Date of publication: April 24, 2025.

# A Review of Blockchain Rewarding Strategies and Corresponding Consensus Protocols

**Basem Assiri[1], Haitham Assiri[2], Shadab Alam[3], Shams Siddiqui[4], and Hussein Zangoti[5]**
[1,2,3,4]Computer Science Department, Faculty of Engineering and Computer Science, Jazan, Saudi Arabia, Postal Code: 82817
[5]Department of Electrical and Electronics Engineering, Faculty of Engineering and Computer Science, Jazan, Saudi Arabia, Postal Code: 82817

Corresponding author: Basem Assiri (e-mail: babumussmar@jazanu.edu.sa).

**ABSTRACT:** The development of blockchain technology has facilitated its application in many areas of life due to its ability to enable decentralization in processing and storage. To support blockchain's application in various fields, its algorithms, and consensus protocols should be developed. Nowadays, there are many consensus protocols, each of which can be applied to the appropriate field, considering the cost of each protocol. Users should be motivated to use blockchain and participate in its processes. Considering the processing, communication, and storage costs, effective reward mechanisms are necessary to compensate users and encourage participation. Therefore, this study investigates and reviews a variety of blockchain consensus protocols and corresponding reward strategies. The study analyses twenty-two consensus protocols, explaining how they work, and their advantages and disadvantages. In addition, this paper discusses the types of reward strategies, their sources, limitations, and future. According to the nature of consensus protocols, they are classified into seven categories, which are computational-based, wealth-based, behavioral-based, fairness-based, fault-tolerance-based, leader-based, and transactional-based. The study aims to provide information on the future paths of blockchain consensus mechanisms, promoting a more profound understanding of their capabilities and constraints in many situations.

**INDEX TERMS:** Blockchain, Consensus Protocols, Rewarding Strategy.

## I. INTRODUCTION

Blockchain technology has revolutionized digital transactions by introducing a decentralized, secure, and transparent ledger system. The blockchain consists of a network of nodes that share a ledger and vote on decisions. In a blockchain network, nodes verify transactions, group the valid transactions into a new block, propose the new block to other nodes, verify the new block, vote to approve it, and append it to the ledger or disapprove it. Undoubtedly, the ledger consists of a chain of all approved blocks, and every node has a consistent copy of the ledger [1]–[3]. Therefore, nodes compete for participation in such processes based on a consensus protocol.

Blockchain consensus protocols guarantee that every node in the network agrees on a single and verifiable state of the truth. Protocols are essential to the functionality and integrity of blockchain networks. For authenticating transactions, protecting the network, and preserving trust among participants, these protocols are critically important. However, the effectiveness of these protocols is influenced by two factors that have a significant impact on their success. These two factors are the nature of the application fields and the mechanisms used to reward honest participants or to punish malevolence.

Firstly, in order to support the application of blockchain in various fields, the consensus protocols should be developed and customized. There are many consensus protocols, each of which can be applied to the appropriate field. Secondly, considering the cost and to motivate proper participation, the protocols should involve reward mechanisms that compensate for the cost and motivate participants. In fact, governments need more analyses and investigations to be able to apply blockchain technologies in the areas of healthcare, education, national security, economy, and finance. For example, in 2022, the USA government required more studies and investigations to maintain its digital assets and issue the Digital Dollar [4], [5].

Therefore, in this study, a wide variety of blockchain consensus protocols have been investigated, with a particular emphasis placed on the nature of the protocol, processing cost, rewarding techniques, and punishment mechanisms employed by each protocol. In addition, the research explores the complex mechanics of reward and punishment in different consensus protocols, emphasizing their importance in preserving network integrity and trust. Indeed, the main contributions of this paper are as follows:

- **Comprehensive Analysis:** Detailed examination of the nature of various consensus protocols.
- **Rewarding Strategies:** Systematic analysis of diverse rewarding strategies to incentivize honest participation.
- **Punishment Mechanisms:** Exploration of punishment mechanisms to deter malicious behavior.
- **Efficiency:** Highlighting the main characteristics of the consensus protocols such as energy consumption, scalability, security, and fairness.

The rest of the paper is organized as follows: Section II reviews the research methodology and constraints. Section III describes various consensus protocols, advantages, disadvantages, and their rewarding strategies. Section IV presents a discussion of the implications of our findings. Finally, Section V concludes the paper and outlines some challenges and future research directions.

## II. RESEARCH METHOD

This section outlines the research method used for this research work. The primary objective of this study is to provide a comprehensive review and comparative analysis of blockchain consensus protocols and their associated rewarding strategies. Given its decentralized and distributed nature, blockchain technology relies heavily on consensus mechanisms to ensure the integrity, security, and functionality of the network. These mechanisms vary widely in design and implementation, each offering distinct benefits, challenges, and efficiencies. This facilitates blockchain application in different domains. Additionally, the rewarding strategies associated with these protocols play a crucial role in motivating participants to maintain the network's stability and security. To achieve the study's objectives, the research uses a systematic and multi-faceted framework, divided into three key stages: a literature review, an analysis of the consensus protocols, and an evaluation of rewarding strategies. Each stage was meticulously planned and executed to ensure a thorough and unbiased examination of the current state of blockchain consensus mechanisms.

The first stage involves conducting a comprehensive literature review to gather the existing knowledge on blockchain consensus protocols and rewarding strategies. The review included peer-reviewed journal articles, conference papers, technical reports, and white papers published between 2018 and 2024. Databases such as IEEE Xplore, SpringerLink, and Google Scholar were extensively searched using keywords like "blockchain consensus mechanisms," "rewarding strategies," "Proof of Work," "Proof of Stake," "Protocol History," and "Byzantine Fault Tolerance." The review aimed to identify seminal works, emerging trends, and gaps in the existing literature that this study could address. This stage also helped frame the research questions and provided the theoretical foundation for the subsequent stages.

In the second stage, the research focused on a detailed analysis of various blockchain consensus protocols and their associated rewarding strategies. This study categorized the protocols based on their underlying mechanisms. For each protocol, the research examined the operational principles, security features, scalability potential, and energy efficiency. Special attention was given to how these protocols manage the trade-offs between decentralization, security, and performance. The analysis also considered the applicability of each protocol to different blockchain use cases, ranging from cryptocurrencies and smart contracts to specialized applications like supply chain management and Internet of Things (IoT) networks [6], [7].

The final stage of the research framework involved evaluating the rewarding strategies associated with each consensus protocol. Rewarding mechanisms are critical in blockchain systems because they provide incentives for participants (such as miners or validators) to engage in activities that uphold the network's integrity and security. This stage analyzed how different protocols implement rewards through transaction fees, newly minted coins, or innovative approaches like reputation- based rewards or game-theoretical models. The evaluation also considered the effectiveness of these strategies and the use of punishment in promoting honest participation, deterring malicious behavior, and ensuring long-term network sustainability.

In short, the analysis categorized and evaluated various consensus protocols and reward strategies based on their underlying mechanisms, security features, scalability, energy efficiency, and applicability to different blockchain use cases. The following consensus protocols and reward strategies were examined in detail:

1) Proof of Work
2) Proof of Exercise
3) Proof of Space or Capacity
4) Proof of Stake
5) Delegated Proof of Stake
6) Leased Proof of Stake
7) Proof of Burn
8) Proof of Transfer
9) Proof of Authority
10) Unique Node List
11) Ripple
12) Proof of Importance
13) Proof of Reputation
14) Proof of Contribution
15) Proof of Elapsed Time
16) Proof of Fairness
17) Practical Byzantine Fault Tolerance
18) Delegated Byzantine Fault Tolerance
19) Federated Byzantine Agreement
20) Proof of Quality of Service
21) Reliable, Replicated, Redundant and Fault Tolerant
22) Directed Acyclic Graph

## III. CONSENSUS PROTOCOLS AND REWARDING STRATEGIES

This section provides an overview of various consensus protocols used in blockchain networks and the corresponding

rewarding strategies. For each protocol, we will discuss its background, operational principles, advantages, disadvantages, and the strategies used to reward participants based on their roles and contributions to the network.

### A. PROOF OF WORK (POW)

#### 1) HISTORY

PoW was introduced in 1993 by Cynthia Dwork and Moni Naor as a computational technique to combat spam emails and denial-of-service attacks. However, it gained significant prominence with the introduction of Bitcoin in 2008 by a group under the pseudonym Satoshi Nakamoto. The PoW consensus protocol was used as the fundamental method for reaching consensus in Bitcoin, and later on, it was also implemented in various other blockchain networks [8]–[10]. Moreover, Proof of Activity is another consensus protocol that enables the preparation of a blank block using PoW, so other miners can fill it out using other consensus protocols such as Proof of Stake.

#### 2) POW DESCRIPTION

PoW entails miners competing with their computational skills to solve complex mathematical puzzles. A new block of transactions must be proposed by the first miner to solve the problem; this block is then validated by the remaining miners. Miners verify that the transactions of the proposed block comply with the network's rules, such as the prohibition of double-spending. This procedure is demanding in terms of resources and computation power. PoW variants that have been modified incorporate algorithms such as SHA-256 (used in Bitcoin) and Ethash (used in Ethereum) [11], [12]. Miners combine pending transactions with other data, such as the preceding block's hash, to mine a new block, using a cryptographic hashing technique. The miner adjusts the nonce to hash data repeatedly until it satisfies a network-set diffi- culty threshold. Once a miner successfully finds a valid hash, they broadcast the new block to the network. Moreover, to validate a proposed block, upon receiving the proposed block, other miners independently verify the validity by verifying transactions and proof of work. Miners accept valid blocks and extend the blockchain from this new block [13], [14].

#### 3) ADVANTAGES AND DISADVANTAGES

Advantages

- Proven security against Sybil attacks and manipulation.
- The network is decentralized, indicating that no single entity has control over it.
- Encourages participation by providing mining rewards. Disadvantages.
- High energy consumption owing to computational de- mands.
- The network is susceptible to 51% attacks when one entity has control over the majority of the network's computational power.
- The low transaction throughput presents scalability problems.

#### 4) POW REWARDING STRATEGIES

If a miner succeeds in adding a new block to the blockchain, they are rewarded with newly minted cryptocurrency, as well as transaction fees. There is a process known as halving that takes place at predetermined intervals, and this process is responsible for the gradual reduction of the reward over time. The purpose of this falling incentive is to both regulate the rate of inflation of the cryptocurrency and to encourage early adoption of the cryptocurrency. In addition, miners may be eligible for incentives if they participate in the governance of the network or if they support particular protocol updates [15]–[18].

### B. PROOF OF EXERCISE (POX) OR (POEX)

#### 1) HISTORY

PoeX is used as an abbreviation to differentiate between Proof of Exercise and Proof of Transfer, which are also denoted as (PoX). PoeX is a consensus mechanism that was developed by researchers in the blockchain and scientific computation fields, focusing on leveraging computational efforts to solve practical scientific problems. The concept gained traction in the late 2010s, driven by academic research and discussions within the blockchain community aimed at addressing PoW's inefficiencies [19]–[21].

#### 2) POEX DESCRIPTION

PoeX is a consensus protocol that replaces PoW's typical hash-based puzzles with real-world matrix-based scientific computation problems. The choice of matrix-based problems is due to their composability and vast range of real-world applications, making PoeX a meaningful and long-term ap- proach to blockchain consensus. PoeX works as follows:

- **Task Proposals:** An employer (E) with a scientific computation problem (referred to as eXercise X) stores the problem in a highly available database (XDB) and generates a hash digest. The employer then creates an eXercise Transaction (XT) with the problem details and deposits a credit.
- **eXercise Bidding and Mining:** Miners (M) select eXercises from the XBoard, where eXercise Transactions are presented. Miners are allocated work at random to prevent collusion. They commit to resolving the problem by initiating a Deal Transaction (DT) and depositing credit.
- **Solving and Verifying:** Miners generate a hash digest (H(Y')) after solving the given problem and storing the solution in the database. Auditors then use a probabilistic verification scheme to confirm the solution. Verification results are submitted by auditors as Audit Transactions (AT).
- **Block Commitment:** The miner adds the block to the blockchain and appends references to all associated transactions to the block header after receiving a sufficient number of Passed Reports from auditors. Next, claims are made for the miner's deposited credits.

To propose a new block, miners select pending exercises from the XBoard and solve the given matrix-based problems. They then combine the solutions with additional data (such as the previous block's hash) to generate a new block proposal. After that, validators are selected through a random assignment of eXercises, which is done to prevent collusion and ensure fairness. Auditors, or verifiers, use a probabilistic verification scheme to verify the solutions once they have solved their assigned problem [19]–[21].

#### 3) Advantages And Disadvantages

Advantages

- Useful computation is provided as it redirects the computational resources to solve real-world scientific challenges, making the process useful beyond the blockchain network.
- Random task assignment and transaction shuffling reduce the possibility of collusion among miners and task providers.
- Matrix-based problems enable collaborative verification, making the approach more robust.
- Focuses on relevant computations, which reduces the consumption of energy associated with standard PoW systems.

Disadvantages

- PoeX is more complicated to develop and implement because it requires sophisticated mechanisms for managing and verifying the scientific computations.
- Verifying scientific computations introduces additional complexity and overheads compared to simpler hash-based verification.
- Participation may be restricted if miners are required to possess specialist expertise or equipment to tackle particular scientific problems.

#### 4) PoeX Rewarding Strategies

In PoeX, miners earn rewards by solving scientific problems. Once auditors have validated the solutions, rewards are credited. In which credit deposits are made by both employers and miners to demonstrate their commitment to problem's solution and verification. These credits are reclaimed after successful completion and verification. Auditors also are incentivized to provide correct verification reports. They earn credits for completed reports and are penalized for filing fake or un- successful reports. The rewards can be from transactions' fees and from other sources, such as prizes for solving some computations [19]–[21].

### *C. PROOF OF SPACE OR CAPACITY (POSPACE)*

#### 1) History

PoSpace was introduced in 2013 by Dziembowski and others. It allows miners to provide resources such as storage capacity or other hardware to serve the system. After that, Burstcoin, Storj, Chia, and SpaceMint have adapted PoSpace in their applications [22], [23].

#### 2) PoSpace Description

In blockchain technology, PoSpace, capacity or usability, offers an alternate approach, where they allow miners to provide their resources, such as storage capacity or other hardware to support blockchain processes such as transactions' validation and blocks' mining. As much as miners serve the system, they are rewarded. They are also given more chances to propose or validate a new block [22]–[24].

#### 3) Advantages and Disadvantages

Advantages

- Less power consumption.
- Enable more cooperation and decentralization.
- Having more hardware resources speeds up the mining process.

Disadvantages

- If a miner has more hardware resources, then this miner is able to control the system.
- A miner with more hardware resources, is able to attack the system and cause security threats. Additionally, if the miner soddenly withdraws the resources, the whole system may be affected and this can cause a denial-of-service issue.

#### 4) PoSpace Rewarding Strategies

In PoSpace miners are rewarded as much as the amount of storage space that they dedicate to the system. For newly joined miners with small capabilities, the rewards are increased for encouragement [25]. In other applications, the miner is rewarded if the hash value is calculated using its resources.

### *D. PROOF OF STAKE (POS)*

#### 1) History

PoS has been introduced to avoid the high computation demand of PoW. In 2012, PoS was first proposed and then it was first used in Peercoin cryptocurrency [14], [15]. After that many cryptocurrencies have used PoS, mainly Ethereum, which is one of the most important and famous cryptocurrencies that recently switched to PoS [15], [16].

#### 2) PoS Description

Using PoS, miners stake some assets to the blockchain system, and the miner who stakes the highest amount will be selected to propose a new block. Then, miners with the next highest stakes will be selected to validate the new proposed block. For example, if a miner owns 50% of the stake in the system, the chance to be selected is 50% among the other miners [17], [18], [26]–[29]. There are some versions of PoS such as Delegated Proof of Stake and Leased Proof of Stake, which will be explained later on [30].

#### 3) Advantages and Disadvantages

Advantages

- Less power consumption.
- Less computation requirements.
- Faster than a traditional mining process.
- Solves the issue of double-spending.

Disadvantages

- If a miner has more than 50% of the system stake, this miner is able to attack the system and approve illegal blocks, which is a security threat.
- The miner with the highest stake will be a target for attackers. The failure of this miner may result in security issues such as denial of service.
- There is no chance for poor and newly joined miners as they cannot compete with rich ones, while rich miners keep competing and winning. This makes them richer. The more open and inclusive the system (that includes more validators without restrictions), the less fairness in reward distribution [31].
- It encourages money stagnation because miners try not to spend money to be able to compete.

#### 4) PoS Rewarding Strategies

In PoS, the miner who succeeds in block creation or validation will be rewarded using transaction fees [17], [18]. There are two types of staking, active and passive. In active staking the miners stake an amount and try to participate in transaction and block validating. Thus, they are rewarded in response to each valid activity. However, in passive staking, the miners stake some amount to secure the system without participating. This works as an investment or staking money for interest. Therefore, they are rewarded with a specific percentage per month or per year. In some cryptocurrencies, the reward percentages are fixed, while in others the percentages vary from one day to another. One of the main strategies to secure the system is to punish miners who misbehave by cutting some of their stake or another systematic punishment designed to punish conspiring parties [17]. Some researchers apply game theory to introduce a fair reward-sharing strategy that suggests the number of participants and the number of pools to satisfy the Nash equilibrium, which imply efficiency, fairness, and security [32], [33].

### *E. DELEGATED PROOF OF STAKE (DPOS)*

#### 1) History

DPoS was first introduced by Dan Larimer in 2013. In 2015, the first application of DPoS was on the BitShares cryptocurrency, then it has been applied to many other cryptocurrencies such as Lisk, Cadano, Ark, Steem, and TRON.

#### 2) DPoS Description

DPoS is a modified version of PoS, that enables stakeholders to elect a group of miners as delegates to propose and validate blocks. Every time, some of the delegates take on the responsibility to propose and validate a block as a group. For every cycle, other delegates are selected. In case of one miner misbehaves, the other miners vote to exclude it from the group [17], [18], [26], [27]. In addition, it is suggested to delegate the node that no one else believes in, to avoid security issues [34].

#### 3) Advantages and Disadvantages

Advantages

- More decentralization compared to PoW and PoS.
- Solves the issue of double-spending.
- More security as it does not provide a clear target to attack. In addition, any delegate that misbehaves will be detected during the validation process and excluded.
- More efficient since it requires less computation and less power consumption, as the delegated validators group is a subset of the whole miners set.
- Faster than PoW and PoS as the delegated validators group is a subset of the whole miners' set.

Disadvantages

- If a miner has more than 50% of the system stake, or a group of miners cooperate and gather more than 50% of the system stake, they are able to attack the system and approve illegal blocks, which is a security threat.
- There is no chance for poor and newly joined miners as they cannot compete with rich ones, while the rich miners keep competing and winning. This makes them richer.
- Delegates can cooperate and form lobbies to control system decisions.
- Less scalability than PoW and PoS.

#### 4) DPoS Rewarding Strategies

Stakeholders practice passive staking as they stake and delegate others to validate transactions and blocks. Therefore, the stakeholders should elect the delegates who bring better rewards to everyone. In DPoS, the rewards are shared among stakeholders and delegates in different and predefined percentages. The delegates, integrate their computation re- sources to perform the task efficiently and fast, so then they can earn more rewards and share them equally or according to the provided resources portions. Moreover, rewards can be in any form of liquidity such as cash (cryptocurrencies), certificates, stakes, and others.

### *F. LEASED PROOF OF STAKE (LPOS)*

#### 1) History

Although LPoS is less popular than other consensus algorithms, it is in use by some cryptocurrencies such as WAVES and Nix. WAVES cryptocurrency was established in 2016, and it uses LPoS. Another cryptocurrency that uses LPoS is Nix which was launched in 2018 [17].

#### 2) LPoS Description

In LPoS, a miner can lease some cryptocurrencies from riches as an investment. Then, the miner stakes the leased cryptocurrencies to the system, so there is more chance to be selected as a validator [17]. When the miner validates transactions or blocks, the miner wins some rewards (from transaction fees). After that, the miners pay the lease amounts back to the lender. Indeed, the leasing process is conducted through transactions and smart contracts. Initially, a smart contract is executed to fulfill the leasing agreement. Accordingly, a leasing transaction is executed to hold the leasing amount, so the lessee can use it without changing the original ownership. At the end, another transaction is conducted to enable the lessee to pay part of the reward to

the lender. In case the lease contract is violated or the leasing period finishes, another transaction is conducted to cancel the leasing.

#### 3) Advantages and Disadvantages

Advantages

- Less power consumption.
- Less computation requirement.
- Fast mining process.
- There is a chance for poor and newly joined miners to participate since they can lease, stack, compete, and win, which eventually makes them rich.
- Solves the issue of double-spending.

Disadvantages

- If a miner has more than 50% of the system stake, this miner can attack the system and approve illegal blocks, which is a security threat.
- The miner with the highest stake will be a target for attackers. The failure of these miners may result in security issues such as a denial of service, Sybil attack, and others [34].

#### 4) LPoS Rewarding Strategies

The Lenders practice passive staking as they lend cryptocurrencies to the lessee and the lessee participates in the trans- actions' validating process. In LPoS, the rewards are the transaction fees earned by the lessee. Then the lessee pays the rent amount in the agreement to the lender.

### *G. PROOF OF BURN (POB)*

#### 1) History

PoB, initially conceptualized by developer Stuart Popejoy in 2012, has emerged as a persuasive alternative consensus mechanism in the middle of the dominance of PoW and PoS [35]. While Proof of Burn did not receive the same level of broad adoption as its competitors, it has garnered a significant amount of interest within the blockchain community. As a result of its ability to address issues regarding energy usage and network security, it has promoted exploration in a variety of blockchain projects and exchanges such as Slimcoin [17], [35].

#### 2) PoB Description

PoB is a consensus mechanism used in blockchain networks to achieve agreement on the state of the distributed ledger. It operates on the principle of burning or destroying cryptocurrency tokens as a means to gain the right to mine or validate blocks within the network. PoB takes a different approach to consensus mechanisms like PoW and PoS, which need processing power or cryptocurrency stakes. PoB participants transmit their Bitcoin tokens to an "unspendable" address to burn them. The irreversible practice of burning tokens shows commitment and involvement in the blockchain ecosystem. In the beginning miners "burn" a specified quantity of cryptocurrency by exchanging it for an address from which it is impracticable to retrieve or spend. Burning tokens allows participants to propose or validate blocks and act as proof of their investment or commitment to the network. The method used to choose which blocks to validate can differ from one PoB implementation to another, but it usually considers things like the total number of tokens burned and for how long they have been burned [17], [35], [36].

#### 3) Advantages and Disadvantages

Advantages

- Provides an alternative to energy-intensive PoW and capital-intensive PoS.
- Burning tokens promotes a long-term commitment to the network and can help with network security.
- The token supply is reduced, which could lead to an increase in scarcity and value.
- Initial token holders may have a significant advantage, as they can afford to burn tokens without affecting their overall holdings.

Disadvantages

- Lacks widespread acceptance and established precedents compared to other consensus mechanisms.
- Finding the right burning rate or criteria for participation might be challenging and susceptible to manipulation.

#### 4) PoB Rewarding Strategies

Participants in PoB do not receive newly minted tokens as a direct reward for validating blocks. Conversely, they are granted the privilege of participating in block validation and have the potential to accrue transaction fees or other incentives produced by the network. Moreover, as a result of diminished supply and heightened scarcity, the increased value of the remaining tokens may indirectly benefit the participants [35], [36].

### *H. PROOF OF TRANSFER (POX)*

#### 1) History

PoX is a relatively newer concept in the realm of blockchain consensus mechanisms. Although no one individual or organization is credited with its creation, PoX has steadily gained popularity in discussions aiming at improving the efficiency and sustainability of blockchain networks. PoX has provided innovative ways to consensus that tries to solve the challenges and limitations given by existing protocols. Despite the lack of a clear debut date, PoX has emerged as a focus point of research and study within the blockchain community, indicating its potential to influence the future growth and evolution of blockchain technology [37], [38].

#### 2) PoX Description

A blockchain network can reach consensus through the use of PoX, which is a modified version of PoB. This method requires miners to transfer cryptocurrency as collateral in order to propose a new block or to take part in the process of block validation. PoX transfers cryptocurrency to another user instead of burning it (as in PoB). The transfer process can be part of any trading or exchange process. Miners are selected based on transferred tokens, reputation, and network performance. The selection process aims to achieve a balance between computational effort (similar to PoW) and economic stake (similar to PoS) [37], [38].

#### 3) Advantages and Disadvantages

Advantages

- Potentially more energy-efficient than PoW by reducing the computing power consumption.
- Promotes long-term network commitment through token stakes (burns) as collateral.
- Aligns the economic incentives with network security and consensus, similar to PoS.

Disadvantages

- Balancing computational effort and an economic stake through implementation complexity.
- Potential centralization if a few entities accumulate significant staked tokens.
- Limited real-world acceptance and testing compared to existing consensus mechanisms.

#### 4) PoX Rewarding Strategies

In PoX, participants are typically rewarded with transaction fees and possibly newly minted tokens for successfully validating blocks. Depending on the particular implementation of PoX and the regulations that are established by the blockchain network, the precise strategy for rewarding may be different from one instance to another. Participants who stake tokens also have the potential to earn rewards based on their stake and participation in block validation [37], [38].

### *I. PROOF OF AUTHORITY (POAUTH)*

#### 1) History

The term PoAuth was first introduced and popularized by Gavin Wood, co-founder of Ethereum, around 2017. It was initially conceived as part of Ethereum's broader exploration of consensus mechanisms beyond PoW, which was seen as too energy-intensive and slow for certain types of applications [39], [40]. Nowadays, PoAuth is ideal for applications that require high throughput and quick consensus and where the integrity of validators can be reliably assured. It's commonly used in corporate environments, inter-bank settlements, sup- ply chain management, and other applications where efficiency and speed are more critical than absolute decentralization [41]–[43]. Another shape of PoAuth is Proof of Medical Trust (PoMT), which helps in finding trusted miners in healthcare systems [44].

#### 2) PoAuth Description

PoAuth is a groundbreaking consensus mechanism that emerged as an innovative alternative to the more traditional PoW and PoS. It was specifically tailored to meet the needs of networks seeking efficient transaction processing and reduced computational overhead. PoAuth has been particularly appealing in the context of private and consortium blockchains. These are environments where all participants are known and vetted, reducing the need for a trustless system. PoAuth offers these networks a way to maintain high through- put and quick consensus without the computational waste and energy costs [39], [40]. PoAuth is a consensus mechanism used in blockchain networks where transactions and blocks are validated by approved accounts known as "validators." These validators are often chosen based on their reputation and reliability, which is crucial since the system's integrity heavily depends on their honesty and ethical behavior. The validators in a PoAuth network are pre-selected based on their reputation and trustworthiness. They are often known entities such as companies or individuals who have undergone identity verification and are considered reliable. According to this reputation, validators are ranked and so they are selected to propose or validate new blocks. Validators who have the same rank are ordered randomly or in a fixed way based on the network's configuration Since the validators are trusted entities, this process is generally quicker and does not require multiple confirmations as in other systems [36], [45]–[48].

#### 3) Advantages and Disadvantages

Advantages

- PoAuth is more efficient than PoW and PoS, as it allows for faster transaction processing since only a few trusted validators are involved in the consensus process, eliminating the need for complex problem-solving.
- PoAuth operates with a much lower energy footprint since it relies on the authority and identity of its validators rather than mining.
- More scalability with fewer nodes required to reach consensus. PoAuth networks can handle more transactions per second compared to PoW, making it more scalable for certain applications.
- Less susceptible to 51% attacks [49], since validators are pre-selected and trusted entities, which are a significant threat in decentralized PoW and PoS systems.
- Operating a PoAuth requires significantly less capital in terms of hardware and ongoing energy costs compared to PoW, making it a cost-effective solution for many businesses and organizations.
- Suitable for permissioned blockchains, where the environment is controlled and the validators are known entities, which aligns well with organizational use cases requiring privacy and internal control.

Disadvantages

- Centralization risks as PoAuth inherently involves a smaller number of validators, which can lead to centralization, potentially undermining the decentralized ethos of blockchain technology.
- The effectiveness of PoAuth is heavily dependent on the trustworthiness of its validators. If validators act maliciously or collude, the integrity of the entire network can be compromised.

#### 4) PoAuth Rewarding Strategies

PoAuth achieves consensus when a validator's block is accepted by other nodes in the network. Given the trust-based model, PoAuth can offer immediate finality (reward); once a block is created and accepted. It rewards authorities for certifying and ordering transactions. In PoAuth, the validators are rewarded according to the reputation and trustworthiness score, which reflects their rank in the authority group [48]. The reputation score increases and decreases based on the nodes' behaviors, which changes the nodes' ranks existence in the authorized group.

### *J. UNIQUE NODE LIST (UNL)*

#### 1) History

The concept of UNL is integral to Ripple's consensus mechanism, introduced by Ripple Labs during Ripple's inception. Ripple Labs and its founding members, including Jed Mc- Caleb and Chris Larsen, were instrumental in conceptualizing and deploying UNL [50], [51]. In which selected trusted nodes are listed in UNL, which process transactions. Proof of Vote is another form of UNL, where the miners who belong to different sections of the consortium blockchain are able to reach a consensus through a voting mechanism [52].

#### 2) UNL Description

The use of UNL enhances trust by requiring validation from a trusted set of nodes. Thus, the UNL consensus mechanism ensures that transactions are accurately verified and agreed upon by a majority of nodes in UNL. In UNL validators verify transactions, group them, and send them as proposals to other validators. Then, validators compare their validated group with other groups and vote on the overlapping transactions. If a transaction receives enough votes (by 50% of the validators), it proceeds to the next round. The round continues until the transaction receives more than 80% of the votes. This process ensures that the transactions are validated by multiple trusted nodes, leading to a highly secure and reliable network

Advantages

- Fast validation, since the transactions are validated only by some of the UNL nodes.
- Low transaction fees.
- Suitable for a large-scale network.
- Strong scalability as more transactions can be validated efficiently.
- Suitable for a private or consortium blockchain.

Disadvantages

- Not realistic for public blockchain as it has less decentralization since Ripple depends on a UNL.
- High connectivity requirements.
- Security issues like the UNL can misuse the control over decisions.

#### 3) UNL Rewarding Strategies

Since the main application of UNL is financial payment gateways, the protocol gets timeout in a few seconds as part of the secure payment, which does not require much effort in comparison to PoW for example. Therefore, transaction fee is enough to be used as a reward.

### *K. RIPPLE*

#### 1) History

In 2004, Fugger introduced RipplePay for digital payment and exchange. In 2014, Ripple used to produce XRP cryptocurrency [53].

#### 2) Ripple Description

RippleNet provides many mechanisms and financial procedures such as a specific consensus ledger, transaction protocol, and structure network. The ripple network includes a large number of validators who validate transactions, then they are grouped into a candidate set. On the other hand, a group of trustworthy validators which is called Unique Node List (UNL) is elected. Each member in the UNL validates transactions, groups them into its candidate set, and sends them to all other nodes. These nodes compare their own candidate sets with others. If the transaction is validated by 80% of nodes, it is added to the new block, and the new block is linked to the ledger [26], [53].

#### 3) Advantages and Disadvantages

Advantages

- Fast validation, since the transactions take 3 to 5 seconds to be validated.
- Low transaction fee.
- Scalable as more transactions can be validated efficiently.
- The Ripple platform supports many other currencies for exchange and cooperates with other financial bodies.

Disadvantages

- Less decentralization since Ripple depends on a UNL.
- Security issue as the UNL can misuse their control over decisions.
- The platform is affected by the process of supply and demand, which will be reflected in the price of the cryptocurrency.

#### 4) Ripple Rewarding Strategies

Ripple is used in XRP cryptocurrency, where the system is pre-mined, so there is an amount of cryptocurrency before the system is launched. These pre-mined coins are used as financial reserves in the system. Now, each transaction has a transaction fee that is added to the system reserve. From the reserve, the system distributes rewards to truthful validators [19], [53].

### *L. PROOF OF IMPORTANCE (POI)*

#### 1) History

PoI is a consensus mechanism that was developed to address some of the limitations seen in other consensus models. In 2015, PoI was introduced primarily by the NEM (New Economy Movement) blockchain platform, which sought to create a more equitable and active blockchain ecosystem. NEM's developers aimed to design a platform that was not only efficient and scalable but also one that incentivized active participation and contribution to the network rather than just the passive holding of assets. The developers of NEM noticed that in PoS systems, the richest holders of the currency often have disproportionate control over the network, potentially leading to centralization issues. PoI was developed as a solution to this problem by considering not just the amount of currency held (stake) but also the activity level of the participants (im- portance) [54], [55]. PoI is most suitable for social networks, reward systems, investment, and gaming.

#### 2) PoI Description

PoI seeks to address some of the limitations of earlier consen- sus models. It was developed to encourage not only

investment in the network but also active participation. The core of PoI is the importance score, which determines a node's ability to add new blocks to the blockchain. This score is calculated based on several factors, including:

- Vesting of coins: A certain number of coins must be held in the account for some time, transitioning them from a balance to a vested balance. The more coins a node has vested, the higher its potential importance.
- Transaction partners and volume: PoI encourages users to transact with others rather than just holding funds. It assesses the net amount transferred over time and the diversity of transactions involving different accounts. This means that transferring funds to different users in the network positively affects a user's score.
- Overall network activity: The individual's transaction activity is evaluated in the context of the total network activity, ensuring that their importance score reflects both personal and network-wide engagement [37].

Accordingly, nodes with higher importance scores are more likely to be chosen to create the next block and validate the proposed ones [54]–[56].

#### 3) Advantages and Disadvantages

Advantages

- It encourages active participation, not just holding tokens but also conducting transactions, which helps to maintain a vibrant and healthy blockchain ecosystem.
- PoI is an energy-efficient protocol, as it does not require intensive computational work to mine new blocks.
- It reduces the wealth concentration by taking into account factors such as transaction frequency and diversity in addition to the balance held. PoI helps to mitigate the "rich-get-richer" problem which is common in PoS systems.
- It supports decentralization by valuing contributions like transaction volume and diversity. PoI supports a more decentralized network structure, reducing the risk of centralization around a few wealthy nodes.
- Enhances network security since active participation is required by PoI to contribute to network security, as a higher number of engaged users increases the network's resilience against various types of attacks, including double-spending.

Disadvantages

- PoI's effectiveness depends heavily on high levels of network activity. In quieter networks with fewer transactions, it can be harder for participants to improve their scores, which may lead to stagnation.
- New participants with lower balances and fewer network connections may find it challenging to increase their importance score, which can create an entry barrier and potentially discourage new users from joining the net- work.

#### 4) PoI Rewarding Strategies

In PoI, nodes work to improve their importance scores, by being active in the network, processing more transactions, processing large and frequent transactions, and cooperating with other accounts. All of these operations are rewarded which increases the node's PoI score. Having a higher PoI score enables a node to issue a new block and it will be rewarded by getting all of the transaction fees for these transactions within the new block [37], [55], [56].

### *M. PROOF OF REPUTATION (POR)*

#### 1) History

PoR was introduced by Zhuang et al. in 2019 as part of the effort to improve consensus mechanisms by leveraging node reputation to achieve higher efficiency and security in blockchain networks [57], [58].

#### 2) PoR Description

PoR is a way to reach consensus in blockchains using reputable nodes participating in the network. The nodes' reputations are usually calculated based on a trust score associated with each node. This score is updated, for instance, after a node generates a new block or verifies a transaction [57]. In general, a node with a high reputation score can propose a new block and the next nodes with high reputation scores can validate the block and participate in the consensus process [58]–[60].

#### 3) Advantages and Disadvantages

Advantages

- PoR improves the transaction rates in a reputation-based environment due to the existence of trust that can expedite the verification process.
- Fairness of the miner selection process.
- Motivates nodes to be active in the network.

Disadvantages

- One significant limitation of reputation-based consensus is the necessity for a trusted or permissioned environment. This restricts the system's applicability in open, decentralized networks where trust is not pre-established.
- Enhancing throughput in permissionless blockchains remains a challenge due to the reliance on reputation systems. These systems may struggle to scale efficiently in a fully decentralized and open setting which can lead to potential bottlenecks.

#### 4) PoR Rewarding Strategies

An example of the rewarding strategy in PoR is as follows: upon the successful creation of a new block, a fixed reward is distributed among all consensus participants where each node receives a portion of the reward proportional to its reputation [56], [60]. The rewards can be from transaction fees.

### *N. PROOF OF CONTRIBUTION (POC) OR (POCO)*

#### 1) History

In 2021, PoC is a consensus mechanism designed to recognize and reward various forms of participation in a blockchain net- work. PoC represents a more holistic approach to blockchain consensus mechanisms, focusing on a variety of contributions made by the network participants rather than solely on their computational power or financial stake. PoC is particularly relevant in environments where

collaborative efforts and di- verse forms of participation are key to the network's success and sustainability [61]. It is suitable for social networks, community governance platforms, collaborative development platforms, educational platforms, and academic research.

#### 2) PoC Description

The first step in implementing PoC is to clearly define what constitutes a valuable contribution to the network. This can include code development, network maintenance, community engagement, content creation, and even active participation in governance or decision-making processes. Then, contributions must be measurable and verifiable. This often involves the implementation of systems or protocols that can automatically track and verify contributions, such as smart contracts that log activities and their outcomes. In some cases, peer review or community voting might be used to assess contributions that are not easily quantifiable. Once contributions are tracked and verified, their value needs to be calculated. This calculation can be based on predefined metrics that may weigh different types of contributions according to their perceived value to the network. For example, fixing a critical network bug might be valued more highly than writing a community blog post. For block creation and validation, participants with higher scores are more likely to be chosen to create the next block or validate it. In general case, the proposed block is broadcast to the entire network, ensuring that all network participants or nodes have an opportunity to review and validate its contents [59], [62].

#### 3) Advantages and Disadvantages

Advantages

- Encourages diverse participation, since PoC incentivizes a wide range of contributions, not just the monetary or computational, encouraging participants to contribute in various ways such as development, governance, content creation, and community support.
- Fostering a culture of contribution can strengthen community bonds and increase the collective commitment to the network's success.
- More decentralization.
- PoC is flexible and adaptable as the criteria for valuable contributions can be adjusted based on the network needs and goals.
- Enhances network security and resilience.

Disadvantages

- Complexity in term of value measurement.
- PoC results in a high administrative overhead for monitoring, validating, and rewarding various types of contributions.
- Focusing on measurable contributions might lead participants prioritizing activities that are explicitly rewarded, potentially neglecting other important but less tangible aspects of network participation.

#### 4) PoC Rewarding Strategies

PoC emphasizes rewarding participants based on their contributions to a blockchain network. This approach is designed to encourage a variety of valuable activities that sustain and enhance the network. The functioning of PoC can be complex, as it involves multiple dimensions of contribution and often requires sophisticated systems to assess and reward these contributions. In fact, based on the calculated value of these contributions, the participants are rewarded. These rewards can be in the form of cryptocurrency, increased voting power, reputation scores, or other benefits designed to incentivize continued participation and investment in the network. The PoC system often includes mechanisms for continuously adjusting how contributions are measured and rewarded. This adaptability helps ensure that the system remains fair and relevant as the network's needs and the external environment change [61], [62].

### *O. PROOF OF ELAPSED TIME (POET)*

#### 1) History

Proof of Elapsed Time (PoET) is a consensus mechanism primarily developed and popularized within the context of permissioned blockchain networks. In 2016, PoET development was closely associated with Intel, one of the world's lead- ing technology companies, which designed PoET to lever- age specific hardware features for security and efficiency in blockchain operations. PoET was introduced by Intel as part of its Sawtooth Lake blockchain platform, which is now part of the Hyperledger consortium under the Linux Foundation. This platform was designed to cater to enterprise-level blockchain applications, focusing on scalability, security, and ease of integration with any existing systems [27], [39].

#### 2) PoET Description

The Proof of Elapsed Time (PoET) consensus mechanism is designed to provide a fair and energy-efficient method for achieving consensus within a blockchain network, particularly in permissioned or enterprise settings. It leverages trusted execution environments (TEEs) to ensure that the process is secure and resistant to manipulation. Initially, each participating node in the blockchain must have access to a TEE, such as Intel's Software Guard Extensions (SGX). The node sets up its environment within this secure enclave to initiate the PoET process. Now, inside the secure enclave, a random wait time is generated for each node. This wait time is the key element of PoET; it determines how long a node must wait before it is eligible to propose a new block. The wait time is generated in a way that ensures it cannot be predicted or influenced by external factors or the nodes themselves. Therefore, each node enters a sleeping state for the duration of its assigned wait time, consuming minimal energy. Once a node's wait time expires, it wakes up and claims the right to propose a new block. The node then creates a block and includes in it a special PoET certificate that proves it has indeed waited for the designated time. Moreover, other nodes verify the PoET certificate attached to the new block. They check that the certificate is valid and that the waiting time was adhered to, confirming that the block was proposed fairly. This process relies on the inherent

security of the TEE, which is designed to be tamper-proof [63]–[65].

#### 3) Advantages and Disadvantages

Advantages

- PoET minimizes energy consumption by eliminating the need for extensive computational efforts and competition, relying instead on a time-based mechanism.
- Fairness in block creation is guaranteed since every participating node has an equal chance of being selected to forge the next block. Selection is based on randomly assigned wait times, promoting fairness across the network [55].
- Low resource requirement, since it does not require solving complex mathematical puzzles. PoET can be run on devices with lower computational power, making it ideal for IoT devices and networks with varied hardware capabilities.
- PoET enhances scalability as it can handle more nodes without significant impacts on performance.
- PoET reduces the possibility of centralization because PoET's random timer system does not inherently favor nodes with more powerful hardware.
- Cost-effectiveness is achieved by reducing the need for high-end hardware and energy consumption [55], [66].

Disadvantages

- Dependence on TEEs as PoET's security and effectiveness heavily rely on the integrity of secure hardware such as Intel's SGX. Any vulnerabilities in this hardware could compromise the entire network [67].
- Limited to specific hardware, since PoET operates on the premise of using trusted execution environments, it is constrained to platforms that support these environments, limiting the diversity of the hardware that can participate in the network.
- Despite reducing computational costs, the initial setup and maintenance of secure hardware environments can be costly and complex, particularly for smaller organizations and individual participants.
- Hardware failure risks, since the dependence on hardware functionality means that hardware failures could lead to significant issues within the blockchain, including downtime or a loss of consensus capability [67].

#### 4) PoET Rewarding Strategies

PoET provides a fair chance for every node to propose and validate blocks. Therefore, the nodes are fairly rewarded. In addition, PoET gives nodes a chance according to their reputation score. The reputation score increases and decreases based on the nodes' behaviors.

### *P. PROOF OF FAIRNESS (POF)*

#### 1) History

PoF is a consensus protocol proposed in 2024. It applies an auction-based model within consensus protocol to maintain both the system budget and the reward system [68].

#### 2) PoF Description

PoF is an auction-based consensus protocol, where the auctioneer system first determines the transaction's processing cost and time limit. The miners bid the rewards they expect to propose a new block of transactions according to the auctioneer's conditions. The reverse auction is applied, and the miners are ordered ascendingly according to their beds, The winner will be the one who can perform the task with minimum reward. The next x nodes in the ascending-ordered list are selected to validate the proposed block. This gives a chance to every node in the system because some tasks are doable [68].

#### 3) Advantages and Disadvantages

Advantages

- More fairness.
- There is a chance for poor and newly joined miners to participate in the doable tasks.
- Powerful nodes participate in difficult tasks and get fair rewards.
- The miner selection process and reward system are dynamic.
- Flexible rewards maintain the system budget.

Disadvantages

- Less decentralization as the auctioneer system controls part of the mechanism.
- The security of the bidding strategy is vital.

#### 4) PoF Rewarding Strategies

In PoF, miners are rewarded with transaction fees. The rewards should be greater than the transaction's processing cost. The miners bid the rewards they expect to propose a new block of transactions. If the miner wins proposing or validating a new block, they will be rewarded with the same amount bid. The system will not exceed the cost margin thresholds [68].

### *Q. PRACTICAL BYZANTINE FAULT TOLERANCE (PBFT)*

#### 1) History

PBFT is a committee-based consensus protocol that was developed in 1999 by Castro and Liskov [69]. It was designed to address the limitations of the earlier Byzantine Fault Tolerance (BFT) protocols by offering improved performance and practicality for real-world applications.

#### 2) Description

The PBFT protocol consists of three phases to tolerate faults and commit to transactions (in a block). The phases are (PrePrepare, Prepare, and Commit). In Pre-Prepare, a node can validate transactions and broadcast a new block of the validated transaction to all network participants for voting. The next phase is Prepare, in which the nodes vote on the new block. In the Commit phase, the block is committed and added to the blockchain when the number of in-favor votes exceeds a desirable threshold (mostly two-thirds of the votes) [70], [71].

#### 3) Advantages and Disadvantages

Advantages

- Nowadays, the PBFT consensus protocol is extensively adopted as the leading consensus protocol in blockchains.
- Enhancing security, efficiency, throughput, and reducing confirmation delays compared to other major blockchain consensus protocols.

Disadvantages

- The PBFT communication complexity (especially as the network size grows), scalability, and fault tolerance issues limit its business application [72]–[74]

#### 4) Rewarding Strategies

The PBFT can integrate various incentive mechanisms to encourage node participation and honest behavior in the network. This can include transaction fees or external reward systems depending on the specific application [75].

### *R. DELEGATED BYZANTINE FAULT TOLERANCE (DBFT)*

#### 1) History

Based on the PBFT protocol, the NEO Blockchain project proposed the DBFT consensus algorithm in 2014, made by Da Hongfei and Erik Zhang [76]. The DBFT elects trusted nodes to achieve consensus which can enhance scalability and efficiency in high-volume transactions smart contracts.

#### 2) DBFT Description

The DBFT was originally developed for the NEO Blockchain project which aims to achieve faster confirmation time for block and transactions by selecting a set of validators through real-time blockchain voting. A set of validators is delegated to validate transactions and blocks instead of all nodes. The delegates follow the same phases that are mentioned in PBFT. In March 2019, an enhanced version, DBFT 2.0, was released to improve both the robustness and safety of the blockchain by integrating a three-stage consensus process with the addition of a recovery mechanism. A third version of DBFT 3.0 was proposed which includes an additional consensus phase (totaling four phases: PrepareRequest, PrepareResponse, Pre- Commit, and Commit). In PrepareRequest, a delegated node sends a new proposed block to the other delegates. In PrepareResponse, the delegates validate the proposed block and vote. In Pre-Commit, the delegates count the votes and confirm the final decision with others. In the Commit phase, the majority confirms the final decision. Pre-Commit is added to enable rolling back before committing [76], [77].

#### 3) Advantages and Disadvantages

Advantages

- Achieves faster block and transaction confirmation times due to its efficient validator selection process [24].
- Less power consumption and fewer computations.

Disadvantages

- Centralization risk as nodes need to establish a trust relationship between them, which may reduce blockchain decentralization.
- The centralized behaviors can result in security threats.

#### 4) DBFT Rewarding Strategies

The DBFT employs a rewarding strategy or an incentive model that consists of transaction fees and network fees. These fees are distributed as follows: 10% for the NEO holders who have completed a transfer or voting, 10% to the committee and consensus nodes for managing and governing the Neo network, and finally 80% for voters who successfully vote [76].

### *S. FEDERATED BYZANTINE AGREEMENT (FBA)*

#### 1) History

FBA was introduced by Mazieres in 2015 as part of the Stellar Consensus Protocol (SCP) project to achieve worldwide con- sensus asynchronously. In addition, Ripple and UNL share similarities with FBA, in term of having a trusted list and validation process [78].

#### 2) FBA Description

Rather than relying on global majority voting or agree- ment, each participant in the SCP identifies a list of important other participants, who are sufficient enough to validate transactions or reach an agreement. Then, the nodes accept the decision of the trusted nodes when the agreement reaches a quorum or quorum slice. A quorum is the minimum number of trusted nodes that should agree on the block to commit it. FBA also uses quorum slices, which is a subset of a quorum, that convince others to agree based on trust [78].

#### 3) Advantages and Disadvantages

Advantages

- SCP can feature decentralized control, low latency, flexible trust, and asymptotic security.
- Avoids central authority, achieves consensus in seconds, trusts any desirable party, and applies hash and digital signatures for security.

Disadvantages

- The safety of the SCP depends on the nodes selecting sufficient quorum slices because of misconfiguration risks and unethical financial behavior by users.
- Transaction delays due to filtering where performance and latency are not optimal.
- If all nodes leave simultaneously, the system requires a consensus reset which may need central coordination.

#### 4) FBA Rewarding Strategies

When FBA was introduced, the rewarding strategy did not exist. Hence, it was criticized for its safety and the lack of incentives [79]. In a recent work proposed by [80], they implemented a fair reward distribution based on Cooperative Game Theory (CGT) that distributes rewards based on a node's contribution. Although the paper does not specify the kind of rewards, their goal was to show that FBA is compatible with incentives.

### *T. PROOF OF QUALITY OF SERVICE (PROOF OF QOS)*

#### 1) History

Proof of QoS is a leader-based mechanism, that was first men- tioned in a work published in 2019 by a team of

researchers led by Bin Yu and Joseph Lui [81]. It has recently been used to integrate blockchain, cloud computing, and edge computing [81], [82].

#### 2) Proof of QoS Description

Proof of QoS is centered around the concept of quality of service (QoS). Based on QoS, the collection of sub-regions nominates a leader. After that BFT initiates the election process. This consensus protocol enables throughput and the fairness property is considered among all participants. The system is divided into four regions, where each region has three miners. To elect the representative of a region, minors in the subregions suggest four candidate nominations. The nominated miners share the transactions and apply PBFT. Additionally, the nominated nodes send the new block to the region. The remaining nodes verify the identity of the minor and they validate the correctness of the block attach the new block to the ledger, and proceed further [81], [82].

#### 3) Advantages and Disadvantages

Advantages

- High transaction throughput.
- Fairness among all nodes.
- Openness.

Disadvantages

- Can't deploy in high-performance infrastructures.
- It suffers from centralization and security issues as it is a leader-based mechanism.

#### 4) Proof of QoS Rewarding Strategies

In Proof of QoS, the committee members claim rewards from proposed blocks. Nodes with similar QoS factors and probability claim the reward and provide fairness among the nodes. The rewards mechanism of the leader-based mechanism and PBFT can be applied to Proof of QoS.

### *U. RELIABLE, REPLICATED, REDUNDANT AND FAULT TOLERANT (RAFT)*

#### 1) History

RAFT is an alternative to the Paxos consensus algorithm that was introduced in 1989 by Leslie Lamport. The Paxos consensus algorithm enables reaching consensus within a distributed system while some participants experience periodic failure and communication issues. RAFT is a leader-based mechanism that was introduced by Diego Ongaro and John Ousterhout, in 2014 and has been used for both consortium and private blockchain. RAFT is widely used for managing replicated logs, such as databases and container orchestration systems [83], [84].

#### 2) RAFT Description

In RAFT a group of nodes agrees upon a state or single value of the system. Indeed, RAFT is one shape of leader-based algorithms, where all nodes agree on the same sequence for the logging data. The leader has a record of logs, all nodes act to follow the same logging record of the leader. Therefore, a node is considered to be a successful validator, when the logs in the majority of nodes are replicated in its logging record. Indeed, to create a new block, the leader selects a miner to propose the new block. This miner is the one that replicates the leader's logs records the most. Then, all nodes validate the proposed block, and the leader promotes agreement based on the log replication regarding block validation [83]–[85]. This also requires to application of a secure data sharing scheme [86].

#### 3) Advantages and Disadvantages

Advantages

- Easy to implement.
- Enhances understandability and reduces the number of states.
- Stronger degree of coherency.
- Suitable for fault tolerant systems.

Disadvantages

- Cost of additional mechanisms and complexity.
- Raft's log entries flow in only one direction, outward from the leader, which affects decentralization.

#### 4) RAFT Rewarding Strategies

In RAFT, rewarding strategies can be implemented at a higher level in systems built on top of RAFT. Developers can design and implement their reward mechanisms based on the specific requirements of their application. For example, leaders should be rewarded according to how much they can maintain system consistency and reach consensus, while followers should be rewarded according to how much they replicate the leader and the majority [87].

## *V. DIRECTED ACYCLIC GRAPH (DAG)*

#### 1) History

DAG's application in cryptocurrency gained prominence with projects like the Internet of Things Application (IOTA), which debuted in 2015 on the NXT platform. The specific application of DAG to cryptocurrencies does not have a single inventor and instead evolved through multiple projects. DAG is a variant of Distributed Ledger Technology (DLT) that pro-vides enhanced decentralization, less energy consumption, and faster transactions. Compared to traditional consensus mechanisms, DAG is adopted by many projects due to its user-friendly hosting solutions. For different kinds of hierarchy, DAG has some modified forms such as BlockDAG and UL-Block [88]–[91].

#### 2) DAG Description

DAG employs the idea of directed acyclic graphs where trans- actions are considered as graph vertices and the edges repre- sent the dependency between transactions. The transactions can be validated simultaneously and added to the graph. The dependent transactions will be connected by edges as they are validated one after the other. In DAG, the validated transac- tions are added directly to the chain (graph) in a specific order, and there is no need to compete to create a block [88], [89].

#### 3) Advantages and Disadvantages

Advantages

- High scalability and connectivity.
- High throughput as no mining process is required.
- Low transaction fees.
- Solves the double spending issue.

Disadvantages

- Security concerns, particularly with smaller networks, as the transactions are validated and added directly to the DAG without block creation, hashing, or block validation.
- Initial phases might require a coordinator for network integrity and to arrange the validator's joining process.

#### 4) DAG Rewarding Strategies

DAG protocols usually don't involve traditional mining; thus, they do not have direct rewarding mechanisms for transaction validation. Instead, the incentive to participate in the network comes from the utility of the system and potentially from transaction fees (which are low) in some implementations. Therefore, research introduces a reward strategy to incen- tivize miners to serve systems of public ledgers. In which, miners are rewarded with a fixed fee as they participate in transaction validation, plus the transaction fees of the valid transactions are added to an approved block [89].

## IV. DISCUSSION

In a democratic electronic system, all nodes participate in system processes. So, keeping network members synchronized is achieved through a consensus mechanism. When decentralization is implemented, each network member is granted equal voting rights in system decisions. Therefore, it is essential to establish rules that allow the nodes (network members) to reach an agreement and globally execute new system updates. The consensus mechanism in a decentralized network ensures that all participating nodes have an equal opportunity to propose and validate updates. As a result, the network can collectively decide on its next update. Each node in a blockchain continuously communicates with others, as they all maintain a copy of the network's transactions. Through consensus, the nodes agree on the current state of the ledger, preserving its operational integrity and enabling decentralization without disorder. This consensus not only ensures agreement on the current state but also eliminates errors and protects the network from threats like double-spending and Sybil attacks, where malicious actors use fake nodes to manipulate the network.

As early as 2009, Bitcoin was the first widely recog- nized blockchain model that employed the PoW consensus algorithm. In this way, PoW became one of the first kinds of consensus system. However, periodic developments and implementations have led to the development of other, more innovative consensus protocols.

This section explores the nature of consensus protocols and the associated reward strategies.

**TABLE 1.** The Categories of Consensus Protocols

| Categories | Consensus Protocols |
|---|---|
| Computational-based | PoW, PoeX and PoSpace |
| Wealth-based | PoS, DPoS, LPoS, PoB, and PoX |
| behavioral-based | PoAuth, UNL, Ripple, PoI, PoR, and PoC |
| Fairness-based | PoET and BoF |
| Fault-tolerance-based | PBFT, DBFT and FBA |
| Leader-based | Proof of QoS and RAFT |
| Transactional-based | DAG |

### A. *OVERVIEW OF THE NATURE OF THE CONSENSUS PROTOCOLS*

Consensus protocols can be categorized into computational-based, wealth-based, behavioral-based, fairness-based, fault-tolerance-based, leader-based, and transactional-based as shown in Table 1.

First, the computational-based consensus protocols include PoW, PoeX, and PoSpace. The fundamental consensus proto- col, PoW, is employed by Bitcoin, enabling cryptocurrency miners to resolve intensive mathematical calculations. It is used to calculate the correct hash of a block by modifying the block's nonce. The first miner to solve the problem correctly is permitted the privilege of adding a new block. PoeX also uses computational power to resolve real-world matrix-based scientific computation problems instead of a hash calculation. Both protocols are usable for systems with high computational demands. While PoSpace helps to provide hardware resources to facilitate such computations.

Second, wealth-based consensus protocols include: PoS, DPoS, LPoS, PoB, and PoX. They all move the emphasis away from computational capacity and towards economic stake. The quantity of cryptocurrency a miner possesses, stakes, leases, burns, transfers, or uses efficiently to support the system will enhance the miner's chance to contribute or validate a new block. These protocols save energy and are useful for economic systems such as cryptocurrency in-vestments and management systems in order to cope with economic matters such as currency rates, currency trading, inflation, and recession. For example, in the case of inflation, the use of PoB ensures that cryptocurrency coins are burned and permanently removed from circulation to prevent them from coming back to the money supply.

Third, behavioral-based protocols are PoAuth, UNL, Rip-ple, PoI, PoR, and PoC. All of them replace the energy and wealth capacities in a participants' behavior. They give scores and ranks to miners according to their activities, conduct, and ethics, which also enables blockchain applications in other areas. These protocols are useful for centralized or partially decentralized situations, these protocols are necessary for preserving the trustworthiness and stability of the network. In addition, they are suitable for systems that rely on one user's active interactions. Additionally, they are also useful for systems that require high-speed actions and responses.

Fourth, PoET and PoF focus on providing fair participation among users. PoET, designed for permissioned blockchains, uses trusted execution environments (TEEs) to assign random wait times to nodes, allowing them to propose blocks based on time rather than computational power, wealth, or reputation. PoET is suitable for enterprise-level blockchain applications.

Fifth, PBFT and its variations, such as DBFT and FBA, offer effective procedures for Fault Tolerance. They enable reaching consensus and continuing to function normally even while some of the nodes in the network are malfunctioning.

Sixth, leader-based protocols such as PoQoS and RAFT compromise decentralization for speed and certainty.

Notably, both RAFT and PoQoS also fall under fault-tolerance-based protocols. They can offer the added benefit of maintaining network stability and resilience whenever the possibility of faults exists.
Seventh, some applications use unique approaches such as DAG structures to rapidly validate transactions and grow without the need for traditional blocks, or by treating each transaction itself as a block. It is also a graph-based model which is suitable for graph-based blockchain applications.
Finally, some of these consensus protocols are hybrids and intersect with other categories. For example, Proof of Weight involves the features of PoS, PoI, PoR, and PoC; while Proof of Identity involves features of PoF and PoAuth. This allows them to be applied in various areas and use cases.

### B. *REWARDING STRATEGIES*

This section discusses the diversity in rewarding strategies, punishment strategies, and rewarding limitations. Firstly, there is significant diversity in term of rewarding used across different protocols, as follows:

- Newly mined cryptocurrency as in PoW, PoSpace, PoB, and PoX.
- Transaction fee as in all consensus protocols that are applied to cryptocurrency systems such as PoW, PoS, and others.
- System reserves such as in PoS, Ripple and, UNL.
- Prizes for solving some computations or performing tasks such as in PoeX.
- Different forms of liquidity such as certificates, stokes, and others as used by PoS, DPoS, and PoC.
- Reputation and trust scores such as in PoAuth, PoI, PoR, PoC, and PoET.
- More privileges such as increasing voting power as in PBFT, DBFT, FBA, and QoS.

Now, we focus on the rewarding procedures. All consensus protocols give rewards when miners perform tasks correctly such as transaction validation, block creation, block validation, and other tasks. These tasks can be updating specific protocols as in PoW, providing storage space as in PoSpace, and using a passive stake as in PoS and its variants. In addition, PoET links rewards to the duration of time waiting, which is suitable for permissioned blockchain networks. PoF uses the auction-based system for miners selection and rewarding. PoeX, PoX, PoAuth, UNL, Ripple, PoI, PoR, and PoC link rewards to the miner's activities and manners. RAFT focuses on a leader and follower agreement. This paper illustrates different kinds of reward strategies that can be involved in new versions of the consensus protocols. For example, a new application that uses PoW could include a reputation score as a rewarding strategy to control the misbehaviors of miners.
Secondly, to guarantee the adequate behaviors of miners, there is a diverse range of punishments available. Unlike PoW protocols, which use the economic disincentive of wasted computational resources to discourage malicious behavior, PoS and PoB use smart contracts to cut tokens in cases of dishonest miners. PoeX, PoX, PoAuth, UNL, Ripple, PoI, PoR, and PoC use reputation scores to encourage and punish miners. Fault tolerance and leader-based protocols often employ mechanisms to identify and reject nodes that are not functioning properly, maintaining the integrity of the network [1], [3].
Thirdly, there are some limitations to the existing protocols and rewarding strategies. New kinds of tokens should be involved such as free educational courses, real estate assets, marketing products, services, IoT sensors, and art pieces (such as videos, paintings, and music) [92]–[95]. Those tokens can be transparently exchanged using blockchain applications. They can be also stored or reserved to maintain their price through supply and change management. Additionally, to enhance supply, these tokens can be produced and supplied to communities in the form of rewards, or in exchange for another product that requires to be cut [96]–[98]. Moreover, the existing systems lack soft tokens, such as human resources requirements, student attributes, and laborer skills, where some skills need to be promoted, developed, and assessed in the community.

## V. CONCLUSIONS

This work explores the application of blockchain technology in many areas through exploring the nature of consensus protocols. In addition, miners are motivated by different rewarding strategies. Therefore, this work investigated a wide range of consensus protocols and their corresponding rewarding strategies. It highlights the primary contributions of comprehensive analysis, exploration of punishment mechanisms, and places an emphasis on efficiency and security. It categorizes the consensus protocol into seven categories for application. It shows the limitations of the existing rewards, suggesting the other nine types. In the future, we will work on designing customized consensus protocols and develop the existing ones for specific real-life applications. Enhancing rewarding and punishment strategies for each protocol is another area of improvement.

## ACKNOWLEDGMENT

The authors gratefully acknowledge the funding of the Deanship of Graduate Studies and Scientific Research, Jazan University, Saudi Arabia, through project number: (RG24-S0149).

## REFERENCES

[1] B. Assiri and W. Z. Khan, ‘‘Enhanced and lock-free tendermint blockchain protocol,’’ in 2019 IEEE International Conference on Smart Internet of Things (SmartIoT). IEEE, 2019, pp. 220–226.
[2] K. K. Vaigandla, R. Karne, M. Siluveru, and M. Kesoju, ‘‘Review on blockchain technology: architecture, characteristics, benefits, algorithms, challenges and applications,’’ Mesopotamian Journal of CyberSecurity, vol. 2023, pp. 73–84, 2023.
[3] B. Assiri and W. Z. Khan, ‘‘Fair and trustworthy: Lock-free enhanced tendermint blockchain algorithm,’’ TELKOMNIKA (Telecommunication

Computing Electronics and Control), vol. 18, no. 4, pp. 2224–2234, 2020.

[4] F. R. B. of Boston and M. I. of Technology Digital Currency Initiative, ''Project hamilton phase 1 executive summary,'' https://www.bostonfed.org/publications/one-time-pubs/project-hamilton- phase-1-executive-summary.aspx, 2022, accessed on 05-January-2025.

[5] T. W. House, ''Fact sheet: President biden to sign execu- tive order on ensuring responsible development of digital assets,'' https://www.whitehouse.gov/briefing-room/statements- releases/2022/03/09/fact-sheet-president-biden-to-sign-executive-order- on-ensuring-responsible-innovation-in-digital-assets/, 2022, accessed on 05-January-2025.

[6] A. Singh, S. C. Satapathy, A. Roy, and A. Gutub, ''Ai-based mobile edge computing for iot: Applications, challenges, and future scope,'' Arabian Journal for Science and Engineering, vol. 47, no. 8, pp. 9801–9831, 2022.

[7] N. Farooqi, A. Gutub, and M. O. Khozium, ''Smart community challenges: enabling iot/m2m technology case study,'' Life Science Journal, vol. 16, no. 7, pp. 11–17, 2019.

[8] I. G. A. K. Gemeliarana and R. F. Sari, ''Evaluation of proof of work (pow) blockchains security network on selfish mining,'' in 2018 International seminar on research of information technology and intelligent systems (ISRITI). IEEE, 2018, pp. 126–130.

[9] H. Baniata and A. Kertesz, ''Approaches to overpower proof-of-work blockchains despite minority,'' IEEE Access, vol. 11, pp. 2952–2967, 2023.

[10] A. Singh, A. Gutub, A. Nayyar, and M. K. Khan, ''Redefining food safety traceability system through blockchain: findings, challenges and open issues,'' Multimedia Tools and Applications, vol. 82, no. 14, pp. 21 243–21 277, 2023.

[11] N. T. T. Thuy, L. D. Khai et al., ''A fast approach for bitcoin blockchain cryptocurrency mining system,'' Integration, vol. 74, pp. 107–114, 2020.

[12] R. Beer and T. Sharma, ''A quick look at cryptocurrency mining: Proof of work,'' in 2022 2nd International Conference on Innovative Practices in Technology and Management (ICIPTM), vol. 2. IEEE, 2022, pp. 651– 656.

[13] A. Capponi, S. Olafsson, and H. Alsabah, ''Proof-of-work cryptocurren- cies: Does mining technology undermine decentralization?'' Management Science, vol. 69, no. 11, pp. 6455–6481, 2023.

[14] W. Zhao, S. Yang, X. Luo, and J. Zhou, ''On peercoin proof of stake for blockchain consensus,'' in Proceedings of the 2021 3rd International Conference on Blockchain Technology, 2021, pp. 129–134.

[15] C. Lepore, M. Ceria, A. Visconti, U. P. Rao, K. A. Shah, and L. Zanolini, ''A survey on blockchain consensus with a performance comparison of pow, pos and pure pos,'' Mathematics, vol. 8, no. 10, p. 1782, 2020.

[16] E. Kapengut and B. Mizrach, ''An event study of the ethereum transition to proof-of-stake,'' Commodities, vol. 2, no. 2, pp. 96–110, 2023.

[17] A. Chauhan, Rishabh, L. N. Shankar, and P. Mittal, ''A deep dive into blockchain consensus protocols,'' in Smart Trends in Computing and Com- munications: Proceedings of SmartCom 2021. Springer, 2022, pp. 571–581.

[18] A. Jain and D. S. Jat, ''A review on consensus protocol of blockchain technology,'' Intelligent Sustainable Systems: Selected Papers of WorldS4 2021, Volume 2, pp. 813–829, 2022.

[19] D. P. Oyinloye, J. S. Teh, N. Jamil, and M. Alawida, ''Blockchain con- sensus: An overview of alternative protocols,'' Symmetry, vol. 13, no. 8, p. 1363, 2021.

[20] A. Wahab and W. Mehmood, ''Survey of consensus protocols,'' arXiv preprint arXiv:1810.03357, 2018.

[21] C. Chenli, B. Li, Y. Shi, and T. Jung, ''Energy-recycling blockchain with proof-of-deep-learning,'' in 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE, 2019, pp. 19–23.

[22] O. A. Logachev and S. N. Fedorov, ''On a class of descrete functions for proof-of-space blockchain consensus protocols,'' International Journal of Open Information Technologies, vol. 8, no. 12, pp. 33–38, 2020.

[23] M. J. Heule, ''Proofs of unsatisfiability,'' in Handbook of Satisfiability. IOS Press, 2021, pp. 635–668.

[24] J. Xu, C. Wang, and X. Jia, ''A survey of blockchain consensus protocols,'' ACM Computing Surveys, vol. 55, no. 13s, pp. 1–35, 2023.

[25] I. Giacomelli, ''Filecoin: from proof-of-space blockchain to decentralized storage.'' CrypTorino 2021, p. 27, 2024.

[26] S. R. Chowdhary, ''A systematic analysis on blockchain consensus algo- rithms and security threats,'' International Journal of Computer Science and Mobile Computing, vol. 11, no. 7, pp. 8–17, 2022.

[27] N. Bhutani, G. K. Chadha, and V. Nehra, ''Analysis of different consensus algorithms with development of blockchain based cryptocurrency and initial coin offering,'' in 2021 9th International Conference on Reliabil- ity, Infocom Technologies and Optimization (Trends and Future Direc- tions)(ICRITO). IEEE, 2021, pp. 1–9.

[28] S. Kotha and P. Patel, ''Blockchain in depth,'' International Journal of Engineering and Computer Science, vol. 9, no. 5, pp. 25 029–25 038, 2022.

[29] M. Veinović et al., ''Comparative analysis of consensus algorithms in blockchain networks,'' in Sinteza 2021-International Scientific Conference on Information Technology and Data Related Research. Singidunum University, 2021, pp. 128–133.

[30] I. F. T. Alyaseen et al., ''Consensus algorithms blockchain: A comparative study,'' International

Journal on Perceptive and Cognitive Computing, vol. 5, no. 2, pp. 66–71, 2019.

[31] S.-N. Li, F. Spychiger, and C. J. Tessone, ‘‘Reward distribution in proof-of- stake protocols: A trade-off between inclusion and fairness,’’ IEEE Access, vol. 11, pp. 134 136–134 145, 2023.

[32] L. Brünjes, A. Kiayias, E. Koutsoupias, and A.-P. Stouka, ‘‘Reward sharing schemes for stake pools,’’ in 2020 IEEE european symposium on security and privacy (EuroS&p). IEEE, 2020, pp. 256–275.

[33] F. Saleh, ‘‘Blockchain without waste: Proof-of-stake,’’ The Review of fi- nancial studies, vol. 34, no. 3, pp. 1156–1190, 2021.

[34] A. Barhanpure, P. Belandor, and B. Das, ‘‘Proof of stack consensus for blockchain networks,’’ in Security in Computing and Communications: 6th International Symposium, SSCC 2018, Bangalore, India, September 19– 22, 2018, Revised Selected Papers 6. Springer, 2019, pp. 104–116.

[35] K. Karantias, A. Kiayias, and D. Zindros, ‘‘Proof-of-burn,’’ in Financial Cryptography and Data Security: 24th International Conference, FC 2020, Kota Kinabalu, Malaysia, February 10–14, 2020 Revised Selected Papers 24. Springer, 2020, pp. 523–540.

[36] A. A. Menon, T. Saranya, S. Sureshbabu, and A. Mahesh, ‘‘A comparatıve analysis on three consensus algorithms: proof of burn, proof of elapsed time, proof of authority,’’ in Computer Networks and Inventive Commu- nication Technologies: Proceedings of Fourth ICCNCT 2021. Springer, 2022, pp. 369–383.

[37] D. Wang, C. Jin, H. Li, and M. Perkowski, ‘‘Proof of activity consensus algorithm based on credit reward mechanism,’’ in Web Information Systems and Applications: 17th International Conference, WISA 2020, Guangzhou, China, September 23–25, 2020, Proceedings 17. Springer, 2020, pp. 618–628.

[38] Z. Ai and W. Cui, ‘‘A proof-of-transactions blockchain consensus protocol for large-scale iot,’’ IEEE Internet of Things Journal, vol. 9, no. 11, pp. 7931–7943, 2021.

[39] S. Fahim, S. K. Rahman, and S. Mahmood, ‘‘Blockchain: A comparative study of consensus algorithms pow, pos, poa, pov,’’ Int. J. Math. Sci. Comput, vol. 3, pp. 46–57, 2023.

[40] U. S. Aditya, R. Singh, P. K. Singh, and A. Kalla, ‘‘A survey on blockchain in robotics: Issues, opportunities, challenges and future directions,’’ Jour- nal of Network and Computer Applications, vol. 196, p. 103245, 2021.

[41] A. C. An, P. T. X. Diem, T. Van Toi, L. D. Q. Binh et al., ‘‘Building a product origins tracking system based on blockchain and poa consensus protocol,’’ in 2019 international conference on advanced computing and applications (ACOMP). IEEE, 2019, pp. 27–33.

[42] S. B. Wankhede and D. Patel, ‘‘The proof of authority consensus algorithm for iiot security,’’ in The International Conference on Recent Innovations in Computing. Springer, 2022, pp. 803–811.

[43] J. Yang, J. Dai, H. B. Gooi, H. D. Nguyen, and A. Paudel, ‘‘A proof-of- authority blockchain-based distributed control system for islanded micro- grids,’’ IEEE Transactions on Industrial Informatics, vol. 18, no. 11, pp. 8287–8297, 2022.

[44] S. Gopikrishnan, P. Priakanth, G. Srivastava, and C. V. Joe, ‘‘Scheisb: Design of a high efficiency iomt security model based on sharded chains using bio-inspired optimizations,’’ Computers and Electrical Engineering, vol. 111, p. 108925, 2023.

[45] G. A. F. Rebello, G. F. Camilo, L. C. Guimaraes, L. A. C. de Souza, G. A. Thomaz, and O. C. M. Duarte, ‘‘A security and performance analysis of proof-based consensus protocols,’’ Annals of Telecommunications, pp. 1– 21, 2022.

[46] M. M. Islam, M. M. Merlec, and H. P. In, ‘‘A comparative analysis of proof-of-authority consensus algorithms: Aura vs clique,’’ in 2022 IEEE International Conference on Services Computing (SCC). IEEE, 2022, pp. 327–332.

[47] Q. Wang, R. Li, Q. Wang, S. Chen, and Y. Xiang, ‘‘Exploring unfair- ness on proof of authority: Order manipulation attacks and remedies,’’ in Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security, 2022, pp. 123–137.

[48] M. A. Manolache, S. Manolache, and N. Tapus, ‘‘Decision making using the blockchain proof of authority consensus,’’ Procedia Computer Science, vol. 199, pp. 580–588, 2022.

[49] S. Altalhi and A. Gutub, ‘‘A survey on predictions of cyber-attacks utilizing real-time twitter tracing recognition,’’ Journal of Ambient Intelligence and Humanized Computing, pp. 1–13, 2021.

[50] X. Si, M. Li, Z. Yao, W. Zhu, J. Liu, and Q. Zhang, ‘‘An efficient and secure blockchain consensus protocol for internet of vehicles,’’ Electronics, vol. 12, no. 20, p. 4285, 2023.

[51] S. Pahlajani, A. Kshirsagar, and V. Pachghare, ‘‘Survey on private blockchain consensus algorithms,’’ in 2019 1st International Conference on Innovations in Information and Communication Technology (ICIICT). IEEE, 2019, pp. 1–6.

[52] K. Li, H. Li, H. Wang, H. An, P. Lu, P. Yi, and F. Zhu, ‘‘Pov: An efficient voting-based consensus algorithm for consortium blockchains,’’ Frontiers in Blockchain, vol. 3, p. 11, 2020.

[53] B. Lashkari and P. Musilek, ‘‘A comprehensive review of blockchain consensus mechanisms,’’ IEEE access, vol. 9, pp. 43 620–43 652, 2021.

[54] B. Xiao, C. Jin, Z. Li, B. Zhu, X. Li, and D. Wang, ‘‘Proof of importance: A consensus algorithm for importance based on dynamic authorization,’’ in IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology, 2021, pp. 510–513.

[55] S. Aggarwal and N. Kumar, ‘‘Cryptographic consensus mechanisms,’’ in Advances in computers. Elsevier, 2021, vol. 121, pp. 211–226.
[56] A. O. Bada, A. Damianou, C. M. Angelopoulos, and V. Katos, ‘‘Towards a green blockchain: A review of consensus mechanisms and their energy consumption,’’ in 2021 17th international conference on distributed com- puting in sensor systems (DCOSS). IEEE, 2021, pp. 503–511.
[57] Q. Zhuang, Y. Liu, L. Chen, and Z. Ai, ‘‘Proof of reputation: A reputation- based consensus protocol for blockchain based systems,’’ in Proceedings of the 1st International Electronics Communication Conference, 2019, pp. 131–138.
[58] J. Yu, D. Kozhaya, J. Decouchant, and P. Esteves-Verissimo, ‘‘Repucoin: Your reputation is your power,’’ IEEE Transactions on Computers, vol. 68, no. 8, pp. 1225–1237, 2019.
[59] D. P. Oyinloye, J. S. Teh, N. Jamil, and J. Teh, ‘‘Sim-p—a simplified consensus protocol simulator: Applications to proof of reputation-x and proof of contribution,’’ IEEE Internet of Things Journal, vol. 10, no. 6, pp. 5083–5094, 2022.
[60] J. Yuan and L. Njilla, ‘‘Lightweight and reliable decentralized reward system using blockchain,’’ in IEEE INFOCOM 2021-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). IEEE, 2021, pp. 1–6.
[61] H. Song, N. Zhu, R. Xue, J. He, K. Zhang, and J. Wang, ‘‘Proof-of- contribution consensus mechanism for blockchain and its application in intellectual property protection,’’ Information processing & management, vol. 58, no. 3, p. 102507, 2021.
[62] T. Xue, Y. Yuan, Z. Ahmed, K. Moniz, G. Cao, and C. Wang, ‘‘Proof of con- tribution: A modification of proof of work to increase mining efficiency,’’ in 2018 IEEE 42nd annual computer software and applications conference (COMPSAC), vol. 1. IEEE, 2018, pp. 636–644.
[63] T. Aslam, A. Maqbool, M. Akhtar, A. Mirza, M. A. Khan, W. Z. Khan, and S. Alam, ‘‘Blockchain based enhanced erp transaction integrity archi- tecture and poet consensus,’’ Computers, Materials & Continua, vol. 70, no. 1, pp. 1089–1109, 2022.
[64] M. A. Kumar, V. Radhesyam, and B. SrinivasaRao, ‘‘Front-end iot ap- plication for the bitcoin based on proof of elapsed time (poet),’’ in 2019 Third International Conference on Inventive Systems and Control (ICISC). IEEE, 2019, pp. 646–649.
[65] M. Zouina and B. Outtai, ‘‘Towards a distributed token based payment system using blockchain technology,’’ in 2019 international conference on advanced communication technologies and networking (commnet). IEEE, 2019, pp. 1–10.
[66] N. Ramkumar, G. Sudhasadasivam, and K. Saranya, ‘‘A survey on different consensus mechanisms for the blockchain technology,’’ in 2020 Interna- tional Conference on Communication and Signal Processing (ICCSP). IEEE, 2020, pp. 0458–0464.
[67] H. Wang, G. Chen, Y. Zhang, and Z. Lin, ‘‘Multi-certificate attacks against proof-of-elapsed-time and their countermeasures.’’ in NDSS, 2022.
[68] A. Alamer and B. Assiri, ‘‘Proof of fairness: Dynamic and secure consensus protocol for blockchain,’’ Electronics, vol. 13, no. 6, p. 1056, 2024.
[69] M. Castro, B. Liskov et al., ‘‘Practical byzantine fault tolerance,’’ in OsDI, vol. 99, no. 1999, 1999, pp. 173–186.
[70] L. Yang, Y. Zou, M. Xu, Y. Xu, D. Yu, and X. Cheng, ‘‘Distributed consen- sus for blockchains in internet-of-things networks,’’ Tsinghua Science and Technology, vol. 27, no. 5, pp. 817–831, 2022.
[71] X. Qi, Z. Chen, Z. Zhang, C. Jin, A. Zhou, H. Zhuo, and Q. Xu, ‘‘A byzan- tine fault tolerant storage for permissioned blockchain,’’ in Proceedings of the 2021 International Conference on Management of Data, 2021, pp. 2770–2774.
[72] K. Venkatesan and S. B. Rahayu, ‘‘Blockchain security enhancement: an approach towards hybrid consensus algorithms and machine learning techniques,’’ Scientific Reports, vol. 14, no. 1, p. 1149, 2024.
[73] J. Yang, Z. Jia, R. Su, X. Wu, and J. Qin, ‘‘Improved fault-tolerant consen- sus based on the pbft algorithm,’’ Ieee Access, vol. 10, pp. 30 274–30 283, 2022.
[74] O. Onireti, L. Zhang, and M. A. Imran, ‘‘On the viable area of wireless practical byzantine fault tolerance (pbft) blockchain networks,’’ in 2019 IEEE global communications conference (GLOBECOM). IEEE, 2019, pp. 1–6.
[75] C. Li, J. Zhang, X. Yang, and L. Youlong, ‘‘Lightweight blockchain consensus mechanism and storage optimization for resource-constrained iot devices,’’ Information Processing & Management, vol. 58, no. 4, p. 102602, 2021.
[76] I. M. Coelho, V. N. Coelho, R. P. Araujo, W. Yong Qiang, and B. D. Rhodes, ‘‘Challenges of pbft-inspired consensus for blockchain and enhancements over neo dbft,’’ Future Internet, vol. 12, no. 8, p. 129, 2020.
[77] S. Basudan, ‘‘Ipfs-blockchain-based delegation model for internet of medi- cal robotics things telesurgery system,’’ Connection Science, vol. 36, no. 1, p. 2367549, 2024.
[78] E. W. Nugroho, ‘‘Analyzing the federated byzantine agreement blockchain network for liveness using multiple online analytical processing,’’ in 2023 7th International Conference on Information Technology (InCIT). IEEE, 2023, pp. 135–140.
[79] M. Kim, Y. Kwon, and Y. Kim, ‘‘Is stellar as secure as you think?’’ in 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). IEEE, 2019, pp. 377–385.

[80] C. Ndolo, M. Florian, and F. Tschorsch, ‘‘Fair reward distribution in feder- ated byzantine agreement systems,’’ in 2023 5th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS). IEEE, 2023, pp. 1–8.

[81] B. Yu, J. Liu, S. Nepal, J. Yu, and P. Rimba, ‘‘Proof-of-qos: Qos based blockchain consensus protocol,’’ Computers & Security, vol. 87, p. 101580, 2019.

[82] Y. Zhang, L. Zhang, Y. Liu, and X. Luo, ‘‘Proof of service power: A blockchain consensus for cloud manufacturing,’’ Journal of Manufacturing Systems, vol. 59, pp. 1–11, 2021.

[83] X. Xu, L. Hou, Y. Li, and Y. Geng, ‘‘Weighted raft: An improved blockchain consensus mechanism for internet of things application,’’ in 2021 7th International Conference on Computer and Communications (ICCC). IEEE, 2021, pp. 1520–1525.

[84] Y. Li, Y. Fan, L. Zhang, and J. Crowcroft, ‘‘Raft consensus reliability in wireless networks: Probabilistic analysis,’’ IEEE Internet of Things Journal, vol. 10, no. 14, pp. 12 839–12 853, 2023.

[85] T. Wang, D. Huang, and S. Zhang, ‘‘Consensus algorithm analysis in blockchain: Pow and raft,’’ Wireless Blockchain: Principles, Technologies and Applications, pp. 27–72, 2021.

[86] A. M. A. Alamer, ‘‘A secure and privacy blockchain-based data sharing scheme in mobile edge caching system,’’ Expert Systems with Applications, vol. 237, p. 121572, 2024.

[87] H. Dong, W. Xiong, D. Goyal, Y. Zhang, W. Chow, R. Pan, S. Diao, J. Zhang, K. Shum, and T. Zhang, ‘‘Raft: Reward ranked finetuning for generative foundation model alignment,’’ arXiv preprint arXiv:2304.06767, 2023.

[88] Z. Hussein, M. A. Salama, and S. A. El-Rahman, ‘‘Evolution of blockchain consensus algorithms: a review on the latest milestones of blockchain consensus algorithms,’’ Cybersecurity, vol. 6, no. 1, p. 30, 2023.

[89] J. He, G. Wang, G. Zhang, and J. Zhang, ‘‘Consensus mechanism design based on structured directed acyclic graphs,’’ Blockchain: Research and Applications, vol. 2, no. 1, p. 100011, 2021.

[90] M. Revanesh, J. M. Acken, and V. Sridhar, ‘‘Dag block: Trust aware load balanced routing and lightweight authentication encryption in wsn,’’ Future Generation Computer Systems, vol. 140, pp. 402–421, 2023.

[91] A. Tokhmetov, V. Lee, and L. Tanchenko, ‘‘Development of dag blockchain model,’’ Scientific Journal of Astana IT University, 2023.

[92] Z. Zhao, ‘‘Fulfilling the right to follow: using blockchain to enforce the artist’s resale right,’’ Cardozo Arts & Ent. LJ, vol. 39, p. 239, 2021.

[93] O. Shmatko, T. Borova, S. Yevseiev, and O. Milov, ‘‘Tokenization of educa- tional assets based on blockchain technologies,’’ ScienceRise: Pedagogical Education, no. 3 (42), pp. 4–10, 2021.

[94] R. M. Garcia-Teruel, ‘‘Legal challenges and opportunities of blockchain technology in the real estate sector,’’ Journal of Property, Planning and Environmental Law, vol. 12, no. 2, pp. 129–145, 2020.

[95] B. I. Mohideen and B. Assiri, ‘‘Internet of things (iot): classification, secured architecture based on data sensitivity, security issues and their countermeasures,’’ Journal of Information & Knowledge Management, vol. 20, no. supp01, p. 2140001, 2021.

[96] T. M. Tan and S. Saraniemi, ‘‘Trust in blockchain-enabled exchanges: Future directions in blockchain marketing,’’ Journal of the Academy of marketing Science, vol. 51, no. 4, pp. 914–939, 2023.

[97] M. A. Kashem, M. Shamsuddoha, T. Nasir, and A. A. Chowdhury, ‘‘Supply chain disruption versus optimization: a review on artificial intelligence and blockchain,’’ Knowledge, vol. 3, no. 1, pp. 80–96, 2023.

[98] A. Alamer and S. Basudan, ‘‘A security and privacy-preserving accessing data protocol in vehicular crowdsensing using blockchain,’’ in Proceedings of Seventh International Congress on Information and Communication Technology: ICICT 2022, London, Volume 2. Springer, 2022, pp. 315–327.