Proof of belief
	Proof of reputation
	Hyper Delegation Proof of Randomness

To produce and validate blocks, consensus algorithms use many techniques; blocks in the Blockchain combine many transactions, and a few nodes in the network can generate them. [17,18,] They are added to the chain and cryptographically linked to each other after block validation. The adaptability of consensus algorithms is determined by several aspects, transaction speed, scalability, etc. As previously mentioned, there are several essential consensus algorithms.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 4 November 2022 doi:10.20944/preprints202211.0085.v1

2.3. Most common consensus mechanism

2.3.1. PoW

Proof-of-work consensus allows a decentralized network to agree in transaction order. This stops users from "double spending" their coins and makes the chain extremely hard to attack or manipulate. Miners must compete in a race of trial and error to find the nonce for a block using the proof-of-work protocol [19]. A miner will continually run a dataset, which can only be obtained by downloading and running the entire chain (as a miner does) through a mathematical function when racing to build a block. The dataset builds a mixHash below a target nonce according to the block difficulty. Trial and error is the most effective method for doing this. The difficulty determines the hash target. The smaller the target, the less valid hashes there are. Other miners and clients can easily verify this once it has been produced. Even if just one transaction changed, the hash would change dramatically, indicating fraud. Hashing makes it simple to detect fraud. However, proof-of-work is a significant disincentive to assaulting the chain as a whole. The quantity of energy necessary to keep the network safe is a crucial criticism of proof-of-work.

2.3.2. PoS

In terms of the market capitalization of blockchain networks, (PoS) is the second most popular consensus mechanism after Proof of Work (PoW). PoS is a variant of PoW, an old method of consensus that was first presented with Bitcoin. Despite Bitcoin's initial success, PoW has been unable to match the need for more effective rates, as new blockchains necessitate substantial crashes and rapid transaction rates. Proof of Stake (PoS) is a concept that claims that users can enter or confirm transactions in blocks based on the currency they own. This signifies that the majority of the miner's coins have a high mining potential. [20]

A list of validators, block makers or forgers, is kept on the Blockchain. The Blockchain chooses a validator at random whenever new blocks need to be created. The chosen validator verifies the transactions and offers new blocks for approval by all validators. All current validators then vote on new blocks; the validator's stake determines the voting power. Those who propose invalid transactions, blocks, or votes deliberately, that is, those who purposefully jeopardize the chain's integrity, may lose their stakes. When the new blocks are accepted, the blocked developer can collect the transaction fee for their efforts.[21] PoW blocks are submitted to regulators, while PoS blocks have relied on miner networks. The technique of PoS verification is known as forging. The native token must be staked if the node wants to participate in the blockchain process. There is no need to spend electricity or money on hardware. The regulations for PoS networks vary depending on the situation, but the basic premise is the same: nodes who want to be authentic must lock a limited amount of tokens that serve as collateral. Compared to the PoW method, PoS is thought to be more energy-efficient and environmentally friendly; it is also said to be more secure.

2.3.3. DBFT

Delegated Byzantine Fault Tolerance, like PoS, uses a voting system to select delegates and speakers. In DBFT, ordinary nodes vote for delegates (bookkeeping nodes), with each ordinary node having the same number of votes regardless of income. Speakers are subsequently chosen at random from among these delegates. Delegates are in charge of keeping track of citizen demands (network transactions) and documenting them in the ledger. To validate the authenticity of a block, the randomly selected speaker proposes it and broadcasts it to other delegates, who then compare the speaker's block to their own. [22] At least two-thirds of the delegates must agree on the proposed block before it can be adopted and added to the network. If less than two-thirds of the delegates agree, a new speaker is chosen randomly, and the process begins again.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 4 November 2022 doi:10.20944/preprints202211.0085.v1

2.3.4. PBFT

The approach of Practical Byzantine Fault Tolerance is optimized for asynchronous systems and is supposed to be high-performance with a low overhead runtime and only a tiny latency increase. In the pBFT model, all nodes are sorted in a sequence, with one node serving as the primary node (leader) and the others serving as backup nodes. [23,24] All of the nodes in the system communicate with one another, and the goal is for all of the honest nodes to reach a consensus on the system's state by a majority vote. Nodes often connect, showing that messages originated from a particular peer node and were not altered during transmission. The capacity of the pBFT model to enable transaction finality without the requirement for confirmations, as in Proof-of-Work models like Bitcoin's, is one of its key features. If all of the nodes in a pBFT system agree on a proposed block, it becomes final. This is made possible by the fact that, as a result of their communication, all honest nodes agree on the system's status at that precise time. Another notable advantage of the pBFT paradigm over PoW systems is significantly lower energy consumption. Every block in a Proof-of-Work scheme, such as Bitcoin, requires a PoW round. As a result, the Bitcoin network's annual electricity usage by miners rivals small countries.

2.3.5. PoET

Proof of elapsed time (PoET) is a blockchain network consensus mechanism method that uses a fair lottery system to prevent high resource utilization and energy consumption while keeping the process efficient. The algorithm decides mining rights and blocks winners using a randomly generated elapsed time on a blockchain network. The PoET algorithm improves transparency by ensuring lottery results are verifiable by external participants by running a trustworthy code in a safe environment. Each participating node in the network must wait for a predetermined time, and the first node to fulfill the waiting period wins the new block. Each node in the blockchain network produces a random wait time and sleeps for that time. The first to wake up, that is, the one who has waited the least amount of time, commits a new block to the Blockchain, sending the essential information to the whole peer network. The process is then repeated for the next block's finding. Two crucial elements must be ensured by the PoET network consensus method. [25] To begin with, the technique assures that the participating nodes choose a genuinely random time rather than a shorter duration picked by the participants on purpose to win. Second, the process ensures that the winner has completed the required waiting period.

2.3.6. Proof of Capacity

Proof of capacity (PoC) is a consensus mechanism method used in blockchains that allows mining devices in the network to decide mining rights and validate transactions using their available hard drive space. This is in contrast to using the processing power of the mining device (as in the proof of work method) or the miner's cryptocurrency stake (as in the proof of stake algorithm). Plotting and mining are two steps in the proof-of-capacity protocol. First, the hard drive is plotted: a list of all potential nonce values is constructed by hashing data, including a miner's account, over and over again. Each nonce comprises 8192 hashes, numbered from 0 to 8191. All hashes are coupled into "scoops," which are groups of two neighboring hashes. For example, hash 0 and 1 equals scoop 0, hash 2 and 3 equals hash 1, and so on. The second phase is the actual mining, which entails calculating a scoop number by a miner.[26,27]

2.3.7. Proof of Burn

Proof-of-burn (PoB) is a blockchain consensus process that uses less energy than proof-of-work (PoW). By burning coins, decentralized platforms using the PoB approach ensure that miners reach a consensus. The process of permanently removing cryptos from circulation is known as burning. PoB-powered blockchains employ it to validate transactions, even though it reduces inflation. However, unlike PoW-based decentralized platforms like Bitcoin, Proof-of-Burn validates transactions using virtual mining machines

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 4 November 2022 doi:10.20944/preprints202211.0085.v1

rather than real ones. Simply put, PoB miners burn coins to demonstrate their presence in the network and gain permission to mine. The number of coins miner burn measures his virtual mining strength. As a result, the more coins you have, the more power you have, and vice versa. It is worth noting that, just like in PoW systems, more mining power enhances the pace with which new blocks are discovered. As a result, the miner receives higher incentives. The coin burn procedure on proof-of-burn (PoB) networks entails sending the coins to an "eater address." The public can verify this address, but it is inaccessible. Eater addresses are randomized and do not include private keys.[28] Proof-of-burn is similar to proof-of-stake (PoS) in that both consensus processes rely on coin interaction to keep the network secure. Coins locked in PoS systems, unlike PoB systems, are not permanently deleted; their holders can still access and sell them if they desire to quit the network. PoB, on the other hand, creates a coin scarcity, whereas PoS does not. It is worth noting that the PoB technique is a novel consensus algorithm. As a result, it has yet to be demonstrated to work on massive networks. The PoB technique has several advantages, including being sustainable and having a highly decentralized mining process.

2.3.8. Federated Byzantine Agreement

Federated Byzantine Agreements (FBA) is a type of Byzantine fault tolerance in which each byzantine general is in charge of their Blockchain. Because of its high throughput, network scalability, and cheap transaction costs, a Federated Byzantine Agreement (FBA) is deployed. Stellar and Ripple are two well-known cryptocurrencies that use the Federated Byzantine Agreement (FBA). Even though Ripple invented the Federated Byzantine Agreement (FBA) consensus mechanism, Stellar was the first cryptocurrency to use it successfully. Before users seek any performance from the Federated Byzantine Agreements (FBA), nodes must be known and verified ahead of time. Individual nodes in the FBA network make decisions about whom they trust, and quorums of nodes develop as a result of those decisions. A quorum is the minimum number of nodes required for a solution to be correct, and a block is validated and added to the Blockchain once a quorum is formed. The FBA makes use of quorum slices, which are subsets of quorums that can persuade specific network nodes to concur with them.[29]

2.3.9. PoA

Instead of tokens, network participants stake their identities, which is the idea of the algorithm. This means that, unlike most blockchain protocols, validators in PoA systems are known entities who risk their reputations in exchange for the ability to validate blocks.[30] PoA is impractical for public blockchains like Bitcoin and Ethereum, including hundreds or even thousands of validating nodes, because of the identity requirement. As a result, PoA networks tend to have fewer validating nodes, making them less decentralized. They also have a high throughput capacity, which is a plus. Proof of authority, like PoS, involves little computational work and no specialized equipment. However, PoA networks usually only accept entities with a proven track record as validators, making that position challenging to get for the average person.[31]

3. Evaluation of scalability of consensus algorithm

The scalabilities in public Blockchain are the aspect of multiple parameters depending on the type of consensus algorithm; in most cases, the propagation delay in the Blockchain network is due to the broadcasting process of all the transactions to the nodes [32-36] Furthermore, the second parameter could be the consensus model, following papers evaluated the performance and proposed consensus models, and each consensus algorithm has its scalability [37- 47]. Moreover, the increasing number of nodes results in the time delay in transactions called latency; here are the factors that may lead to scalability.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 4 November 2022 doi:10.20944/preprints202211.0085.v1

Table 4. Scalability parameters.

Factors	Refer	Ref
Tran-saction Through-put	Determines the number of blocks that can be proceeded and added to the Blockchain per second, denoted as transactions per second (Tps).	[49]
Latency	Latency in Blockchain refers to the processing time for a transaction measured Starting from getting an input till the transaction is completed at the output.	[50][51]
Storage	Storage is another vital aspect to consider is scalability in public Blockchain because the storage required grows in parallel with the number of nodes and transactions. As a result, full nodes that store complete block data require much storage.	[32][33]
Block Size	In Bitcoin, a block is typically around 1 M.B. in size. This is a relatively small value, and it restricts the number of transactions that can be saved. Large block sizes can aggregate more transactions, resulting in higher throughput and reduced latency, but larger blocks also result in longer block propagation times because heavier blocks take longer to send across the network.	[32][36]
Number of nodes	Nodes are entities that are connected to the blockchain network. When many nodes are connected to a network, the inter-node latency increases. As the number of nodes grows, so does the number of transactions, and as a result, more transactions are involved in the consensus process. This will very certainly have an impact on transaction performance and latency.	[44][45]
Consensus model	The consensus model defines how the decision is taken in Blockchain most the consensus model Emphasizes security. It increases the latency of the network	[50][51]
Compu-tation energy	Energy requires to compute a transaction	[52]
Network load	This implies the number of transactions being carried by the network.	[41][46]

4. Discussion

4.1. Energy consumption

Since consensus techniques like PoW require a lot of computational power to select a block leader, their energy consumption contributes to environmental global warming and carbon footprints [48]. Bitcoin uses proof-of-work (PoW), which, according to Cambridge, accounts for about 110 Terawatt Hours of annual electricity demand, or roughly 0.55% of the world's total electricity production. Additionally, a few of these protocols (PoA, PoPF, for example) deal with this problem by putting a cap on the number of miners or by allocating different levels of mining difficulty (PoPF, PoRX). Some consensus algorithms, such as PoB and PoL, depend on miners competing to perform various tasks, such as maximizing a certain value (benefit) or building machine learning models rather than hashing. The energy usage of Bitcoin is seen in Figure 1.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 4 November 2022 doi:10.20944/preprints202211.0085.v1

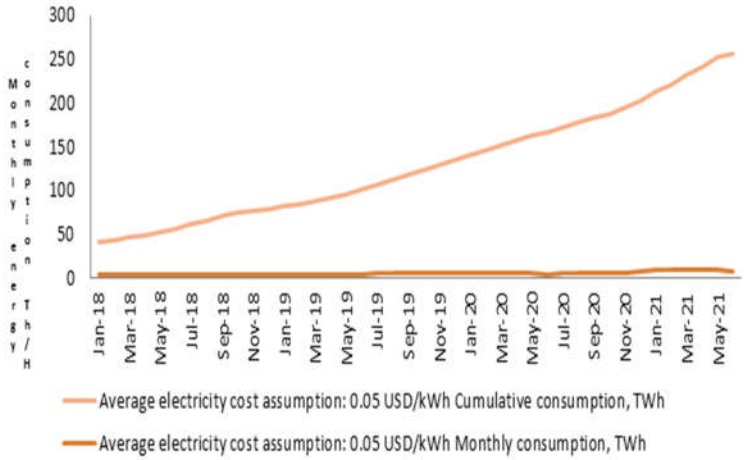

Figure 1. Bitcoin electricity consumption.

Security: PoS claims to resist the 51 %attack because rogue nodes will lose reputation as they publish more consecutive blocks. Due to a validation phase that prohibits nodes from being picked as block leaders in sequential order, the PoB and PoA protocols resist the 51 % attack. However, despite being immune to a 51% assault, PoB can still be defeated with less processing power than PoW. Only malicious nodes with a probability of 50% or less can be tolerated by the remaining protocols since they are PoW variants or modifications. PoF allows for a diversity rate of 0.7 percent, therefore in order to take over a chain, an adversary must gain the support of 75% of the active nodes. PoR, on the other hand, is a blockchain network with permissions where each participating node's involvement is verified using their public keys. [53] [54] As shown in table 5.

Table 5. Performance of consensus protocols.

	Performance of consensus protocols		
	Energy consumption	**Security**	**Transaction time**
PoW	Very High	Secure	Very slow
PoS	Normal	Secure	Fast
PoA	Normal	Secure	Slow
PBFT	Very low	Least secure	Fast
PoET	Low	Secure	Normal
B	Very high	Secure	Normal
DPoS	Normal	Secure	slow
PoR	Normal	Secure	Normal
PoEx	Normal	Secure	Normal

Throughput: Proof of Authority (PoA), which combines PoW and PoC, does not require a lot of computer power. It has a higher throughput than PoW as a result. In PoPF, each participating node is ranked, and n accountants are chosen to compete for the right to manufacture blocks. Accountants in higher positions have simpler mining than those with lower positions. Decentralization is ensured via the ranking system without periodically raising the difficulty level. [40] [41] As a result, PoPF theoretically has a larger throughput than PoW, with the processing speed of each player serving as the only physical limit. PoEx makes use of accumulated PoW to lower node mining difficulty, improving throughput because nodes will have lower miner challenges and be able to obtain the desired hash values more quickly. The PoV consensus protocol provides lower transaction validation delay than PoW, leading to faster throughput.

Scalability: PoF is far more scalable than PoS and PoW because to its off-chain data storage and smaller block size, enabling more users to participate without degrading the

 doi:10.20944/preprints202211.0085.v1

network's overall performance. PoR has been shown to be more scalable than PoW since it requires less time to reach a consensus as the number of players increases. In PoA, nodes compete to solve a computational problem. [43] [45] Additionally, PoA demands the gathering of input data that is stochastically stored, preventing centralization by accumulating computing power. Its scalability ought to be similar to PoW but less so than that of PoS as a result.

5. Conclusion

Over a decade ago, blockchain technology was established to perform peer-to-peer digital currency transactions amongst many untrustworthy network participants without using a third party. Scalability, transaction time, false block formation, security, and privacy are still proving to be barriers to blockchain and IoT integration. As the demand for a flexible, scalable, and energy-efficient consensus mechanism grows, Blockchain becomes increasingly essential. We discovered in our investigation that scalability is a result of many parameters such; transaction throughput, number of nodes, storage, block size, high communication, latency, cost. PoF is far more scalable than PoS and PoW due to its off-chain data storage and smaller block size, and because PoA is a combination of PoW and PoC, it does not require a significant amount of CPU resources. It has a higher throughput than PoW as a result. In PoPF, each participating node is ranked, and n accountants are chosen to compete for the right to manufacture blocks. Additionally, we have discovered that consensus methods, like PoW, consume a lot of energy because they require a lot of processing power to select a block leader, which contributes to environmental global warming and carbon footprints. To develop and implement a novel consensus process that will result in the cat-off energy usage, more study is required and address the transaction throughput.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

PoW (Proof of Work)

PoET (Proof of Elapsed Time)

PoA (Proof of Authority)

PoS (Proof of Stake)

PBFT (Practical Byzantine Fault Tolerance)

POC (Proof of Capacity)

POP (Proof of Participation and Fees)

FBA (Federated Byzantine Agreement)

PoV (Proof of Vote)

PoR (Proof of Reputation)

 doi:10.20944/preprints202211.0085.v1

PoX-R (Proof of X-repute)

PoL (Proof of Location)

PoB (Proof of Burn)

References

1. F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," IEEE Communications Surveys Tutorials, vol. 18, no. 3, pp. 2084–2123, third quarter 2016.
2. Park, J.; Park, J. Blockchain security in cloud computing: Use cases, challenges, and solutions. Symmetry 2017, 9, 164.
3. Md Sadek, M Chowdhury, A. Colman, A. Hoque: Blockchain Consensus Algorithms: A Survey, IEEE.
4. Lepore, C.; Ceria, M.; Visconti, A.; Rao, U.P.; Shah, K.A.; Zanolini, L. A Survey on Blockchain Consensus with a Performance Comparison of PoW, PoS, and Pure PoS. Mathematics 2020, 8, 1782.
5. Wang, W.; Hoang, D.T.; Hu, P.; Xiong, Z.; Niyato, D.; Wang, P.; Wen, Y.; Kim, D.I. A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks. IEEE Access 2019,
6. Ismail, L.; Materwala, H. A Review of Blockchain Architecture and Consensus Protocols: Use Cases, Challenges, and Solutions.Symmetry 2019,
7. Xiao, Y.; Zhang, N.; Lou, W.; Hou, Y.T. A Survey of Distributed Consensus Protocols for Blockchain Networks.
8. Sharkey, S.; Tewari, H. Alt-PoW: An Alternative Proof-of-Work Mechanism. Proceedings of the 2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON), Newark, CA, USA, 4–9 April 2019. [CrossRef]
9. Sankar, Lakshmi Siva, and Sindhu, M and Sethumadhavan, M "Survey of consensus protocols on blockchain applications" 4th International Conference on Advanced Computing and Communication Systems (ICACCS). IEEE, 1–5, 2017.
10. Bano, S., Sonnino, A., Al-Bassam, M., Azouvi, S., McCorry, P., Meiklejohn, S., and Danezis, G. "Consensus in the Age of Blockchains.". arXiv preprint arXiv:1711.03936, 2017.
11. Mukhopadhyay, Ujan and Skjellum, Anthony and Hambolu, Oluwakemi and Oakley, Jon and Yu, Lu and Brooks, Richard. "A brief survey of cryptocurrency systems." Proceedings of the 14th annual conference on privacy, security, and trust (PST). IEEE, 745– 752, 2016.
12. Portal, D.; Mohanty, S.P. Proof of Authentication: IoT-Friendly Blockchains. IEEE Potentials 2019, 38, 26–29. [CrossRef]
13. Lu, Y. Blockchain: A Survey on Functions, Applications, and Open Issues. J. Ind. Integer. Manag. 2018, 3, 1850015. [CrossRef]
14. Seibold, Sigrid and Samman, George "Consensus: Immutable agreement for the Internet of value." https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/kpmgblockchain-consensus-mechanism.pdf KPMG. 2016.
15. Polge, J.; Robert, J.; Le Traon, Y. Permissioned blockchain frameworks in the industry: A comparison.ICT Express 2020.
16. https://searchcio.techtarget.com/feature/What-are-the-4-different-types-of-blockchain-technology
17. Weng S, Yue D, Huang C. Distributed Economic Dispatch Based on Consensus Algorithm Under Event-Triggered Mechanism[M]// Intelligent Computing, Networked Control, and Their Engineering Applications. 2017.
18. Yoo S E, Lee B J, Kim KT, et al. Blockchain-based consensus algorithm. Korean Society of Computer Information Conference. 2018.
19. Wang S, Qin B, Chen J, et al. Blockchain Estimation Model Based on PoW Mechanism. Journal of Cyber Security, 2018.
20. Li W, Andreina S, Bohli J M, et al. Securing Proof-of-Stake Blockchain Protocols. 2017.
21. King, S.; Nadal, S. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake." self-published paper. 2012, pp. 1–6. Available online: https://download.csdn.net/download/vinsuan1993/9963770 (accessed on 1 April 2020)
22. NEO White Paper, http://docs.neo.org/en-us/, accessed 2019, 2014
23. Y. Amir, B. Coan, J. Kirsch, J. Lane, Byzantine replication under attack, in 2008 IEEE International Conference on Dependable Systems and Networks With FTCS and DCC (DSN), IEEE, 2008, pp. 197–206.
24. A. Clement, E.L. Wong, L. Alvisi, M. Dahlin, M. Marchetti, Making Byzantine fault-tolerant systems tolerate Byzantine faults, in 6th USENIX Symposium on Networked Systems Design and Implementation, vol. 9, 2009, pp. 153–168.
25. A. Gervais, K. Wüst and H. Ritzdorf, "On the Security and Performance of Proof of Work Blockchains," IACR Crystal. ePrint Arch., 2016
26. S. Dziembowski, S. Faust, V. Kolmogorov and K. Pietrzak, "Proof of Space," in International Association for Cryptologic Research (IACR), 2013.
27. Davick, "Help Proof-of-space," https://en.wikipedia.org/wiki/Proof-of-space.
28. Iain Stewart. Proof of Burn. Retrieved from: https://en.bitcoin.it/wiki/Proof_of_burn
29. L. Lamport, R. Shostak, and M. Pease, 1982. The Byzantine Generals Problem. ACM Transactions on Programming Lang. and Sys., Vol. 4, No. 3,382—401
30. Proof of Authority. https://github.com/paritytech/parity/wiki/Proof-of-Authority-Chains.
31. Parity Technologies. https://www.parity.io.
32. Sedky, G.; El Moggy, A. BCXP: Blockchain-Centric Network Layer for Efficient Transaction and Block Exchange over Named Data Networking. In Proceedings of the 2018 IEEE 43rd Conference on Local Computer Networks (LCN), Chicago, IL, USA, 1–4 October 2018; pp. 449–452.

33. Hazari, S.S.; Mahmoud, Q.H. A Parallel Proof of Work to Improve Transaction Speed and Scalability in Blockchain Systems. Proceedings of the IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC 2019), Las Vegas, NV, USA, 7–9 January 2019; pp. 916–921.
34. Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; De Caro, A.; Enyeart, D.; Ferris, C. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. In Proceedings of the 13th EuroSys Conference, Porto, Portugal, 23–26 April 2018; pp. 1–15.
35. Chauhan, A.; Malviya, O.P.; Verma, M.; Mor, T.S. Blockchain and Scalability. In Proceedings of the 2018 IEEE International.Conference on Software Quality, Reliability and Security Companion (QRS-C), Lisbon, Portugal, 16–20 July 2018; pp. 122–128.
36. Sanka, A.I.; Cheung, R.C. Efficient High-Performance FPGA Based NoSQL Caching System for Blockchain Scalability and Throughput Improvement. In Proceedings of the 26th International Conference on Systems Engineering (ICSEng 2018), Sidney, Australia, 18–20 December 2018; pp. 1–8.
37. Cong, K.; Ren, Z.; Pouwelse, J. A Blockchain Consensus Protocol with Horizontal Scalability. In Proceedings of the 2018 IFIP Networking Conference (IFIP Networking) and Workshops, Zurich, Switzerland, 14–16 May 2018; pp. 1–9.
38. Manshaei, M.H.; Jadliwala, M.; Maiti, A.; Fooladgar, M. A Game-Theoretic Analysis of Shard-Based Permissionless Blockchains.IEEE Access 2018, 6, 78100–78112. [CrossRef]
39. Asgaonkar, A.; Palande, P.; Joshi, R.S. Is the Cost of Proof-of-Work Consensus Quasilinear? In Proceedings of the ACM India Joint International Conference on Data Science and Management of Data, Goa, India, 11–13 January 2018; pp. 314–317.
40. Wang, J.; Wang, H. Monoxide: Scale-out Blockchains with Asynchronous Consensus Zones. Proceedings of the 16th (USENIX)Symposium on Networked Systems Design and Implementation (NSDI '19), Boston, MA, USA, 26–28 February 2019; pp. 95–112.
41. Zhang, Q.; Liu, Y.; Chen, L.; Ai, Z. Proof of Reputation: A Reputation-Based Consensus Protocol for Blockchain-Based Systems. In Proceedings of the 2019 International Electronics Communication Conference, Okinawa, Japan, 7–9 July 2019; pp. 131–138.
42. Spasovski, J.; Eklund, P. Proof of Stake Blockchain: Performance and Scalability for Groupware Communications. In Proceedings of the 9th International Conference on Management of Digital EcoSystems, Bangkok, Thailand, 7–10 November 2017; pp. 251–258.
43. Vukoli'c, M. The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication. In International Workshop on Open Problems in Network Security; Springer: Berlin/Heidelberg, Germany, 2015; pp. 112–125.
44. Yin, J.; Wang, C.; Zhang, Z.; Liu, J. Revisiting the Incentive Mechanism of Bitcoin-NG. Australasian Conference on information security and Privacy; Springer: Berlin/Heidelberg, Germany, 2018; pp. 706–719.
45. Gao, Y.; Kawai, S.; Nobuhara, H. Scalable Blockchain Protocol Based on Proof of Stake and Sharding. J. Adv. Comput. Intell. Intell. Inform. 2019, 23, 856–863. [CrossRef]
46. Han, R.; Foutris, N.; Kotselidis, C. Demystifying Crypto-Mining: Analysis and Optimizations of Memory-Hard Pow Algorithms. In Proceedings of the 2019 IEEE International Symposium on Performance Analysis of Systems and Software (ISPASS), Madison, WI, USA, 24–26 March 2019; pp. 22–33.
47. Jiang, Y.; Lian, Z. High Performance and Scalable Byzantine Fault Tolerance. In Proceedings of the 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chengdu, China, 15–17 March 2019; pp.1195–1202.
48. Bitcoin Could Cost Us Our Clean-Energy Future|Grist. Available online: https://grist.org/article/bitcoincould-cost-us-our-clean-energy-future/ (accessed on 31 December 2018).
49. Ouattara, H.F.; Ahmat, D.; Ouédraogo, F.T.; Bissyandé, T.F.; Sié, O. Blockchain Consensus Protocols. In Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering; Springer International Publishing: Cham, Switzerland, 2018; pp. 304–314
50. Nguyen, G.-T.; Kim, K. A Survey About Consensus Algorithms Used in Blockchain. J. Inf. Process. Syst. 2018, 14, 101–128.
51. Wang, X.; Zha, X.; Ni, W.; Liu, R.P.; Guo, Y.J.; Niu, X.; Zheng, K. Survey on Blockchain for Internet of Things. Comput. Commun. 2019, 136, 10–29.
52. https://ccaf.io/cbeci/index
53. The P + epsilon Attack. Available online: https://blog.ethereum.org/2015/01/28/p-epsilon-attack/
54. Deirmentzoglou, E.; Papakyriakopoulos, G.; Patsakis, C. A Survey on Long-Range Attacks for Proof of Stake Protocols. IEEE Access 2019, 7, 28712–28725.