A survey on blockchain consensus mechanism: research overview, current advances and future directions

Mingyue Xie and Jun Liu
The School of Software Engineering, Chongqing University of Posts and Telecommunications, Chongqing, China
Shuyu Chen
Chongqing University, Chongqing, China, and
Mingwei Lin
Fujian Normal University, Fuzhou, China

Received 6 May 2022
Revised 6 July 2022
9 August 2022
Accepted 16 August 2022

Abstract

Purpose – As the core technology of blockchain, various consensus mechanisms have emerged to satisfy the demands of different application scenarios. Since determining the security, scalability and other related performance of the blockchain, how to reach consensus efficiently of consensus mechanism is a critical issue in the blockchain.

Design/methodology/approach – The paper opted for a research overview on the blockchain consensus mechanism, including the consensus mechanisms' consensus progress, classification and comparison, which are complemented by documentary analysis.

Findings – This survey analyzes solutions for the improvement of consensus mechanisms in blockchain that have been proposed during the last few years and suggests future research directions around consensus mechanisms. First, the authors outline the consensus processes, the advantages and disadvantages of the mainstream consensus mechanisms. Additionally, the consensus mechanisms are subdivided into four types according to their characteristics. Then, the consensus mechanisms are compared and analyzed based on four evaluation criteria. Finally, the authors summarize the representative progress of consensus mechanisms and provide some suggestions on the design of consensus mechanisms to make further advances in this field.

Originality/value – This paper summarizes the future research development of the consensus mechanisms.

Keywords Blockchain, Consensus mechanism, Byzantine fault-tolerant, Consistency

Paper type Research paper

1. Introduction

Digital cryptocurrencies represented by Bitcoin have promoted the acceleration of the world economy (Mar *et al.*, 2021; Matzutt *et al.*, 2021; Mišić *et al.*, 2020; Wu *et al.*, 2022). As a supporting technology of cryptocurrency, blockchain is essentially a decentralized database (Tenorio-Fornés *et al.*, 2021). It has drawn extensive interest due to its decentralized, tamper-proof, traceable, programmable and other characteristics (Berdik *et al.*, 2021; Meng *et al.*, 2021;

This work was supported by the Chongqing Research Program of Basic Research and Frontier Technology (Grant No. cstc2021jcyj-msxmX0530 and Grant No. cstc2020jcyj-msxmX0804), and the Graduate Scientific Research and Innovation Foundation of Chongqing (Grant No. CYS22457), and the Technology Innovation and Application Development Projects of Chongqing (Grant No. cstc2021jscx-gksbX0032, cstc2021jscx-gksbX0029), and the Key R&D plan of Hainan Province (Grant No. ZDYF2021GXJS006).

Data Availability: The data used to support the findings of this study are included within the article.
Conflict of Interest: The authors declare that they have no conflict of interest.

International Journal of Intelligent Computing and Cybernetics

1756-378X
DOI 10.1108/IJICC-05-2022-0126

Madhura and Mahalakshmi, 2022). Recently, the emergence of Ethereum provides various modules for users to deploy applications (Kim *et al.*, 2021; Wang *et al.*, 2021a; Wood, 2014), reducing the cost and speeding up the deployment of the application. In terms of data processing for applications, the chained structure is used to validate and store data in blockchain (Li *et al.*, 2021a) as illustrated in Figure 1. Meanwhile, a distributed consensus mechanism for nodes is utilized to generate and update data (Khan *et al.*, 2021).

In recent years, blockchain has shown great potential in the fields of logistics, healthcare, finance and the internet of Things (IoT) (Liu *et al.*, 2021a; Mukta *et al.*, 2022; Du *et al.*, 2020; Huo *et al.*, 2022), etc. According to different application scenarios, blockchain is divided into three types, namely public blockchain, private blockchain and consortium blockchain (Wang *et al.*, 2021b; Chen *et al.*, 2021a; Yuen, 2020; Liang *et al.*, 2021). Specially, nodes can join and exit the network freely to participate in accessing and modifying data in the public blockchain (Lei *et al.*, 2020). Currently, digital cryptocurrencies and smart contract platforms operate on the public blockchain (Saad *et al.*, 2020). The write permissions of the nodes in the private blockchain are controlled by the internal organization. The read permissions can be selectively open to the external organization (Cao *et al.*, 2020). Therefore, private blockchain is applicable for internal data management and auditing (Gourisetti *et al.*, 2020). The consortium blockchain is partially decentralized. Each node corresponds to an entity organization owning to its characteristics. Any institutional node joining the consortium blockchain needs to get permission from the organization (Yang *et al.*, 2021; Wang *et al.*, 2021c). Therefore, the current business community pays more attention to the establishment and usage of consortium blockchain (Treiblmaier *et al.*, 2021).

Blockchain is a revolutionary technology for distributed data storage, peer-to-peer transmission, consensus mechanism and encryption algorithm (Chen *et al.*, 2021b; Xu *et al.*, 2021a; Li *et al.*, 2021b; Liang *et al.*, 2020; Liu *et al.*, 2022; Pu *et al.*, 2020), etc. The blockchain architecture is divided into six layers as shown in Figure 2 (Li *et al.*, 2021c; Lao *et al.*, 2020). With the rapid development of blockchain technology, the demand for a higher level of service quality poses a more serious challenge to the design of the blockchain, e.g. the transaction processing performance (Long *et al.*, 2021). Mainstream blockchain platforms, such as Bitcoin, can handle around seven transactions per second (Nakamoto, 2008; Wood, 2014; Sun *et al.*, 2021a). As a key technology in blockchain, the consensus mechanism directly affects the transaction processing ability, scalability and security of the blockchain (Bouraga, 2021; Zhang *et al.*, 2021; Abishu *et al.*, 2022; Javaid and Sikdar, 2021).

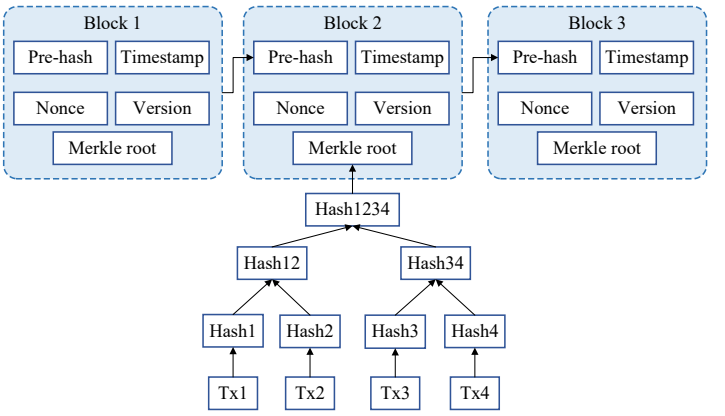

Figure 1.
The chained structure of blockchain

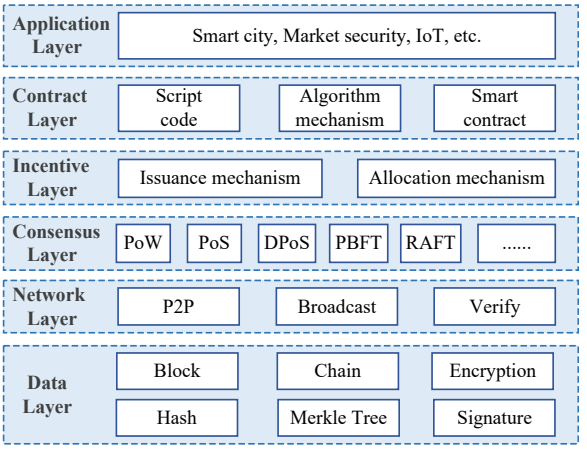

Figure 2.
The architecture of blockchain

The typical consensus mechanisms in blockchain system include proof of work (PoW) (Cachin and Vukolic, 2017), proof of stake (PoS) (Vasin, 2014), delegated PoS (DPoS) (Larimer, 2014), practical Byzantine fault tolerance (PBFT) (Castro and Liskov, 2002) and RAFT (Ongaro and Ousterhout, 2015), etc. Various consensus mechanisms exist in blockchain, but no one is suitable for all application scenarios (Kudva *et al.*, 2021; Yan *et al.*, 2021). In this survey, we focus on the key issues of the consensus mechanisms in blockchain. The consensus process, pros and cons of the mainstream consensus mechanisms are systematically and comprehensively analyzed. Then, we classify and compare the consensus mechanisms according to their characteristics. Finally, the improvements of the consensus mechanism in the future are clarified to promote the development of blockchain technology.

The rest of this survey is organized as follows. The existing reviews on consensus mechanism are introduced in Section 2. Section 3 describes the analysis of mainstream consensus mechanisms. Section 4 specifies the categorization of existing consensus mechanisms. The comparative performance analysis of the existing consensus mechanisms is done in Section 5. Section 2 introduces the existing literature employing consensus mechanisms in different domains. Section 7 points out the existing research and future directions in the development of consensus. Section 8 draws the conclusion.

2. Related work

As the key technology of blockchain, the consensus mechanisms vary with different blockchain networks. Motivated by the first consensus mechanism in Bitcoin, a plethora of variants are presented to endow blockchain with better performance. As various consensus mechanisms are come up with, it is of profound significance to explicitly investigate and compare them. In recent years, the surveys on consensus mechanisms mainly include the following contents.

Zheng *et al.* (2017) introduce and compare six typical consensus mechanisms in terms of node identity management, energy saving and tolerated power of adversary. Nguyen and Kim (2018) focus on introducing the proof-based consensus and voting-based consensus mechanism. Considering the indispensable role of consensus mechanisms in the blockchain-enabled IoT system, Cao *et al.* (2019) discuss PoW and PoS and list their limitations in IoT. Wang *et al.* (2019) summarize the designing details of consensus mechanism in

permissionless blockchain and the consequent influence of the blockchain networks. Salimitari *et al.* (2020) analyze the various consensus mechanisms that are applied to resource-constrained IoT network. Wan *et al.* (2020) survey the recent progress of consensus mechanisms with a comparison of their performance and other characters. According to the CAP theorem (consistency, availability and partition tolerance) on blockchain, Carrara *et al.* (2020) survey the probabilistic consensus mechanisms and deterministic consensus mechanisms. Fu *et al.* (2021) analyze various consensus mechanisms and classify according to their design in different phases of a proposed unified consensus algorithm process model. Johar *et al.* (2021) focus on the survey of the consensus algorithms of the public and private blockchain. The algorithms are categorized according to the employment in different scenarios. Ferdous *et al.* (2021) analyze three types of consensus algorithms leveraged in public blockchain using a comprehensive taxonomy of properties. Bouraga (2021) proposes a four-category classification framework, namely origin, design, performance and security, to reflect the recent advances in consensus mechanisms. Liu *et al.* (2021c) introduce the characteristics, performance and fault tolerance of the consensus algorithms and compare their performance differences. Verma *et al.* (2022) focus on different consensus mechanisms applying formal methods and discuss their usages and limitations.

Nevertheless, these surveys have shown limitations in terms of consensus categorization and qualitative performance. And the consensus process and characteristics of some mainstream consensus mechanisms are not clearly listed in a unified form. Our work is to introduce the mainstream consensus mechanisms and classify them and their derived consensus according to the consensus process. Then, we summarize and analyze the future research on blockchain consensus mechanisms by giving an explicit comparison from four dimensions of performance and other critical particularities.

3. Analysis of mainstream consensus mechanisms

In the following subsections, we will introduce the mainstream consensus mechanisms in blockchain, including their consensus processes, the advantages and disadvantages.

3.1 PoW consensus mechanism

The PoW is one of the most typical consensus mechanisms in blockchain and is utilized by most public blockchain. The consensus mechanism applied in Bitcoin is PoW. In Bitcoin, miners are rewarded for mining according to their computing power (Baliga *et al.*, 2018), which is mainly used to compute hash values using a hash algorithm in blockchain (Song *et al.*, 2021). Hash value is computed uniformly after block generation rather than individually for each transaction. Bitcoin uses the SHA-256 hash algorithm, which requires a huge amount of computing power. For miners, the difficulty of hash value computing is the same, and only miners with more computing power can package transactions to generate blocks more quickly. However, the block generated by only one miner is eventually identified, resulting in a huge waste of resources (Li *et al.*, 2020). The consensus process of PoW is as shown in Figure 3. If the hash value calculated by the miner is equal to the target value, the block is created. Otherwise, the miner adjusts the nonce to recalculate.

In general, PoW consensus mechanism faces the 51% attack. If an attacker is willing to spend more computing power than an honest miner, it could disrupt the transaction. However, it takes more computing power for an attacker to destroy a blockchain than mining. Therefore, more miners are earning profit by mining rather than attacking. This feature of the PoW consensus mechanism ensures the security of mining.

The advantages of the PoW consensus mechanism are as follows:

(1) Complete decentralization avoids the cost of establishing and maintaining centralized credit bureaus.

(2) The PoW consensus mechanism is straightforward and easy to implement.

(3) The cost of attack is higher than that of normal mining to ensure its security.

(4) A large number of nodes can be received in the consensus process.

(5) The more computing power a node puts in, the more likely it is to get a new block reward.

The disadvantages of the PoW consensus mechanism are as follows:

(1) Mining wastes a lot of computing power and energy.

(2) To ensure decentralization, the confirmation time of blocks is difficult to shorten, and the consensus is reached in a long period.

(3) A new blockchain will need to find a different hash algorithm or face Bitcoin's computing power attacks.

Aiming to the existing problems of PoW consensus mechanism, some solutions have been proposed. The Greedy Heaviest-Observed Sub-Tree (GHOST) (Sompolinsky and Zohar, 2015) exploited the baric subtree strategy to generate the main chain, addressing the selfish mining problem. Ethereum (Wood, 2014) uses a merkel-prefix tree instead of a merkel-tree, and introduces an uncle block structure that dramatically reduces block generating time, thereby increasing throughput to 15 TPS. Bitcoin-NG (Eyal *et al.*, 2016) improves the block structure by dividing it into *key blocks* for leader election and *microblocks* for containing the ledger entries, providing a new idea for blockchain expansion.

3.2 PoS consensus mechanism

The rewards are earned rewards according to the holding time and amount of coins, corresponding to the stake nodes deposited in the PoS consensus mechanism (Xu *et al.*, 2021b). The higher the stake, the higher the chance to validate the block and win the reward. The PoS consensus mechanism saves the time and computing power consumed than the PoW. However, the low cost of mining may produce double costs and be difficult to motivate miners to work, leading to the low security of the PoS (Yang *et al.*, 2019). Most projects based on blockchain applying PoS are gradually transitioning from PoW to PoS, such as Blackcoin (Blackcoin team, 2020) and Ethereum (Wood, 2014). In the PoS consensus mechanism, all schemes need to be approved by miners who hold more than half of the stocks.

The specific consensus process of PoS is shown in Figure 4 as follows.

(1) Block producers election. Miners pledge their coins for coinage. The longer the coinage is, the greater the probability of miner becoming block producer is, which satisfies the inequality:

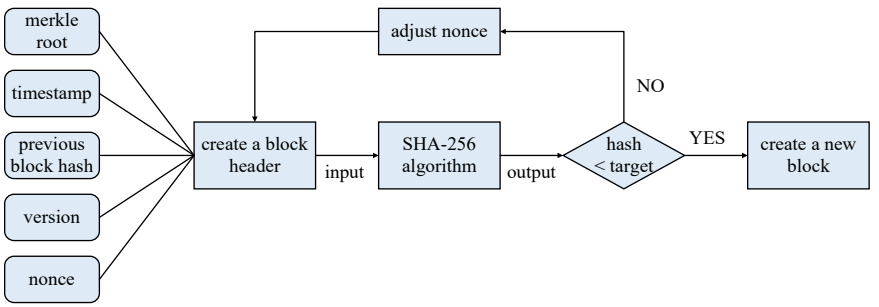

Figure 3.
The PoW consensus process

$$\text{hash}(\text{block}_{\text{header}}) \leq \text{target} * \text{coinage}$$

where hash(block_header) is a hash value, and coinage is the number multiplied by the remaining usage time of coins owned by a miner.

The coinage affects the ability to calculate the hash results rather than computing power. Therefore, the problem of huge resource wasting is solved in the PoS consensus mechanism. It also solves the problem of 51% attacks due to the impossibility for miners to own 51% of the coins in the blockchain network.

(2) Block proposal. Block producers collect transactions in the blockchain. Then the legitimate transactions are packaged into a new block that will be broadcast in the blockchain system.

(3) Block validation. The verification node verifies the new block. If the verification succeeds, the block is added to update the blockchain. Then the next round of consensus starts. Otherwise, the proposed block is discarded and a new block producer is elected in blockchain.

The advantages of the PoS consensus mechanism are as follows:

(1) It saves plenty of computing power and energy because nodes do not consume extra computing power for mining.

(2) It saves the time of generating blocks and reaching consensus, thus improving consensus efficiency.

The disadvantages of the PoS consensus mechanism are as follows:

(1) The algorithm is complex and difficult to implement.

(2) Miners hold tokens for profit rather than selling them, leaving miners with more tokens vulnerable.

(3) Mining is low cost and easy to be attacked, resulting in poor security.

Compared with PoW consensus mechanism, PoS does not calculate meaningless hash values, reducing the energy consumption greatly. Due to the existence of coinage attack and long-distance attack, Blackcoin (Blackcoin team, 2020) has improved the inequality to be satisfied for mining as proofhash < target * coins. The node must remain online for stake accumulation to solve the coinage attack. Ouroboros (David *et al.*, 2018) adds the concept of periods. If the node for generating block is not online in each period, the round does not generate blocks. The verifier verifies the legality of the transaction and packages the legitimate transaction to the node. Therefore, the long-distance attack is solved.

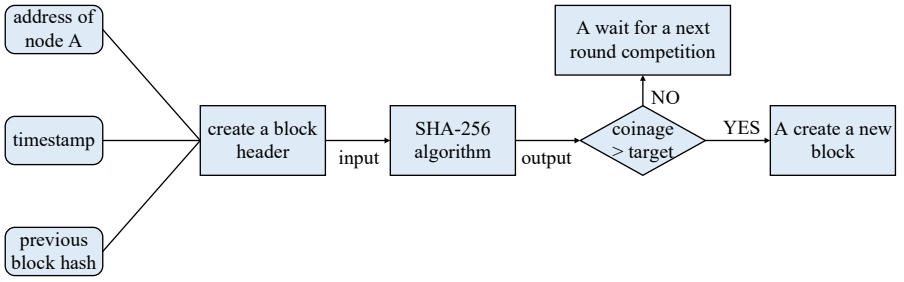

Figure 4.
The PoS consensus process

3.3 DPoS consensus mechanism

The DPoS consensus mechanism is an evolved version of the PoS consensus mechanism. Each shareholder has influence in proportion to its shareholding, and the vote of 51% of shareholders will be irreversible and binding. Each shareholder may assign its voting right to the delegates to achieve 51% approval. The delegates with the most votes can take turns generating blocks. Each delegate is assigned a period to generate blocks (Liu and Xu, 2021). A new block can be created every 30 s in DPoS. The delegate will receive a payment equal to 10% of the transaction fee contained in a block. If a delegate fails to perform its duty, e.g. failing to generate a block, its voting right will be revoked. Then a new delegate will be elected to replace it in the blockchain network.

The consensus process of DPoS is as shown in Figure 5. Suppose that n nodes are voted as delegates, constructing a delegate set B. Then the delegate $B[i]$ ($i = 1, 2, \ldots, n$) is responsible for creating and generating new blocks in turn.

The advantages of the DPoS consensus mechanism are as follows:

(1) Similar to the PoS consensus mechanism, it saves computing power and energy.

(2) It saves the time of generating new blocks, improving the efficiency of consensus reaching.

(3) The verification carried out by the elected delegates makes the consensus efficient.

The disadvantages of the DPoS consensus mechanism are as follows:

(1) It is less decentralized.

(2) Coins are still needed in the DPoS consensus mechanism.

(3) Nodes with high rights may vote for themselves and bribe other nodes to vote for them in the delegate election process, resulting in cheating.

DPoS consensus mechanism can verify transactions at the second level and provide higher security than existing PoS in a short period of time, resisting attacks with less than 51% stake. Any changes to the system (including version updates, function additions, stake modifications, etc.) must be approved by more than 51% of the shareholder. The blocks are generated in sequence, meaning that the probability of a transaction from the beginning of the broadcast until more than 1/2 confirmed blocks is 99.9%. Under normal circumstances, a new block is deemed irreversible when more than half of the witnesses give their confirmation. The throughput of EOS can reach millions, but the election of witnesses consumes a lot of resources, resulting in unsatisfactory throughput. And the generation of the block depends on 21 witnesses greatly, causing the centralization problem.

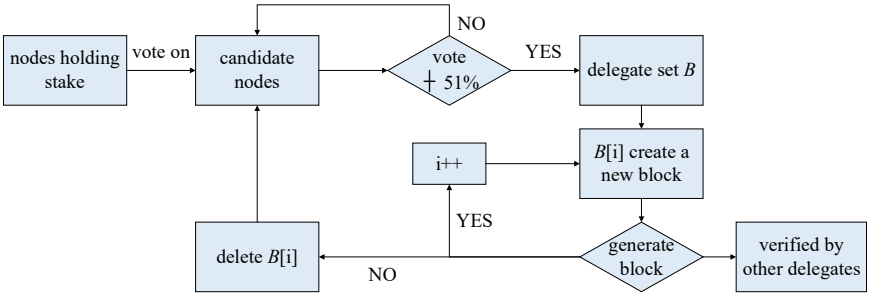

Figure 5.
The DPoS consensus process

3.4 PBFT consensus mechanism

PBFT is a seminal state machine replication protocol, requiring that all nodes of the system jointly maintain a state (Castro and Liskov, 1999). PBFT allows no more than one-third of the total number of nodes in the network to be Byzantine nodes. It mainly consists of three basic protocols, among which consistency protocol is the core (Li *et al.*, 2022).

In the PBFT consensus mechanism, the client and the consensus nodes (including a primary and backups) work together to complete the consensus process. Specially, the primary node generating blocks is voted by the whole network nodes. The client will issue a request to the primary. It will be decided whether the request can be executed or not after the primary and backups have agreed upon the request. The specific consensus process is composed of the following and is shown in Figure 6.

(1) *Request*: The client sends a request to the primary node.

(2) *Pre-prepare*: The primary node assigns a sequence number corresponding to the request. Then a *pre-prepare* message is constructed and broadcast to the backup nodes.

(3) *Prepare*: After receiving the *pre-prepare* message, each backup node broadcasts a *prepare* message to other backup nodes. All backup nodes broadcast messages to each other.

(4) *Commit*: All nodes validate the message and broadcast a *commit* message. The request will be executed if verified successfully.

(5) *Reply*: The client waits for responses from different nodes. If the client receives a correct response from $f+1$ identical *reply* messages (f is the number of Byzantine nodes), it indicates that the nodes in the network have reached a consensus.

The advantages of the PBFT consensus mechanism are as follows:

(1) It is high consistency and correctness of consensus results.

(2) Consensus confirmation time is fast.

The disadvantages of the PBFT consensus mechanism are as follows:

(1) The algorithm complexity is too high.

(2) The consensus efficiency is low if overmuch nodes join.

Nodes can access the system and broadcast communication mode only after being authenticated, resulting in poor PBFT consensus mechanism scalability. The primary node

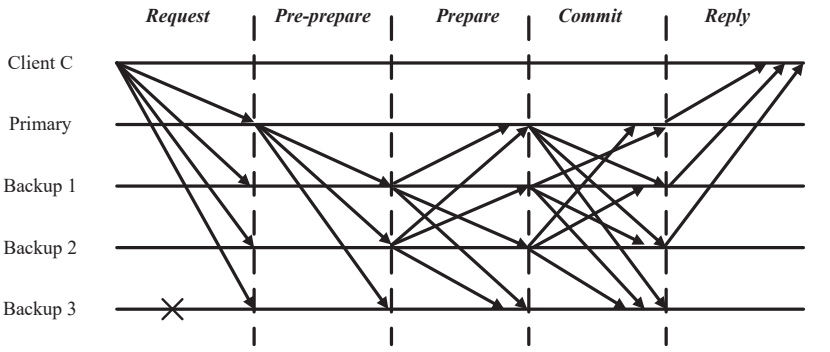

Figure 6.
The PBFT consensus process

sorts the request message and proposes the block and sends the *pre-prepare* message to all the consensus nodes with time complexity $O(n)$. Due to applying the many-to-many communication mode, each backup must broadcast the *prepare* and *commit* message with time complexity $O(2n)$. Then, the time complexity of all backups is $O(2n) \times O(n) = O(2n^2)$. Therefore, the time complexity of consistency protocol is about $O(n^2)$. Furthermore, the performance of the consistency protocol decreases significantly with the increasing number of nodes.

3.5 RAFT consensus mechanism

The RAFT is a strong consistency protocol for reaching consensus under non-Byzantine failures (Wang *et al.*, 2021d). It ensures that the system can still handle requests from a client in the case of the non-byzantine failure of nodes. A RAFT cluster typically has five nodes, allowing the system to have two failed nodes. Each node has three states: leader, follower and candidate (Li *et al.*, 2022).

Leader: The leader is responsible for synchronizing logs, handling requests from clients and keeping the heartbeat in touch with followers.

Follower: All nodes are in the follower state at startup. The node becomes a candidate if it does not receive the leader message.

Candidate: The candidate is responsible for voting. A node converts from follower to candidate and initiates an election. After a leader is elected, the candidate changes its state as the leader.

RAFT consensus mechanism state transition is shown in Figure 7 and consists of two main stages:

(1) Leader election

- Initially, all nodes are started as followers and the election is started.
- If a follower does not receive a heartbeat request from the leader, the node becomes a candidate node and remains so until a leader is elected or a new round of elections is initiated.
- Then the candidate will send the request vote to other nodes and become the leader if more than half of the nodes agree. If the election expires and no leader is elected, a new election begins.
- After completing the leader election, the leader periodically sends a heartbeat to other nodes to express that leader is still running. Then the election timer is reset for these nodes.

(2) Log replication

- The client presents a command to the leader. After receiving the command, the leader adds the command to the local log. If the command state is uncommitted, the replication state machine will not execute the command.

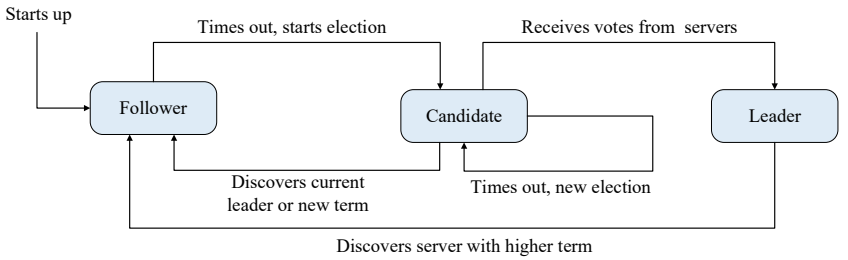

Figure 7.
The RAFT consensus process

- The leader then copies the command to the other nodes and waits for them to write the command to the log. If the existing nodes fail, the leader retries until all nodes have saved the command to the log. Then the leader submits the command and returns the result to the client.

After the leader submits the command, the next heartbeat has a message notifying the other nodes to submit the command. The other nodes apply the command from the leader to the state machine. Then, each node maintains consistency.

The advantages of the RAFT consensus mechanism are as follows:

(1) High efficiency of network transmission and consensus exists in RAFT.

(2) It saves energy due to no mining.

(3) The algorithm is simpler because Byzantine nodes are not considered.

The disadvantages of the RAFT consensus mechanism are as follows:

(1) It is incomplete decentralization due to excessive reliance on the leader.

(2) It has a brief fork in the network due to a certain amount of network fluctuation or competition, leading to confirming repeatedly.

(3) It performs poor performance in high concurrency scenarios due to sequential voting.

The leader election plays crucial role of the time requirements in RAFT. A stable leader can be elected and maintained as long as the system meets the following time requirements.

$$\text{broadcastTime} \ll \text{electionTimeout} \ll \text{MTBF}$$

where broadcastTime denotes the average time for the other servers in the cluster to receive a response, electionTimeout denotes the timeout limit for the election and MTBF is the average time between failures of a server. However, the RAFT is partially decentralized due to its over-reliance on the leader, which is not acceptable on the public blockchain. Therefore, RAFT is generally used for private blockchain and consortium blockchain. Afterwards, the network bifurcations occur under certain network fluctuations in RAFT, requiring multiple confirmations.

4. Consensus categorization

According to the consensus algorithm introduced above, in this survey, we summarize the categorization of consensus mechanisms shown in Table 1, including (1) proving-based type, (2) voting-based type, (3) alternating-based type, (4) VRF-based type and (5) hybrid-based type.

4.1 Proving-based type

The mechanisms in this type include PoW, PoS and their variants. Proving-based consensus mechanisms mostly run on anonymous P2P network with high decentralization or incentive mechanism. The PoW consensus mechanism performs the allocation of currency and the determination of accounting rights according to the miner's workload. The computing power of nodes determines the allocation of the accounting rights in PoW. The winner of the computing power competition will receive the corresponding block accounting right and bitcoin awards. Nodes with more stake have greater privileges in the PoS consensus mechanism, which are responsible for generating blocks and are rewarded with blocks. That is, the stake of a node affects its block generating probability.

Type	Consensus	Ref.
Proving-based	Proof of work (PoW)	Cachin and Vukolic (2017), Ball *et al.* (2018), Wen *et al.* (2022), Eyal *et al.* (2016)
	Proof of stake (PoS)	Vasin (2014)
	Proof of negotiation (PoN)	Abishu *et al.* (2022)
	Proof of driving (PoD)	Kudva *et al.* (2021)
	Proof of contribution (PoC)	Song *et al.* (2021)
	Proof of federated learning (PoFL)	Qu *et al.* (2021)
	Proof of useful work (uPoW)	Ball *et al.* (2017), Baldominos and Saez (2019)
	Blockchain reputation-based consensus (BRBC)	Oliveira *et al.* (2020)
	Proof of activity (PoA)	Bentov *et al.* (2014)
	K-medoids cluster-based proof of action (KPoA)	Wang *et al.* (2021e)
Voting-based	RAFT	Ongaro and Ousterhout (2015), Tan *et al.* (2022)
	Paxos	Lamport (1998)
	RTChain	Sun *et al.* (2021a)
	Post-quantum consensus	Yi *et al.* (2021)
Alternating-based	Delegated proof of stake (DPoS)	Larimer (2014), Liu and Xu (2021), Xu *et al.* (2020), Liu *et al.* (2021b), Luo *et al.* (2018)
	Practical Byzantine fault tolerance (PBFT)	Castro and Liskov (2002), Li *et al.* (2021d)
	Performance-optimized consensus	Zhang *et al.* (2021)
	Concurrent PBFT (C-PBFT)	Xu *et al.* (2021c)
VRF-based	AlgoRand	Chen and Micalib (2019), Guo *et al.* (2022)
	Dfinity	Hanke *et al.* (2018)
	Ouroboros Praos	David *et al.* (2018)
	Voting-based decentralized consensus (VDC)	Sun *et al.* (2021b)
Hybrid-based	RAFT-based PBFT(R-PBFT)	Li *et al.* (2022)
	Decred	Dursun and Üstündağ (2021), Decred community introduction to Decred governance (2019)
	Delegated Byzantine fault tolerance (DBFT)	NEO white paper (2014)
	ELASTICO	Luu *et al.* (2016)
	DPOSP (PBFT-DPoS hybrid)	Sun *et al.* (2020)

Table 1. Consensus mechanisms categorization

4.2 Voting-based type

The consensus algorithms of the voting-based type mainly focus on the design of the leader selection phase. In the traditional distributed system, most consensus mechanisms obtain the approvals of the majority directly through voting. During the consensus process for each round of leader election, the nodes broadcast requests to the other nodes to vote for it. The candidate node getting the majority of votes wins the election and then becomes the leader. The traditional consistency mechanisms, such as Paxos (Lamport, 1998) and RAFT are voting-based type. Paxos is a consensus protocol designed by Lamport to keep distributed systems consistent. A leader voting is required either when the server is initially started or when the server cannot remain connected to the leader while it is running. Due to the complexity and difficulty, its various variations, such as RAFT, are proposed. RAFT is a consensus mechanism that strongly depends on the leader.

4.3 Alternating-based type

The delegates have permission to generate blocks in the DPoS consensus mechanism. These delegates take turns packaging transactions and generating a new block on a

predetermined schedule. Note that each delegate can generate blocks in turn. In particular, if a delegate is unable to generate a block at a given time, the block generation authority is given to the delegate corresponding to the next period. The primary node in PBFT and its variants is determined by view number and node number.

4.4 VRF-based type

In blockchain system, the disadvantage of centralization is brought of partial consensus mechanisms while improving the throughput rate and reducing latency. Therefore, several consensus mechanisms based on Verifiable Random Function (VRF) (Jager, 2015) are proposed. In these consensus mechanisms, some nodes are selected in the Internet to participate in the consensus process combining the VRF algorithm for a period of time. Then, the PoS consensus mechanism or PBFT consensus mechanism is employed by the selected nodes.

The consensus mechanism based on the VRF algorithm make up for the disadvantages of relatively centralized consensus mechanism while retaining the advantages of higher efficiency and performance, and giving both decentralization and performance a good consideration. However, the consensus mechanism based on the VRF algorithm also has some disadvantages. In order to construct a relatively fair and non-attack-prone committee by random means, a fairly large number of nodes are required to be involved, such as more than 2,000 nodes. However, this is not easy to construct in reality. Take Algorand (Chen and Micalib, 2019) as an example, its assumption of network is a strongly synchronous network, which is not consistent with the real world. In addition, the lack of incentive mechanisms and penalty mechanisms also makes the network more vulnerable to malicious attacks.

4.5 Hybrid-based type

Hybrid consensus mechanism refers to the application of two or more consensus mechanisms in the underlying architecture. Rational use of hybrid consensus mechanisms can make up for the inefficiency, loss of safety protection or sacrifice of centralization caused by a single consensus mechanism. The common hybrid consensus mechanisms are as follows:

(1) The hybrid consensus combined PoW and PoS

Decred applies a hybrid consensus mechanism combining PoW and PoS (Dursun and Üstündağ, 2021; Decred community introduction to Decred governance, 2019). Specifically, miners in the PoW consensus mechanism package transactions and generate new blocks. Then, miners in PoS vote on whether to accept or reject the blocks. Once a block is accepted, three-fifths of the votes must be cast to validate the block. The votes and transactions of the block are packaged by the next PoW miner. Compared with the PoW consensus mechanism, verifying the blocks packaged by miners in PoS enables checking miners' evil, such as, protecting against 51% power attacks, forced hard forks, packing empty blocks of PoW miners, etc. Meanwhile, Decred becomes the highest attack cost under the same conditions. An attacker not only gets 51% hash computing power but also 37% of the total votes. This hybrid consensus mechanism provides additional security.

(2) The hybrid consensus combined PoW and PBFT

To achieve a balance between security and performance, Truechain [1] uses the hybrid consensus mechanism that combines the PoW and PBFT. PoW is not responsible for updating the ledger due to its low running speed. PBFT is mainly responsible for recording transactions due to its high efficiency. In addition, the nodes in PBFT are selected from the nodes of PoW. While retaining the characteristics of consensus reaching efficiency in the PBFT consensus mechanism, the election and supervision rights of PBFT nodes are handed

over to nodes in PoW. Meanwhile, the security of the entire network is guaranteed due to the quick validation of transaction records provided by PBFT nodes. The communication complexity of PBFT determines that the nodes participating in the consensus are limited. Taking advantage of the fact that PoW can accommodate an infinite number of nodes. The hybrid consensus mechanism can make up for this weakness.

(3) The hybrid consensus combined PoS and PBFT

The delegated BFT (DBFT) consensus mechanism, which includes accounting nodes and common nodes, is an improved consensus mechanism combining DPoS and PBFT (NEO white paper, 2014). The common nodes vote for accounting nodes based on their equity stake. The accounting nodes participate in block generating. Similar to DPoS consensus mechanism, the accountant is selected from the accounting nodes through voting. There is only one accountant who initiates a new block proposal in each consensus process. Once more than two-thirds of the accounting nodes agree to the proposal, the transactions in this proposal are packaged into a new block. This block is irreversible, and all transactions in it are fully confirmed.

4.6 Analysis and comparison

At present, the blockchain has developed into the third generation. The first and second generations of blockchain are public blockchain, which mainly use PoW consensus mechanism, PoS consensus mechanism and hybrid consensus mechanism. The third generation of blockchain is the consortium blockchain. It uses PBFT consensus mechanism or its variants. In this subsection, the advantages and disadvantages of the above types of consensus mechanisms are described in Table 2, as well as the design objectives of the existing literature.

5. Consensus comparison

From the previous introduction of blockchain consensus mechanisms, it is obvious that each consensus mechanism has its different design emphases, thus presenting disparate advantages and disadvantages. To better compare these characteristics, we briefly compare these consensus mechanisms from four evaluation dimensions as follows:

Energy consumption

The process of hashing and verifying the transactions using the SHA-256 algorithm consumes a lot of power. Because each transaction requires the participation of all nodes in blockchain, many computer terminals do a lot of calculations to complete it, which inevitably consumes numerous powers. As the power of blockchain networks continues to increase significantly, this trend will also lead to more energy consumption. In addition, in the process of reaching consensus, the computing resources consumed in blockchain system also include CPU, memory, storage, etc.

Scalability

It mainly considers the changes in system load and network traffic when the number of system members and transactions to be confirmed increases, which is usually measured by network throughput. Transaction per second (TPS) refers to the ratio of the total amount of transactions that are ultimately successfully stored in the blockchain to the elapsed time, which is an important index to measure the concurrency capability of the system. The higher the throughput, the more efficient the consensus mechanism is and the more capable of processing transactions.

Type	Advantages	Disadvantages	Design goals
Proving-based type	High scalability, Public blockchain	Low efficiency, High resource cost, High latency	Low resource consumption (Kudva *et al.*, 2021; Ball *et al.*, 2017, 2018) Energy-recycling (Qu *et al.*, 2021) High scalability (Palai *et al.*, 2018; Eyal *et al.*, 2016; Sompolinsky and Zohar, 2015) High throughput (Wen *et al.*, 2022; Eyal *et al.*, 2016) Block generation confirmation (Baldominos and Saez, 2019) (Feng *et al.*, 2020) Block generation right (Song *et al.*, 2021) Consensus node qualification verification (Oliveira *et al.*, 2020; Wang *et al.*, 2021e)
Voting-based type	High transaction, High efficiency, Confirmation latency	Low scalability, High communication cost, Decentralization risk	Consensus node qualification verification (Sun *et al.*, 2021a) High efficiency (Ongaro and Ousterhout, 2015; Yi *et al.*, 2021; Tan *et al.*, 2022) Consistency (Lamport, 1998)
Alternating-based type	High scalability	Decentralization risk, High efficiency	Low resource consumption (Larimer, 2014) Consistency (Castro and Liskov, 2002) Consensus node qualification verification (Zhang *et al.*, 2021; Liu and Xu, 2021; Xu *et al.*, 2020; Liu *et al.*, 2021b; Luo *et al.*, 2018) Low communication cost (Li *et al.*, 2021d) High scalability (Xu *et al.*, 2021c)
VRF-based type	High efficiency, High justice	Low communication efficiency	High time efficiency (Sun *et al.*, 2021b) Scalability (Chen and Micalib, 2019; Guo *et al.*, 2022) Decentralization (Hanke *et al.*, 2018) Various types of attacks (David *et al.*, 2018)
Hybrid-based type	High scalability, High throughput	Decentralization risk	Scalability enhance (Luu *et al.*, 2016) Scalable storage (Li *et al.*, 2022) Blockchain governance (Dursun and Üstündağ, 2021; Decred community introduction to Decred governance, 2019) High scalability (NEO white paper, 2014) Low resource consumption (Sun *et al.*, 2020)

Table 2.
Design goals of consensus mechanisms based on the pros and cons

Efficiency

It includes the time of block generation and transaction confirmation. Shorter block generation time means that the newly generated blocks takes less time to be broadcast in the

entire network. However, if the block generation interval is short, the transaction confirmation speed will be faster, resulting in collisions. Therefore, different consensus mechanisms will consider the balance of efficiency and revenue, and set relatively stable block generation time.

Security

It refers to the ability of fault tolerance and resisting security threats such as double spending attacks and selfish mining. In the process of realizing consistency in blockchain system, the most important security issue is to prevent and detect double spending attack. After generating a new block, the honest node broadcasts it in the blockchain network. Selfish mining is a theoretical attack method that threatens security and fairness. By releasing blocks generated by a node, it can obtain higher relative rewards with appropriate strategies.

The consensus mechanism comparison results are shown in Table 3. In terms of energy consumption, PoW has the largest energy consumption of other consensus mechanisms. Due to a fixed difficulty for the hash calculation within a given time, the probability of success is uniquely determined by the speed at which the miner iterates. Therefore, mining requires a large number of hash operations, which need to consume power and various computing resources. If a block is not generated, resources will be consumed until it succeeds. In addition, computing the appropriate hash value has no practical or scientific value.

It takes about ten minutes in bitcoin to mine a valid block due to the hash difficulty, and confirming a transaction takes at least 10 min. However, other consensus mechanisms have a much faster response time than PoW and can reach consensus at the second level, such as PBFT and RAFT.

The performance of the PBFT consensus mechanism is not good as other consensus mechanisms. PBFT only applies to permissioned blockchain. Nodes need to communicate with each other, leading to high communication complexity. In general, the performance of the PBFT consensus mechanism degrades quickly when the number of nodes exceeds 100, which means its scalability is low (Mar *et al.*, 2021).

Through the comparative analysis of the mainstream consensus mechanisms, the existing consensus mechanisms mainly have the following issues.

(1) High energy consumption. For instance, A great deal of computing power is used to calculate random numbers to gain block generating rights in the PoW consensus mechanism and its variants, resulting in a large amount of resource waste. Bitcoin has attracted most of the computing power now, which is relatively limited overall. Therefore, it is hard for other applications using the PoW consensus mechanism to get the same amount of computing power to secure themselves in blockchain.

	PoW	PoS	DPoS	PBFT	RAFT
Decentralization	Complete	Complete	Complete	Incomplete	Incomplete
Numbers of nodes	Unlimited	Unlimited	Unlimited	Limited	Unlimited
Energy consumption	High	Low	Low	Low	Low
Block generation	Long	Short	Short	Short	Short
Transaction confirmation	Long	Short	Short	Immediate	Immediate
Scalability	High	High	High	Low	Low
Throughput	Low	Low	High	High	High
Consistency	Probability	Probability	Probability	Finality	Finality
Fault tolerance	50%	50%	50%	33%	50%
Permission	No	No	No	Yes	Yes
Example	Bitcoin	Peercoin	EOS	Tendermint	Etcd

Table 3. Comparison of mainstream consensus mechanisms

(2) Long consensus reaching process. Although the second-level consensus mechanisms have existed at present, it is still difficult to meet the transaction requirements in the financial system and other practical application scenarios. For example, visa can peak at more than 65,000 transactions per second.

(3) Concentrated interest. For example, miners are rewarded with corresponding tokens after successful block generating in the PoS consensus mechanism. Therefore, the higher the balance of the corresponding token, the higher the probability of getting the accounting right. That is, the higher the probability of getting the token reward, which will lead to the concentration of interests.

(4) Low cost of evil. The majority consensus mechanisms lack necessary punishment for the misdeeds of miners with more computing power and interests, leading to the bifurcation of the system and reducing the security of the blockchain system.

(5) A threat to decentralization. The existing consensus mechanism tends to result in the accounting right being owned by a few people, which goes against the concept of decentralization of blockchain.

6. Recent advancements

In the previous sections, we have provided a survey on five types of consensus mechanisms for blockchain networks, namely, the proving-based type, the voting-based type, the alternating-based type, the VRF-based type and the hybrid-based type. In general, consensus mechanisms are classified according to different forms of consensus reaching. In this section, we provide the recent studies on the application of consensus mechanisms in different fields.

In recent years, applications in various fields employing the consensus mechanism have become a research hotspot. In terms of finance, Matzutt *et al.* (2021) proposed CoinPrune to address the scalability issues of cryptocurrencies without changing Bitcoin's consensus rules. The users with higher credit (i.e. banks, and regulators) are considered the consensus nodes for the transaction confirmation and consensus in terms of supply chain finance innovation (Du *et al.*, 2020). RTChain (Sun *et al.*, 2021a) uses a verifiable random function (VRF) to generate the leader in the consensus process, saving computing resources for E-commerce Blockchain. In terms of IoT applications, the Groupchain (Lei *et al.*, 2020) establishes a leader group to realize effective consensus reaching for inspiration of IoT services computing. As owning the advantages of high security and consensus efficiency, PBFT is employed for the optimization model of industrial IoT (IIoT) (Cao *et al.*, 2020). A dynamic proof of work (dPoW) (Javaid and Sikdar, 2021) consensus mechanism is proposed, which can scale according to the incoming communication traffic rate of IIoT devices. In terms of energy trading, Yang *et al.* (2021) utilized the PoS consensus mechanism to support P2P energy trading, enhancing the security of transactions. A novel consensus mechanism combining PBFT and Proof of Reputation called PBFT-based PoR (PPoR) (Abishu *et al.*, 2022) is proposed in blockchain-enabled energy trading. Qu *et al.* (2021) proposed a proof of federated learning (PoFL) consensus mechanism for energy-recycling, avoiding wasting resources. Sun *et al.* (2020) designed an efficient and promising consensus algorithm, called DPOSP, which combined the PBFT and DPOS consensus mechanisms for the vehicle-to-vehicle (V2V) energy trading. In terms of vehicular networks, Wang *et al.* (2021c) presented a byzantine fault tolerance-based PoS (BFT-based PoS) to reach consensus efficiently in vehicular networks. Kudva *et al.* (2021) proposed a proof of driving (PoD) consensus mechanism to select miners efficiently and fairly for blockchain-based vehicular ad hoc network (VANET) applications. The PBFT consensus mechanism is employed to achieve consensus in vehicular social networks, which can prevent malicious manipulation of vehicles (Pu *et al.*, 2020).

For the other existing studies related to the consensus mechanism applications, please refer to Table 4.

With the further development of blockchain technology, especially with the optimization of the underlying ledger structure, more emerging consensus mechanisms are bound to emerge. From the above summary, the decentralized consensus mechanism has a wide range of applications and potential in various industries, which may change or even subvert the existing model in many fields. With the development of technology, the consensus mechanism needs to be improved and innovated.

7. Consensus development

With more applications built on blockchain system recently, the performance of blockchain has become one of the main bottlenecks. Researchers are attempting to design new consensus mechanisms to improve energy consumption, scalability, efficiency and security. A table summarizing the technologies is presented in Table 5.

The huge amount of energy required in the PoW consensus mechanism raises serious concerns and has become a subject of serious study. To address the energy waste of PoW, Qu *et al.* (2021) proposed a PoFL consensus mechanism. Its approach is to reinvest the energy waste in PoW into federated learning. To take full advantage of the vast amount of energy spent in blockchain, Ball *et al.* (2017, 2018) proposed an uPoW mechanism. The hardness is based on different computational problems, such as orthogonal vectors, etc. Similarly, Baldominos and Saez (2019) proposed an uPoW scheme, focusing on the block mining process that is equivalent to the training of an artificial intelligence model. Wen *et al.* (2022) proposed a quantum blockchain consensus mechanism. A great deal of computational power and energy are saved by not having to solve classical mathematical problems.

Since the scalability of blockchains is impeded by the new transactions and slow transaction verification rate. Palai *et al.* (2018) presented a scheme to address the blockchain size problem, reducing blockchain storage overhead for systems that have transferable transactions. Luu *et al.* (2016) proposed a new distributed agreement protocol for permission-less blockchains called ELASTICO. The mining network is isolated in a demonstrably secure manner into multiple shards that process disjoint sets of transactions in parallel. Therefore, ELASTICO enhances the blockchain scalability through the proposed sharding technology. Existing schemes designed different algorithms to increase the capacity and throughput of the blockchain. Eyal *et al.* (2016) presented Bitcoin-NG, a new scalable blockchain protocol, based on the same trust model as Bitcoin. Bitcoin-NG breaks down the Bitcoin's operations into leader election and transaction serialization. It increases the capacity of the blockchain and reduces the time it takes for certain

Topic	Ref.
Blockchain applicability framework	Gourisetti *et al.* (2020), Zhang *et al.* (2021), Xu *et al.* (2021b), Wang *et al.* (2021d), Li *et al.* (2022), Oliveira *et al.* (2020)
Decentralized Framework for Fair Data Processing	Li *et al.* (2021a)
Wireless networks broadcasting	Long *et al.* (2021)
trust evaluation in Pervasive Social Networking (PSN)	Yan *et al.* (2021)
Intellectual property (IP) protection	Song *et al.* (2021)
Blockchain governance	Dursun and Üstündağ (2021), Decred community introduction to Decred governance (2019), Hanke *et al.* (2018)
Trading of agricultural supply chain system	Kyzy *et al.* (2021)

Table 4.
Consensus mechanism applications

Target issue	Ref.	Categorization	Technology/Solution
Energy consumption	Qu *et al.* (2021)	Proving-based type	Federal learning
	Ball *et al.* (2017)	Proving-based type	Fine-grained complexity theory
	Ball *et al.* (2018)	Proving-based type	Worst-case Assumptions
	Baldominos and Saez (2019)	Proving-based type	Deep learning models training
	Wen *et al.* (2022)	Proving-based type	Quantum zero-knowledge proof
Scalability	Zhang *et al.* (2021)	Alternating-based type	Nodes' trust values
	Kudva *et al.* (2021)	Proving-based type	Service Standard Score
	Li *et al.* (2022)	Hybrid-based type	A consistent hash algorithm
	Palai *et al.* (2018)	Proving-based type	Block summarization
	Luu *et al.* (2016)	Hybrid-based type	Sharding
	Eyal *et al.* (2016)	Proving-based type	Block classification
	Li *et al.* (2021d)	Alternating-based type	Multi-layer design
Efficiency	Sun *et al.* (2021a)	Voting-based type	Verifiable random function
	Abishu *et al.* (2022)	Hybrid-based type	Integration of consensus mechanisms
	Luo *et al.* (2018)	Alternating-based type	Ring-based coordinator
	Feng *et al.* (2020)	Proving-based type	Negotiation rules
	Sun *et al.* (2021b)	VRF-based type	VRF algorithm
	Wang *et al.* (2021e)	Proving-based type	K-medoids clustering
	Tan *et al.* (2022)	Voting-based type	State monitoring mechanism
	Guo *et al.* (2022)	VRF-based type	VRF algorithm
Security	Song *et al.* (2021)	Proving-based type	Nodes' contribution values
	Liu and Xu (2021)	Alternating-based type	Vague set
	Wen *et al.* (2022)	Proving-based type	Quantum zero-knowledge proof
	Sompolinsky and Zohar (2015)	Proving-based type	The longest-chain rule
	Oliveira *et al.* (2020)	Proving-based type	Reputation-based
	Yi *et al.* (2021)	Voting-based type	Post-quantum threshold signature
	Xu *et al.* (2020)	Alternating-based type	Vague set
	Liu *et al.* (2021b)	Alternating-based type	Probabilistic linguist term set
	David *et al.* (2018)	VRF-based type	VRF algorithm

Table 5.
Improvement of consensus mechanisms based on target issues

transactions to be confirmed. Li *et al.* (2021d) proposed an extensible multi-layer consensus mechanism based on PBFT, including a new two-layer PBFT model and a general X-layer PBFT model, reducing the communication complexity of nodes.

Previous research has established improvements to enhance the efficiency of consensus reaching. Luo *et al.* (2018) proposed a ring-based coordinator algorithm to elect the delegates in the DPoS consensus mechanism, ensuring the fairness of the system. To create blocks more efficiently, Feng *et al.* (2020) designed a PoN consensus mechanism for random-honest miners' selection. Sun *et al.* (2021b) presented a VDC algorithm for consortium blockchain to achieve better performance in time delay and transaction throughput with security and low energy cost. Wang *et al.* (2021e) designed a KPoA consensus algorithm. The empirical evidences suggest that KPoA gains an improvement in consensus efficiency and throughput. To decrease the time consumption of consensus process, a RAFT consensus algorithm with leadership transfer is presented (Tan *et al.*, 2022), which has significantly improved

consensus efficiency. The propose VRF constructions (Guo *et al.*, 2022) can significantly reduce the computing power of consensus protocol in blockchain.

An alternative to the longest-chain rule called GHOST is proposed (Sompolinsky and Zohar, 2015) to change the bitcoin's longest chain rule. It applies the most baric subtree strategy to generate main chain, solving the selfish mining problem. Therefore, it ensures security while ensuring high throughput. Oliveira *et al.* (2020) designed the BRBC mechanism. Specially, reputable miners are responsible for verifying blocks. It is claimed that BRBC can effectively exclude more than 50% of all nodes with malicious behavior, ensuring the security of consensus process. In addition, due to utilizing the quantum communication techniques (Wen *et al.*, 2022), the security of this consensus mechanism is independent of the computing power owned by miners. Yi *et al.* (2021) proposed a consensus algorithm based on the new post-quantum threshold signatures in blockchain, and verified that the proposed algorithm is more efficient and secure compared with the conventional consensus algorithms. The Ouroboros Praos (David *et al.*, 2018) provides security against fully-adaptive corruption in the semi-synchronous setting using the VRF algorithm.

However, the current consensus algorithms are not impeccable and still need improvement. According to the current research, the future research direction of blockchain consensus algorithm is mainly focused on the following five aspects.

(1) The improvement of scalability in consortium blockchain.

The design of consensus algorithms with high throughput and low delay is the focus of the development of blockchain technology. As an application scenario favored by enterprises and other organizations, consortium blockchain has been implemented in traceability, supply chain and other fields. However, the overall performance (i.e. throughput) of the consortium blockchain system usually cannot exceed the upper limit of the performance of a single node (Li *et al.*, 2021e). This leads to poor scalability of consortium blockchain, which further limits application scenarios (Kyzy *et al.*, 2021). The application of consortium blockchain can be realized by the virtue of scalability, high transaction performance and interoperation of multi-chain architecture. Therefore, cross-chain consensus mechanisms in multi-chain architectures, including isomorphic or heterogeneous blockchain, will be one of the research directions in the future.

(2) The improvement of resource utilization.

It is considered to change the consensus node competition resources into a more greenway. In addition to considering the existing computing power competition, coinage comparison, disk space competition and authentication time competition, the lower cost of resource competition pattern should also be designed. Otherwise, the efficiency and value produced by resource consumption can be regarded as the criterion for accounting right competition.

(3) The improvement of the initiative of nodes to participate in consensus process.

In the consensus process of blockchain, there are still some situations such as the non-cooperation of participating nodes. For instance, due to the time, effort and skill required in the voting process, the vast majority of shareholders never participate in voting in the DPoS consensus mechanism. Therefore, the initiative of nodes in the network to participate in the consensus process should be improved in various ways. For example, the existing reward distribution mechanism should be optimized and improved to enhance the consensus efficiency in blockchain. Nodes are encouraged to participate in the operation and maintenance of consensus mechanism with honest behavior by designing reasonable and feasible reward and punishment mechanism. Malicious users need to be reasonably punished while giving certain rewards to the whistleblowers. In addition, given the current situation

that rewards are too centralized and leaders get the majority of rewards, redistributing the proportion of rewards and establishing a reasonable reward and punishment mechanism are critically important in the consensus mechanisms. The payoff for doing evil is less than the incentives that can encourage more users to participate in the operation of the consensus mechanism with an honest attitude.

(4) The improvement of the credibility of the voting mode.

Consensus mechanisms based on voting type have a common disadvantage, that is, there are untrustworthy factors in the voting process. Since the power of the nodes elected is higher than that of ordinary nodes, there will be a few nodes cheating to be elected successfully. Therefore, a fair voting algorithm can be designed to ensure the normal operation of voting. The voting tendency of nodes can also be considered by referring to the decision-making behaviors of human beings in real life. For example, vague set (Xu *et al.*, 2020), Pythagorean fuzzy sets (PFSs) (Lin *et al.*, 2021b) and probabilistic linguist term set (PLTS) (Liu *et al.*, 2021b; Chen *et al.*, 2021b; Xu *et al.*, 2021a; Li *et al.*, 2021b; Liang *et al.*, 2020; Lin *et al.*, 2018a, b, 2019a, b, 2020, 2021a) are introduced in the election of delegates in the DPoS consensus mechanism. Similarly, a node mutual evaluation strategy can be designed to rank and remove consensus nodes promptly, thus making voting more efficient.

(5) The improvement of the effectiveness of cross-sharding consensus.

Sharding stems from the expansion of a database by dividing a database into smaller, manageable parts to improve performance (Membrey *et al.*, 2010; Corbett *et al.*, 2013). Applying the idea of sharding in blockchain can significantly improve the overall performance and storage capacity, and provide a feasible solution for blockchain to deal with highly concurrent transactions (Mizrahi and Rottenstreich, 2021). However, the consensus mechanisms are no longer suitable for the current sharding technology. Since each shard only stores its state and transaction data, inter-shard communication is required to complete cross-shard transactions to reach a consensus on the processing results of each shard, which increases the complexity of communication. Therefore, how to design the consensus algorithm between sharding to ensure the security of the blockchain as well as the quick confirmation of the results of sharding is a focus of the following research. Furthermore, various types of attacks need to be considered to prevent attackers from destroying the consensus results of the shard blockchain.

8. Conclusions

The development of blockchain technology has attracted wide attention in various fields. This survey focuses on the consensus mechanism, which is one of the core technologies of blockchain system. We first introduce consensus mechanisms that have been applied in different domains in recent years. Then, the principle and the respective consensus processes of mainstream consensus mechanisms (PoW, PoS, DPoS, PBFT, etc.) are analyzed and elaborated. Then consensus mechanisms are roughly divided into five categories, including proving-based type, voting-based type, alternating-based type, VRF-based type and hybrid-based type. Thus, this survey compared and summarized the performance of the different types of consensus mechanisms from the aspects of security, energy consumption, efficiency and scalability. However, the current improvement of consensus mechanisms is imperfect. Finally, we summarize the development of consensus mechanism and suggest a few future directions in this area.

Note

1. https://www.truechain.pro/

References

Abishu, H.N., Seid, A.M., Yacob, Y.H., Ayall, T., Sun, G.L. and Liu, G.S. (2022), "Consensus mechanism for blockchain-enabled vehicle-to-vehicle energy trading in the internet of electric vehicles", *IEEE Transactions on Vehicular Technology*, Vol. 71 No. 1, pp. 946-960.

Baldominos, A. and Saez, Y. (2019), "Coin.AI: a Proof-of-useful-work scheme for blockchain-based distributed deep learning", *Entropy*, Vol. 21 No. 8, p. 723.

Baliga, A., Solanki, N., Verekar, S., Pednekar, A., Kamat, P. and Chatterjee, S. (2018), "Performance characterization of hyperledger fabric", *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pp. 65-74.

Ball, M., Rosen, A., Sabin, M. and Vasudevan, P.N. (2017), "Proofs of useful work", *IACR Cryptology ePrint Archive*, p. 203, available at: https://eprint.iacr.org/2017/203.

Ball, M., Rosen, A., Sabin, M. and Vasudevan, P.N. (2018), "Proofs of work from worst-Case assumptions", *Advances in Cryptology—CRYPTO*, Vol. 10991, pp. 789-819.

Bentov, I., Lee, C., Mizrahi, A. and Rosenfeld, M. (2014), "Proof of activity: extending bitcoin's proof of work via proof of stake", *IACR Cryptology ePrint Archive*, Vol. 2014, p. 452.

Berdik, D., Otoum, S., Schmidt, N., Porter, D. and Jararweh, Y. (2021), "A survey on blockchain for information systems management and security", *Information Processing and Management*, Vol. 58 No. 1, 102397.

Blackcoin team (2020), "Blackcoin cryptocurrency", available at: https://blackcoin.org/.

Bouraga, S. (2021), "A taxonomy of blockchain consensus protocols: a survey and classification framework", *Expert Systems with Applications*, Vol. 168, 114384.

Cachin, C. and Vukolic, M. (2017), "Blockchain consensus protocols in the wild", *31st International Symposium on Distributed Computing*, Vol. 1, pp. 1-16.

Cao, B., Li, Y.X., Zhang, L., Zhang, L., Mumtaz, S., Zhou, Z.Y. and Peng, M.G. (2019), "When Internet of Things meets blockchain: challenges in distributed consensus", *IEEE Network*, Vol. 33 No. 6, pp. 133-139.

Cao, B., Wang, X.S., Zhang, W.Z., Song, H.B. and Lv, Z.H. (2020), "A many-objective optimization model of industrial internet of things based on private blockchain", *IEEE Network*, Vol. 34 No. 5, pp. 78-83.

Carrara, G.R., Burle, L.M., Medeiros, D.S.V., de Albuquerque, C.V.N. and Mattos, D.M.F. (2020), "Consistency, availability, and partition tolerance in blockchain: a survey on the consensus mechanism over peer-to-peer networking", *Annals of Telecommunications*, Vol. 75, pp. 163-174.

Castro, M. and Liskov, B. (1999), "Practical Byzantine fault tolerance", *Proceedings of the third symposium on Operating systems design and implementation (OSDI)*, pp. 173-186.

Castro, M. and Liskov, B. (2002), "Practical Byzantine fault tolerance and proactive recovery", *ACM Transactions on Computer Systems (TOCS)*, Vol. 20 No. 4, pp. 398-461.

Chen, J. and Micalib, S. (2019), "Algorand: a secure and efficient distributed ledger", *Theoretical Computer Science*, Vol. 777, pp. 155-183.

Chen, X., Nguyen, K. and Sekiya, H. (2021a), "An experimental study on performance of private blockchain in IoT applications", *Peer-to-Peer Networking and Applications*, Vol. 14 No. 5, pp. 3075-3091.

Chen, S.Y., Xie, M.Y., Liu, J. and Zhang, Y.N. (2021b), "Improvement of the DPoS consensus mechanism in blockchain based on PLTS", *2021 7th IEEE Intl Conference on Big Data Security on Cloud (BigDataSecurity)*, pp. 32-37.

Corbett, J.C., Dean, J., Epstein, M., Fikes, A., Frost, C., Furman, J.J., Ghemawat, S., Gubarev, A., Heiser, C., Hochschild, P., Hsieh, W., Kanthak, S., Kogan, E., Li, H., Lloyd, A., Melnik, S., Mwaura, D., Nagle, D., Quinlan, S., Rao, R., Rolig, L., Saito, Y., Szymaniak, M., Taylor, C., Wang, R. and Woodford, D. (2013), "Spanner: Google's globally distributed database", *ACM Transactions on Computer Systems*, Vol. 31 No. 3, pp. 1-22, Article No. 8, doi: 10.1145/2491245.

David, B., Gaži, P., Kiayias, A. and Russell, A. (2018), "Ouroboros praos: an adaptively-secure, semi-synchronous proof-of-stake blockchain", *Proceedings of International Association for Cryptologic Research*, pp. 66-98.

Decred community introduction to Decred governance (2019), available at: https://docs.decred.org/governance/introduction-to-decred-governance.

Du, M.X., Chen, Q.J., Xiao, J., Yang, H.H. and Ma, X.F. (2020), "Supply chain finance innovation using blockchain", *IEEE Transactions on Engineering Management*, Vol. 67 No. 4, pp. 1045-1058.

Dursun, T. and Üstündağ, B.B. (2021), "A novel framework for policy based on-chain governance of blockchain networks", *Information Processing and Management*, Vol. 58 No. 4, 102556.

Eyal, I., Gencer, A.E., Sirer, E.G. and Renesse, R. (2016), "Bitcoin-Ng: a scalable blockchain protocol", *Proceedings of the 13th USENIX Conference on Networked Systems Design and Implementation*, pp. 45-59.

Feng, J.Y., Zhao, X.Y., Chen, K.X., Zhao, F. and Zhang, G.H. (2020), "Towards random-honest miners selection and multi-blocks creation: proof-of-negotiation consensus mechanism in blockchain networks", *Future Generation Computer Systems*, Vol. 105, pp. 248-258.

Ferdous, M.S., Chowdhury, M.J.M. and Hoque, M.A. (2021), "A survey of consensus algorithms in public blockchain systems for crypto-currencies", *Journal of Network and Computer Applications*, Vol. 182, 103035.

Fu, X., Wang, H.M. and Shi, P.C. (2021), "A survey of blockchain consensus algorithms: mechanism, design and applications", *Science China Information Sciences*, Vol. 64, 121101.

Gourisetti, S.N.G., Mylrea, M., Patangia, M. and Patangia, H. (2020), "Evaluation and demonstration of blockchain applicability framework", *IEEE Transactions on Engineering Management*, Vol. 67 No. 4, pp. 1142-1156.

Guo, G.L., Zhu, Y., Chen, E., Zhu, G.Z., Ma, D. and Chu, W.C. (2022), "Continuous improvement of script-driven verifiable random functions for reducing computing power in blockchain consensus protocols", *Peer-to-Peer Networking and Applications*, Vol. 15, pp. 304-323.

Hanke, T., Movahedi, M. and Williams, D. (2018), "Dfinity technology overview series, consensus system", *arXiv preprint*, arXiv:1805.04548.

Huo, R., Zeng, S.Q., Wang, Z.H., Shang, J.J., Chen, W., Huang, T., Wang, S., Yu, F.R. and Liu, Y.J. (2022), "A comprehensive survey on blockchain in industrial internet of things: motivations, research progresses, and future challenges", *IEEE Communications Surveys and Tutorials*, Vol. 24 No. 1, pp. 88-122.

Jager, T. (2015), "Verifiable random functions from weaker assumptions", *Proceedings of Theory of Cryptography Conference*, pp. 121-143.

Javaid, U. and Sikdar, B. (2021), "A checkpoint enabled scalable blockchain architecture for industrial internet of things", *IEEE Transactions on Industrial Informatics*, Vol. 17 No. 11, pp. 7679-7687.

Johar, S., Ahmad, N., Asher, W., Cruickshank, H. and Durrani, A. (2021), "Research and applied perspective to blockchain technology: a comprehensive survey", *Applied Sciences*, Vol. 11 No. 14, p. 6252.

Khan, D., Jung, L.T. and Hashmani, M.A. (2021), "Systematic literature review of challenges in blockchain scalability", *Applied Sciences*, Vol. 11 No. 20, p. 9372.

Kim, H.M., Bock, G.W. and Lee, G. (2021), "Predicting Ethereum prices with machine learning based on blockchain information", *Expert Systems with Applications*, Vol. 184, 115480.

Kudva, S., Badsha, S., Sengupta, S., Khalil, I. and Zomaya, A. (2021), "Towards secure and practical consensus for blockchain based VANET", *Information Sciences*, Vol. 545, pp. 170-187.

Kyzy, I.E., Song, H.M., Vajdi, A., Wang, Y.L. and Zhou, J.L. (2021), "Blockchain for consortium: a practical paradigm in agricultural supply chain system", *Expert Systems with Applications*, Vol. 184, 115425.

Lamport, L. (1998), "The part-time parliament", *ACM Transactions on Computer Systems*, Vol. 16 No. 2, pp. 133-169.

Lao, L., Li, Z.C., Hou, S.L., Xiao, B., Guo, S.T. and Yang, Y.Y. (2020), "A survey of IoT applications in blockchain systems: architecture, consensus, and traffic modeling", *ACM Computing Surveys*, Vol. 53 No. 1, pp. 1-32, Article No. 18, doi: 10.1145/3372136.

Larimer, D. (2014), "Delegated proof-of-stake (dpos)", *Bitshare Whitepaper*, available at: http://www.bts.hk/dpos-baipishu.com.

Lei, K., Du, M.Y., Huang, J.Y. and Jin, T. (2020), "Groupchain: towards a scalable public blockchain in fog computing of IoT services computing", *IEEE Transactions on Services Computing*, Vol. 13 No. 2, pp. 252-262.

Li, K., Cheng, L.Q. and Teng, C. (2020), "Voluntary sharing and mandatory provision: private information disclosure on social networking sites", *Information Processing and Management*, Vol. 57 No. 1, 102128.

Li, G.C., Zhao, Q.L., Wang, Y., Qiu, T., Xie, K. and Feng, L. (2021a), "A blockchain-based decentralized framework for fair data processing", *IEEE Transactions on Network Science and Engineering*, Vol. 8 No. 3, pp. 2301-2315.

Li, P.L., Xu, H.X. and Ma, T.J. (2021b), "An efficient identity tracing scheme for blockchain-based systems", *Information Sciences*, Vol. 561, pp. 130-140.

Li, W.Z., He, M.S. and Haiquan, S. (2021c), "An overview of blockchain technology: applications, challenges and future trends", *2021 IEEE 11th International Conference on Electronics Information and Emergency Communication (ICEIEC)*, pp. 31-39.

Li, W.Y., Feng, C.L., Zhang, L., Xu, H., Cao, B. and Imran, M.A. (2021d), "A scalable multi-layer PBFT consensus for blockchain", *IEEE Transactions on Parallel and Distributed Systems*, Vol. 32 No. 5, pp. 1146-1160.

Li, Y.X., Qiao, L. and Lv, Z.H. (2021e), "An optimized Byzantine fault tolerance algorithm for consortium blockchain", *Peer-to-Peer Networking and Applications*, Vol. 14 No. 5, pp. 2826-2839.

Li, C.L., Zhang, J. and Yang, X.M. (2022), "Scalable blockchain storage mechanism based on two-layer structure and improved distributed consensus", *The Journal of Supercomputing*, Vol. 78 No. 4, pp. 4850-4881.

Liang, W., Fan, Y.K., Li, K.C., Zhang, D.F. and Gaudiot, J.L. (2020), "Secure data storage and recovery in industrial blockchain network environments", *IEEE Transactions on Industrial Informatics*, Vol. 16 No. 10, pp. 6543-6552.

Liang, W., Zhang, D.F., Lei, X., Tang, M.D., Li, K.C. and Zomaya, A.Y. (2021), "Circuit copyright blockchain: blockchain-based homomorphic encryption for IP circuit protection", *IEEE Transactions on Emerging Topics in Computing*, Vol. 9 No. 3, pp. 1410-1420.

Lin, M.W., Xu, Z.S., Zhai, Y.L. and Yao, Z.Q. (2018a), "Multi-attribute group decision-making under probabilistic uncertain linguistic environment", *Journal of the Operational Research Society*, Vol. 69 No. 2, pp. 157-170.

Lin, M.W., Wang, H.B., Xu, Z.S., Yao, Z.Q. and Huang, J.L. (2018b), "Clustering algorithms based on correlation coefficients for probabilistic linguistic term sets", *International Journal of Intelligent Systems*, Vol. 33 No. 12, pp. 2402-2424.

Lin, M.W., Chen, Z.Y., Liao, H.C. and Xu, Z.S. (2019a), "ELECTRE II method to deal with probabilistic linguistic term sets and its application to edge computing", *Nonlinear Dynamics*, Vol. 96 No. 3, pp. 2125-2143.

Lin, M.W., Huang, C. and Xu, Z.S. (2019b), "MULTIMOORA based MCDM model for site selection of car sharing station under picture fuzzy environment", *Sustainable Cities and Society*, Vol. 53, 101873.

Lin, M.W., Huang, C., Xu, Z.S. and Chen, R.Q. (2020), "Evaluating IoT platforms using integrated probabilistic linguistic MCDM method", *IEEE Internet of Things Journal*, Vol. 7 No. 11, pp. 11195-11208.

Lin, M.W., Chen, Z.Y., Xu, Z.S., Gou, X. and Herrera, F. (2021a), "Score function based on concentration degree for probabilistic linguistic term sets: an application to TOPSIS and VIKOR", *Information Sciences*, Vol. 551, pp. 270-290.

Lin, M.W., Chen, Y.Q. and Chen, R.Q. (2021b), "Bibliometric analysis on Pythagorean fuzzy sets during 2013-2020", *International Journal of Intelligent Computing and Cybernetics*, Vol. 14 No. 2, pp. 104-121.

Liu, Y. and Xu, G.X. (2021), "Fixed degree of decentralization DPoS consensus mechanism in blockchain based on adjacency vote and the average fuzziness of vague value", *Computer Networks*, Vol. 199, 108432.

Liu, H.O., Zhou, Y.Y., Zhang, Y.M. and Su, Y.Y. (2021a), "A rough set fuzzy logic algorithm for visual tracking of blockchain logistics transportation labels", *Journal of Intelligent and Fuzzy Systems*, Vol. 41 No. 4, pp. 4965-4972.

Liu, J., Xie, M.Y., Chen, S.Y., Ma, C. and Gong, Q.H. (2021b), "An improved DPoS consensus mechanism in blockchain based on PLTS for the smart autonomous multi-robot system", *Information Sciences*, Vol. 575, pp. 528-541.

Liu, T., Yuan, Y. and Yu, Z.Y. (2021c), "The service architecture of Internet of things terminal connection based on blockchain technology", *The Journal of Supercomputing*, Vol. 77, pp. 12690-12710.

Liu, J., Zhao, J., Huang, H.H. and Xu, G.X. (2022), "A novel logistics data privacy protection method based on blockchain", *Multimedia Tools and Applications*, Vol. 81, pp. 23867-23887.

Long, T., Qu, S., Li, Q., Kang, H.Q., Fu, L.Y., Wang, X.B. and Zhou, C.H. (2021), "Efficient block propagation in wireless blockchain networks and its application in bitcoin", *IEEE Transactions on Network Science and Engineering*, Vol. 8 No. 4, pp. 3349-3368.

Luo, Y.H., Chen, Y.Q., Chen, Q. and Liang, Q.L. (2018), "A new election algorithm for DPoS consensus mechanism in blockchain", *2018 7th International Conference on Digital Home (ICDH)*, pp. 116-120.

Luu, L., Narayanan, V., Zheng, C.D., Baweja, K., Gilbert, S. and Saxena, P. (2016), "A secure sharding protocol for open blockchains", *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 17-30.

Madhura, K. and Mahalakshmi, R. (2022), "Designing an optimized confidential-data management system using preeminent access-control and block-chain", *International Journal of Intelligent Computing and Cybernetics*, Vol. ahead-of-print No. ahead-of-print, doi: 10.1108/IJICC-12-2021-0295.

Mar, G.A., Jose, M.F., Lorena, G.M. and David, A. (2021), "Achieving cybersecurity in blockchain-based systems: a survey", *Future Generation Computer Systems*, Vol. 124, pp. 91-118.

Matzutt, R., Kalde, B., Pennekamp, J., Drichel, A., Henze, M. and Wehrle, K. (2021), "CoinPrune: shrinking bitcoin's blockchain retrospectively", *IEEE Transactions on Network and Service Management*, Vol. 18 No. 3, pp. 3064-3078.

Membrey, P., Plugge, E. and Hawkins, D. (2010), "Sharding", in Pohlmann, F., Lowman, M. and Markham, J. (Eds), *The Definitive Guide to MongoDB: The NoSQL Database for Cloud and Desktop Computing*, Apress, New York, ISBN: 9781430230519.

Meng, T., Zhao, Y., Wolter, K. and Xu, C.Z. (2021), "On consortium blockchain consistency: a queueing network model approach", *IEEE Transactions on Parallel and Distributed Systems*, Vol. 32 No. 6, pp. 1369-1382.

Mišić, J., Mišić, V.B., Chang, X., Motlagh, S.G. and Ali, M.Z. (2020), "Modeling of bitcoin's blockchain delivery network", *IEEE Transactions on Network Science and Engineering*, Vol. 7 No. 3, pp. 1368-1381.

Mizrahi, A. and Rottenstreich, O. (2021), "Blockchain state sharding with space-aware representations", *IEEE Transactions on Network and Service Management*, Vol. 18 No. 2, pp. 1571-1583.

Mukta, R., Paik, H., Lu, Q.H. and Kanhere, S.S. (2022), "A survey of data minimisation techniques in blockchain-based healthcare", *Computer Networks*, Vol. 205, 108766.

Nakamoto, S. (2008), "Bitcoin: a peer-to-peer electronic cash system", available at: https://bitcoin.org/bitcoin.pdf.

NEO white paper (2014), available at: http://docs.neo.org/en-us/ (accessed 2019).

Nguyen, G.T. and Kim, K. (2018), "A survey about consensus algorithms used in blockchain", *Journal of Information Processing Systems*, Vol. 14 No. 1, pp. 101-128.

Oliveira, M.T., Reis, L.H.A., Medeiros, D.S.V., Carrano, R.C., Olabarriaga, S.D. and Mattos, M.F. (2020), "Blockchain reputation-based consensus: a scalable and resilient mechanism for distributed mistrusting applications", *Computer Networks*, Vol. 179, 107367.

Ongaro, D. and Ousterhout, J.K. (2015), "In search of an understandable consensus algorithm", *USENIX Annual Technical Conference 2014*, pp. 305-319, available at: https://raft.github.io/raft.pdf.

Palai, A., Vora, M. and Shah, A. (2018), "Empowering light nodes in blockchains with block summarization", *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pp. 1-5.

Pu, Y.W., Xiang, T., Hu, C.Q., Alrawais, A. and Yan, H.Y. (2020), "An efficient blockchain-based privacy preserving scheme for vehicular social networks", *Information Sciences*, Vol. 540, pp. 308-324.

Qu, X.D., Wang, S.L., Hu, Q. and Cheng, X.Z. (2021), "Proof of federated learning: a novel energy-recycling consensus algorithm", *IEEE Transactions on Parallel and Distributed Systems*, Vol. 32 No. 8, pp. 2074-2085.

Saad, M., Spaulding, J., Njilla, L., Kamhoua, C.A., Shetty, S., Nyang, N.D. and Mohaisen, D. (2020), "Exploring the attack surface of blockchain: a comprehensive survey", *IEEE Communications Surveys and Tutorials*, Vol. 22 No. 3, pp. 1977-2008.

Salimitari, M., Chatterjee, M. and Fallah, Y.P. (2020), "A survey on consensus methods in blockchain for resource-constrained IoT networks", *Internet Things*, Vol. 11, 100212.

Sompolinsky, Y. and Zohar, A. (2015), "Secure high-rate transaction processing in bitcoin", in Böhme, R. and Okamoto, T. (Eds), *Financial Cryptography and Data Security. FC 2015. Lecture Notes in Computer Science*, Springer, Berlin, Heidelberg, Vol. 8975, doi: 10.1007/978-3-662-47854-7_32.

Song, H.Y., Zhu, N.F., Xue, R.X., He, J.S., Zhang, K. and Wang, J.Y. (2021), "Proof-of-contribution consensus mechanism for blockchain and its application in intellectual property protection", *Information Processing and Management*, Vol. 58 No. 3, 102507.

Sun, G., Dai, M., Zhang, F., Yu, H.F., Du, X.J. and Guizani, M. (2020), "Blockchain enhanced high-confidence energy sharing in internet of electric vehicles", *IEEE Internet of Things Journal*, Vol. 7 No. 9, pp. 7868-7882.

Sun, Y., Xue, R., Zhang, R., Su, Q.Q. and Gao, S. (2021a), "RTChain: a reputation system with transaction and consensus incentives for e-commerce blockchain", *ACM Transactions on Internet Technology*, Vol. 21 No. 1, pp. 1-24.

Sun, G., Dai, M., Sun, J. and Yu, H.F. (2021b), "Voting-based decentralized consensus design for improving the efficiency and security of consortium blockchain", *IEEE Internet of Things Journal*, Vol. 8 No. 8, pp. 6257-6272.

Tan, P.L., Zou, W.S. and Tang, W.Q. (2022), "A consensus algorithm with leadership transfer-LTRaft", *15th China Conference on Wireless Sensor Networks (CWSN)*, pp. 235-249.

Tenorio-Fornés, A., Tirador, E.P., Sánchez-Ruiz, A.A. and Hassan, S. (2021), "Decentralizing science: towards an interoperable open peer review ecosystem using blockchain", *Information Processing and Management*, Vol. 58 No. 6, 102724.

Treiblmaier, H., Swan, M., Filippi, P., Lacity, M.C., Hardjono, T. and Kim, H. (2021), "What's next in blockchain research?: - an identification of key topics using a multidisciplinary perspective", *Data Base*, Vol. 52 No. 1, pp. 27-52.

Vasin, P. (2014), "Blackcoin's proof-of-stake protocol v2", available at: https://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf.

Verma, S., Yadav, D. and Chandra, G. (2022), "Introduction of formal methods in blockchain consensus mechanism and its associated protocols", *IEEE Access*, Vol. 10, pp. 66611-66624.

Wan, S.H., Li, M.J., Liu, G.Y. and Wang, C. (2020), "Recent advances in consensus protocols for blockchain: a survey", *Wireless Networks*, Vol. 26 No. 8, pp. 5579-5593.

Wang, W.B., Hoang, D.T., Hu, P.Z., Xiong, Z.H., Niyato, D., Wang, P., Wen, Y.G. and Kim, D.I. (2019), "A survey on consensus mechanisms and mining strategy management in blockchain networks", *IEEE Access*, Vol. 7, pp. 22328-22370.

Wang, T.T., Zhao, C.H., Yang, Q., Zhang, S.L. and Liew, S.C. (2021a), "Ethna: analyzing the underlying peer-to-peer network of Ethereum blockchain", *IEEE Transactions on Network Science and Engineering*, Vol. 8 No. 3, pp. 2131-2146.

Wang, X., Ni, W., Zha, X., Yu, G.S., Liu, R.P., Georgalas, N. and Reeves, A. (2021b), "Capacity analysis of public blockchain", *Computer Communications*, Vol. 177, pp. 112-124.

Wang, S.M., Ye, D.D., Huang, X.M., Yu, R., Wang, Y.J. and Zhang, Y. (2021c), "Consortium blockchain for secure resource sharing in vehicular edge computing: a contract-based approach", *IEEE Transactions on Network Science and Engineering*, Vol. 8 No. 2, pp. 1189-1201.

Wang, L., Bai, Y., Jiang, Q., Leung, V.C.M., Cai, W. and Li, X.X. (2021d), "Beh-raft-chain: a behavior-based fast blockchain protocol for complex networks", *IEEE Transactions on Network Science and Engineering*, Vol. 8 No. 2, pp. 1154-1166.

Wang, D., Jin, C.G., Xiao, B.B., Li, Z. and He, X. (2021e), "Proof-of-activity consensus algorithm based on K-medoids clustering", *Big Data Research*, Vol. 26, 100266.

Wen, X.J., Chen, Y.Z., Fan, X.C., Zhang, W., Yi, Z.Z. and Fang, J.B. (2022), "Blockchain consensus mechanism based on quantum zero-knowledge proof", *Optics and Laser Technology*, Vol. 147, 107693.

Wood, G. (2014), "A secure decentralized generalized transaction ledger", *Ethereum Project Yellow Paper*, available at: http://gavwood.com/paper.pdf.

Wu, J.J., Liu, J.L., Chen, W.L., Huang, H.W., Zheng, Z.B. and Zhang, Y. (2022), "Detecting mixing services via mining bitcoin transaction network with hybrid motifs", *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, Vol. 52 No. 4, pp. 2237-2249.

Xu, G.X., Liu, Y. and Khan, P.W. (2020), "Improvement of the DPoS consensus mechanism in blockchain based on vague sets", *IEEE Transactions on Industrial Informatics*, Vol. 16 No. 6, pp. 4252-4259.

Xu, G.X., Dong, J.N. and Ma, C. (2021a), "A certificateless encryption scheme based on blockchain", *Peer-to-Peer Networking and Applications*, Vol. 14 No. 5, pp. 2952-2960.

Xu, Y.T., Yang, X.Y., Zhang, J.L., Zhu, J.W., Sun, M.S. and Chen, B. (2021b), "Proof of engagement: a flexible blockchain consensus mechanism", *Wireless Communications and Mobile Computing*, Vol. 6185910, pp. 1-6185910:10.

Xu, X.L., Zhu, D.W., Yang, X.X., Wang, S., Qi, L.Y. and Dou, W.C. (2021c), "Concurrent practical Byzantine fault tolerance for integration of blockchain and supply chain", *ACM Transactions on Internet Technology*, Vol. 21 No. 1, pp. 1-17, Article No. 7, doi: 10.1145/3395331.

Yan, Z., Peng, L., Feng, W. and Yang, L.T. (2021), "Social-chain: decentralized trust evaluation based on blockchain in pervasive social networking", *ACM Transactions on Internet Technology*, Vol. 21 No. 1, pp. 1-28, Article No. 17, doi: 10.1145/3419102.

Yang, F., Shi, Y., Wu, Q.Q., Li, F., Zhou, W., Hu, Z.Y., Xiong, N.X. and Zhang, Y. (2019), "The survey on intellectual property based on blockchain technology", *2019 IEEE International Conference on Industrial Cyber Physical Systems (ICPS)*, pp. 743-748.

Yang, J.W., Paudel, A. and Gooi, H.B. (2021), "Compensation for power loss by a proof-of-stake consortium blockchain microgrid", *IEEE Transactions on Industrial Informatics*, Vol. 17 No. 5, pp. 3253-3262.

Yi, H.B., Li, Y.P., Wang, M., Yan, Z.X. and Nie, Z. (2021), "An efficient blockchain consensus algorithm based on post-quantum threshold signature", *Big Data Research*, Vol. 26, 100268.

Yuen, T.H. (2020), "PAChain: private, authenticated and auditable consortium blockchain and its implementation", *Future Generation Computer Systems*, Vol. 112, pp. 913-929.

Zhang, P.Y., Zhou, M.C., Zhao, Q.X., Abusorrah, A. and Bamasag, O.O. (2021), "A performance-optimized consensus mechanism for consortium blockchains consisting of trust-varying nodes", *IEEE Transactions on Network Science and Engineering*, Vol. 8 No. 3, pp. 2147-2159.

Zheng, Z.B., Xie, S.A., Dai, H.N., Chen, X.P. and Wang, H.M. (2017), "An overview of blockchain technology: architecture, consensus, and future trends", *Proceedings of IEEE international congress on big data (BigData Congress)*, pp. 557-564.

Corresponding author
Jun Liu can be contacted at: junliu@cqupt.edu.cn