2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)
Banff Center, Banff, Canada, October 5-8, 2017

A Review on Consensus Algorithm of Blockchain

Du Mingxiao*, Ma Xiaofeng*, Zhang Zhe**, Wang Xiangwei*, Chen Qijun*
*Department of Control Science and Engineering,
Tongji University
Shanghai, China
Email: dumingxiao@hotmail.com
**Fintech Laboratory,
QianBao Financial Services Company
Beijing, China

***Abstract*—Blockchain is the basic technology of bitcoin. With the value appreciation and stable operation of bitcoin, blockchain is attracting more and more attention in many areas. Blockchain has the characteristics of decentralization, stability, security, and non-modifiability. It has the potential to change the network architecture. The consensus algorithm plays a crucial role in maintaining the safety and efficiency of blockchain. Using a right algorithm may bring a significant increase to the performance of blockchain application. In this paper, we reviewed the basic principles and characteristics of the consensus algorithms and analyzed the performance and application scenarios of different consensus mechanisms. We also gave a technical guidance of selecting a suitable consensus algorithm and summarized the limitations and future development of blockchain technology.**

Keywords—blockchain; consensus; distributed system; digital currency; bitcoin

I. INTRODUCTION

The blockchain was firstly introduced in the treatise [1] "Bitcoin: A peer-to-peer electronic cash system" by Satoshi Nakamoto in 2008. It is the underlying technology of bitcoin. The traditional transactions require a centralized trusted institution. The confirmation and record of the transactions depend entirely on the trusted institution, which may cause many problems of transaction cost, efficiency, and security. Decentralization is the core feature of blockchain and it can be used to solve these problems. All the nodes in the blockchain have equal status. These nodes achieve consensus by using the prior agreement of the rules and following the principle of majority dominance. They implement the functions of data distributed storage and transaction information recognition in the situation that the other nodes are not fully trusted. So we can effectively solve the transaction problems.

Bitcoin is the first blockchain application in the financial field. With the development of the blockchain technology, blockchain has been concerned by the government, financial institutions, and technological enterprises. For example, the British government issued the report [2] about blockchain to promote the application of blockchain in centralized digital currency and government affairs in January 2016. All major banks in the world are actively exploring the application of blockchain technology. In August 2016, UBS, Deutsche Bank, Bank of Santander and Bank of New York Mellon jointly developed a digital currency system with blockchain technology to help financial markets improve the speed of payment. Bank of Santander, the largest bank in Spain, believes that if all banks in the world use the blockchain, they can save about $20 billion every year. World Economic Forum predicts that 10% of the world's GDP will be stored on the blockchain network by 2027 [3].

In the academic field, the blockchain technology is also attracting more and more attention. The study of blockchain can be divided into three categories. Firstly, study on the digital currency that based on blockchain, including the decentralized and centralized digital currency [4]. Secondly, study on the application of blockchain technology in non-digital currency scenarios such as the application of blockchain in smart city [5] and medical information security management [6, 7]. Thirdly, study on underlying blockchain technology. More and more researchers realize that the blockchain can be stripped out from the digital currency to create a revolutionary technical architecture in other areas. Some researchers have begun to study the underlying technologies such as the difficulty control of mining[8], the scalability of consensus algorithms [9] and the smart contract [10].

Blockchain technology includes the point-to-point(P2P) communication, consensus algorithms, distributed storage technology, encryption algorithms, and so on. But at present, the research on blockchain is mainly focused on the application of Bitcoin or blockchain in different areas. So in this paper, we introduce the existing common consensus algorithms in chapter II and analysis the performance and shortcomings of the consensus algorithms. Then we give a guidance on how to select the suitable consensus algorithm in different scenarios in chapter III. Finally, we summarize this paper in chapter IV.

II. THE CONSENSUS ALGORITHMS

In the applications of blockchain, we need to solve two problems- double spending and Byzantine Generals Problem [11]. Double spending problem means reusing the currency in two transactions at the same time. The traditional currency is the entity, so we will not face the problem of double spending while using traditional currency. We can also solve the double spending problem in the Internet transactions with the centralized trusted institutions. Blockchain solves this problem with the method of verifying the transactions by many distributed nodes together. Byzantine Generals Problem is the problem in the distributed system. The data can be delivered between different nodes through peer-to-peer communications. However, some nodes may be maliciously attacked, which will lead to the changes of communication contents. Normal nodes need to distinguish the information that has been tampered and obtain the consistent results with other normal nodes. This also needs the design of the corresponding consensus algorithm.

The consensus algorithm has been studied for many years in distributed system. There are some transplantable consensus algorithms applied in blockchain. We make a detailed description of the principles of these consensus algorithms in this section.

A. PoW (Proof of Work)

PoW is the consensus algorithm used in bitcoin. Its core idea is to allocate the accounting rights and rewards through the hashing power competition among the nodes. Based on the information of the previous block, the different nodes calculate the specific solution of a mathematical problem. It's difficult to solve the math problem. The first node that solves this math problem can create the next block and get a certain amount of bitcoin reward. Satoshi Nakamoto used HashCash to design this mathematics problem in bitcoin [12]. The specific calculation steps are as follows:

1) Get the difficulty: After the production of every 2016 blocks, bitcoin mining algorithm will dynamically adjust the difficulty value according to the hash rate of the whole network.

2) Collect transactions: Collect all pending transactions on the network after the production of the last block. Then calculate the Merkle Root of these transactions and fill in the block version number, the 256-bit hash value of the previous block, the current target hash value, Nonce random number and other information.

3) Calculating: Traverse the Nonce from 0 to 2^{32} and calculate the double SHA256 hash value in step 2. If the hash value is less than or equal to the target value, the block can be broadcasted. The node complete accounting After the verification of other nodes.

4) Restarting: If the node can't work out the hash value at a certain time, it repeats step two. If any other node completes the calculation, then it restarts from step 1.

PoW takes the workload as the safeguard. The newly created block is linked to the blocks in front of it. The length of the chain is proportional to the amount of workload. All nodes trust the longest chain. If anyone wants to tamper with the blockchain, he needs to control more than 50% of the world's hashing power to ensure that he can become the first one to generate the latest block and master the longest chain. The gains from tampering can be much greater than the cost. So the PoW can effectively guarantee the safety of the blockchain.

B. PoS(Proof of Stake)

PoS has been mentioned in the first bitcoin project, but it was not used because of the robustness and other reasons. The earliest application of PoS is PPCoin [13]. In PoS, the digital currency has the concept of coin age. Coin age of a coin is its value multiplied by the time period after it was created. The longer one node holds the coins, the more rights it can get in the network. Holders of the coins will also receive a certain reward according to the coin age. In the design of PPCoin, mining is also needed to get the accounting rights. The formula is *proofhash* < *coin age* * *target*. The proofhash is a composed hash value of the weight factor, the unspent output value and the fuzzy sum of current time. PoS limits the hashing power of each node. The difficulty of mining is inversely proportional to coin age.

PoS encourages the coins holders to increase the holding time. With the concept of coin age, the blockchain is no longer entirely relying on the proof of work. That effectively solves the resource wasting problem in PoW. The security of the blockchain using PoS improves with the increasing value in the blockchain. The attackers need to accumulate a large number of coins and hold them long enough to attack the blockchain. This also greatly increases the difficulty of attack.

Besides the PPCoin, there are also many other coins using PoS such as the Nxt [14] and BlackCion [15]. But they consider the rights of the nodes and use a random algorithm to allocate accounting rights.

C. DPoS(Delegated Proof of Stake)

In the initial design stage of bitcoin, Satoshi Nakamoto hoped that all the participants can use the CPU to mine. So the hashing power can match the nodes and each node has the opportunity to participate in the decision-making of the blockchain. With the development of technology and the appreciation of bitcoin, the machines that are specially designed for mining are invented. The hashing power is grouped in the participants that have large numbers of mining machines. The ordinary miners rarely have the opportunity to create a block.

BitShares is an example of DPoS [16]. In the blockchain with DPoS, each node can select the witnesses based on its stake. In the whole network, the top *N* witnesses that have participated in the campaign and got the most votes have the accounting right. The number *N* of witnesses is defined such that at least 50% of voting stakeholders believe there is sufficient decentralization [17]. The elected witnesses create new blocks one by one as assigned and get some rewards. The witnesses need to ensure adequate online time. If a witness is unable to create its assigned block, the activity of that block will be moved to the next block and the stakeholders will vote for a new witness to replace it. The blockchain using DPoS is more efficient and power-saving than PoW and PoS.

D. PBFT(Practical Byzantine Fault Tolerance)

In distributed systems, Byzantine Fault Tolerance can be a good method to solve the transmission errors. But early Byzantine system requires exponential operations. Until 1999, the PBFT(Practical Byzantine Fault Tolerance) system [18] was proposed and the algorithm complexity was reduced to a polynomial level, which greatly improved efficiency. The process of PBFT is shown in figure 1. It consists of five states:

1) Request: The client sends a request to the master server node, the master node gives the request a timestamp.

2) Pre-prepare: The master server node records the request message and gives it an order number. Then the master node broadcasts a pre-prepare message to the other following server nodes. The other server nodes initially determine whether to accept the request or not.

3) Prepare: If a server node chooses to accept the request, it broadcasts a prepare message to all the other server nodes and receives the prepare messages from the other nodes. After

having collected 2*f*+1 messages, if a majority of nodes choose to accept the request, then it will enter the commit state.

4) Commit: Each node in commit state sends a commit message to all the other nodes in the server. At the same time, if a server node receives 2*f*+1 commit messages, it could believe that most nodes reach a consensus to accept the request. Then the node executes the instructions in the request message.

5) Reply: the server nodes reply to the client. If the client does not receive a reply because of the network delay, the request is resent to the server nodes. If the request has been executed, the server nodes only need to send the reply message repeatedly.

E. Raft

After the Byzantine Generals Problem was raised, Lamport proposed Paxos algorithm to solve the consistency problem in certain conditions in 1990.

But because the content of the paper is difficult to understand, it was not accepted. Lamport republished the paper [19] in 1998 and the Paxos was briefly reintroduced in 2001[20]. Then Paxos occupies the dominant position in the field of consistency algorithm. Many other algorithms are derived from it. But Paxos algorithm is too theoretical. The people have great difficulty in understanding it and engineering implementation. In 2013, Standford's Ongaro and others published the paper and proposed Raft algorithm[21]. Raft achieves the same effect as Paxos and is more convenient in engineering implementation and understanding.

Raft cluster generally contains 5 server nodes. Up to two nodes are allowed to crash at the same time. The server node as shown in figure 2 has three states: leader, follower, and candidate. There is only one leader in a term and the leader is responsible for handling all clients' requests.

III. ANALYSIS OF THE CONSENSUS ALGORITHMS

All the consensus algorithms have their own characteristics. In this chapter, we analysis the safety, verification speed, throughput (transactions per second, TPS), fault tolerance, scalability and shortcomings of the consensus algorithms and the usage in different scenarios.

A. Performance

PoW and PoS solve the safety problem by using the share

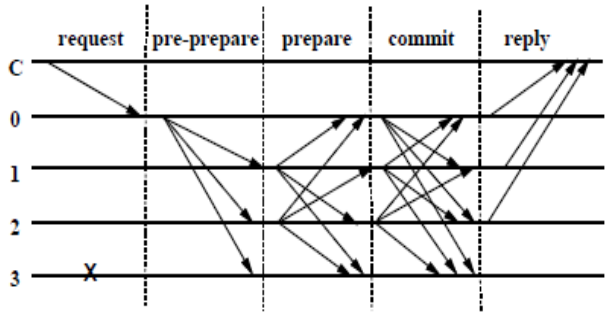

Fig. 1. Steps of PBFT[18]

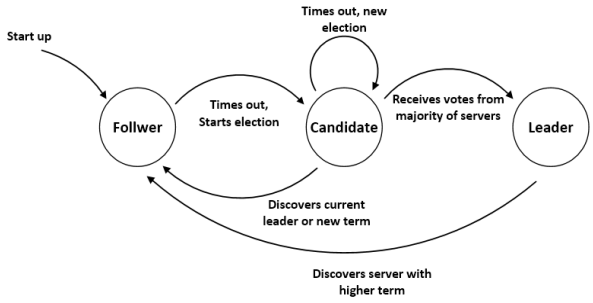

Fig. 2. States transfer of RAFT

ledger of the whole network. The system is stable as long as the longest chain is guaranteed by the honest nodes. We take PoW as an example to provide a proof of safety.

Hypothesis: the total hashing power in the network is H_0, the average time for creating a new block is T_0, the total hashing rate of honest nodes is pH_0 and the total hashing rate of malicious nodes qH_0. The difficulty is changeless when calculating the double spending probability. One transaction is verified after *n* blocks.

Firstly, we calculate the probability P_z for a malicious node to catch up with the honest chain in the case of *z* blocks falling behind. It is analogous to the Binomial Random Walk with an absorbable wall. There is a particle on the x-axis. The particle can move unit distance with the probability *q* to the left or *p* to the right ($p+q=1$) each time. Initially, the particle is located at $x = z$. The particle will stop moving if it arrives at $x = 0$. P_z equals the probability of arriving at $x = 0$. So:

$$P_0 = 1,\ \lim_{z\to\infty} P_z = 0 \tag{1}$$

$$P_z = pP_{z+1} + qP_{z-1},\ z = 1,2,\cdots,\infty \tag{2}$$

If q < p, use

$$C_z = P_{z+1} - P_z,\ \mathrm{r} = q/p \tag{3}$$

From formula (2), we get

$$P_z - P_0 = \sum_{k=0}^{z-1}(P_{k+1} - P_k) = \frac{1-r^z}{1-r}C_0 \tag{4}$$

Then, with formula (1) we can get:

$$P_z = r^z = (\frac{q}{p})^z, q < p \tag{5}$$

It is easy to prove

$$P_z = 1, q \geq p \tag{6}$$

So we can conclude

$$P_z = \begin{cases} 1, & q \geq p \\ (\frac{q}{p})^z, & q < p \end{cases} \quad (7)$$

We can see in (7): if the total hashing power of malicious is more than 50% of the whole network hashing power, the double spending attack will finally success. Then we need to calculate the probability of success in double spending with n blocks to wait while $q < p$.

We assume that a node will restart hashing if it fails to work out the right hash in t time. The honest nodes' total probability of success in t time is tp/T_0 and the malicious nodes' is tq/T_0.

If the malicious nodes want to succeed in double spending attack, they have to wait for n blocks until the transactions have been verified. In this period, both the honest nodes and the malicious nodes have tried nT_0/tp times and the honest nodes have success n times. So the malicious nodes' successful times λ will be a Poisson distribution with expected value:

$$\lambda = nq/p$$

So the malicious nodes' success probability of double spending is

$$P = \sum_{k=0}^{n} \frac{\lambda^k e^{-\lambda}}{k!} \left(\frac{q}{p}\right)^{n-k} + \sum_{k=n+1}^{n} \frac{\lambda^k e^{-\lambda}}{k!} \quad (8)$$

Equal to

$$P = 1 - \sum_{k=0}^{n} \frac{\lambda^k e^{-\lambda}}{k!} [1 - \left(\frac{q}{p}\right)^{n-k}] \quad (9)$$

We visualize the results of formula (9) with different n in figure 3. It's easy to conclude from the result that the transaction is safe only if we wait for enough blocks to confirm the transaction. The blockchain using PoW or PoS can tolerate up to 50% malicious nodes.

For the purpose of reducing bifurcation and waiting for enough blocks to confirm, the throughput of blockchain using PoW or PoS is limited. In this blockchain, all the nodes can mine according to the pre-set rules. The throughput and verification speed is not related to the number of nodes. Therefore, such a blockchain network has almost unlimited scalability.

In the blockchain using DPoS, the elected witnesses are responsible for creating blocks and confirming transactions. For the reduction of verification nodes, the blockchain with DPoS can accelerate the speed of creating the blocks and verifying the transactions. The throughput and transaction verification speed of DPoS are faster than PoW or PoS. The scalability is also unlimited.

The blockchain using PBFT consists of $3f+1$ server nodes and each node needs to collect $2f+1$ messages in the communication. So this blockchain system can tolerate at most 33% malicious nodes. PBFT also contains the mechanism of view change. The view change mechanism is to replace the master node with a following node when the master node has

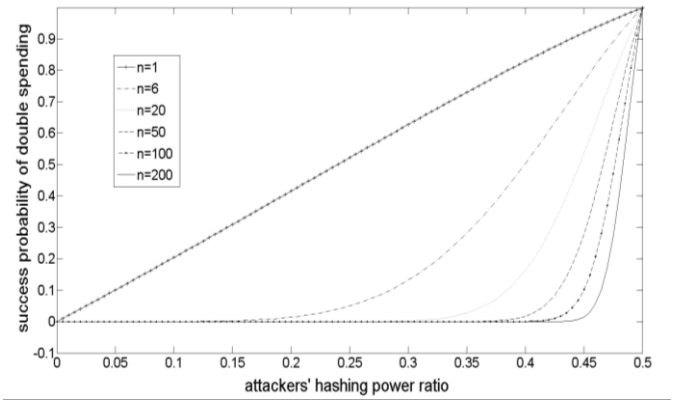

Fig. 3. Relationship between hashing power ratio and double spending

an error or the system cannot complete the client's request in a long time. As the nodes in PBFT need to communicate with every node to reach the agreement, the scalability is limited. PBFT is more suitable for the permissioned blockchain system with high-speed network and a small number of nodes.

Raft has high efficiency and simplicity and it has been widely used in the distributed systems. In the blockchain with RAFT, the leader occupies an absolutely dominant position. The blockchain cannot tolerate malicious nodes and can tolerate up to 50% nodes of crash fault. It is important to guarantee the absolute security of the leader node. The throughput is limited by the maximum performance of one node. The scalability is limited by the architecture of RAFT.

The comparison of the five consensus algorithms is shown in table I.

B. Limitation

PoW also has weaknesses such as waste of resources, slow speed of transaction verification and concentration of hashing power:

1) Waste of resources: the nodes which have high hashing power can get the corresponding bitcoins as rewards. This is the main way to get the bitcoin, which forces people to upgrade the hardware. Participants need to spend a lot of money to buy the special mining machines and the machine needs to consume a large amount of electricity in the process of calculation. These characteristics also make the application of PoW some limitations.

TABLE I. COMPARISON OF THE FIVE CONSENSUS ALGORITHMS

characteristics	consensus algorithms				
	PoW	***PoS***	***DPoS***	***PBFT***	***RAFT***
Byzantine fault tolerance	50%	50%	50%	33%	N/A
crash fault tolerance	50%	50%	50%	33%	50%
verification speed	>100s	<100s	<100s	<10s	<10s
throughput(TPS)	<100	<1000	<1000	<2000	>10k
scalability	strong	strong	strong	weak	weak

2) The slow speed of transactions: In order to reduce the production of single block or branch of the chain, the calculating time of each block must not be too short. The average calculating time of the block is 10 minutes. But the time interval between the two blocks is not sure. The largest interval in history is more than one hour while the minimum interval is less than one second. This time has a great limitation in the application of instant payment.

3) The concentration of hashing power: With the increase of mining difficulty, it's hard for a single one to figure out the math problem. In order to solve this problem, some organizations have set up the "mining pool", and the miners in a mining pool solve the math problem together. After a pool solving the math problem and obtaining the bitcoin as rewards, the miners allocated the bitcoin according to their contribution. But because of the existence of the mining pool, the global hashing power become concentrated. If the hashing power of one pool or some combined pools is more than 50%, they can easily have a monopoly on accounting. figure 4 shows the monthly hashing power rankings. At present, the global top six mining pools' hashing power has been more than 50% of global hashing power.

PoS is similar to PoW. The miners also need to work out the right hash to create new blocks and they have to wait for a certain number of blocks to confirm the transactions. PoS did not essentially solve the problem of resources wasting, slow trading and concentration of hashing power in PoW. Besides, the coin age is also destroyed in usual transactions, which may make participants more interested in collecting the coins instead of using them.

In the blockchain with PBFT, the verification functions are done in the server. One server node needs to communication with all the other nodes. The data processing size and time consumption are huge. As the size of the network increases, the efficiency of consensus will drastically decrease. Besides, PBFT server nodes need to have a high degree of confidence, so PBFT cannot be used in the permissioned blockchain.

In Raft, the leader occupies an absolute dominance. It's very important to defend the safety of the leader. Once the leader is maliciously controlled, the system will be completely destroyed. In addition, the system performance is limited by the maximum throughput of the node.

C. Application Scenarios

The blockchain can be divided into three categories: public blockchain, private blockchain, and permissioned blockchain. According to the previous section, it is better to use the corresponding consensus algorithm in different scenarios.

A public blockchain means that it is accessible to all the people in a public area. Everyone can become one of the nodes and make contributions to obtain the rewards following the rules. There are no trust relationships among the nodes. Public blockchain is completely open and decentralized. All transactions on the public blockchain can never be changed or revoked. PoW, PoS, and DPoS consensus algorithms are common choices of public blockchain.

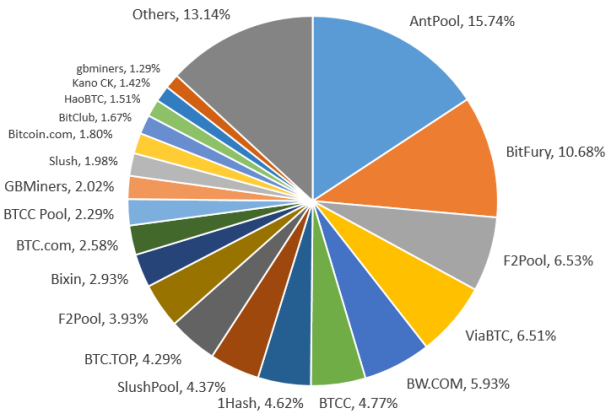

Fig. 4. Ratios of the mining pools[22]

Private blockchain means that the owner of the blockchain has the highest authority to change the information. The rest of the nodes have limited access to read. Compared to the public blockchain, the private blockchain has the characteristics of easy modification and low transaction cost. Transaction verification of the private blockchain only need some designated high credit nodes. Private blockchain is applied to more closed networks such as the intranet. It is more important to solve the crash faults than Byzantine faults. We can use PBFT and RAFT consensus mechanisms according to the network size.

Permissioned blockchain means that the blockchain is composed of many parties and the main nodes are pre-specified by the participants. The members of the permissioned blockchain do not fully trust the others. Each participant selects its own consensus node according to the rules. Transactions need to be recognized by most consensus nodes. The degree of openness and centralization of the consortium blockchain lies between the public and private blockchain. The permissioned blockchain is suitable for the semi-closed network, which is built by different enterprises. There may be conflicts among different enterprises and some nodes can become malicious nodes, so it is better to use PBFT in this scenario.

IV. SUMMARY

Blockchain has the characteristics of decentralization, stability, security, non-modifiability and so on. With the development of technology, the blockchain is attracting more and more attention in different areas. This paper makes a systematic review of the usual consensus algorithms used in the blockchain. Consensus algorithm is the core technology of blockchain, but current research of the consensus mechanism is still in its infancy. The consensus algorithm specially designed for different scenarios is still very rare. How to make the blockchain performance better in a particular scenario? We still need further research.

ACKNOWLEDGMENT

This research is affiliated with the Tongji-QianBao Joint Fintech Laboratory of Tongji University.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Consulted, 2009.

[2] "Distributed ledger technology: beyond block chain,", 2016.

[3] P. Rizzo, "World Economic Forum Survey Projects Blockchain 'Tipping Point' by 2023,", 2015.

[4] G. Danezis and S. Meiklejohn, "Centrally Banked Cryptocurrencies," 2015.

[5] K. Biswas and V. Muthukkumarasamy, "Securing smart cities using blockchain technology," in 18th IEEE International Conference on High Performance Computing and Communications, 14th IEEE International Conference on Smart City and 2nd IEEE International Conference on Data Science and Systems, HPCC/SmartCity/DSS 2016, December 12, 2016 - December 14, 2016, 2016, pp. 1392-1393.

[6] P. T. S. Liu, "Medical record system using blockchain, big data and tokenization," in 18th International Conference on Information and Communications Security, ICICS 2016, November 29, 2016 - December 2, 2016, 2016, pp. 254-261.

[7] Y. Xiao, H. Wang, D. Jin, M. Li, and J. Wei, "Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control," Journal of Medical Systems, vol. 40, p. 218, 2016.

[8] D. Kraft, "Difficulty control for blockchain-based consensus systems," Peer-to-Peer Networking and Applications, vol. 9, pp. 397-413, 2016-01-01 2016.

[9] M. Vukoli, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," in IFIP WG 11.4 International Workshop on Open Problems in Network Security, iNetSec 2015, October 29, 2015 - October 29, 2015, 2016, pp. 112-125.

[10] F. Idelberger, G. Governatori, R. Riveret, and G. Sartor, "Evaluation of Logic-Based Smart Contracts for Blockchain Systems,", Cham, Switzerland, 2016, pp. 167-83.

[11] L. Lamport, R. Shostak and M. Pease, "The Byzantine Generals Problem," Acm Transactions on Programming Languages & Systems, vol. 4, pp. 382-401, 1982.

[12] A. Back, "Hashcash - A Denial of Service Counter-Measure," in USENIX Technical Conference, 2002.

[13] S. King and S. Nadal, "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake,", 2012.

[14] Nxtwiki, "Whitepaper:Nxt,", 2015.

[15] P. Vasin, "BlackCoin's Proof-of-Stake Protocol v2,".

[16] "https://bitshares.org/,".

[17] "https://bitshares.org/technology/delegated-proof-of-stake-consensus/,".

[18] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in Symposium on Operating Systems Design and Implementation, 1999, pp. 173--186.

[19] L. Lamport, "The part-time parliament," Acm Transactions on Computer Systems, vol. 16, pp. 133-169, 1998.

[20] L. Lamport, "Paxos Made Simple," Acm Sigact News, vol. 32, 2001.

[21] D. Ongaro and J. Ousterhout, "In search of an understandable consensus algorithm," Draft of October, 2013.

[22] "http://qukuai.com/,".