International Journal of Internet of Things and Big Data
Vol.4, No.1 (2019), pp.31-44
http://dx.doi.org/10.21742/ijtbd.2019.4.1.05

# Research on Blockchain Hybrid Consensus Algorithm Based on Internet of Things

Zhipeng Fan[1]

[1]*Harbin University of Commerce, Harbin, China*
[1]*hsdfzp@126.com*

***Abstract***

*This article explains the relevant content and related concepts of the blockchain, and studies the architecture and several core technologies of the blockchain. This article introduces the consensus problem and the distributed consistency problem, and elaborates the principles of several consensus algorithms that are widely used in the blockchain, including the PoW consensus algorithm, the PoS consensus algorithm, and the PBFT consensus algorithm. In view of the shortcomings of a single consensus algorithm, a hybrid consensus algorithm was redesigned. This article proposes that the PBFT consensus algorithm has a high execution efficiency, and is mainly responsible for the processing of transactions and smart contracts to meet the consensus algorithm's demand for high execution efficiency. Open the Byzantine committee node rotation election function in PBFT to PoW nodes. The committee nodes are selected by PoW nodes, and any node can participate and become a PoW node to ensure the degree of decentralization of the consensus algorithm, and thereby ensure the security of the consensus algorithm. Experimental results and data show that compared with the original consensus algorithm, the hybrid consensus algorithm is better in terms of throughput and latency. The hybrid consensus algorithm combines the two-consensus algorithm consensus of PBFT and PoW to solve the problem of decentralization and performance. Contradiction.*

***Keywords:*** *Internet of Things; Blockchain; Trust mechanism; Hybrid consensus algorithm*

## 1. Introduction

With the increasing popularity of cryptocurrency, blockchain technology has attracted the attention of the industry and academia. People can think of blockchain as a shared computing environment in which members are equal and can join and withdraw freely. This is the premise of a common consensus agreement.

The Internet of Things has developed to the present, and its application range has become more and more extensive, almost in all fields [1]. However, smart devices that can be accessed by the Internet of Things are not guaranteed to be trusted, and can even be said to be malicious. Just imagine if someone wants to obtain personal data in your computer, he can do so by attacking weak links in the network. The purpose of hacking into your home network.

In blockchain technology, all nodes only need to reach an agreement on the public ledger through a consensus algorithm. The most important thing in the blockchain is the block, and each block that has been mined will be linked to the previous block. To a certain extent, this structure of "chain" between blocks is the connotation of blockchain. The blocks in the

**Article history:**
Received (July 4, 2019), Review Result (August 7, 2019), Accepted (September 11, 2019)

Print ISSN: 2207-3507, eISSN: 2207-3515 IJITBD

blockchain are the foundation of the ledger. Different from the usual accounting that we understand, all the blocks in the blockchain cannot delete or change any information. Every time new data is added, it can also be said to be a new account, which must be stored in a brand new block. All records in the blockchain can also be said to be all blocks. Once the accounting is successful, the data cannot be changed or deleted. Therefore, the blockchain's review of new blocks is quite strict. In the process of adding a new block, the most important thing is how to judge the eligibility of the block, which involves one of the cores of the blockchain-the consensus mechanism. A decentralized blockchain requires all nodes to maintain the normal operation of the blockchain together and reach a consensus without a central service.

The issue of consensus first received attention in the mathematics community. As early as 1959, Edmund Eisenberg and David Gale studied how to form a consensus probability distribution among a group of individuals under certain conditions. Subsequently, the issue of consensus has received extensive attention from different academic circles. Barbara Liskov et al. proposed Practical Byzantine Fault Tolerance [7] in 1999, referred to as PBFT, which is a practical Byzantine fault-tolerant algorithm. This algorithm reduces the complexity of the Byzantine agreement, so subsequent researchers can better apply the practical Byzantine fault-tolerant algorithm [8]. In 2008, the author under the pseudonym Satoshi Nakamoto published the earliest blockchain literature-"Bitcoin: A Peer-to-Peer Electronic Cash System" [1]. In July 2018, the United Bitcoin (UB) implemented a hybrid consensus algorithm of PoW and PoS. In 2015, NEO proposed the Authorized Byzantine Fault Tolerance (DBFT) consensus algorithm. In 2018, Eric Zhang and his team released True Chain [2], proposing a hybrid consensus algorithm based on PoW (Proof of Work) and PBFT (Practical Byzantine Fault Tolerance) algorithms. The Raft consensus algorithm proposed by Diego Ongaro and John Ousterhout [3]. Paxos [4,5], first proposed and published by Lamport in 1998, is mainly used in non-Byzantine scenarios [6], generally in distributed databases. Because these databases are managed and maintained by a single organization, their nodes are trusted. Such algorithms generally only support Crash Fault-Tolerant (CFT). Since in a decentralized blockchain network, nodes do not know and trust each other, and there is the possibility of deception and malicious behavior, it is not directly applicable to the consensus mechanism of the blockchain.

The PoA consensus mechanism, which combines PoW and PoS algorithms, was proposed in December 2014 [7]. The consensus mechanism distributes part of the tokens mined by PoW to all active nodes in a lottery. The higher the stake, the higher the stake. The greater the probability of being drawn.

## 2. Blockchain technology

### 2.1. Blockchain concept and architecture

Blockchain has the characteristics of concentration, transparency and preventing historical data from being tampered with. The protocol does not require any trusted third party, and all distributed nodes participate in consensus. In the public chain, any node can freely join and leave the network, the number of nodes will change from time to time, and this change is unpredictable. Once the block data in the blockchain reaches a certain "depth" (for example, in Bitcoin, the "depth" is set to more than 6 blocks [8]), it can be determined that the block content will hardly be affected. tamper.

Most of the current applications of blockchain technology are based on Bitcoin, but most of these applications are based on the Bitcoin architecture for different extensions, which are slightly different from the original Bitcoin architecture. Among them, Blockchain technology

has attracted much attention in the financial industry. Research scholars in the financial industry believe that the use of blockchain technology can rebuild the existing IT infrastructure in this field from the lowest level. The basic structure of the blockchain is divided into three levels, as shown in [Figure 1].

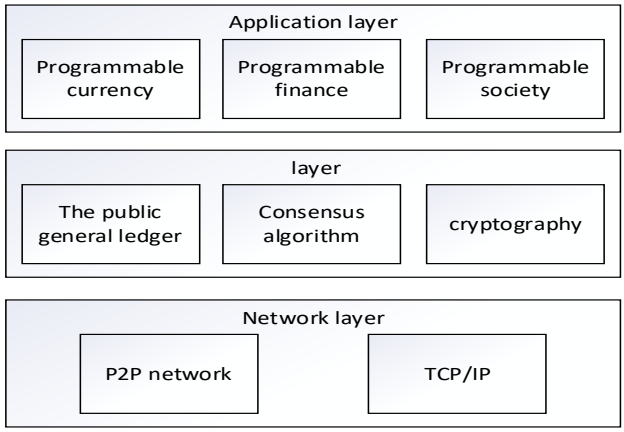


Figure 1. The basic architecture of blockchain

The characteristics of the blockchain include the ability to be decentralized, to have a reliable database, to be open source and programmable, its maintenance is guaranteed by the collective, and it allows transactions to be anonymous. It can be said that if a system does not have all of the above characteristics, it will not be recognized as an application based on blockchain technology [8].

### 2.2. The core technology of blockchain

Many core technologies involved in the blockchain are related to computers and communications. For example, in cryptography, the SHA256 algorithm is used in Bitcoin. In addition, it also includes distributed system communication technology, database technology and P2P (Peer to Peer) technology. P2P network technology is actually a peer-to-peer network technology. Any two nodes in the network have an equal relationship. Based on this, the blockchain technology can be successfully implemented [9]. In essence, it can be regarded as a distributed accounting ledger. For all nodes on it, the two nodes are in a peer-to-peer relationship, and communication can be carried out between any mutual nodes.

The distributed ledger of the blockchain is a ledger with specific technology. From a technical point of view, blockchain is the same as distributed ledgers. They both use consensus algorithms to ensure data consistency, and they are both decentralized [10]. However, because the Byzantine problem is not within the scope of traditional distributed ledgers, the consensus algorithms they use are slightly different. From the perspective of the traditional ledger structure, there is a central organization responsible for the management of all data in the system. Strictly speaking, the distributed ledger with this structure cannot be regarded as a truly decentralized system.

A P2P network (Peer-to-Peer Network) is a peer-to-peer network, or peer-to-peer computing. In theory, it is a kind of networking formed by the peer-to-peer computing model at the application layer, or a form of network. At the same time, it is also a distributed task and workload among peers. Application architecture. The most recent application of P2P

 

technology in real life is the domestic Xun lei software, which uses P2P network technology. The blockchain system is based on network communication and exchanges information completely through the Internet. It does not rely on any traditional circuit switching functions, but is based on IP communication protocols and distributed networks. There is no hierarchical structure in the network, and there is no special central node. Each node has to undertake functions including verification blocks and network routing, and its status is equivalent to [11].

In Bitcoin, a block can be seen as a bookkeeping book that records all transaction information in Bitcoin. The content on the block is permanently embedded, and the embedded content covers the currency income and expenditure of all users. These contents can be successfully queried by other personnel. In the distributed database system of the blockchain, each client node has a copy of all the data stored in the block, and these nodes jointly maintain the security of the database [11]. The normal operation of the database will not cause problems because the data of any one node is destroyed, because the complete database is still stored in other undamaged nodes.

There are more than one encryption algorithms in the blockchain, not only hash algorithms, but elliptic curve encryption algorithms are also in Bitcoin, an asymmetric encryption algorithm that encrypts transactions in Bitcoin. There is a pair of keys related to mathematical problems in the asymmetric encryption algorithm. In this pair of keys, one is responsible for encrypting data information, and the encrypted data information can only be decrypted by the other key. Among them, the private one is called the private key, and the public one is called the public key. For the simplest example, take a bank account as an example. The public key is public. It is like an account opened at the bank, while the private key is not public, like the password or the password of the account opened at the bank. Like the signature of the owner of this account. The public key can be calculated from the private key, but the opposite is not true, that is, the private key cannot be derived from the public key.

## 3. Consensus algorithm

### 3.1. Consensus and distributed consistency

The consensus problem is a classic problem. As early as 1959, for a specific probability space, Edmund Eisenberg and David Gale studied a group of individuals with their own subjective probability distributions and explained the formation process of consensus probability distributions [12]. Since then, in sociology, management Studies on consensus issues have gradually begun in the fields of science, economics, and especially computer science.

The main focus of the early research on consensus in the field of computer science was the problem of distributed consistency. This problem is actually one of the fundamental problems in distributed computing, that is, how to ensure that the data of all nodes in a distributed system cluster is exactly the same and It can be guaranteed that all nodes can finally reach a consensus on a certain proposal through negotiation.

Strictly speaking, proof of work is a weak consensus algorithm, which has not yet proven its correctness and has not reached a consensus conclusion [13]. However, based on traditional distributed consensus algorithms, these algorithms give proof of correctness, and are consistent with the definition of consensus, and are strong consensus algorithms. Vukolić M et al. [14] detailed the proof mechanism represented by the Pow consensus mechanism and the consensus mechanism based on the improvement of the traditional distributed consensus algorithm in terms of node management, performance, delay scalability, resource consumption, and whether

to generate tokens, etc. Analysis, and compare their respective characteristics. [Table 1] shows some comparative data between the PoW consensus mechanism algorithm and the traditional distributed consensus algorithm.

Table 1 Comparison of PoW consensus algorithm and traditional distributed consensus algorithm

| | PoW consensus algorithm | Based on traditional distributed consensus algorithm |
|---|---|---|
| Node management | No need for node management, nodes can join or exit the network at will | Yes, permission is required to enter the network |
| performance | Poor, and will be affected by the blockchain bifurcation | High, the highest throughput can reach the network capacity |
| delay | High, need block confirmation | Low, related to network latency |
| Scalability | Good, system performance is generally not affected by the number of nodes | The more the number of poor system nodes, the worse its performance, and it may even reach unavailability. |
| resource consumption | High, a large number of hash calculations, wasting a lot of resources | Low |
| Whether to generate tokens | Yes, it acts as an incentive | No |

### 3.2. PoW algorithm

In Proof of Work, every node that wants to solve the hash problem needs to be realized through the way of computing power. The node that can solve the problem first will get the right to book this time. Means to ensure data consistency.

Miners who play an important role in the Bitcoin system. Miners are essentially nodes that perform SHA256 calculations, and the process of generating blocks is called mining. Mining pools are usually divided into P2P mining pools and managed mining pools. P2P mining pool is considered to be a decentralized mining pool server, and its principle is similar to the blockchain system. P2P mining pool is also called share chain. The miners in the hosted mining pool need to send proof of work that meets the difficulty to the pool manager, which means that the miners who join the hosted mining pool need to use their own computing power to continuously try to generate new legal blocks.

All nodes participating in the Bitcoin consensus process use methods that are constantly trying to verify whether their own random value is a solution to a SHA256 mathematical problem. In the Bitcoin system, this problem is easy to verify, but it is more difficult to solve it forward. One of the advantages of PoW is that it does not require node management, and this feature allows the services of the blockchain system to cover the entire network, so it has good scalability, which means that any node can become the Bitcoin system Miners then participate in the operation of the system, including processes such as mining, dissemination, and verification.

However, while the Bitcoin system has high scalability through the characteristics of PoW, it also has performance disadvantages such as high latency and low throughput. The reason why such a high-latency phenomenon occurs is because it takes a lot of time to solve the problem. In the process of collecting and packaging transactions by different miner nodes, the number of transactions that can be successfully confirmed per unit time is very limited, which also leads to the scene of massive transactions. The throughput of the blockchain is limited, and

 

the number of transactions that can be loaded per unit time is much smaller than the number of transactions generated.

### 3.3. PoS algorithm

The full name of PoS is Proof of Stake, and its Chinese name is Proof of Stake. This concept first appeared in the white paper of Sunny King, the founder of Diandian. The word Stake means share. As the name suggests, PoS is similar to the equity we usually understand. Its initial purpose was to solve the problem of a large amount of waste of resources in PoW mining. The blockchain project that first started to use the consensus mechanism of proof of rights and interests was the dot coin produced in 2012 [15]. Ethereum adopts the PoW consensus mechanism in the first three phases, and at the beginning of the fourth phase, Ethereum adopts the proof-of-stake mechanism.

PoS is different from PoW in that it does not need to consume computing power to obtain accounting rights. Compared with PoW, PoS reduces the consumption caused by digital operations to a certain extent, and the performance has been correspondingly improved. However, it is still a method of obtaining accounting rights based on the competition of hash calculations, and its supervisory ability is weak. The fault tolerance of the consensus mechanism is the same as that of PoW. PoS is more suitable for networks with fixed tokens and will not cause inflation [16]. Its revenue rewards mainly come from user transactions. Each network node in PoS is linked to an address. The more tokens this address holds, the greater the probability that it will get the next block produced.

A new concept is introduced in PoS, which is coin age. Its English name is Coin Age, which literally means the number of coins multiplied by the number of days.

The basic logic and steps of PoW mining are to first seek a nonce smaller than the target value. This step can be expressed by the formula:

$$Hash(block_{header}) < Target \tag{1}$$

It can be seen from the formula that the target value of all miners under PoW is the same, as long as the hash of the calculation result is smaller than the target value, which is simply the number of leading zeros.

In the PoS system, this formula is changed to:

$$Hash(block_{header}) < Target * CoinAge \tag{2}$$

It can be seen that one more variable is introduced called Coin Age, which is coin age. This variable will cause the target value seen by each miner to be different. If your coin age is older, it means that it is easier for you to get the answer. The Target here is consistent with PoW, and is inversely proportional to the difficulty of the entire network, and is used to control the block generation speed.

### 3.4. PBFT algorithm

PBFT means Practical Byzantine Fault Tolerance, this algorithm was proposed by Barbara Liskov et al. in 1999. It solves the problem of low efficiency of the original Byzantine fault-tolerant algorithm and reduces the complexity of the algorithm from exponential to polynomial, making the Byzantine fault-tolerant algorithm feasible in practical system applications [17].

Practical Byzantine fault-tolerant algorithms are mainly used in the central bank's digital currency and Bumon blockchain. PBFT is a state mechanism copy replication algorithm, that is, the service is modeled as a state machine. Status and copy replication at different nodes in the distributed system [18]. Each copy of the state machine saves the state of the service and

also implements the operation of the service. The set consisting of all the copies is represented by a capital letter N, and each copy is represented by an integer from 0 to N-1. For the convenience of description, let us assume that N=3F 1. Here F is the maximum number of replicas that may fail. Although there may be more than 1 copy of 3F, the extra copy does not improve reliability beyond reducing performance.

In simple terms, the PBFT algorithm process is: the client first sends a request to the master node to call the service operation, and then the master node sends the request to other replicas by broadcasting. All copies execute the request and send the result back to the client. The client needs to wait for F 1 different replica nodes to return the same result as the final result of the entire operation [19]. The PBTF execution process is shown in [Figure 2]. Among them, C is the client that sends the request message, 0, 1, 2, and 3 are the servers, and server 3 is the down server.

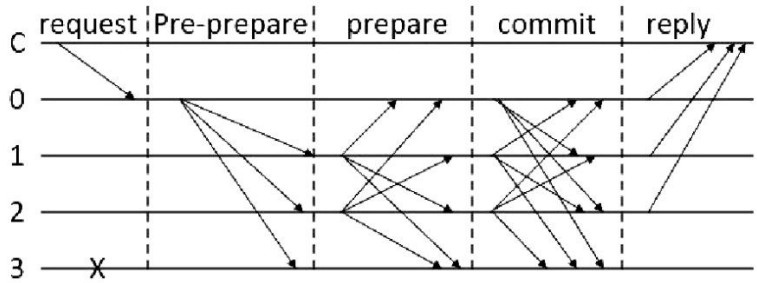


Figure 2 PBFT execution process

## 4. Hybrid consensus algorithm

### 4.1. Hybrid consensus analysis

In the mixed consensus, there is a design paradigm in which PBFT and PoW are combined to obtain better results. There are also many hybrid consensuses, and the basic consensus algorithms used are PoW and PoS. Under normal circumstances, hybrid consensus will use the PBFT protocol, which works in a secure setting by default, and all identities are a priori, as a fast path for processing a large number of incoming transactions. The PoW protocol selects the Byzantine committee based on the performance of the node in PoW.

The hybrid consensus algorithm design is mainly based on True Chain's hybrid consensus, and some modifications and improvements have been made to adapt to the IoT application scenarios we are concerned about. According to the protocol proposed in the literature, the hybrid consensus algorithm can be based on a hybrid block chain structure, which can be understood as a mixture of two block chains, which are called slow chain and fast chain respectively.

 

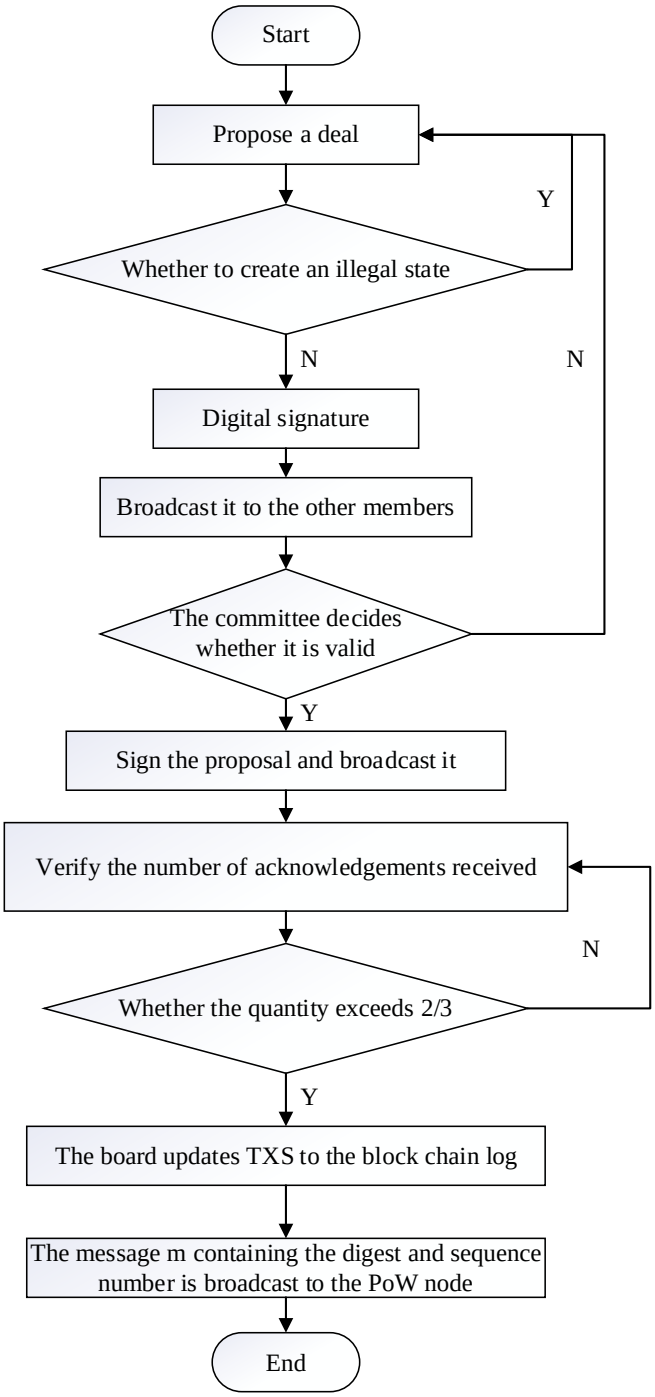


Figure 3 Fast chain transaction processing flowchart

The so-called fast chain is a chain that executes transactions and smart contracts in a hybrid blockchain structure, which can efficiently and quickly complete accounting tasks and is responsible for transaction processing. The slow chain means that the execution speed in the hybrid blockchain structure is slower and cannot meet the user's demand for high efficiency, but its decentralization is higher. The slow chain is used to ensure the decentralization of the

hybrid blockchain structure. The nodes in the fast chain act as members of the Byzantine committee and reach an agreement through PBFT voting. Transactions and smart contracts are executed on the fast chain to achieve high throughput. The members of the Byzantine committee are randomly rotated every fixed time T, and the new committee will select the best from PoW miners. This method can effectively enhance decentralization. In this method, anyone with a computer can join and become a PoW node.

In the fast chain setting, the permissioned Byzantine committee is a group of nodes that can communicate with each other and vote for or disapprove of the leader's recommendations. These nodes do not assume that they trust each other, which means that a subset of these nodes may be malicious. Through an in-depth analysis of the Byzantine generals problem, it is concluded that when more than 2/3 of the nodes are honest nodes, a consensus can always be reached. The algorithm flow chart of fast chain for transaction processing is shown in [Figure 3].

### 4.2. Hybrid consensus algorithm

Less than 1/3 of the participating nodes in the Byzantine hypothesis are corrupt. That is to say, in a permissionless environment, this assumption means that the quality of the fast chain (that is, the proportion of non-malicious nodes in the blockchain) 3/2fQ needs to be guaranteed to keep the chain consistent and active. The committee instance is switched after a fixed period of time (using the slow link as the logical clock). The slow chain is expected to produce a block every 10 minutes, and a rotation frequency of 144 blocks is set here. A new committee is simply a slow chain in the latest csize block composed of miners. In hybrid consensus, selfish mining is more harmful because power is more concentrated on a few high-hash nodes. If a selfish miner controls more than 25% of the blockchain's hashing power, he can control more than 33% of block production. According to the election process, this selfish miner is likely to control more than one-third of the Byzantine Council. If he happens to be untrustworthy, then this fast chain will lose its activity.

In the fast-chain block structure, the two most important attributes are "transactions" and "signs". You can also see the three attributes "TxHash", "GasLimit" and "GasUsed" in the block header. This shows that the main function of the fast chain block is to execute transactions, collect transactions and collect signatures from Byzantine committee members.

In the double-chain structure, PBFT is used as a fast chain, PoW is used as a slow chain, the fast chain is used for storage of ledgers and transactions, and the slow chain is used for mining and committee elections. Selecting open to the public chain, using the PoW consensus algorithm to select committee nodes, improves the efficiency of consensus, and each consensus node is composed of business participants or regulators, security and stability are guaranteed by business stakeholders, and the consensus delay is large reduce.

### 4.3. Simulation experiment analysis

Throughput is a measure of the ability of a system to process transactions, requests, and transactions per unit time, and it is an important indicator of the system's concurrency capability. In this article, we use TPS (Transaction Per Second) to express. The transaction throughput in blockchain applications refers to the total number of transactions divided by the time between the transaction sent to the transaction confirmation and written into the blockchain, which can be expressed by formula 3:

$$TPS = \frac{ST}{\Delta t} \tag{3}$$

 

Where Δt is the time from transaction issuance to block confirmation, that is, the block generation time, and ST represents the number of transactions contained in the block during the period.

The time interval is 10s, 20s, 40s, 60s, 100s, 300s, etc. 6 different times (block generation time), each time interval is tested 20 times, and the average value of 20 times is taken as its TPS. For 6 different time intervals, the total number of transactions for each test is plotted in [Figure 4].

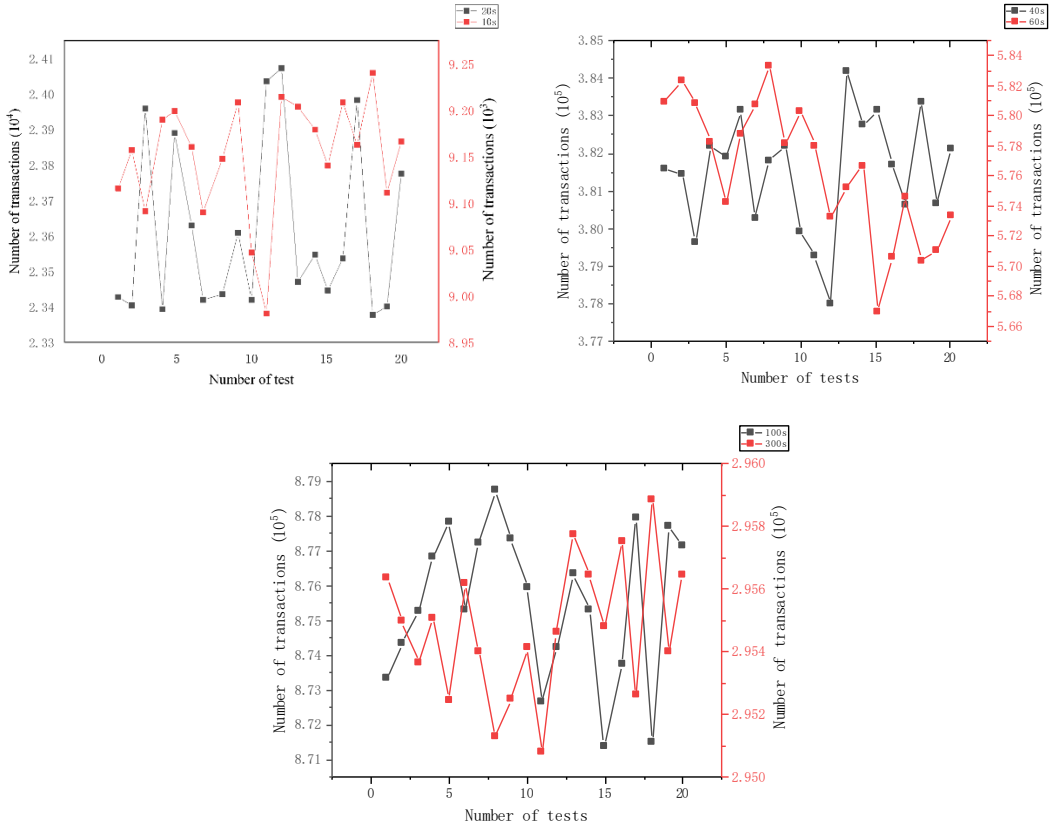


Figure 4 The total number of transactions in different time intervals

Take the average of these 120 times as the TPS value of the mixed consensus. [Figure 5] shows the relationship between TPS and block generation time.

From the simulation results, it can be clearly seen that the TPS increases with the increase of the block generation time interval. When the time interval reaches 52s, the tps reaches the peak value of 1.26×104.

Since PoW and PoS are the consensus algorithms of the public chain system, from official documents and existing tests, the performance comparison with the hybrid consensus algorithm is shown in [Table 2].

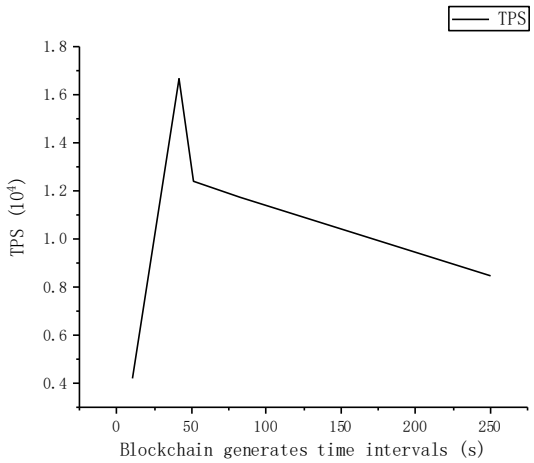


Figure 5 Relationship between TPS and block time

Table 2 PoW, PoS, and hybrid consensus performance indicators

| Indicators | PoW | PoS | Mixed consensus |
|---|---|---|---|
| TPS | <7 | 5-10 | Over ten thousands |
| Delay time | Minute level | Minute level | Second level |
| Confirmation time | 10min | 10min | Under 60sec |
| Resource consumption | High | A little high | Low |

The throughput of the PBFT algorithm and the hybrid consensus algorithm is compared for the blockchain consensus mechanism. Through the comparison test, as shown in [Figure 6], the two algorithms reached the peak throughput at a time interval of 52s, and the TPS of the hybrid consensus algorithm reached 1.26×104. And PBFT can only reach 1.14×104. In contrast, the results of the hybrid consensus algorithm are relatively good.

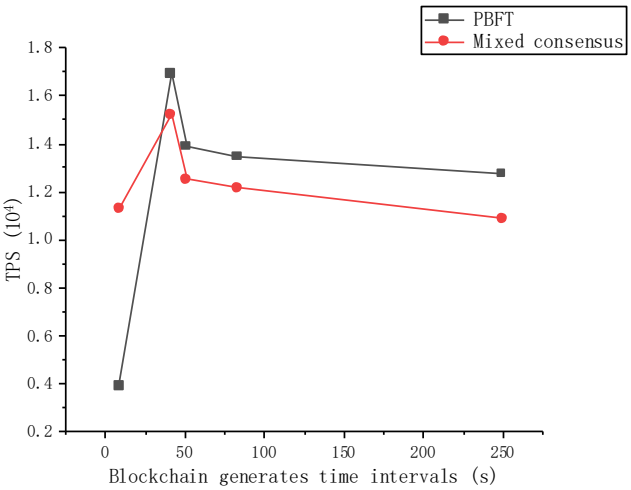


Figure 6 Comparison of throughput between PBFT algorithm and hybrid consensus algorithm

The simulation results are as follows:

During the simulation test, 6 different block generation times were selected at intervals of 10s, 20s, 40s, 60s, 100s, 300s, etc. Each time interval was tested 20 times, and the average of the 20 times was taken as its throughput. Through testing, the throughput of the hybrid consensus algorithm increases with the increase of the block generation time interval. When the time interval reaches 52s, the TPS reaches its peak and the maximum throughput can reach 1.26×104, while PBFT can only reach 1.14×104. In contrast, the hybrid consensus algorithm has a better throughput.

## 5. Conclusion

The hybrid consensus algorithm in this article is based on the True Chain basic architecture. The PBFT consensus algorithm has high execution efficiency and is responsible for the processing of transactions and smart contracts to meet the consensus algorithm's demand for high execution efficiency. Open the Byzantine committee node rotation election function in PBFT to PoW nodes. The committee nodes are selected by PoW nodes. Any node can participate and become a PoW node to ensure the degree of decentralization of the consensus algorithm, thereby ensuring the consensus algorithm safety. Experimental results and data show that, compared with the original consensus algorithm, the hybrid consensus algorithm is better in terms of throughput and latency. The hybrid consensus algorithm combines the two consensus algorithm consensus of PBFT and PoW. From the perspective of effect, the hybrid consensus algorithm Algorithms can basically achieve high efficiency while taking into account the nature of decentralization.

## References

[1] Natamoto S., “Bitcoin: A peer-to-peer electronic cash system,” **(2009)**

[2] Sharma A, Jasper L, Zhang H, et al., “True chain: Highly performant decentralized public ledger,” vol.86, pp.641-649, **(2018)**

[3] Ongaro D, John O., “In search of an understandable consensus algorithm (extended version),” vol.45, pp.48-60, **(2014)**

[4] Leslie L., “The part-time parliament,” ACM Transactions on Computer Systems, vol.16, no.2, pp.133-169, **(1998)**

[5] Lamport L., “Paxos made simple,” ACM Sigact News, vol.32, no.4, pp.18-25, **(2001)**

[6] Lamport L, Reed B C, Junqueira F P, et al., “In Search of an Understandable Consensus Algorithm,” Proceedings of USENIX ATC’ 14: 2014 USENIX Annual Technical Conference, pp.305-319, **(2014)**

[7] Bentov I, Lee C, Rosenfeld M, et al., “Proof of activity: Extending bitcoin’s proof of work via proof of stake,”. Performance evaluation review, vol.42, no.3, pp.34-37, **(2014)**

[8] Decker C, Wattenhofer R. “IEEE 2013 IEEE Thirteenth International Conference on Peer-to-Peer Computing (P2P) – Trento, Italy” IEEE P2P 2013 Proceedings – Information propagation in the Bitcoin network, IEEE Thirteenth International Conference on Peer-to-peer Computing. IEEE, pp.1-10, **(2013)**

[9] Turek J, Shasha D. “The many faces of consensus in distributed systems,” Computer, vol.25, no.6, pp.8-17, **(1992)**

[10] Kogias E K, Jovanovic P, Gasser L, et al. “OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding,” 2018 IEEE Symposium on Security and Privacy. USA: IEEE, pp.583-598, **(2018)**

[11] Luu L, Narayanan V, Zheng C, et al. “A Secure Sharding Protocol For Open Blockchains,” 23rdACM Conference on Computer and Communications Security (CCS), pp.17-30, **(2016)**

[12] Eisenberg E, Gale D. “Consensus of Subjective Probabilities: The Pari-Mutuel Method,” Annals of Mathematical Statistics, vol.30, no.1, pp.165-168, **(1959)**

[13] Dolev D, Strong H R. “Authenticated Algorithms for Byzantine Agreement,” Siam Journal on Computing, vol.12, no.4, pp.656-666, **(1983)**

[14] Lampson B W. “How to Build a Highly Available System Using Consensus,” Lecture Notes in Computer Science, vol.1151, pp.1-17, **(1996)**

[15] King S, Nadal S. “Ppcoin: Peer-to-peer crypto-currency with proof-of-stake,” self-published paper, August, **(2012)**, 19: 1.

[16] Gaži P, Kiayias A, Russell A. “Stake-bleeding attacks on proof-of-stake blockchains,” 2018Crypto Valley Conference on Blockchain Technology (CVCBT). IEEE, pp.85-92, **(2018)**

[17] Castro M, Liskov B. “Practical Byzantine Fault Tolerance,” Symposium on Operating Systems Design& Implementation, **(1999)**

[18] Abraham I, Gueta G, Malkhi D, et al. “Revisiting Fast Practical Byzantine Fault Tolerance,” vol.12, pp.1-13, **(2017)**

[19] Abraham I, Malkhi D, Nayak K, et al. “Solida: A Blockchain Protocol Based on Reconfigurable Byzantine Consensus,” vol.9, pp.1-17, **(2016)**

 

***This page is empty by intention.***