A research on the consensus mechanisms

Jiawei Peng[1, †], Yijun Wu[2, †] and Kunfeng Yuan[3, 4, †]

[1] Faculty of Information Management, Beijing Information Science and Technology University, Beijing, 100192, China
[2] Faculty of Information Technology, Beijing University of Technology, Beijing, 100124, China
[3] School of Computing and Mathematical Sciences, University of Waikato, Hamilton, 3204, New Zealand

[4] Corresponding author's e-mail: ky109@students.waikato.ac.nz
[†] These authors contributed equally.

Abstract. A distributed and decentralized ledger widely used in the computer science and financial fields called blockchain has provided safe and fast transactions for multiple parties. Also, check the transaction by each node on the blockchain. The consensus mechanism is the core of the blockchain. It lets all the nodes reach an agreement for those transactions, which ensures security and accuracy and make Bitcoin valuable and popular. Two of the most mainstream Consensus mechanisms are Proof of Work (PoW) and Proof of Stake (PoS), and Proof of Authority (PoA) is the new one that will apply in the future. Many discourses talk about consensus mechanisms, most of which are review papers. Those papers mainly show a specific aspect of a consensus mechanism or introduce the primary notion, but they rarely explain the corresponding relationship between theories and cryptocurrency. So, the purpose is to give a clear structure, connect the consensus mechanism to its application and simplify the reader's understanding. This paper aims to provide an overview of the consensus mechanism, including its general definition, concepts of different mechanism variants, and advantages and disadvantages. For the structure below, the essay introduces the notion of consensus mechanism and how PoW, PoS, and PoA work. Then summarize the papers based on these three consensus mechanisms, describing the theories of many consensus mechanisms and comparing the advantages and disadvantages. The essay also creates a comparison table about these three consensus mechanisms to embody the content above the stem better.

Keywords: consensus mechanism, blockchain, cryptocurrency, application.

1. Introduction

Over the last decade, blockchain has experienced significant development and has become applied in various industries [1]. It has attracted much popularity in both computer science and financial fields. *Blockchain* is a decentralized ledger that enables secure, transparent, and tamper-proof transactions without intermediaries. It allows multiple parties to transact anonymously, and every node on the blockchain will verify every transaction.

As one of the essential technologies applied in blockchain, the consensus mechanism is used in distributed computing that aids distributed networks in reaching a consensus regarding the worth of some shared data [2]. The consensus mechanism makes everyone recognize the distributed ledger and makes Bitcoin valuable and payable. It precisely ensures the security and accuracy of transactions on the blockchain, which is why blockchain and bitcoin have been admitted and transacted. In recent years, the mainstream development trend of the consensus mechanism is from Proof-of-Work to Proof-of-Stake, and Proof-of-Authority may become the mechanism applied in next-generation cryptocurrencies.

There are now a large number of papers on consensus mechanisms in the blockchain field. Most of these are review papers. Some focus on a specific aspect of a consensus mechanism. Others introduce the basic concept of various consensus mechanisms based on PoW, and so on. For example, the PoS mechanism has two mainstream principles applied to PPcoin and Ethereum. However, many papers confuse them together. And do not indicate which principle corresponds to which cryptocurrency. In this paper, the purpose is to make the paper structure more clearly and introduce the specific consensus mechanism with its specific application cryptocurrency to present these consensus mechanisms more clearly for readers to understand better.

This paper aims to provide an overview of the consensus mechanism, including a general definition, concepts of different mechanism variants, and advantages of disadvantages. The remainder of this chapter is organized as follows. In the second part, the essay introduces the concept of consensus mechanism and the principles of PoW, PoS, and PoA, respectively. Then by summarizing the papers, it describes in detail the principles of many consensus mechanisms based on these three mechanisms and outlines their advantages and disadvantages. Finally, the essay summarizes a comparison table of the above mechanisms better to present their differences, advantages, and disadvantages.

2. Consensus mechanism

As one of the four core blockchain technologies, the consensus mechanism is used to maintain the global unity of the state of distributed ledger and ensure the safety of the entire blockchain network. Consensus Mechanism is a pattern or method to achieve a standard view among different groups, nodes, validators, or entities. Create rules and relevant protocols to let those nodes or entities agree on all the legitimate transactions simultaneously, even with high handle speed. After that, those nodes will add these transactions to the blockchain. It can unify those single and distributed nodes to have the same opinions and ideas. In addition, the consensus mechanism is responsible for increasing fault tolerance and activity in the blockchain network operation [3]. Therefore, the consensus mechanism is an indispensable element of blockchain and the key to ensuring the regular operation of a blockchain system. Unlike the centralized network, blockchain is a decentralized system that allows transactions to be recorded and verified securely and transparently without a central authority or intermediary. Due to the decentralized nature of blockchain, the blockchain system will inevitably be affected by incorrect data submitted by malicious nodes. Consensus Mechanism has to ensure that all nodes maintain a consistent view of the shared ledger, even in the presence of malicious actors. The blockchain consensus mechanism has two properties. The first is to verify the data to ensure its correctness of the data. It then selects a node through the consensus mechanism to create a block containing transactions to the blockchain. The consensus mechanism enables transaction validation with a large number of votes in a short time. A large number of unrelated nodes quickly votes for a transaction. If these nodes can reach a consensus, the whole network is considered to have reached a consensus on the transaction. It enables decentralized networks of nodes to agree on a shared state and validate new transactions. The consensus mechanism solves the problem of recording and copying the transaction history between untrusted nodes in an open-access network. Consensus mechanisms allow a large number of nodes to synchronize global blockchain data without authentication [1]. By using Consensus Mechanism, blockchain can work more efficiently without centralized organizations. The choice of consensus mechanism can have significant implications for a blockchain system's security, scalability, and energy efficiency, making it an essential consideration for blockchain developers and users. There are several consensus mechanisms

2.1. PAXOS

The first proposed consensus mechanism is PAXOS. Node communication in a distributed system is divided into "Shared memory" and "Message passing" models. The distributed system based on the message-passing communication model will inevitably produce a slow, freeze, or restart process, resulting in message delay, loss, and duplication. PAXOS is primarily responsible for selecting a single value when the network causes the above problems. In this way, the consensus resolution can be guaranteed regardless of any abnormal situation mentioned above [3].

PAXOS divides the roles of nodes into proposers, acceptors, and learners. [3] Proposers propose including the serial number and the value. Acceptors decide whether a proposal is accepted after receiving it and forwarding a message. However, if multiple proposals are accepted by acceptors, or exactly half of the acceptors numbered X and half of the acceptors numbered Y, then a unity problem occurs. Therefore, PAXOS has a set of rules to prevent uniformity problems. PAXOS limits acceptors to accepting proposals only from proposers. In the execution of the algorithm, each acceptor can accept only one proposal, X, and will not accept proposals with a number smaller than X. Therefore, the serial number of the proposal can be used as a timeline throughout the process of algorithm execution. If proposers want to update the proposal, they can propose with a higher number. Acceptors must also notify the proposer to interrupt the proposal if they find a proposal with a higher number. After the acceptors have responded, the proposer needs to collect whether most acceptors have accepted the proposal. If the proposal receives more than N/2 - 1 acceptances, the proposal is deemed to have been accepted by most acceptors. Acceptors broadcast the accepted values to all learners. If rejected, the proposer must develop new values to update the proposal.

The premise of the PAXOS algorithm is that there is no Byzantine checkmate problem. Because PAXOS was the first proposed consensus mechanism, it was a primitive consensus and could not solve the Byzantine general problem. The Byzantine Checkmate problem is the most common in the blockchain. This problem is caused by instability in the nodes participating in the blockchain due to hardware failure, network problems, or under attacks.

2.2. Proof of Work (PoW)

*T*he proof-of-work mechanism is one of the mainstream consensus mechanisms used in cryptocurrency, and it is also the earliest one proposed in the mainstream consensus mechanism. PoW mechanism requires the user to perform relatively complex hashing calculations by consuming time and energy as proof. The main principle of PoW calculation is the hash function. Select any value x in the hash function h() to get h(x). Let the function change x will trigger the avalanche effect. In this case, h(x) can be considered a one-way hash function, and x cannot be deduced backward by h(x). Specifying the characteristics of search h(x) lets the user do the exhaustive calculation and achieve the proof of work.

The blockchain has a nonce. Miners race to find the specified hash by hashing the block header and the nonce. Miners who find accepted nonce first will be allowed to add a block to the blockchain and receive a reward for that block. Therefore, miners will broadcast the target value in the whole network after obtaining it. Each node in the network will be asked to confirm the authenticity of the hash value and append the newly appended blocks to their blockchain [3].

2.3. Proof of Stake (PoS)

The birth of PoS can be traced back to 2011, a netizen named Quantum Mechanic first proposed Proof of Stake in the famous Bitcoin community Bitcointalk forum.

Unlike the PoW mechanism, which requires miners to solve complex mathematical problems to validate transactions, PoS relies on validators who hold a stake in the network to verify transactions. In the PoS system, a node can validate (equally to the mining process in PoW) block transactions based on their stake value [4], e.g., digital tokens that a person holds in cryptocurrencies. Due to the principle that PoS applied, the PoS mechanism has lower energy consumption, and the validators are more motivated to maintain the blockchain's correctness and integrity.

Nowadays, two main models of PoS are widely used in blockchains. The first is the model represented by Peercoin, the first digital currency to apply the PoS mechanism, which introduces the concept of coinage. The equity is essentially the coin's age, the number of tokens multiplied by the length of the most recent transaction [5]. The following is the formula of the algorithm:

$$coinAge = coins * coindays \tag{1}$$

$$\text{blockHash} <= \text{Target} * \text{coinAge} \tag{2}$$

The concept of coins represents the number of coins held by the nodes. The idea of coin days represents the number of days on the tokens. Target is the mining difficulty value for the whole network. In this model, validators with more coinage are more likely to be chosen to create new blocks. This method dramatically improves the efficiency of mining. The second is a model represented by the Bitcoin Casper protocol. It requires the verifier to deposit their voting bloc. If the block is confirmed, validators will get rewards. Otherwise, validators will lose a part of their deposits as a penalization. Users will be penalized by having their deposits cleared if they exhibit malicious behaviors, such as voting for checkpoints that clash with one another [6].

2.4. Proof of Authority (PoA)

In the blockchain system, the wide use of the Consensus Mechanism is Proof of Work and Proof of Stake. Proof of Authority is a new Consensus Mechanism, and it has been proposed in recent years. This algorithm provides high performance. It also provides a practical and efficient solution for blockchains. Proof of Authority emphasizes the importance of identity. The nodes are a group of validators, they stake their reputation to ensure the whole chain and have the authority to create new nodes, which means those nodes who prove their identity can create new nodes, but these new nodes should pass the preliminary authentication. Because Proof of Authority is based on the participant’s reputation and identity, so does not need strong computing power and fast hardware. This method accelerates the speed of transactions and provides an efficient model. For the basic theory of Proof of Authority, first, all the participants in PoA blockchain elect authority, which is the validator. While there are new transactions, not unlike other consensus mechanisms that send transaction information among each node, those participants in the PoA blockchain send those transactions to the validators. Validators handle and verify those transactions, ensuring the whole blockchain is stable. After validators sign those transactions, all the ordinary nodes synchronize the data of those transactions and relevant information from validators.

The safety of Proof of Authority and its blockchain can be verified; at first, the election of validators is strict, they should share their reputation and identity, which means it is hard for them to give false data or be controlled by others because all the ordinary nodes can see the status and conditions of validators and the process of the elect is strict too, it can also prevent Denial-of-service attacks and 51% attack well. However, Proof of Authority still needs more. Considering the factors above, it is easy to see that PoA has centralized problems. Validators are the center of the blockchain network. Although ordinary nodes can see it, they need help to supervise. So, the election of validators is decentralized, while there are many validators from different countries and profit groups, which can solve this problem. Next, ordinary nodes also have complete information on those transactions, so they can verify some prominent transactions which are illegal.

3. PoW, PoS, PoA related

3.1. PoW-based mechanism

POW has apparent advantages. It allows all the nodes to participate, so it is truly decentralized. Furthermore, its safety is guaranteed. Unless the attacker's computing power can exceed 50% of the entire network (51% of attacks), it is difficult for the attack to succeed. Therefore, the consistency of the transaction state of the blockchain network can be guaranteed.

However, the disadvantages of PoW are also very obvious. PoW's efficiency is low. Bitcoin can only confirm about seven transactions per second, which cannot meet the speed of commercial demand. Furthermore, it is very energy intensive. The total energy invested in cryptocurrencies may exceed the amount in some small countries. This consumption results in much-wasted energy. As the difficulty of mining across the net continued to improve, some owners of significant computing power began to monopolize computing power through much equipment. This phenomenon led to a concentration of computing power, contrary to the original idea of decentralization.

3.1.1. Proof of Work time. PoWT is an alternative to PoW, mainly to solve the problem of computing waste in PoW. In PoW, blocks adjustment difficulty wastes computational power. PoWT adds a block of time properties. This change increases the transaction speed of the blockchain and the mining capacity, bringing the transaction speed and mining capacity into line. This solution eliminates the waste of computing power by proposing a variable block creation rate related to mining capacity [3].

3.1.2. Snow White. P. Daian et al. proposed a consensus mechanism called Snow White. Snow White uses a "sleepy consensus" paradigm as its core. This protocol does not need to limit the number of participants. It believes consistency can be guaranteed if most online users remain honest [7]. Snow White has a process for selecting committee nodes. These committee nodes are considered trusted nodes in the blockchain, and they vote to elect the leader of the newly created block. Unlike PoW, Snow White provides a timestamp for the hash function as an alternative to nonce. The nodes of the Snow-White mechanism can withstand multiple reorganizations of committees and the presence of dishonest nodes, so it has high stability [3] [8].

3.1.3. Hybrid Proof of Work. Lynx introduced HPoW as an alternative to PoW. This mechanism maximizes the computational contribution of miners by eliminating incentives. Instead of rewarding the fastest miners, the system rewards randomly selected miners. Because of this incentive mechanism, the proof method does not require any hashing ability. As a restriction, HPoW does not allow a miner to receive a reward for 30 minutes in a row [9].

3.1.4. Proof of Ddos. The PoD method is one of the alternatives to PoW. This method provides a large amount of network traffic to incentivize the actor to attack the victim server, which is also called malicious PoW. This approach selects the server fairly, and then the actor needs to establish a large number of TLS connections to the target server, using encryption response to prove that they have established a large number of links. That is how miners prove they were involved in a DDOS attack on a target server. This method can also be used to measure a target's bandwidth utilization or resource consumption [10].

3.1.5. Proof of Burn. As an alternative to PoW, PoB is more efficient and sustainable than traditional PoW solutions. Miners use eater addresses to transmit and burn coins. The eater is an unrecoverable address containing a public key without any private key to prevent a coin from being retrieved. Coins are permanently lost when sent to the eater. Users burn coins to represent an investment in the blockchain and gain virtual mining power. So, the user burns coins to gain mining power, and the more they burn, the more power they gain. PoB and PoW are similar in calculating block validation. All transactions that transfer coins to an eater address will be recorded, and hash values will be calculated using the SHA-256. Finally, the user with the lowest hash value gets the mining rights [3] [11].

3.1.6. Fast Paxos. FAST PAXOS is an extension of traditional PAXOS. This solution bypasses the leader and transfers the proposal directly to the validator. This approach saves one message latency compared to traditional PAXOS. Therefore, this method speeds up the learning process and improves fault tolerance. If a conflict occurs, add a message delay. If a conflict occurs, add a message delay [3][12].

3.1.7. Proof of useful work. PoUW is also an alternative to PoW and has the properties of PoW. This scheme is based on delegates of polynomials of lower order. The client issues low-degree polynomial problems. The miner deals with issues issued by the principal and selects the block to be mined from among the issues issued. At the end of the mining, the miner attaches proof of use details to the block. The verifier verifies whether the problem is solved using the block's hash. Based on this scheme, PoUW can be applied to solve many practical problems [3][9].

To solve the existing problems of consensus mechanisms, people put forward a lot of new consensus mechanisms. Most consensus mechanisms derive new changes from the original foundation or fill the original shortcomings. PoWT, Snow White, HPoW, and other mechanisms have improved the mining efficiency to varying degrees. Some mechanics also try to fix the problem of energy waste in PoW, as shown in Table 1.

Table 1. Proof-of-work.

Type	Main idea	Advantages	Disadvantages
PROOF OF WORK TIME	Eliminate waste of computing power by adjusting transaction speed and mining time	Avoid wasting computing power	It doesn't solve the speed problem
SNOW WHITE [8]	Join the committee system based on POW	High stability	
HYBRID PROOF OF WORK [9]	Based on POW, the incentive system was changed to randomly reward miners	No hashing ability is required	It still hasn't solved the problem of slow transactions.
PROOF OF DDoS [10]	Get rewards for participating in DDOS attacks on targeted websites	Can be used to measure the bandwidth utilization or resource consumption of the target	
PROOF OF BURN [11]	Burn coins to gain mining ability	More efficient and sustainable	
FAST PAXOS [12]	Bypass the leader and transfer the proposal directly to the validator	Improved fault tolerance compared with traditional PAXOS	
PROOF OF USEFUL WORK	Mining capability is obtained by resolving published low-order polynomial delegates	It can solve practical problems	

3.2. PoS-based mechanism

3.2.1. PPcoin. Sunny King and Scott Nadal proposed a Peer-to-Peer cryptocurrency named PPcoin with Proof-of-Stake, which is the first time a digital currency applied the PoS mechanism. The main idea of PPcoin is to define a concept of coin age to play a role in the minting process. The coin age represents a period in which nodes hold a certain number of coins. Once the nodes spend the coins, system destroy their coinage corresponding to the coins. For example, Eric holds 100 coins for 20 days, and then Eric has 2000 coin-days of coinage. If Eric spends the 200 coins, the coinage of the 200 coins will be consumed. It means that even if Eric immediately gets the 200 coins back through the transaction, the coinage of his current 200 coins will be 0. In the minting process, the mining difficulty decreases, and the likelihood of finding the block increases as more coinages are spent [5]. The PPcoin's mechanism can set a more superficial matching hash target value for nodes that invest more coinage so that these nodes can spend less computing resources to reach the target and create blocks. This mining mechanism reflects the essence of the PoS mechanism. That is, the coin stake weight invested by the node will determine the eligibility to establish a new block.

Some advantages are presented in [13]. First, PPcoin's PoS mechanism dramatically reduces energy consumption because it uses a finite search space (specifically, one hash per unspent wallet output per second) for hashing rather than an unbounded search space like proof-of-work [14]. Second, it can reduce the risk of a 51% attack. In the PoS mechanism, it is almost impossible for an attacker to control 51% of the stake in the entire network. In addition, the attacker will lose all his coin age once he launches an attack, which significantly reduces the frequency and success rate of the system being attacked. Third, it can mitigate the risk of a long-range and double-spending attack in PPcoin networks. The system introduces checkpoints in the blockchain history, making it more difficult for attackers to rewrite. In simple terms, checkpoints prevent the blockchain from reorganizing from very far historical blocks.

After PPcoin, more and more cryptocurrencies, such as Nxt and Black coin, began to adopt the exact PoS consensus mechanism.

3.2.2. Ethereum with Casper Protocol. Vitalik Buterin and Virgil Griffith proposed a consensus mechanism called Casper based on PoS, which was used for the transition of Ethereum from PoW to PoS mechanism. On September 15, 2022, the two Ethereum chains that adopted PoS and PoW were merged successfully, which means that Ethereum will fully adopt the PoS mechanism.

Unlike PPcoin's PoS mechanism, the Casper protocol is based on the Byzantine fault tolerant (BFT) consensus algorithm. Due to the BFT, regardless of network latency, the algorithm cannot finish conflicting blocks as long as more than two-thirds of the participants are honestly following the protocol. [15]. In Casper, validators are responsible for proposing and verifying blocks and must stake a certain number of coins as collateral to participate. Selection System will randomly select validators to propose blocks and reward them for doing so correctly. However, validators can also be penalized if they act maliciously. Vitalik Buterin and Virgil Griffith establish that Casper satisfies two crucial properties: accountable safety and plausible liveness. Accountable safety ensures that finalizing two conflicting checkpoints is possible if at least one-third of validators violate a slashing condition [15]. On the other hand, plausible liveness ensures that a new checkpoint can always be finalized without any validator violating a slashing condition if at least two-thirds of the validators follow the protocol [15].

Owing to the mechanism of Casper, some merits can be concluded:

1)Like all PoS mechanisms, the Casper protocol has higher energy efficiency than the PoW mechanism.

2)The Casper protocol has improved security and reliability. It utilizes a "punishment mechanism," whereby validators who do not follow the rules lose a portion of their tokens. It incentivizes validators to act by the rules, ensuring the network's security.

3)It has faster transaction confirmation times.

It avoids the issue of the slow transaction confirmation times caused by great mining difficulty in PoW.

The Casper protocol also provides a solution to possible attacks on PoS. A unique fork selection rule applied in Casper for the long-range attack can prevent attackers from rolling back a solidified block to create a fork because it follows the chain with the enormous reasonable checkpoint height. Solidified blocks are not allowed to be changed. Catastrophic Crashes mean more than one-third of validators crash simultaneously because of the network, computer failure, or some malicious motive. The solution is to implement a method that gradually drains the deposit of any validator who does not vote for checkpoints until the deposit sizes drop low enough that the validators who are voting constitute a supermajority [15].

3.2.3. Delegated Proof of Stake (DPoS). DPoS is a blockchain consensus algorithm proposed and applied by Bitshares chief developer Dan Larimer in April 2014. It is an improvement of the PoS mechanism.

Unlike in PoS, where everyone can randomly become a validator by investing their stakes, in DPoS, validators are selected by network nodes to verify and attach new blocks [5]. Each tokens holder can use his tokens as voting rights and vote for a witness he trusts. Once the election is complete, the witness can validate the transaction and package the blocks. The witness must be responsible for other equity nodes. The witness will be eliminated if he or she does not sign the corresponding block [5].

The main advantage of DPoS over PoS is that it can improve the throughput and performance of the blockchain network by having only a small set of elected witnesses participate in block validation. Additionally, DPoS is more decentralized than PoS because token holders have the freedom to vote for their preferred witnesses. Besides, the DPoS mechanism has solved the capacity limitation brought by traditional consensus, dramatically accelerating the speed of transaction confirmations and block creation [5]. However, DPoS has disadvantages, such as the potential for centralization, oligopoly control, and election fraud.

To sum up, the PoS mechanism shows more advantages than the PoW mechanism. The most significant advantage is its better energy-consumption performance. Due to this, the POS mechanism initially replaced the POW mechanism to become the mainstream digital currency in the world today. However, the PoS consensus mechanism has its demerits and weakness, producing many new attacks. It may cause excessive power of specific nodes to manipulate the entire blockchain network. Besides, a cryptocurrency that applies a pure PoS mechanism will encounter some problems when it starts because the cryptocurrency is very centralized at the beginning. It is why most cryptocurrencies still adopt a PoS/PoW hybrid system today, as shown in Table 2.

Table 2. Proof-of-Stake.

Type	Main idea	Advantages	Disadvantages
PPcoin[14]	Using coinage to simplify the difficulty of mining	High energy-efficient high transaction throughput	Tend to produce the Matthew effect and the centralization
Casper [15]	Based on the BFT algorithm. punishment and incentive system validators to verify transactions and create new blocks	High energy-efficient high transaction throughput	Tend to produce the Matthew effect and the centralization
DPoS[5][13]	Validators selection mechanism	Highest energy-efficient Highest transaction throughput	Partial decentralization

3.3. Proof of Authority mechanism

3.3.1. Basic notion, main idea, and comparing. Manuel Adelin Manolache, Sergiu Manolache, and Nicolae Tapus first presented the primary notion and the advantages and disadvantages of Proof of Work and Proof of Stake first. Then the author gives the idea that Proof of Authority is an alternative to those two consensus mechanisms above, not only having the same security level but also providing faster and cheaper business speed without capacity by using the identity and reputation of the node as a stake [16].

PoA provides fast transactions through trusted identity authorization, attracting attention due to its high performance and error tolerance for failures [17]. For the operating method, PoA uses verifiable random functions to ensure the randomness and verifiability of the selected leader node, using signature and verification algorithms. Then other nodes can verify the identity of the leader node, ensuring the security of the leader node, which are those validators, and thus it can prove the whole PoA blockchain network. There are also serval conditions of consensus mechanisms like PoA: Agreement, which means every single node should raise an agreement with the same value; Termination and validity. Moreover, it gives the process of common consensus mechanisms:

1) Elect the leader nodes or what people call validators.
2) Create a new block supervised by the validators.
3) Every single node test, verify and update the new blockchain.

PoA also follows this mechanism and process, but some part of the PoA is different.

Shashank Joshi shows the main idea of Proof of Authority: Proof of Authority is a regulated or permission consensus protocol that wants to have a consensus among those authorized nodes and validators. PoA is a BFT algorithm based on validators' reputations and identities [18]. For the construction and the condition of PoA, including liveliness, tolerance, and visibility, those nodes and validators in the PoA blockchain network must prove their identity and reputation to all participants, this information is public, and every user on the network can see it.

Shashank Joshi also compares PoA to PoW and PoS in a PoW network, getting Bitcoin to need to solve the hash problem and have to compete with other nodes, but PoA has no need to compete and compute [18]; PoA emphasizes the reputation, not like PoS stake, which can make the blockchain network more scalable and bigger. PoA has its advantages. Blocks and node creators can be easily identified because they are all real entities on the network, and they also allow blocks to be used and created on a fixed time and can give a cheaper cost than any other private blockchain. It also shows some factors about how PoA work, its condition, and its method for regular operation, such as The validators in the PoA blockchain network must provide true and accurate information about their reputation [16], Giving long-term personal reputation and assets investment, which can reduce the risk of malicious agents and attacks; The PoA blockchain should have a strict and public standard about choosing the validators, and the rules and the process should be expected for every single validator. Those above are some factors, and here are some notions: All the validators must confirm their reputation to prove the network, which means each of them will put their identity into uncertain circumstances as a stake, sometimes the circumstance is unsafe, but those validators have to face the risk of it; There are also unsuitable candidates or validators, so the PoA blockchain network should check those validators' information in a fixed time to ensure the honesty and integrity of the whole blockchain.

Finally, there is widespread use of the PoA blockchain called Vechain [16], which also shows the new theory about a new algorithm based on PoA called VPoA [17].

3.3.2. Advantages. For advantages of Proof of Authority. PoA has high-risk tolerance because of the truth of validators [16]. However, it is hard to ask them to act maliciously. With that PoA network can keep its security well. PoA can also predict the time of block generation, and with the word mentioned above, PoA has a high transaction rate and does not need too many resources for processing and computing like PoW.

There also has a similar idea, which is claimed by [17]: PoA has high fault tolerance which can solve the breakdown well. For the basic, PoA has high transaction speed because the blockchain work by those trusted validators, which provide high-efficiency transactions. PoA consumes fewer resources and can achieve more input and output because there is no transparent competition among those validators [18], giving more stable status while facing those standard blockchain and consensus mechanisms problems and attacks by its high fault tolerance which can solve most of the mistakes. There is a problem with market-based fluctuating processing, but the PoA consensus mechanism will keep itself and will not change on the blockchain network to solve this problem [18]. Another reason that PoA can provide the rate so fast is that PoA has fewer forks in the whole blockchain network, this also reacts on its protocol.

3.3.3. Disadvantages. For limitations, PoA is not entirely decentralized just because all the validators are trusted people registered on the PoA blockchain network [16]. So in some cases, it is a centralized form system, so the users should find a balance between decentralized and efficient transactions, so PoA is more suitable for private blockchains.

Also, the validators' identities and reputations are public to the participants [18]. Thus, everyone knows the information and other details of the validators, which gives a chance for a third party to control those nodes, which increases the risk of those attacks. With this in mind, ensuring that all the nodes and validators are credible in the real world is hard. That is nearly impossible. Also, the PoA blockchain needs more management and control of those nodes. If they want to behave in which harms the blockchain network, it will cause serious problems. So the nodes might be attacked by the third place, one classic attack called The Cloning Attack, and let the leader node, validators become fully transparent and public. The adversary can also let the authority node do malicious actions. Giving summary, PoA sacrifices some part of decentralization for more scalable, so the authority for PoA is concentrated [18], which will have the risk of attack; PoA makes the nodes and validators open to the crowds, which will cause a third-party attack and disturb the blockchain; Even PoA is a reputation-based consensus, but it is hard to defend the malicious behave of some of the validators and authority nodes, because of that, PoA is easily to suffer the cloning attack and control most of the credible nodes.

3.3.4. Summary. Considering all the factors and analyses above, PoA is a reputation-based consensus model providing more efficient blockchains transactions. The validators stake their identity and reputation to create and maintain the blockchain network, giving a better solution and method used in blockchain and bitcoin.

PoA has several advantages, it can provide faster and safer transactions with less resource consumption, and PoA is safer based on its high fault tolerance because the process of choosing validators is strict. For this reason, the PoA blockchain network can be more scalable and stable. All the validators are entities in the real world. In that case, it can spread on a wide scale.

On the other side, PoA still has some limitations, including the centralized system and model problems, to achieve a high transaction rate, and could be more decentralized. The information and details will be public to all the blockchain users, increasing the risk of attacks and causes serious problems which will harm the whole blockchain. PoA also faces the problem of lacking manage the bad behavior of those validators and third parties. So PoA has its disadvantages, as shown in Table 3.

Table 3. Proof of Authority.

Type	Main idea	Advantages	Disadvantages
[16] [17] [18]	A reputation-based consensus algorithm that provides a practical and efficient solution for blockchain	High fault tolerance High-risk tolerance Scalable Less computing power Faster transaction Available, safety validators Trusted nodes	Have centralized problems Have risk of privacy disclosure The information is public Validators are authorities Lack management for bad actions Face the attack from the third-party Hard to define malicious behaviors

4. Conclusion

As one of the four big blockchain technology, the consensus mechanism has experienced from the earliest PAXOS, later famous POW, to POS and POA with potential. In this process, people put forward a lot of common mechanisms. People try to replace the mainstream consensus mechanism with these consensus mechanisms to make up for the deficiency of the mainstream consensus mechanism. This paper introduces the concept of consensus mechanism, the principle, advantages, and disadvantages of three consensus mechanisms. This paper focuses on the three consensus mechanisms to introduce the development process of the consensus mechanism. This paper also introduces part of the consensus mechanism as a substitute for the three consensus mechanisms. These mechanisms introduce the advantages and disadvantages of POW and POS. The authors believe the POA consensus mechanism has enough potential to become the following mainstream consensus mechanism, widely used in cryptocurrency trading.

References

[1] Wang WB, et al. 2019 *IEEE Access* A survey on consensus mechanisms and mining strategy management in blockchain networks vol 7 pp 22328-22370

[2] Zhang P, et al. 2019 *Advances in Computers* Consensus mechanisms and information security technologies vol 115 pp 181-209

[3] B. Lashkari and P. Musilek 2021 *IEEE Access* A Comprehensive Review of Blockchain Consensus Mechanismsin vol 9 pp. 43620-43652

[4] Skh Saad, S.M. and Raja Mohd Radzi, R.Z. 2020 *International Journal of Innovative Computing* Comparative Review of the Blockchain Consensus Algorithm Between Proof of Stake (POS) and Delegated Proof of Stake (DPOS) vol 10 p2

[5] Zhang CQ, Wu CS, and Wang XY 2020 *International Conference on Big Data Engineering* Overview of Blockchain consensus mechanism

[6] Buterin, Vitalik, et al. 2020 *International Journal of Network Management* Incentives in Ethereum's hybrid Casper protocol p 2098

[7] R. Pass and E. Shi. 2016 The sleepy model of consensus

[8] I. Bentov, R. Pass and E. Shi 2016 *IACR Cryptol. ePrint Arch* Snow white: Provably secure proofs of stake vol 2016 p 919

[9] A. Shahaab, B. Lidgey, C. Hewage and I. Khan 2019 *IEEE Access* Applicability and Appropriateness of Distributed Ledgers Consensus Protocols in Public and Private Sectors: A Systematic Review vol 7 pp 43622-43636

[10] E. Wustrow and B. VanderSloot 2016 *Proc. 10th USENIX Workshop* Offensive Technol DDoSCoin: Cryptocurrency with a malicious proof-of-work pp 1–10

[11] F. Tschorsch and B. Scheuermann 2016 *IEEE Commun Surveys Tuts* Bitcoin and beyond: A technical survey on decentralized digital currencies vol 18 pp 2084–2123

[12] L. Lamport 2006 *Distrib. Comput.* Fast Paxos vol 19 pp 79–103

[13] Bada, Abigael O, et al. 2021 *International Conference on Distributed Computing in Sensor Systems (DCOSS)* Towards a green blockchain: A review of consensus mechanisms and their energy consumption

[14] King S and Scott N 2012 *self-published paper* Ppcoin: Peer-to-peer crypto-currency with proof-of-stake

[15] Buterin, Vitalik, and Virgil G 2017 *Preprint* Casper the friendly finality gadget

[16] Manolache M A, Manolache S and Tapus N 2022 *Procedia Computer Science Decision Making using the Blockchain* Proof of Authority Consensus vol 199 pp 580-588

[17] Zhou Y, Hu Z Y, Yang Z G and Liu W Y 2021 *Computer Science and Application* Improved Proof of Authority Consensus Based on Verifiable Random Functions vol 11 pp 383-393

[18] Joshi S 2021 *arXiv preprint* Feasibility of Proof of Authority as a Consensus Protocol Model