Comparison and Discussion on Consensus of Cryptocurrency

Yuan Wang*

Faculty of Information Technology
Macau University of Science and Technology
Macau, China
**1809853gi011003@student.must.edu.mo*

ABSTRACT
Cryptocurrency has become popular, and a large part of cryptocurrency is based on a technology called the blockchain. The consensus protocol is one of the important parts of the blockchain. Through the consensus protocol, the system performance of the blockchain can be judged. Therefore, the consensus protocol is often used as one of the determinants of the quality of cryptocurrency. This article divides various popular blockchain-based cryptocurrencies into two categories from the perspective of consensus protocols and presents the consensus trend of various popular cryptocurrencies based on the perspective of cryptocurrency consensus algorithms.

Keywords: *blockchain; cryptocurrency; consensus*

1. INTRODUCTION

Satoshi Nakamoto proposed Bitcoin in 2008 [1]. As today's largest cryptocurrency, Bitcoin uses the blockchain as the basic technology. With the development and maturity of blockchain technology, many blockchain-based cryptocurrencies have appeared. In the blockchain, the Consensus between each two nodes in a distributed system is important. Whenever a new blockchain-based cryptocurrency appears, its consensus protocol is often used to judge the performance and security of cryptiocurrencies. Different consensus agreements are produced for different purposes such as improving energy consumption, making the block network more stable.

For the stability of the blockchain, the consensus mechanism is essentially the consensus on the block between nodes in the system, that is, the same chain should not have exactly the same attributes in different nodes. The attributes of a block include not only the state of the block, but also the version, content, logo, etc. If the same chain in two nodes is divergent, then an event that violates consensus has occurred. Such conflicts can lead to loss of profits or malicious use by hackers. In other words, when such a consensus conflict event occurs, how the blockchain network reacts to restore the consensus information of the nodes is one of the main contents of the consensus mechanism.

In terms of security, a good consensus mechanism can prevent hacker attacks such as double-spend attack [2]. The essence of the blockchain is composed of the genesis block and multiple blocks containing transaction records in the standard single chain blockchain. In a single chain blockchain, if the main chain has a branch, or called a 'fork', it violates the consensus mechanism and can be regarded as a consensus conflict event. The occurrence of such a fork event often brings losses to the cryptocurrency users and miners. The generation of fork and the rate of block generation are positively correlated, and the increase in block generation speed is the trend of today's cryptocurrency community, so it is very important to solve or reduce the impact and loss caused by fork. At the same time, it also reduces the number of incidents of hackers using forks to attack cryptocurrency users.

Based on the above two reasons, the consensus mechanism is indispensable for all blockchain-based cryptocurrencies. This article mainly divides the consensus mechanism of Cryptocurrency into two major categories. One is we called the traditional consensus protocol technology which the most representative one is the 'Proof of X' type of agreement, including Proof of Work (PoW) used in the early days of Bitcoin and the Ethereum community, Proof of Stack (PoS) used by

Peercoin to the improved PoS used in Ethereum today and the Delegated Proof of Stake (DPoS) used by the EOS community. They use a standard single chain blockchain, and there is no clear division between nodes. Nodes can also participate in transactions as consensus verification nodes. Another type of cryptocurrency uses a consensus mechanism to a certain extent at the expense of some attributes in the traditional consensus protocol, such as the degree of decentralization to achieve higher efficiency, response speed. Such as Ripple Protocol Consensus Algorithm (RPCA) and Tangle network consensus technology [3].

The following paper is organized as follows. Section 2 is a background information of blockchain, section 3 introduces different consensus protocol for popular cryptocurrencies, section 4 compare above consensus protocol and section 5 is the conclusion.

2.BLOCKCHAIN

The essence of the blockchain is a distributed data structure based on Peer to Peer (P2P) network and specific encryption algorithms [4]. It can be seen as a shared database, sharing data and information. A block in the same chain has two kinds, one is the first block, called the genesis block. This block records a unique identification ID representing the beginning of the blockchain. Another one which is the blocks that store data after first one contains two IDs, their own ID and the ID of the previous block. This kind of relationship makes all blocks form a chain structure. These blockchain information are stored in every user node, and every time there is a blockchain update, it will be broadcast to all nodes. This ensures the fairness and justice of using blockchain as a cryptocurrency transaction.

In these cryptocurrencies, the blockchain database, that is, the information stored in each block is the currency's transaction records [1]. Such a blockchain is like a ledger, and all nodes in the network need to contain such ledger information to facilitate verification of the feasibility of subsequent transactions. The consensus mechanism plays a fair and just role in this process, and the purpose is to ensure that the ledger information contained in each node is the same. If the ledger conflicts between different nodes, it means that only one ledger is correct, but the other ledger needs to be discarded. Then the transaction records in the abandoned ledger will be invalidated. Therefore, the consensus process is very important. Whether it can effectively reduce the occurrence of invalid records is an important reference for judging the quality of a consensus mechanism.

The consensus protocol is like a voting machine, which determines who will create the next block. At the same time, the consensus protocol also guarantees the information security of block users. Therefore, the consensus protocol determines the fairness and security of the blockchain. A bad consensus mechanism can easily be used by hackers and cause network paralysis. In addition, a blockchain system can be evaluated by the value of Transactions Per Second (TPS). It presents the efficiency of the system. The consensus protocol is one of the important attributes when determine TPS of the blockchain system.

3.CONSENSUS PROTOCOL FOR POPULAR CRYPTOCURRENCIES

In this section, we introduce consensus protocols for different cryptocurrency networks, including Bitcoin, Peercoin, Ethereum, EOS, Ripple Network.

3.1Bitcoin

Bitcoin (BTC) is one of the first cryptocurrencies to use blockchain as kernel. It uses PoW as its consensus mechanism [1], which is actually very similar to [6]. Almost all PoW meet the following steps to perform [1].

a)A certain account creates a transaction and broadcasts it to notify the miner node to write its own transaction into the block.

b)The miner node writes the collected transaction records into a block.

c)All nodes involved in mining find a proof of work with sufficient difficulty through the POW standard process.

d)Broadcast calculation results.

e)After receiving the broadcast, other nodes verify that this block content is valid, and create a new block after the block as a way to recognize the validity of the previous block.

In the above steps, PoW function, the function difficulty value, and the created block are the three most important intermediate attributes, and the specific values of these attributes often vary according to different cryptocurrencies. In Bitcoin, the PoW function uses SHA256.

As mentioned earlier, one of the essence of the consensus algorithm is to determine who has the power to create new blocks and write them into the main chain. In Bitcoin's PoW, the difficulty value determines approximately how much hash calculation is required to generate a legal block. This difficulty value will vary with the number of blocks with a specific change formula. Therefore, the difficulty of mining Bitcoin can remain stable in theory. Nevertheless, as the value of Bitcoin is getting higher, the number of users increasing, which increases the difficulty of mining, because only

one unit is allowed to successfully mine at a time. In the past 2016-2020, the overall difficulty value is nearly on the upward trend [7].

In this process, user gradually centralized their computing power in order to gain advantages in computing power. It has gradually changed from individual mining to competition between groups, which is not the original intention of Bitcoin. And based on this calculation method, Bitcoin's processing speed TPS is quite low, theoretically only seven transactions per second. But at the same time, the absolute 'computing power = power' makes hacking almost impossible. To control the Bitcoin network, you need to have more than half the computing power of the entire network, which is 51% power of whole network, which is too costly for hackers. So, it does reduce the possibility of being attacked to a certain extent.

3.2Peercoin

PoW algorithm require more and more computing resources. In order to reduce the waste of computing resources and speed up calculations, Proof of Stack (PoS) has emerged. The earliest use of this consensus protocol was the Peercoin (PPC) community that emerged in 2012 [9]. Compared with the PoW requires many calculations, PoS only needs to judge the size of the coinage to determine who has the power to keep accounts in, as in (1).

$$\text{coinage} = \text{number of coins} * \text{holding time of coins} \quad (1)$$

In Peercoin, it is stipulated that the holding time of the coin must be more than 30 days. Compared to PoW, PoS is relatively more secure, because even if you have 51% of the global computing power, it is difficult to launch an attack, because you must also have 51% of the currency, which makes the attack more difficult. In theory, rich user nodes tend to be more honest, that is, they will not do evil. At the same time, it can be found that PoS has not produced any useless calculations. Even if the coinage invested this time is not adopted, it can still be used again next time. Therefore, anyone who participates in mining behave honestly will be rewarded.

But even if the PoW problem is solved, the original PoS still has many flaws. Due to the existence of coinage, rich nodes are getting richer and poorer getting poorer. Secondly, the most serious is that PoS can bet without cost which can use to have no profit attack [10]. In Bitcoin, since mining needs to refer to the previous node, when a fork occurs, it is often only possible to choose one side to continue mining. However, in Peercoin, betting on two branches at the same time does not require any computational cost and one party must win. This makes malicious nodes increasingly support the generation of forks, which seriously affects the stability of the single chain. We can learn that such loopholes are quite serious for the currency of the consensus protocol. Therefore, in order to solve such problems, PoS has undergone a series of upgrades, the most famous of which are the Casper protocol and the DPoS protocol.

3.3Ethereum

Ethereum (ETH) is a popular cryptocurrency that use a mix consensus mechanism include both PoW and PoS. In order to improve TPS, the PoW protocol is used in mining while PoS is used in other aspects. The result is good. TPS has increased from 7 (Bitcoin) to 30-40 (Ethereum). But with the waste of PoW resources, the Ethereum community ready to transition to full PoS.

Vlad Zamfir published Casper [15] to improve the system TPS and the blockchain stability. It is regarded as an intermediate stage of Ethereum's future transition to PoS also be called the second generation of PoS. At the same time, this protocol also solves the Nothing-at-stake attack vulnerability in the first generation of PoS.

The agreement mainly stipulates that all participants who bet on the consensus result need to have a certain deposit for the result. If the final bet result is discarded, then only a part of the deposit can be returned accordingly. Such a mechanism makes it impossible for users to launch 'Nothing at Stake' easily. Because they need to choose the result carefully, which is similar to PoW at this point. In addition, Casper has many other properties, such as 'Transaction Finality', 'Censorship Resistance' and so on. However, the consensus protocol has not yet been applied to Ethereum, and Ethereum still uses the previous consensus mechanism of PoW.

3.4EOS

EOS is a cryptocurrency community officially created in 2018 [11]. The consensus mechanism adopted is the upgraded version of PoS, DPoS, the full name is Delegated Proof of Stake [11]. Compared with coinage in the first generation of PoS as a bargaining chip for the power of accounting, DPoS has specifically set up two witnesses and stakeholders [12] (The node here is still not hierarchical). Each time the bookkeeping is done exclusively by the witness, the stakeholders then vote which witness can be used for the bookkeeping. After the final vote, the top N witnesses become the bookkeepers for this round. In different cryptocurrencies, the number of N is different, and the number of N in EOS is 21 [11].

In the case of smooth work, every time the 21 witnesses generate blocks, the order of the 21 witnesses will be randomly rearranged, and the next round of accounting will be carried out after the arrangement.

There will be a certain reward for each bookkeeping, and the witnesses will generally use the form of dividends to give back a part of the reward to the stakeholders who originally voted for the node.

But when there is a problem in the work process, the list of witnesses may change. Each witness selected as the bookkeeper has two seconds to generate a block and then rotate to the next witness. But in this process, if there are problems such as instability of computing power that result in the failure to generate blocks, then stakeholders can vote for other nodes, and then replace them with new nodes in the next round. Although in theory all nodes can be a member of the accounting list, often only the super nodes in the community will be included in this list. These nodes all have a lot of contribution to the network and have accumulated a certain amount of prestige.

The order in this process is determined after it comes out of the list of bookkeepers, so the efficiency of the block generation of this scheme is very high, and because the ranking is determined, there will be basically no blockchain forks caused by network delay problems [12]. This process allows EOS to have a relatively high TPS, which is about 3600 [17].

However, since the witnesses are selected manually, the fairness is not as strong as the first-generation pure PoS. And because the super nodes are working hard to contribute to the network, the premise is that there is additional currency issuance. If the currency reaches the upper limit, the additional issuance will also stop.

3.5Ripple Network

In all early prove-of-X consensus protocols, there is no hierarchy between nodes. While becoming a transaction node, it can also become a verification node to verify mining. This makes the blockchain network fairer and more decentralized. But what is often brought is the low processing speed of the transaction. In 2014, the ripple network proposed an RPCA mechanism for XRP currency [18]. The nodes are divided into specially verified nodes and transaction nodes, which greatly reduces the network response time. The official TPS data provided by ripple is 1500 [17].

Among them, the stability of the blockchain and the creation of new blocks are completed by verification nodes. Whenever a common transaction node generates a new transaction, it will hand over the transaction to the list of verification nodes that it trusts and broadcast it. If the transaction exists in the 80% trusted verification node at the end, the transaction is established.

The node division of the Ripple network enables transactions to be confirmed in a short time. However, since the trust verification node is trusted by other user nodes in the network, a reliable verification node is an important part of the normal operation of the mechanism. Therefore, the degree of decentralization and security of the protocol has been questioned. The Ripple network hopes to cooperate with banks in various countries, allowing banks to act as verification nodes to ensure the security of network transactions.

4.COMPARISON ANALYSIS AND DISCUSSION

The consensus protocol can determine the security, decentralization, TPS, etc. of the blockchain and cryptocurrency system. But there is no consensus agreement that can take care of all aspects. Whenever the currency is relatively high in a certain attribute, another attribute is often sacrificed.

The early use of ‘Proof of X’ consensus protocol currencies such as Bitcoin and PPC were pursuing a relatively high degree of decentralization and security. Therefore, the transaction processing speed of the system network is relatively ignored. But at that time, the total number of network users was relatively small, and single-digit or tens-digit TPS was enough to satisfy most network members.

But with the popularity of currencies, the users of these cryptocurrencies are beginning to increase. The fixed lower TPS increases as the number of transactions makes the network congested. Therefore, currency communities such as EOS that later used the improved Proof of X type protocol began to sacrifice some centralization to achieve faster transaction processing efficiency. High efficiency and high speed are more and more favored by users. Various traditional cryptocurrencies are moving in this direction. ETH is a good example of witnessing this process. Although ETH still uses the ‘PoW mining’ + ‘PoS transaction’ model, ETH is gradually pushing itself towards a complete PoS protocol, and Casper PoS can be seen as a transition in this process.

Tab.1 is a comparison of various cryptocurrencies. As the processing efficiency increases, other attributes will be relatively reduced.

The first category mentioned above belongs to the standard block chain cryptocurrency, which meets two basic conditions, the structure is a standard block chain single chain structure and nodes are not differentiated. Nodes can serve as transaction nodes of the network and at the same time as verification nodes of the network.

For the first feature mentioned above, the single chain blockchain determines that the cryptocurrency using this structure can only allow one new block to be created at the same time. Therefore, to a certain extent, there is an upper limit on the speed of new block establishment, and it is very difficult for the transaction

of this currency to reach the number of thousands of transactions per second of VISA.

However, some new cryptocurrencies that use DAG (Directed Acyclic Graph), although they are separated from the original single-chain structure of the blockchain, have been greatly improved in TPS. Taking MIOTA used by the IOTA community as an example [19], it uses a multi-chain structure which is called Tangle. The essence of the Tangle structure is a DAG. Unlike traditional blockchains, each unit only contains one transaction, but the network allows asynchronous and concurrent write transactions at the same time.

Consensus mechanism with such a high-concurrency structure can obtain a high TPS value after reasonably optimizing the nodes, and the parallel computing and processing data can reach very high level TPS [17]. The original purpose of this technology is to reduce transaction costs, which is very attractive for systems with a large number of low-cost transactions.

In terms of nodes, traditional nodes are not differentiated. In fact, the purpose is to prevent the centralization of cryptocurrency. This is also the meaning of distributed systems. However, the increase in users makes the original block production rate relatively low. Decentralization determines that each block needs to be inspected by the surroundings, and this inspection process can easily lead to blockage. Therefore, some currencies such as XRP have reduced the relative degree of centralization to increase TPS. They are ready to prevent these central management nodes from betraying by cooperate with international banks to make them become management nodes. This essentially betrays the concept of decentralization but guarantees a high TPS value.

Although Bitcoin's TPS is very low, its high degree of decentralization and high security still attract lots of users. But in addition, most of the consensus protocols adopted by cryptocurrencies are developing in the direction of high TPS. In order to accommodate the increase in the number of users, the processing speed of the system has to be increased. In addition, currencies have begun to try to abandon the standard single-chain structure of the blockchain and turn to a multi-chain, high-concurrency structure, which has brought opportunities for many communities with many small transactions. But users should treat the TPS indicator rationally when choosing a cryptocurrency community, because for a currency, security and stability also need to be guaranteed. Don't blindly pursue a good TPS and ignore other attributes.

The future blockchain can try to increase the size of TPS based on balancing other attributes as much as possible. In the future, there will only be more new users of blockchain currency, so in order to be able to accommodate this increased traffic, it is necessary to speed up the processing speed of the system. On this basis, it is undesirable to discard some of the original properties of blockchain cryptocurrency. For example, sacrificing part of the centralization or using a new structure like DAG.

5.CONCLUSION

This article compares the differences between cryptocurrencies using traditional consensus protocols and cryptocurrencies using non-traditional consensus protocols in chronological order. It is found that the overall currency market has gradually chosen to sacrifice the degree of decentralization to increase TPS, to cope with more users joining the market which means there are more small transactions. There are beginning to be cryptocurrencies that use a master who is separated from the traditional blockchain single chain to achieve a relatively high concurrent processing rate. Some cryptocurrencies have begun to use node differentiation to differentiate community nodes. The purpose is to abandon decentralization and achieve better fairness. The consensus protocol of comparing these cryptocurrencies is to point out a direction for users who have just entered the cryptocurrency. We can make an outlook for the future development of cryptocurrency.

TABLE I. Comparison of different cryptocurrency consensus protocols

Cryptocurrency	Consensus Mechanism used	Degree of decentralization	Degree of safety	TPS	Time
BTC	PoW	high	high	7	2009
PPC	PoS	middle	low	<30	2012
ETH	PoW + PoS	middle	middle	30-40	2013
	Casper PoS[a]	middle	middle	-	2015
EOS	DPoS	low	middle	3600	2018
XRP(Ripple)	RPCA	middle	middle	1500	2014

a. The agreement was proposed in 2015, but it is still just an idea and is not currently being used in Ethereum.

REFERENCES

[1]Satoshi Nakamoto. 2009. Bitcoin: A Peer-to-Peer Electronic Cash System. Cryptography Mailing list at https://metzdowd.com (03 2009).

[2]Christina Comben. 2019. What is a double-spend attack? https://coin-rivet.com/what-is-a-double-spend-attack/

[3]2018. The consensus mechanism of the blockchain and its operating rules. https://zhuanlan.zhihu.com/p/43354601

[4]Crosby, Michael; Nachiappan; Pattanayak, Pradhan; Verma, Sanjeev; Kalyanaraman, Vignesh (16 October 2015). BlockChain Technology: Beyond Bitcoin(PDF) (Report). Sutardja Center for Entrepreneurship & Technology Technical Report. University of California, Berkeley. Retrieved 19 March 2017.

[5]Rüdiger Schollmeier, A Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer Architectures and Applications, Proceedings of the First International Conference on Peer-to-Peer Computing, IEEE (2002).

[6]http://www.hashcash.org/papers/hashcash.pdf, 2002

[7]CoinWarz. (2021 10). Bitcoin Difficulty Chart. https://www.coinwar-z.com/mining/bitcoin/difficulty-chart

[8]Bandara, H.M.N.D, A.P.Jayasumana (2012). "Collaborative Appli-cations over Peer-to-Peer Systems - Challenges and Solutions". Peer-to-Peer Networking and Applications.

[9]Sunny King, Scott Nadal. 2012. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake at https://www.peercoin.net/whitepap-ers/peercoin-paper.pdf

[10]Julian Marinez. 2018. Understanding Proof of Stake: The Nothing at Stake Theory. https://medium.com/coinmonks/understanding-proof-of-stake-the-nothing-at-stake-theory-1f0d71bc027

[11]Ian Grigg. 2018. EOS - An Introduction at https://whitepaper.io/docu-ment/671/eos-1-whitepaper

[12]Steve Walters. 2018. Delegated Proof of Stake (DPoS) - Total Begin-ners Guide. https://www.coinbureau.com/education/delegated-proof-stake-dpos/

[13]Gareth Tyson, Andreas Mauthe, Sebastian Kaune, Mu Mu and Thomas Plagemann. Corelli: A Dynamic Replication Service for Supporting Latency-Dependent Content in Community Networks. In Proc. 16th ACM/SPIE Multimedia Computing and Networking Conference (MMCN), San Jose, CA (2009)

[14]Editorial Team. 2017. What is the Ethereum Casper POS Protocol? https://www.coinbureau.com/education/what-is-the-ethereum-casper-pos-protocol/

[15]Vlad Zamfir. 2015. Introducing Casper “the Friendly Ghost” https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost/

[16]Vitalik Buterin. 2013. A Next-Generation Smart Contract and Decentralized Application Platform. https://ethereum.org/en/whitepa-per/

[17]China Blockchain Technology and Industry Development Forum. https://zhuanlan.zhihu.com/p/133873895

[18]David Schwartz, Noah Youngs, Arthur Britto. 2018. The Ripple Protocol Consensus Algorithm. https://ripple.com/files/ripple_cons-ensus_whitepaper.pdf

[19]Serguei Popov. 2018. The Tangle. https://whitepaper.io/document-/3/iota-whitepaper