The Current State of Blockchain Consensus Mechanism: Issues and Future Works

Shadab Alam
College of Computer Science & IT, Jazan University, Jazan, Saudi Arabia

***Abstract*—Blockchain is a decentralized ledger that serves as the foundation of Bitcoin and has found applications in various domains due to its immutable properties. It has the potential to change digital transactions drastically. It has been successfully used across multiple fields for record immutability and reliability. The consensus mechanism is the backbone of blockchain operations and validates newly generated blocks before they are added. To verify transactions in the ledger, various peer-to-peer (P2P) network validators use different consensus algorithms to solve the reliability problem in a network with unreliable nodes. The security and reliability of the inherent consensus algorithm used mainly determine blockchain security. However, consensus algorithms consume significant resources for validating new nodes. Therefore the safety and reliability of a blockchain system is based on the consensus mechanism's reliability and performance. Although various consensus mechanisms/algorithms exist, there is no unified evaluation criterion to evaluate them. Evaluating the consensus algorithm will explain system reliability and provide a mechanism for choosing the best consensus mechanism for a defined set of problems. This article comprehensively analyzes existing and recent consensus algorithms' throughput, scalability, latency, energy efficiency, and other factors such as attacks, Byzantine fault tolerance, adversary tolerance, and decentralization levels. The paper defines consensus mechanism criteria, evaluates available consensus algorithms based on them, and presents their advantages and disadvantages.**

Keywords*—Blockchain; consensus mechanism; consensus algorithm; data security; distributed systems; bitcoin

I. Introduction

The concept of blockchain revolves around the decentralized recording of digital transactions, eliminating the need for a central authority. These transactions are structured as blocks, which undergo encryption and validation by the majority of participating nodes before being appended to the blockchain. Initially introduced without standardized applications, the Blockchain methodology gained prominence with the advent of Bitcoin in 2008, credited to Satoshi Nakamoto [1]. Originally intended to circumvent the reliance on financial institutions, this innovation aimed to enable direct peer-to-peer transactions among participants. Bitcoin's success in achieving this objective set a precedent, demonstrating how businesses beyond the financial sector could conduct transactions without the intervention of a centralized third party. The structure comprises interconnected data blocks, each encapsulating transactions organized within branches of a Merkle tree, all cryptographically linked to the preceding block [2].

The blockchain operates as a ledger, capturing the complete transaction history in a chronological sequence due to the arrangement of blocks [3]. Among the most pivotal functions within the blockchain are verification and security, which are realized through a dedicated technique known as a consensus algorithm [4]. This algorithm is paramount in the blockchain system, primarily responsible for upholding its credibility, safety, and overall integrity. The consensus mechanism's efficacy directly influences critical aspects such as the stability, throughput, and accessibility of the blockchain system [5]. Within the network, nodes collaborate as validators of transactions, thereby upholding the integrity of the data. Including a block in the chain necessitates the consensus of the majority of nodes, confirming the accuracy of both the transactions contained within the block and the block as a cohesive entity. The foundation of this determination lies in a consensus algorithm implemented at the blockchain level, ensuring the precision of the data. Based on the level of access, blockchain networks can be categorized into two distinct types: private and public [6].

In contrast to public blockchains, which anybody may access and interact with, private blockchain can only be accessed by machines that have been allowed access. A consensus method in the blockchain can force the system's dispersed nodes to debate whether a transaction or block is valid. It allows for the eventual writing of valid data into the blockchain when the nodes have reached a consensus. In a distributed scheme, obtaining consensus between uncertain nodes has been discussed as a "Byzantine" problem in which a herd of army generals has cordoned off the city. Specifically, there is a clash between generals as some choose to attack, and others want to withdraw from the town. The town, assaulted by several generals, would collapse. Therefore, they should agree on whether to attack or retreat [7].

Similarly, the blockchain algorithm's major challenge in distributed ambiance is to achieve consensus [8][9]. Generally, the blockchain is decentralized because of a centralized node for noticing and checking every transaction. It creates a necessity to design and develop protocols or methods that specify all the transactions are legitimate. For this reason, the consensus algorithm is believed as the soul of every blockchain. In a decentralized or distributed environment, the consensus is a crucial issue that defines the mechanism to approve or refuse a block by every agreed node [10]. Once the new block is allowed by every network member, it is then attached to the blockchain [11]. As discussed, the blockchain's primary issue is how to achieve consensus between members of the network. Every algorithm has implemented a broad

spectrum of consensus algorithms with many strengths and weaknesses. The number of current consensus algorithms can create a fuss in choosing and applying them. Therefore, it is necessary to recognize various performance evaluation criteria that include every aspect of the consensus algorithm, besides the profound understanding of current algorithms' limitations for attaining consensus between peers and guaranteeing data security in the blockchain [12]. The main goal of this paper is to present criteria for evaluating the efficiency or the performance of widely known blockchain consensus algorithms and further review and evaluate the existing consensus mechanisms based on these identified parameters.

The subsequent sections of this article are organized as follows: Section II presents the pertinent background research in this domain. Section III offers a concise overview of the prevailing consensus techniques within the realm of blockchain technology. The approach taken to evaluate these consensus algorithms is expounded upon in Section IV. Section V presents a comprehensive analysis of the challenges and limitations inherent in these algorithms, accompanied by suggestions for potential avenues of further exploration. Section VI delves into the existing gaps and research challenges, while the conclusive Section VII provides a comprehensive summary encapsulating the entirety of this study.

II. Related Work

The origins of consensus algorithms can be traced back to concepts of credibility and reliability in distributed algorithms, exemplified by the Byzantine General Problem. In 1999, Castro and Liskov introduced Practical Byzantine Fault Tolerance (PBFT), a novel consensus approach aimed at mitigating trust-related concerns. PBFT fosters trust among participating stakeholders and facilitates efficient data exchange while minimizing latency. Following this, the Proof of Work (PoW) concept emerged in the same year, drawing inspiration from PBFT's principles, and was proposed as a means of validating transactions within open distributed systems. Subsequently, the PoW concept laid the foundation for the operational model of Satoshi's Bitcoin cryptocurrency [1]. PoW involves solving complex puzzles, its functionality hinging on the value in relation to the targeted hash cost. When the cost is lower, a block is mined and subsequently appended to the blockchain.

While doing the literature review on the consensus algorithms, this article identified literature related to consensus and studies associated with comparing the consensus algorithm. To review the metrics and criteria, a systematic review of the consensus algorithms has been done. G. T. Nguyen and K. Kim reviewed the Blockchain consensus algorithms applied in some well-known applications at this time [13]. Bach et al. (2018) present a comparative study of algorithmic steps, scalability, methods, and security risks of popular consensus algorithms. Authors in [14] tested that none of the deterministic consensus protocols could guarantee a mechanism in a decentralized system. Still, Paxos can not only assure steadiness but also the security of the network. As per [15], there is no doubt that Paxos is demanding and challenging to implement and understand, but the modern training standard allows us to achieve a consensus algorithm whenever required [16]. Paxos is the group of protocols for attaining consensus in the network of unreliable or defective processes [17]. Ferdous et al. (2020) analyze a wide range of consensus algorithms employing comprehensive taxonomic properties and investigate the consequences of the different problems that are still widespread in consensus algorithms. They also provided detailed literature on cryptocurrencies belonging to various class consensus algorithms [18]. Alsunaidi and Alhaidar thoroughly analyzed Blockchain technology, focusing on well-known consensus algorithms to identify the characteristics and variables affecting performance and security [19]. Panda et al. presented a thorough analysis of the distributed consensus processes in accordance with the kind of blockchain used. It also does a comparative analysis of the consensus protocols [20]. Sharma and Jain cover the different consensus methods, how they operate, and their applications. Additionally, it looked at blockchain technology, including its benefits and drawbacks [21].

Meneghetti et al. (2020) presented a comprehensive survey of the PoW techniques, attacks, and their current use in cryptocurrency consensus algorithms. They also analyzed some known attacks on these consensus algorithms and then presented them in a coordinated manner according to their core ideas [22]. The consensus algorithm can resolve common problems, such as harmonization among dispersed systems [23]. Consensus algorithms used in the blockchain can determine the legitimacy of distributed transactions in cryptocurrencies. Moreover, it is also used in authorizing the uniqueness of a front-runner of the distributed task. The consensus algorithm ensures reliability amongst state machine replicas and, later on, harmonizes them. The stack of 32 consensus algorithms is sorted into two significant types: proof-based and vote-based [13]. This study illustrates the advantages and disadvantages of all kinds and contrasts them, established on obtrusive characteristics.

Simultaneously, the limits and upcoming growth in technology are also discussed [13],[24]. Yang Xiao et al. (2020) survey provides comprehensive literature on blockchain consensus algorithms. The analysis is done concerning performance, fault tolerance, and vulnerabilities. At the same time, there is also an emphasis on their use cases. Bamkan et al. (2020) comprehensively examined the resources accessible on the consensus algorithms in light of their traits, motivations, and present difficulties [25]. This paper defines the criteria for consensus evaluation as throughput, profitability, degree of decentralization, and vulnerabilities and evaluates the existing blockchain consensus mechanisms based on these criteria [6].

Further, article [2] presents some open issues and challenges in implementing various consensus mechanisms with their virtues and drawbacks. In-depth research on blockchain technology has been done by examining its design, including a range of consensus algorithms and the options for security and data privacy within the blockchain discussed in this article [26]. A survey of the leading consensus mechanisms on blockchain solutions is done in this paper and highlights each one's properties. Additionally, it distinguishes between probabilistic and deterministic consensus procedures [27]. Some other studies also presented a brief review of

consensus algorithms, but these studies are not comprehensive, like [28] surveys highlighting the latest studies in blockchain and consensus algorithms. This paper adds theory and information that may be utilized to choose an appropriate consensus algorithm. It will aid scholars in their continued study of consensus in the context of private blockchain [29]. According to this article, the Byzantine consensus may need to be rethought in light of the blockchain environment, which also looks at prominent blockchain consensus algorithms [30]. Lashkari & Musilek [31] presented a very detailed analysis of existing blockchain consensus algorithms. Ferdous et al. [32] surveyed the consensus algorithms being used in crypto-currencies. Lina Ge et al. (2022) surveyed the PoS-based consensus algorithms and compared them with their advantages and disadvantages [33]. Xiong et al. [34] reviewed the widely used main consensus algorithms, the possible scenarios in which they can be suitable, and their relative disadvantages. Jain & Jat [35] survey some prominent consensus algorithms, reviews the key features and parameters, and compare the presented consensus algorithms based on these.

TABLE I. COMPARATIVE STUDY OF RELATED RESEARCH WORK

Ref	Year	Idea of Paper	Comments
[13]	2018	It reviews the Blockchain consensus algorithms applied for various applications.	None
[19]	2019	The author thoroughly analyzed Blockchain technology, focusing on well-known consensus algorithms to identify the characteristics and variables affecting performance and security.	It is recommended that one of the leading consensus algorithms for public Blockchain networks be improved by introducing a lightweight mechanism.
[20]	2019	This paper presented a thorough analysis of the distributed consensus processes. In accordance with the kind of blockchain used, it also does a comparative analysis of the consensus protocols.	None
[21]	2019	This paper covers the different consensus methods, how they operate, and their applications. Additionally, we looked at blockchain technology, including its benefits and drawbacks.	None
[25]	2020	This survey comprehensively examined the resources accessible on the consensus algorithms in light of their traits, motivations, and present difficulties.	It examined protocols' use cases while analyzing them in terms of fault tolerance, performance, and vulnerabilities.
[6]	2020	This paper defines the criteria for consensus evaluation as throughput, profitability, degree of decentralization, and vulnerabilities and evaluates the existing blockchain consensus mechanisms based on these criteria.	None
[2]	2020	It outlines several unresolved problems and difficulties in implementing various consensus processes and their advantages and disadvantages. The proposed poll would guide blockchain academics and developers as they consider and create the next consensus mechanisms.	None
[26]	2020	In-depth research on blockchain technology has been done by examining its design, which includes a range of consensus algorithms and the options for security and data privacy within the blockchain discussed in this article.	None
[27]	2020	A survey of the leading consensus mechanisms on blockchain solutions is done in this paper and highlights each one's properties. Additionally, it distinguishes between probabilistic and deterministic consensus procedures.	It aims to create a hybrid consensus algorithm relying on communication lines that are only partially synchronized and reaching an agreement on just allowing for one-hop neighbor voting.
[28]	2020	This survey highlights the latest studies in blockchain and consensus algorithms.	None
[29]	2020	This paper adds theory and information that may be utilized to choose an appropriate consensus algorithm. It will aid scholars in their continued study of consensus in the context of private blockchain.	To determine the actual performance indicators of the consensus employed, additional study can be conducted by adjusting the number of loads and peers and assessing it using some benchmarks.
[30]	2020	According to this article, the Byzantine consensus may need to be rethought in light of the blockchain environment, which also looks at prominent blockchain consensus algorithms.	None
[31]	2021	Presented a very detailed analysis of existing blockchain consensus algorithms.	It does not consider the attacks on consensus algorithms.
[32]	2021	It surveys the consensus algorithms being used in crypto-currencies.	It does not consider the attacks on consensus algorithm and consider only crypto-currencies.
[33]	2022	Survey on consensus algorithm for Proof of Stake (PoS)	Discussed only PoS-based consensus algorithm
[34]	2022	Presents the review of main consensus algorithms being widely used, the possible scenarios in which they can be suitable, and their relative disadvantages.	It does not consider the attacks on consensus algorithms.
[35]	2022	This paper surveys some prominent consensus algorithms, reviews the key features and parameters, and compares the presented consensus algorithms based on these.	A limited no of consensus algorithms are taken and further does not consider the attacks on consensus algorithms in detail.
Our Review	2023	Our paper conducted a detailed review of the maximum prominent blockchain consensus algorithm. It further compared these consensus algorithms based on performance and security attack criteria.	Other articles have either covered the security attacks or performance analysis but have not combined both approaches.

Recent surveys on consensus algorithms have examined the limitations and future work of various consensus algorithms. Nonetheless, there is a gap in the existing analysis of the consensus algorithm. The current literature does not provide enough criteria for a comprehensive and comparative analysis of consensus algorithms. Henceforth, this paper aims to provide a complete and detailed analysis of existing and recent consensus algorithms concerning throughput, scalability, latency, and energy efficiency. Table I present a comparative study of previous related and current research work and highlights the significance of the recent research work.

This paper also takes other factors, including attacks, Byzantine fault Tolerance, adversary tolerance, and decentralization levels. Besides comparison, this paper presents the advantages and disadvantages of consensus algorithms. The analysis results are shown in tabular formats, visually illustrating these algorithms in a meaningful way.

III. Parameter for Evaluation

This sub-division will discuss different parameters that categorize consensus algorithms [2].

A. Blockchain Type

Blockchain can be categorized into three primary classes: private, public, and consortium. These classifications are indicative of the governance structure among participants and the specific nature of the blockchain.

B. Scalability and Attacks

In decentralized systems, scalability plays a vital role. In terms of scalability, consensus algorithms are separated, like ELASTICO and Proof of Trust, but PoW is non-scalable.

C. Adversary Tolerance

It quantifies the blockchain's ability to withstand malicious operations. Additionally, it gauges the stability of the blockchain network during catastrophic events. Research has demonstrated that the consensus algorithm exhibits the highest level of tolerance towards adversaries.

D. Throughput

Throughput in the consensus algorithm means how long it takes to confirm the transactions in a blockchain network [36]. It further suggests that the extreme throughput is an absolute rate at which the blockchain can authorize transactions [37].

E. Energy Consumption

Out of the various factors or criteria that disturb the blockchain consensus algorithm's valuation is power utilization. There is a variation in consensus algorithms' energy consumption that cannot be experimentally evaluated due to varied heterogeneous limitations [38].

F. 51% Attack

A 51% attack is commonly known as an assault on a blockchain, typically targeting bitcoins, executed by a group of miners wielding over 50% of the network's mining hash rate or computational power [6]. Usually, these types of threats cannot be evaded theoretically [39]. Blockchain protocols strive to elevate the costs associated with this attack to deter it, although a complete resolution remains elusive.

G. Double Spending Attack

A double-spend is a unique problem related to digital currencies that works when one user spends the digital assets more than once [40]. Since there is no centralized authority to control transactions, the attacker will attempt to generate a regular contract to contain it in a block. Then he will try to outspread the deceitful branch of the system he had shaped until the deceitful branch is confirmed and accepted as the precise branch that consists of the fraudulent transaction [41].

IV. Review of Existing Consensus Algorithm

In simple language, the term consensus means harmony or concord. The consensus algorithm will authorize an agreement among all the nodes, thereby guaranteeing reliability and trust between the unidentified peers. The consensus algorithm also ensures that each block in the existing chain involves every peer node across the system [38]. That enables distinctness and clarity in the added processes or transactions, which defines a mutually beneficial network for every node. It is worth noting that once the block gets verified, it's practically impossible to eliminate or alter them. The consensus algorithm erases all the non-member intermediaries to guarantee the accuracy of the transaction [3]. However, once the consensus involving chain transactions obtains a global status, all nodes or peers become reliable for the blockchain structure. It eventually helps in the authentication of the untrustworthy and uncertain network associated with the self-contradictory person. However, in this part, we will present the utmost significant consensus algorithms commonly utilized in the blockchain system, with their disadvantages and benefit in general.

A. Proof of Work (PoW) [1]

It was presented by Nakamoto and later applied to Bitcoin [1]. Subsequently, this was endorsed by other cryptocurrencies, which include Ethereum, Dogecoin, Monerocoin, and last by not least, Litecoin. It has a high algorithmic cost with a clear quorum design. Hash is a difficult and random mathematical formulation used to confirm the saved operation within blocks [42]. To achieve consensus in a network, miners strive against each challenging computational puzzle. Such puzzles are challenging to solve, but the result can be promptly verified once they are solved. Once the miner found the solution to the new block, it is broadcasted to the network. In turn, all other miners will confirm and verify that the solution is accurate, and then the block may be confirmed [43][2]. The PoW algorithm's benefit is that it comes with a significant amount of security, a decentralized framework, and a permissible level of scalability. On the contrary, it has some disadvantages, including lesser throughput, high block creation time, the inadequacy of energy, dependencies on specialized hardware, high computation cost, and comprehensive bandwidth [9], [19].

B. Proof of Stake (PoS) [33]

It arose as a substitute for PoW, originally used as a consensus algorithm in blockchain technology, and was applied to validate and add new blocks to the chain. PoW requires enormous amounts of energy, which is the main reason for PoS establishment. For this reason, the authors suggested light-weighted consensus protocols for lower-power IoT communication channels [44]. PoS is based on the concept

that individuals can confirm or excavate block transactions according to how many coins they retain [45]. The miners will obtain no award besides the transaction fee in these methods. If the full node is chosen to build a new block, then the lender will gain a proportion of those operations [6].

C. Distributed Proof of Stake (DPoS) [46]

It was introduced by Daniel Larimer [47]. A key feature of this algorithm is its emphasis on decentralization. DPoS structures the network more efficiently, granting each delegate ample time to publish on every node [2]. This approach finds utility in private blockchains due to its semi-centralized characteristics. Within this method, potentially malicious miners are subject to capping based on specific parameters such as intervals and block sizes [9].

D. Practical Byzantine Fault Tolerance (PBFT) [48]

PBFT deals with the byzantine issue of the distributed nodes that can cause 33% of work damage because of chain faults. PBFT is the capability of a distributed network to reach an adequate consensus despite malignant nodes in a system failure or the broadcast of incorrect information. PBFT aims to safeguard against disastrous system failure by decreasing the effect of the malignant nodes [49]. The advantage of this method is its high throughput and energy efficiency. On the other hand, specific points like scanty or no scarce constraints quantifiable for being scalable and network delays while stating every node poll are some of its disadvantages.

E. Proof of Importance (PoI) [50]

In PoI, a miner's application-specific integrated circuit chips are deployed to enhance computing power. It works when any more family of coins has a strong possibility to mine the next block. PoI compensates users with more transactions and the user with a considerable net stake in tackling these restrictions. PoI was first established in the NEM design [50]. In PoI, each node is allocated a significant value. A node carrying out a transaction with a node with great significant worth is, in all probability, to mine the next block even though the node has less stake than another node. It is considered an improvement over the PoS algorithm [2].

F. Proof of Capacity (PoC) [51]

It was introduced in 2015 by Dziembowski. As the name implies, PoC's dynamics revolve around selecting a miner node based on the available memory capacity of an external hard disk. The node with a larger storage capacity can precompute and retain a greater number of solutions for the impending problem before actual mining begins. This approach effectively addresses the intricate challenges associated with node management within the Proof of Work framework, subsequently alleviating broader difficulties. PoC entails the strategic utilization of hard drive resources, encompassing the storage and computation of results on the hard drive prior to the commencement of the mining process.

G. Proof of Burn (PoB) [52]

This method is a substitute for attaining a deal in the blockchain network. This algorithm node in the network has to lose or scorch cryptocurrency to obtain the mining entailment to the permitted source. This method is less like Proof of Work, but the only difference is where the belongings are in the form of cryptocurrency rather than the computing power of a node. The loss of coins reflects the node's longer commitments to stay sincere in the system as it has lost real coins to increase the mining entitlement [2].

H. Delegated Byzantine Fault Tolerance (DBFT) [2]

It can be derived that DBFT monitors the conventional phases of the DPoS protocol in the start-up phase. In this method, the consensus is obtained using a superannuated BFT method by adding extra steps [2]. Here the user will vote and select members to add the new role in the chain based on bulk voting of more or equal to 66% affirmative from the members [42]. It should be noted that fault tolerance of delegated Byzantine is very rarely prone to confront delays from the PBFT, but restricting the number of votes can jeopardize the decentralization of the network [4].

I. Reliable, Replicated, Redundant, And Fault-Tolerant (RAFT) [53]

This method is a Substitute for the Paxos protocol. This method is more straightforward and, at the same time, provides safety and privacy with add-on features[2]. The consensus in this method is reached by choosing a delegate, and then this delegate will be accountable for copying the logs every time the latest user accesses the network. Heartbeat notes will operate as an interfering signal for marking the presence of the forerunner [2]. Each node will have a time-out for the signal's arrangement if it will not get the message before its lapse. After this, there will be a process of selecting the new leader, or else time will reset.

J. Proof of Activity (PoA) [54]

One more consensus algorithm, PoA, was developed by Bentov et al. in the year 2014 [55]. The authors mentioned this algorithm as a union of PoS and PoW. It is a safer algorithm countering Bitcoin's potential assaults and has even ignorable sanctions concerning the network communication and storage area. Nevertheless, through PoS structured protocols, shareholders may engage in downward price spirals; for that reason, the coins that they maintain will produce revenue commensurate to real commerce taking place [2].

K. Proof of Authentication (PoAH) [56]

It is a consensus algorithm aimed at a lightweight and sustainable blockchain for building a lightweight decentralized security system to circumvent central dependencies. PoAH is a cryptographic verification mechanism that is a replacement for the PoW algorithm. This consensus algorithm is appropriate for private and permissible blockchain and makes blockchain application-specific. Besides securing the system, PoAH maintains sustainability and scalability.

L. Proof of PUF-Enabled Authentication (PoP) [57]

It is a comprehensive algorithm that effectively manages both data and device security aspects. This innovative approach combines the utilization of physical unclonable functions (PUF), which serve as integral hardware security components. These PUFs contribute to the system's ability to offer advantages in terms of latency, scalability, and energy consumption. The mechanism involves incorporating a

cryptographic hash of all previously processed data along with the involvement of any device incapable of generating the PUF key in a uniquely generated manner within the PUF module. This integrated approach ensures the robust handling of both data and security keys. In comparison to Proof of Work (PoW), PoP demonstrates a notable increase in speed, while in contrast to Proof of Authority and Hashpower (PoAH), it exhibits a slightly elevated latency.

M. Rock-Scissors-Paper (RSP) [58]

To achieve consensus and avoid attacks by the malicious participant, this algorithm uses three balance variables: Rock, scissors, and Paper. RSP does not directly address the problem of variable difficulty; instead, it proceeds with the consensus based on the device's specification. Furthermore, computations can be performed quickly and easily using a high specification of computing devices. This consensus algorithm reduces the power utilization that is required to limit the maintenance and processing cost.

N. Proof of Research (PoR) [18]

It is a hybrid consensus algorithm that combines Proof of Stake (PoS) with Proof of BOINC (Berkeley Open Infrastructure for Network Computing). This innovative approach is facilitated by Gridcoin, a cryptocurrency that individuals can acquire through the contribution of their computational resources to the BOINC project. PoR bears similarities to PoS, allowing individuals to become investors by possessing a designated quantity of Gridcoin and engaging in the minting process.

O. Proof of Stake Velocity (PoSV) [18]

It is an innovative consensus algorithm crafted to address the challenges encountered within the Proof of Stake framework. PoSV introduces a hybrid approach that integrates seamlessly with conventional PoS algorithms. The fundamental premise of PoSV lies in the concept of stake velocity, which mirrors the concept of money velocity in economics. The core principle driving stake velocity is the augmentation of stake circulation during the PoS consensus process. Investors can actively enhance this stake flow by engaging in the consensus mechanism, thereby staking their cryptocurrency as a dynamic alternative to passively holding it offline. This strategic involvement substantially enhances the security measures and mitigates the issue of inadequate participant engagement often observed in conventional PoS systems.

P. Proof of Familiarity (PoF)[59]

This consensus algorithm is designed to integrate various healthcare stakeholders' medical conclusions. PoF guarantees stakeholders' medical results' privacy and integrity by utilizing previously-stored results using blockchain. Proof of familiarity uses a two-layer security measure to preserve the identity of stakeholders. It first stores stakeholders' identities locally, and then the hash of these are stored in the blockchain.

Q. Proof of Trust (PoT) [60]

Consensus protocol integrates a confidence dimension to satisfy the service sector's practical criteria, i.e., fixing the unfaithful activities that exist so frequently in a transparent, public service network, together with the reward steps. PoT consensus utilizes random logic algorithms to maximize block node unpredictability using time signs and digital signatures. A credibility evaluation of the crowdsourcing membership involved will be done automatically by the improved algorithm. The validity, equity, and stability can be obtained by the PoT.

R. Proof of Luck (POL) [61]

PoL is a blockchain consensus algorithm that uses a random number generator on a trusted execution environment (TEE) platform to select a consensus leader. This allows for fair mining while also enabling quick transaction validation, deterministic confirmation times, and low energy consumption, among other benefits.

S. Leased Proof of Stake (LPoS) [61]

It represents a variant of the PoS consensus mechanism. Notably employed within the Waves platform, this distinctive PoS approach facilitates token holders in "leasing" their tokens to complete nodes, thereby earning a share of the rewards. On conventional PoS networks, individual nodes contribute new blocks to the blockchain. Within the LPoS framework, users have the flexibility to actively operate a full node or alternatively lease their stake to a full node. This engagement in the LPoS ecosystem yields rewards for the participants.

Table II illustrates the comparison of various consensus algorithms on defined parameters.

TABLE II. ANALYSIS OF CONSENSUS ALGORITHMS

Consensus Algorithms	Byzantine fault Tolerance	Adversary tolerance	Decentralizatio n level	Node identity	Throughp ut(tps)	Scalability	Latency	Energy efficiency	51% Attack	Double spending Attack	Trust
PoW [62]	50%	<25%	Decentralized	Permissionless	Low	High	High	No	Vulnerable	Vulnerable	Untrusted
PoS [33]	50%	<51%	Semi-Centralized	Permissionless	Low	High	Medium	Yes	Vulnerable	Difficult	Untrusted
DPoS[46]	50%	<51%	Semi-Centralized	Permissioned	High	High	Medium	Yes	Vulnerable	Vulnerable	Trusted
PBFT[48]	<=33%	<33%	Decentralized	Permissionless	High	Low	Low	Yes	Safe	Safe	Semi-trusted
PoI[50]	50%	N/A	Decentralized	Permissionless	Low	High	Medium	Yes	Safe	Safe	Untrusted
PoC[51]	NA	NA	Decentralized	Permissioned	Low	High	High	Fair	Vulnerable	Vulnerable	Semi-trusted
PoB[52]	NA	<25%	Decentralized	NA	Low	Low	High	No	Vulnerable	Vulnerable	Untrusted
DBFT[2]	NA	<33%	Semi-Centralized	Permissionless	High	High	Medium	Yes	Vulnerable	Vulnerable	Semi-trusted
RAFT[53]	>50%	<50%	Decentralized	Permissionless	High	High	Low	Yes	NA	Safe	Trusted
PoA[54]	>50%	N/A	Decentralized	Permissionless	High	High	Low	No	Vulnerable	Vulnerable	Trusted
PoAh[56]	N/A	N/A	Decentralized	Permission-based	N/A	High	low	low	No known attacks	No known attacks	Trusted
PoP[57]	N/A	N/A	Decentralized	Permissioned	N/A	high	low	low	No known attacks	No known attacks	Trusted
PoR[18]	50%	<51%	Semi-Centralized	Permissionless	Medium	low	medium	medium	Vulnerable	difficult	Untrusted
PoSV[18]	50%	<51%	Semi-Centralized	Permissionless	high	medium	low	low	Vulnerable	difficult	Untrusted
RPS[58]	N/A	N/A	Decentralized	Permissioned	N/A	N/A	N/A	low	No known attacks	No known attacks	Trusted
PoF[59]	N/A	75%	Decentralized	Permissioned	medium	high		low	No known attacks	No known attacks	Trusted
PoT[60]	>50%	N/A	Decentralized	Permissioned	high	high	low	medium	safe	safe	trusted
PoL[61]	N/A	<25%	Decentralized	N/A	high	high	low	yes	safe	safe	trusted
LPoS[61]	N/A	<51%	Decentralized	Permissioned	high	high	high	yes	No known attacks	No known attacks	Semi-trusted

V. ANALYSIS OF CONSENSUS ALGORITHM

The foundation of blockchain rests on a secure and dependable architecture that stems from consensus mechanisms. Different consensus algorithms are applied to specific applications due to the unique demands of each domain. For instance, some domains require swift transaction processing, while others prioritize minimal computational power consumption. The consensus algorithm assumes a pivotal role within the blockchain framework. It operates on the premise that consensus is crucial to achieving unanimous agreement among network nodes during the process of block authentication [63]. The consensus algorithm strives to strike a balance among miners, assigning them equal weight to facilitate arriving at a resolution or decision by the majority of miners.

However, while this approach suits controlled environments, it proves inadequate for public blockchains as it exposes vulnerabilities to Sybil attacks. These attacks involve an individual creating multiple identities to manipulate the blockchain's functioning. In a decentralized ecosystem, a single block's addition is the responsibility of a single participant. The user selection process can be either random or based on specific criteria. Nevertheless, relying on random selection leaves the system susceptible to potential breaches.

Since blockchain is a decentralized network, no single node can handle the entire network. That is why blockchain has endorsed a distributed consensus method to implement the data's uniformity and trustworthiness [64]. PoW [62] is based on the idea that nodes are less likely to attack the network as long as they invest a significant amount of computational effort. In a PoW blockchain, miners must perform computationally intensive tasks to add a block, making it nearly impossible for Sybil attacks to occur. PoW operates through a process called mining, where nodes perform calculations until the correct result is found. In the case of Bitcoin, the mining process involves searching for a random number, or nonce, that generates the correct hash for a block header. Therefore, the miners should be able to carry out specific tasks to calculate the figure. Once the miner overcomes the issue, all the other nodes are responsible for confirming that the response is accurate. Because of the more utilization of energy in PoW, its rendering becomes ineffective in the lower-powered application. Moreover, the nodes that take part in the block's authentication shall not correspond to enhancing the transactions of a block that makes PoW non-scalable [65].

PoS-Proof of Stake creates division among its users based on stake [33]. Any node with a definite volume of stake in their blockchain could be the miner. This algorithm also reassumes that any extra stack user will be less susceptible to a network attack. When any node turns out to be a miner, it will assign a particular quantity of its stack; therefore, a network holds this volume to ensure the user is trustworthy and permissible to do the mining. PoS needs significantly less computing energy, so

Proof of Stake has a very low power utilization than PoW. The only problem with PoS is that the mining procedure always aims at its richest member because they own a more significant stake over the rest of the nodes. DPoS, or Delegated Proof of Stake, is an additional consensus method projected to improve PoS [46]. In this method, only limited members are accountable for validating the blocks rather than only transferring this responsibility to stakeholders. The main advantage of DPoS is quick transactions because fewer nodes participate. Moreover, the selected nodes are capable enough to fine-tune the size of the block and the intervals. Fraudulence can be dealt fastly since substituted nodes are replaced with ease. One more type or alternative of PoS is TaPoS (Transaction as Proof of stake) [66]. Contrary to PoS, in which only a limited number of nodes can assist the security of a network, in TaPoS, each node secures the network. The disadvantage of PoS is the accumulated stack age, although the node is not linked to the network. PoA is projected to compensate nodes based on what activity does and their network ownership [67].

PBFT is projected to aim at asynchronous situations to help in solving BG (byzantine general) problems [48]. This method presumes that beyond two-thirds, all nodes are genuine, and beneath this are malevolent. A front runner gets selected by every block of the family, and then this front runner or leader's job is to validate a block. Another alternative to the BFT is Delegated BFT (DBFT), which works like a DPoS in which only a few nodes are accountable for authenticating and generating the block. One more protocol that is quite similar to PBFT is SCP (Stellar Consensus Protocol). SCP is carried out based on a method or algorithm named FBA (Federated Byzantine Agreement) [68]. The only alteration between PBFT and PCA is that PBFT entails a contract from widely held nodes, whereas SCP depends on a subsection of the nodes, which are considered very important. Table III below presents a concise comparison based on their respective advantages and disadvantages.

TABLE III. COMPARISON OF CONSENSUS ALGORITHMS BASED ON THEIR ADVANTAGES AND CHALLENGES

Consensus Algorithms	Advantages	Challenges
PoW [62]	*Extensive power of decentralization *Extra protected network	*High drafting power (expensive) * High electricity utilization
PoS[66]	*Energy efficient & faster processing * Improved rewards & more significant stakes	*Less decentralization than PoW *Less security than PoW
DPoS[46]	*accelerated processing than PoW and PoS * Enhanced recompenses allocation and energy efficient	*More prone to attacks and is less decentralized *Affluent people control the network
PBFT[48]	*Capable of doing transactions devoid of confirmation *Substantially reduce energy	*Elevated volume of connection between nodes *Difficult in the message's authenticity and is prone to Sybil assaults.
PoI[50]	*Quick and power-efficient *no particular hardware is required for mining.	N/A
PoC[51]	*larger drive sizes	N/A
PoB[52]	*PoB enforcement can be tailored *The power of burnt coins diminishes fractionally every time a fresh block is mined	*Source waste (the burnt coins are lost) *Huge risk protocol, no coin retrieval assurance
DBFT[2]	*Provides perfect decisiveness *Quick transaction delivery	*Prone to 51% attack *Still believed centralized
RAFT[53]	*Could endure catastrophe of up to half of the nodes *Structure clarity and robustness	*Present execution can ensure liveness for one Byzantine failure
PoA[54]	*High security & low transaction fee *Eliminates 51% attack in the blockchain network	*Requires a significant number of assets in the mining phase *Participants can double-sign transactions
PoAh[56]	*Appropriate for private as well as permissioned blockchain *Maintains system sustainability and scalability	N/A
PoP[57]	*PoP is highly scalable *Runs noticeably faster, consumes fewer resources and uses less energy.	N/A
PoF[59]	*The integrity of a medical conclusion.*Privacy of participants	N/A
PoSV[18]	*Raise the overall security of the system *Counter the lack of participant issues in PoS	*Less decentralization than PoW
PoR[18]	*Faster and Energy efficient	*Less security than PoW
RPS[58]	*Efficient power consumption and economical maintenance cost.*Fast processing time	*Specification of devices can result in the polarization of the computing devices.
PoT[60]	*highly scalable*ensures the performance and consistency of the consensus process.	N/A
PoL[61]	*Extensive power of decentralization.*low-latency transaction validation.	*Attacker may confront a limited number of TEEs
LPoS[61]	*Energy efficient & faster processing *Improved rewards & more significant stakes	*Less decentralization than PoW *Less security than PoW

VI. Open Issues and Research Challenges

Some of the open issues and research challenges are emphasized in this section.

A. Overhead

Blockchain introduces significant overhead in terms of traffic, encompassing factors such as storage size, heightened implementation costs, legal compliance considerations, and deficits in information and organization. It presents a substantial challenge, particularly with regard to escalating energy consumption.

B. Cross-compliant Hybrid Alternative (CHA)

Although many providers favor creating consensus solutions based on particular use case requirements, consensus mechanisms still need to handle various requirements. As a result, the CHA class is anticipated to witness a large variety of consensus mechanisms [31].

C. Hybrid Consensus Algorithms

A single particular type of consensus algorithm frequently has more restrictions in practical application scenarios. Examples include the PoW algorithm's resource consumption issue and the PBFT algorithm's difficulty applying only to consortium and private chains, not public ones. The goal of maximizing strengths and avoiding weaknesses can thus surely be achieved by combining the advantages of multiple algorithms into one. Additionally, this offers a fresh concept and point of reference for advancing consensus algorithms in the future [34].

VII. Conclusion

Recent surveys on consensus mechanisms have analyzed the performance and application set-ups, limitations, and future work of various consensus algorithms. Nonetheless, there is a gap in the existing analysis of the consensus algorithm. This paper provides a complete and detailed analysis of current and recent consensus algorithms based on throughput, scalability, latency, and energy efficiency. Further, this paper also evaluates the consensus algorithms based on 51% attacks, Byzantine fault Tolerance, adversary tolerance, and decentralization levels. Besides comparison, this paper presents the advantages and disadvantages of consensus algorithms to understand existing research challenges clearly. This comparison also highlighted the resource requirements for choosing a suitable consensus algorithm for a resource constraint environment. The analysis results have been presented in tabular formats, visually illustrating these algorithms in a meaningful way. These evaluations reflect that PoAh, PoP, PoT, and PoI are promising approaches that have high Byzantine fault Tolerance, and no known attack has been reported till now against these consensus mechanisms. This article has further highlighted the open issues and research challenges affecting the consensus mechanism. These open issues and research challenges can be further researched in detail for future research.

References

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

[2] U. Bodkhe, D. Mehta, S. Tanwar, P. Bhattacharya, P. K. Singh, and W. C. Hong, “A survey on decentralized consensus mechanisms for cyber physical systems,” IEEE Access, vol. 8, pp. 54371–54401, 2020, doi: 10.1109/ACCESS.2020.2981415.

[3] S. Alam et al., “Blockchain-based Initiatives: Current state and challenges,” Comput. Networks, vol. 198, p. 108395, 2021.

[4] T. Aslam et al., “Blockchain based enhanced ERP transaction integrity architecture and PoET consensus,” Comput. Mater. Contin., vol. 70, no. 1, pp. 1089–1109, 2022, doi: 10.32604/cmc.2022.019416.

[5] H. Qin, Y. Cheng, X. Ma, F. Li, and J. Abawajy, “Weighted Byzantine Fault Tolerance Consensus Algorithm for Enhancing Consortium Blockchain Efficiency and Security,” J. King Saud Univ. Inf. Sci., 2022.

[6] S. M. H. Bamakan, A. Motavali, and A. Babaei Bondarti, “A survey of blockchain consensus algorithms performance evaluation criteria,” Expert Systems with Applications, vol. 154. p. 113385, Sep. 2020. doi: 10.1016/j.eswa.2020.113385.

[7] S. Alam, “Security Concerns in Smart Agriculture and Blockchain-based Solution,” in 2022 OPJU International Technology Conference on Emerging Technologies for Sustainable Development (OTCON), 2023, pp. 1–6.

[8] Y. Liu, Z. Zhao, G. Guo, X. Wang, Z. Tan, and S. Wang, “An identity management system based on blockchain,” Proc. - 2017 15th Annu. Conf. Privacy, Secur. Trust. PST 2017, pp. 44–53, 2018, doi: 10.1109/PST.2017.00016.

[9] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” in Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017, Jun. 2017, pp. 557–564. doi: 10.1109/BigDataCongress.2017.85.

[10] M. Shuaib, N. H. Hassan, S. Usman, S. Alam, N. A. A. Bakar, and N. Maarop, “Performance Evaluation of DLT systems based on Hyper ledger Fabric,” 2022 4th Int. Conf. Smart Sensors Appl., pp. 70–75, Jul. 2022, doi: 10.1109/ICSSA54161.2022.9870957.

[11] M. Shuaib et al., “Land registry framework based on self-sovereign identity (SSI) for environmental sustainability,” Sustainability, vol. 14, no. 9, p. 5400, 2022.

[12] M. K. I. Rahmani et al., “Blockchain-based trust management framework for cloud computing-based internet of medical things (IoMT): a systematic review,” Comput. Intell. Neurosci., vol. 2022, 2022.

[13] G. T. Nguyen and K. Kim, “A survey about consensus algorithms used in Blockchain,” J. Inf. Process. Syst., vol. 14, no. 1, pp. 101–128, 2018, doi: 10.3745/JIPS.01.0024.

[14] M. J. Fischer, N. A. Lynch, and M. S. Paterson, “Impossibility of Distributed Consensus with One Faulty Process,” J. ACM, vol. 32, no. 2, pp. 374–382, Apr. 1985, doi: 10.1145/3149.214121.

[15] L. Lamport, “The part-time parliament,” in Concurrency: the Works of Leslie Lamport, Association for Computing Machinery, 2019. doi: 10.1145/3335772.3335939.

[16] D. Ongaro and J. Ousterhout, “In search of an understandable consensus algorithm,” in Proceedings of the 2014 USENIX Annual Technical Conference, USENIX ATC 2014, 2019, pp. 305–319.

[17] B. Turner, “The Paxos Family of Consensus Protocols,” 2007, [Online]. Available: http://www.fractalscape.org/files/paxos-family.pdf

[18] M. S. Ferdous, M. J. M. Chowdhury, M. A. Hoque, and A. Colman, “Blockchain Consensus Algorithms: A Survey,” pp. 1–39, 2020.

[19] 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), Apr. 2019, pp. 1–6. doi: 10.1109/ICCISci.2019.8716424.

[20] S. S. Panda, B. K. Mohanta, U. Satapathy, D. Jena, D. Gountia, and T. K. Patra, Study of Blockchain Based Decentralized Consensus Algorithms, vol. 2019-Octob. IEEE, 2019, pp. 908–913. doi: 10.1109/TENCON.2019.8929439.

[21] K. Sharma and D. Jain, Consensus Algorithms in Blockchain Technology: A Survey. IEEE, 2019, pp. 1–7. doi: 10.1109/ICCCNT45670.2019.8944509.

[22] A. Meneghetti, M. Sala, and D. Taufer, "A survey on pow-based consensus," Annals of Emerging Technologies in Computing, vol. 4, no. 1. pp. 8–18, Jan. 2020. doi: 10.33166/AETiC.2020.01.002.

[23] H. Aissaoua, M. Aliouat, A. Bounceur, and R. Euler, "A Distributed Consensus-Based Clock Synchronization Protocol for Wireless Sensor Networks," Wirel. Pers. Commun., vol. 95, no. 4, pp. 4579–4600, Aug. 2017, doi: 10.1007/s11277-017-4108-4.

[24] A. K. Yadav and K. Singh, "Comparative Analysis of Consensus Algorithms of Blockchain Technology," in Advances in Intelligent Systems and Computing, vol. 1097, 2020, pp. 205–218. doi: 10.1007/978-981-15-1518-7_17.

[25] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A Survey of Distributed Consensus Protocols for Blockchain Networks," vol. 22, no. 2, pp. 1432–1465, 2020, doi: 10.1109/COMST.2020.2969706.

[26] S. Velliangiri and P. Karthikeyan Karunya, Blockchain technology: Challenges and security issues in consensus algorithm. IEEE, 2020, pp. 1–8. doi: 10.1109/ICCCI48352.2020.9104132.

[27] G. R. Carrara, L. M. Burle, D. S. V. Medeiros, C. V. N. de Albuquerque, and D. M. F. Mattos, "Consistency, availability, and partition tolerance in blockchain: a survey on the consensus mechanism over peer-to-peer networking," Ann. des Telecommun. Telecommun., vol. 75, no. 3–4, pp. 163–174, Apr. 2020, doi: 10.1007/s12243-020-00751-w.

[28] S. Alsaqqa and S. Almajali, "Blockchain Technology Consensus Algorithms and Applications: A Survey," Int. J. Interact. Mob. Technol., vol. 14, no. 15, p. 142, 2020, doi: 10.3991/ijim.v14i15.15893.

[29] S. Pahlajani, A. Kshirsagar, and V. Pachghare, "Survey on Private Blockchain Consensus Algorithms," Apr. 2019, pp. 1–6. doi: 10.1109/ICIICT1.2019.8741353.

[30] V. Gramoli, "From blockchain consensus back to Byzantine consensus," Futur. Gener. Comput. Syst., vol. 107, pp. 760–769, Jun. 2020, doi: 10.1016/j.future.2017.09.023.

[31] B. Lashkari and P. Musilek, "A Comprehensive Review of Blockchain Consensus Mechanisms," IEEE Access, vol. 9, pp. 43620–43652, 2021, doi: 10.1109/ACCESS.2021.3065880.

[32] M. S. Ferdous, M. J. M. Chowdhury, and M. A. Hoque, "A survey of consensus algorithms in public blockchain systems for crypto-currencies," J. Netw. Comput. Appl., vol. 182, p. 103035, 2021, doi: https://doi.org/10.1016/j.jnca.2021.103035.

[33] L. Ge, J. Wang, and G. Zhang, "Survey of Consensus Algorithms for Proof of Stake in Blockchain," Secur. Commun. Networks, vol. 2022, 2022.

[34] H. Xiong, M. Chen, C. Wu, Y. Zhao, and W. Yi, "Research on Progress of Blockchain Consensus Algorithm: A Review on Recent Progress of Blockchain Consensus Algorithms," Future Internet, vol. 14, no. 2. 2022. doi: 10.3390/fi14020047.

[35] A. Jain and D. S. Jat, "A Review on Consensus Protocol of Blockchain Technology BT - Intelligent Sustainable Systems," 2022, pp. 813–829.

[36] S. Bano et al., SoK: Consensus in the Age of Blockchains. 2017.

[37] K. Croman et al., "On Scaling Decentralized Blockchains," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 9604 LNCS, Springer Verlag, 2016, pp. 106–125. doi: 10.1007/978-3-662-53357-4_8.

[38] N. Chaudhry and M. M. Yousaf, "Consensus Algorithms in Blockchain: Comparative Analysis, Challenges and Opportunities," in 2018 12th International Conference on Open Source Systems and Technologies (ICOSST), Dec. 2018, pp. 54–63. doi: 10.1109/ICOSST.2018.8632190.

[39] G. Bissias, B. N. Levine, A. P. Ozisik, and G. Andresen, An Analysis of Attacks on Blockchain Consensus. 2016.

[40] S. Zhang and J.-H. Lee, "Double-Spending With a Sybil Attack in the Bitcoin Decentralized Network," IEEE Trans. Ind. Informatics, vol. 15, no. 10, pp. 5715–5722, Oct. 2019, doi: 10.1109/TII.2019.2921566.

[41] D. Dasgupta, K. Datta Gupta, J. M. Shrein, • Kishor, and D. Gupta, "A survey of blockchain from security perspective," J. Bank. Financ. Technol., vol. 3, no. 1, pp. 1–17, Apr. 2019, doi: 10.1007/s42786-018-00002-6.

[42] M. Salimitari and M. Chatterjee, "A survey on consensus protocols in blockchain for IoT networks," arXiv. Sep. 2018.

[43] C. Xu, K. Wang, and M. Guo, "Intelligent Resource Management in Blockchain-Based Cloud Datacenters," IEEE Cloud Comput., vol. 4, no. 6, pp. 50–59, Nov. 2017, doi: 10.1109/MCC.2018.1081060.

[44] S. Alam et al., "Blockchain-Based Solutions Supporting Reliable Healthcare for Fog Computing and Internet of Medical Things (IoMT) Integration," Sustainability, vol. 14, no. 22, p. 15312, 2022.

[45] I. Bashir, Mastering Blockchain: Deeper insights into decentralization, cryptography, Bitcoin, and popular Blockchain frameworks. Packt Publishing Ltd, 2017.

[46] 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, doi: 10.1109/access.2019.2935149.

[47] D. Schuh, Fabian, Larimer, "Bitshares 2.0: general overview," p. 9, 2015, [Online]. Available: https://cryptochainuni.com/wp-content/uploads/bitshares-general-overview.pdf

[48] R. Kotla, L. Alvisi, M. Dahlin, A. Clement, and E. Wong, "Zyzzyva: Speculative Byzantine fault tolerance," ACM Trans. Comput. Syst., vol. 27, no. 4, pp. 1–39, Dec. 2009, doi: 10.1145/1658357.1658358.

[49] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance and Proactive Recovery," ACM Trans. Comput. Syst., vol. 20, no. 4, pp. 398–461, Nov. 2002, doi: 10.1145/571637.571640.

[50] A. N. Nikolakopoulos and J. D. Garofalakis, "NCDawareRank: A novel ranking method that exploits the decomposable structure of the web," in WSDM 2013 - Proceedings of the 6th ACM International Conference on Web Search and Data Mining, 2013, pp. 143–152. doi: 10.1145/2433396.2433415.

[51] S. Dziembowski, S. Faust, V. Kolmogorov, and K. Pietrzak, "Proofs of Space," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 9216, Springer Verlag, 2015, pp. 585–605. doi: 10.1007/978-3-662-48000-7_29.

[52] M. Ghosh, M. Richardson, B. Ford, and R. Jansen, A TorPath to TorCoin: Proof-of-Bandwidth Altcoins for Compensating Relays. 2014.

[53] J. Sousa, A. Bessani, and M. Vukolic, "A byzantine Fault-Tolerant ordering service for the hyperledger fabric blockchain platform," in Proceedings - 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2018, Jun. 2018, pp. 51–58. doi: 10.1109/DSN.2018.00018.

[54] Parity Technologies, "Proof of Authority - POA," 2017. https://www.poa.network/for-users/whitepaper/poadao-v1/proof-of-authority

[55] I. Bentov, A. Gabizon, and A. Mizrahi, "Cryptocurrencies without proof of work," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2016, vol. 9604 LNCS, pp. 142–157. doi: 10.1007/978-3-662-53357-4_10.

[56] D. Puthal, S. P. Mohanty, V. P. Yanambaka, and E. Kougianos, "PoAh: A Novel Consensus Algorithm for Fast Scalable Private Blockchain for Large-scale IoT Frameworks," arXiv, pp. 1–26, Jan. 2020.

[57] S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: A Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in the Internet of Everything (IoE)," IEEE Consum. Electron. Mag., vol. 9, no. 2, pp. 8–16, Mar. 2020, doi: 10.1109/MCE.2019.2953758.

[58] D. H. Kim, R. Ullah, and B. S. Kim, "RSP Consensus Algorithm for Blockchain," 2019 20th Asia-Pacific Netw. Oper. Manag. Symp. Manag. a Cyber-Physical World, APNOMS 2019, pp. 1–4, 2019, doi: 10.23919/APNOMS.2019.8893063.

[59] J. Yang, M. M. H. Onik, N. Y. Lee, M. Ahmed, and C. S. Kim, "Proof-of-familiarity: A privacy-preserved blockchain scheme for collaborative medical decision-making," Appl. Sci., vol. 9, no. 7, p. 1370, Apr. 2019, doi: 10.3390/app9071370.

[60] J. Zou, B. Ye, L. Qu, Y. Wang, M. A. Orgun, and L. Li, "A Proof-of-Trust Consensus Protocol for Enhancing Accountability in Crowdsourcing Services," IEEE Trans. Serv. Comput., vol. 12, no. 3, pp. 429–445, 2019, doi: 10.1109/TSC.2018.2823705.

[61] M. Milutinovic, W. He, H. Wu, and M. Kanwal, "Proof of Luck," in Proceedings of the 1st Workshop on System Software for Trusted Execution, Dec. 2016, pp. 1–6. doi: 10.1145/3007788.3007790.

[62] N. Lasla, L. Al-Sahan, M. Abdallah, and M. Younis, "Green-PoW: An energy-efficient blockchain Proof-of-Work consensus algorithm," Comput. Networks, vol. 214, p. 109118, Sep. 2022, doi: 10.1016/J.COMNET.2022.109118.

[63] M. Du et al., "A review on consensus algorithm of blockchain," in 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Oct. 2017, vol. 2017-Janua, pp. 2567–2572. doi: 10.1109/SMC.2017.8123011.

[64] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," Futur. Gener. Comput. Syst., vol. 107, pp. 841–853, Jun. 2020, doi: 10.1016/j.future.2017.08.020.

[65] S. K. Kim and J. H. Huh, "A study on the improvement of smart grid security performance and blockchain smart grid perspective," Energies, vol. 11, no. 8, p. 1973, Jul. 2018, doi: 10.3390/en11081973.

[66] D. Larimer, "Transactions as proof-of-stake," Cryptochainuni.Com, pp. 1–8, 2013, [Online]. Available: https://cryptochainuni.com/wp-content/uploads/Invictus-Innovations-Transactions-As-Proof-Of-Stake.pdf

[67] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake," ACM SIGMETRICS Perform. Eval. Rev., vol. 42, no. 3, pp. 34–37, Dec. 2014, doi: 10.1145/2695533.2695545.

[68] D. Mazières, "The Stellar Consensus Protocol A federated model for Internet-level consensus," pdfs.semanticscholar.org, 2015.