Advances and Applications in Mathematical Sciences
Volume 20, Issue 1, November 2020, Pages 1-13

A NOVEL COMPARISON OF CONSENSUS ALGORITHMS IN BLOCKCHAIN

VISHAL SHARMA and NIRANJAN LAL

Research Scholar, CSE
School of Engineering and Technology
Mody University of Science and Technology
Lakshmangarh, Sikar, Rajasthan, India
E-mail: er.vishu1983@gmail.com

Computer Science & Engineering
School of Engineering and Technology
Mody University of Science and Technology
Lakshmangarh, Sikar, Rajasthan, India
E-mail: niranjan_verma51@yahoo.com

Abstract

Blockchain is a main technology for different cryptocurrencies. Today blockchain has main research interest in the field of security due to its features like, stability, security, inalterable and decentralization. In blockchain technology, the transactions can be done securely with the help of consensus algorithms in a distributed system which has P2P connections of blocks, without interference of mediator [1]. So the consensus algorithms are playing a key role for preserving the security and integrity of a distributed network in blockchain technology. It is basically used for maintaining the trust in blockchain technology. The consensus algorithms are divided into two types, proof based and voting based. In this paper we have presented the some of the main consensus algorithms of these two types, and examine the weaknesses, strengths and also the types of blockchain in which these algorithms are applicable.

I. Introduction

In the year of 2008, the Satoshi Nakamoto was introducing the original concept of blockchain technology. Nakamoto was used this technology for very first cryptocurrency which was called bitcoin distributed ledger [15].

2010 Mathematics Subject Classification: 94A60.
Keywords: blockchain, consensus algorithm, cryptocurrencies.
Received April 15, 2020; Accepted July 20, 2020

Afterward various cryptocurrencies were developed on the same concept by using the blockchain technology. Conventional transaction processing systems are depends on a central authority who take the responsibilities to process all the transaction in a system. Due to this centralized transaction processing system many issues might be introduce in the system like data privacy, security and efficiency of the system. Blockchain is become a main research direction in many field mainly in the field of data privacy and security due to its Decentralize nature [2].

The blockchain technology is based on various techniques likes distributed system, P2P model, cryptography etc. In the blockchain technology as name implies it has a chain of blocks and each block contains verified data or information. In the blockchain, the first introduce block called as a genesis block which holds the initial transaction in the distributed ledger. Each and every block in a blockchain also stores the hash of its previous block. Each block is belongs to a unique hash which is a mathematical code. If any data or information which stores in the block is modified, the hash of the particular block will be altered. By this chain of blocks, the blockchain makes secure. So above discussed technique makes the blockchain technology temper proof.

When a new transaction wants to process, some nodes of the blockchain network will validate this transaction. These nodes are called miners. After validation check the transaction will be inserted into the block and this block will be added with the existing network of chain. One of the node which add the block to the chin will send the update to all other nodes of the network and While transactions take place on a blockchain, there are nodes on the network that validate these transactions.

If this method for validation takes place, it will create confusion if every node attempt to broadcast a new block simultaneously [1]. So that for solving the above discussed problem, the blockchain network is used a procedure between all nodes to reach a common agreement about the current state of the distributed ledger that is consensus algorithm. Consensus algorithm establishes trust between the anonymous nodes in a distributed computing contextual [4]. Generally the Permission-less (public) and Permissioned (private) are two ways for using blockchain. Permission less (Bitcoin) and permissioned (Hyperledger fabric) blockchain gives equal chance to each node

and only elected nodes for consensus procedure respectively [6]. Table 1 shows the comparison between these two different types of blockchain.

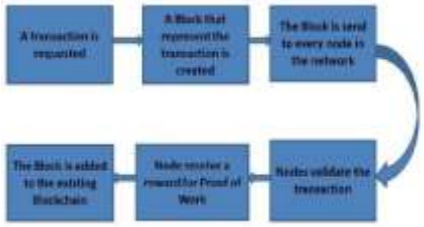

Figure 1. Blockchain Technology [11].

Table 1. Comparison of permissioned and non permissionless blockchain [6, 4].

Characteristics	Permissionless (Public) Blockchain	Permissioned (Private) Blockchain
Type of Environment	Open	Closed
Consensus Participation	Entire Nodes	Only Designated Nodes
Type of Identity	Pseudo Unknown	Registered Participants
Type of Consensus	Proof based	Voting based
Speed of Transaction Processing	Slow	Fast
Types of Consensus Algorithm	Proof of Work, Proof of Stake, Proof of Delegated Stake, etc.	Practical Byzantine Fault tolerance, Paxos, Raft
Centralized	No	Yes
Efficiency	Low	High

Therefore, this paper discusses the various consensus algorithms and analyzes the comparative study of different consensus algorithms. Hence, the rest of the paper is defined as follows: In section III we define the various proof based or lottery based and voting based consensus algorithms and also their pros and cons. In section III we discuss the comparative analysis of different consensus algorithms based on and in section IV we conclude the paper.

II. Main Consensus Algorithm

The meaning of consensus is to reach a general agreement between all the participated nodes or block in the blockchain network. It is the heart of

the blockchain network. By applying the consensus algorithm, blockchain provides the reliability and trust in the network between the anonymous nodes in a distributed computing contextual. Basically, the consensus algorithm ensures that the information which is available on the distributed ledger is not tampered by anyone.

Generally, in the blockchain applications we want to solve the two problems those are double spending and Byzantine general problem. The meaning of the double spending is reusing the coins in the two transactions simultaneously. In the blockchain this problem can be solved by verifying the transaction by all the participated nodes in the network. The other problem, Byzantine general problem is defined as the a condition where involved nodes must agree on a single strategy in order to avoid complete failure, but where some of the involved nodes are corrupt and distributing false information or are unreliable. In this section, we familiarize some main consensus algorithms of the blockchain. As shown in figure2, these algorithms are divided into two parts-lottery based and voting based [6].

Figure 2. Taxonomy of Consensus Algorithm [6].

A. Lottery based Consensus Algorithms

a. PoW (Proof of Work): This was first introduced by Satoshi Nakamoto for the bitcoin cryptocurrency. The concept of the PoW is works on the basis

of enabling the miners to add new blocks of transactions to the blockchain. In order to validate the transaction, the miners should get to solve a cryptographic puzzle which is also known as a hash puzzle. Classical PoW consensus algorithm is built on SHA-256. The other algorithms include the following secure hashing algorithm SHA-3, Scrypt, scrypt-n, scrypt-jane [3]. In this, the first node which solves the puzzle can have a right to create a new block and also acquires the bitcoin as the reward. Figure 3 shows this algorithm [3, 7]. PoW puzzle solving is a very difficult task. Furthermore, the PoW algorithm have some disadvantages, PoW takes a large amount of processing and power and it is also vulnerable to 51% attack. The meaning of 51% is that, if a controlling body holds 51% or more than 51% of nodes in the blockchain network, this body can corrupt the blockchain network by acquisition the bulk of the network [6]. Moreover, as the chain scaled, the time and difficulty for solving the PoW will also increase. Because of PoW consuming lots of time in computing processing, this is not suitable for large and fast-growing networks [12]. The following crypto currencies like Bitcoin, Ethereum, Monero coin, Litecoin, Dogecoin are implementing PoW as a consensus algorithm.

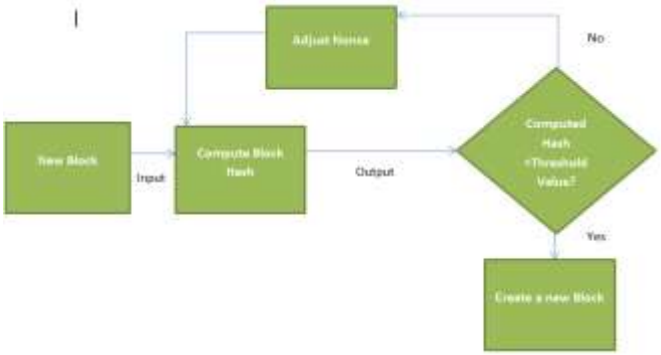

Figure 3. Pow Algorithm [3] [7].

b. PoS (Proof of Stake): This is a better alternative of the PoW.

This algorithm was first introduced by Sunny King and Scott Nadal in 2012. This solves the high energy consumption problem in mining of Bitcoin. For adding new transactional blocks in PoS, every single miner spends some of their coins as stake in the coins of the system [3]. As many coins are in stake, as much participants would be able to add new blocks to the

blockchain. Every single miner will get the reward as a block and share of the transaction fees, for mining the new blocks. The coin age concept was introduced for solving a PoS for size of the stake [6].

For example, if you hold 15 coins for a total of 25 days, then your coin age is 375. If one time a node creates a new block, the coin age of the node will be cleared to 0. The formula for this is, proofhash < coin age ∗ target. Figure 4 shows this algorithm. For creating the blocks, the PoS consensus algorithm can be choosing miners pseudo-randomly for the Blockchain. Due to this no any miner can predict its turn in well advance. This algorithm also solves the monopoly problem of PoW. Also, this algorithm is protected to a 51% attack, it might be imposed fines if any validators would be making false verification process [24]. The following crypto currencies like Decred, Ethereum (soon), Peercoin, are adopting PoS as a consensus algorithm.

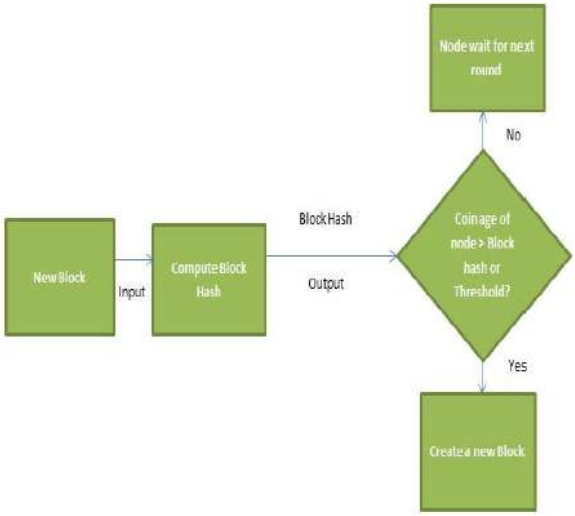

Figure 4. PoS Algorithm [3].

c. DPoS (Distributed Proof of Stake): This is a variation of the PoS. This algorithm was proposed by Daniel Larimer. In DPoS, the stakeholder of the chain can able to elect their delegates those are called as witnesses. They are able to add a new block of the transaction to the blockchain. They can also elect the top witnesses by the concept of voting [13]. If the system is fully decentralized the voting only can be occured. If delegates, the stackerholder can vote and substitute the delegetes with a

better delegates those are continually miss their blocks or publish invalid transactions [3][6][12] as shown in figure 5. The following crypto currencies like Steemit, EOS, BitShares, are adopting DPoS as a consensus algorithm.

d. LPoS (Leased Proof of Stake): This algorithm was proposed by Waves. Waves created the custom token in a decentralized blockchain platform and it consumes less amount of power. LPoS creates a centralized environment inside a decentralized platform and allows the smallholders to get their chance of stalking. In this, the coin holder can get benefit by leased the coins. This coin makes the node stronger or gives more weight, thus increases the chances of being allowed to add a new block to the chain [12].

e. PoA (Proof of Activity): This algorithm was proposed by Cynthia Dwork and Moni Naor. PoA algorithm is a combination of PoW and PoS algorithms. This algorithm offers; low overhead on the network, high level security and less storage space.

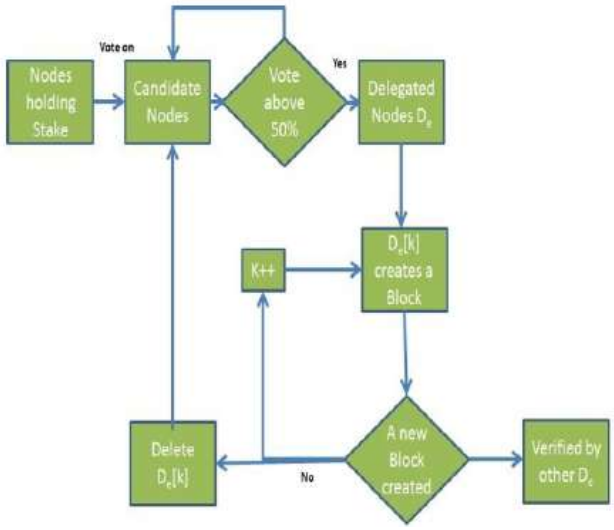

Figure 5. DPoS Algorithm [3].

PoA can be synchronized transactions in a perfect manner. Because creating blocks would be requires a huge part of the total currencies created up to now. It is very difficult for the attacker to monopolize the process. In practice, this attack is very costly. In the beginning, the system performs under the Proof of Work algorithm, as miners compete to solve a critical

cryptographic puzzle after that the process performs under the Proof of Stake - the validated transactions of the particular block get into the blockchain. The following crypto currency as decred is adopting PoA as a consensus algorithm [14].

f. PoI (Proof of Importance): PoI was introduced by NEM. PoI is an advanced version of PoS. Which nodes are eligible to add a block to the network is depends on the score in proportion to the currency vest by the node into the network or the node's importance scale determines. PoI algorithm is formed on to aggregate the nodes by analyze the transaction graph. In this, on the hash basis of hash calculation, the most important nodes will be assigned priority [28].

B. Voting based Consensus Algorithms: In the comparison of the proof-based consensus algorithms, voting based consensus algorithms requires the identification of the nodes that will participate in the verification process before begins the work. Also, all network nodes will together verify the transaction. These voting based consensus algorithm classified into the following three categories:

a. PBFT (Practical Byzantine Fault Tolerance): This is a voting based Byzantine Fault Tolerance mechanism for consensus. This algorithm has high practicality in distributed systems and low algorithm complexity [12]. This algorithm works on the following five phases: request, pre-prepare, prepare, commit and reply. In figure, Working of PBFT is explained. In this the primary node sends the message coming from the client to the other three secondary nodes. In that case if the node number 3 is crashed, this message undergo above defined five phases to reach a consensus among these nodes. Lastly, the client receives the $n+1$ reply from these nodes about completion of a cycle of consensus, where n is the number of faulty nodes in the network. PBFT gives guarantees about common state stability of the nodes and take a reliable action in every round of consensus. This algorithm maintains the aim of strong consistency, that's why it is absolutely a fine mechanism for consensus [6].

Stellar is a new protocol which is an advancement of PBFT. This protocol implements Federated Byzantine Agreement protocol. In FBA, nodes for conduct the consensus process choose the federation.

Though, with this new method, nodes are able to find out if even one of the nodes gets compromised. All of the nodes through majority voting reach an agreement [17].

b. Paxos: This was introduced by Lamport in 2001 [16]. This algorithm solves the consistency problem in a good manner. The objective of this algorithm is to choose a single value in network fault. The concept of this algorithm is that all the nodes in the network are divided into following three types: the proposers, the acceptors and the learners. Everyone whose learns the consensus value in the network, is a learner [3] as shown in figure 6.

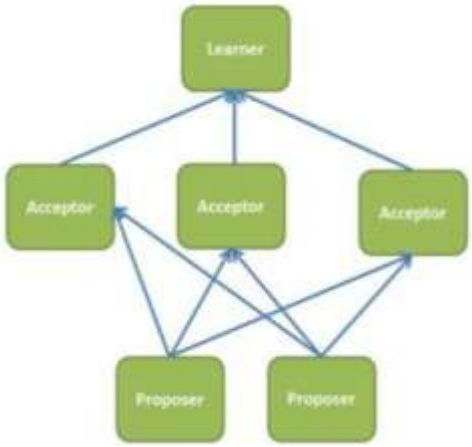

Figure 6. Nodes in Paxos.

The working of Paxos is discussed as under [4].

• In the beginning, the proposer formulates a proposal with a proposal number. This proposal number is known as prepare message and then it will send to the acceptors. The final biggest proposal number considered up to date. Prepare message (proposal number).

• Every acceptor compares the current received proposal number value with all proposer's proposal number and if currently received number have a higher number, then it accepts the proposal otherwise drops it. Furthermore, the acceptor prepares the response message in the following form Prepare response: (accept/reject, proposal number, accepted values) where, proposal number is the largest number the acceptor has received and accepted values are values those are already accepted from other proposer.

• Next a vote is being taken based on the majority decision. In this, the proposer checks rejection of the proposal by majority of the acceptors. If this is true, then the proposer updates this number with the up-to-date proposal number. If this is false, then the proposer further checks whether the majority of the acceptors have already accepted values. If this is true then the proposers value cannot be selected otherwise proposer sends the accepted message.

• As a final point, the proposer directs the accept message in the following format to all the acceptors. Accept message: (proposal number, value). In this, proposal number is same as prepare phase value and value is a single value proposed by proposer.

• Each and every time, for accepts value by the acceptor, acceptor updates the learner nodes about the value so that everyone will learn about the accepted value.

c. Raft: Raft algorithm was proposed by Diego Ongaro and John Ousterhout in 2013. This algorithm can be used as an alternative for Paxos. The main concept behind this algorithm is that the nodes jointly select a leader and the remaining nodes become the followers. The responsibility of the leader is that, leader sends the replicas of state transition log across the followers [4]. The entries of record can flow unidirectional i.e. from the leader to the followers. In this, each and every node at any particular time can be at any of the three states: leader, candidate and follower [12]. This algorithm rounds in cycles, known as term. In this, each term starts with an election process so that one or more candidates attempt to become a leader as shown in figure 7.

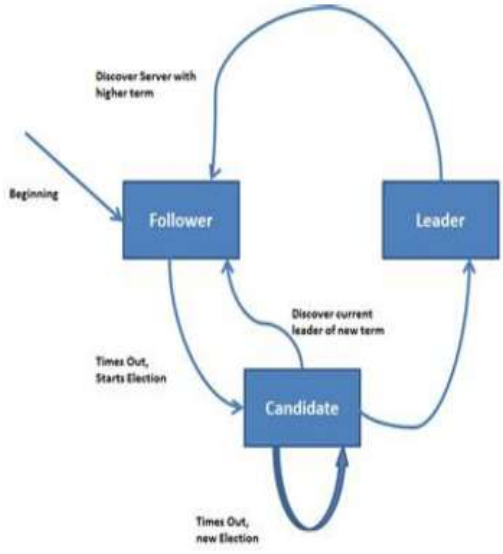

Figure 7. State changes in Raft algorithm.

If this algorithm is matched with Paxos and PBFT, this algorithm has high efficiency and clarity. Therefore Raft has been broadly adopted in distributed systems. Raft algorithm realizes the same safety performance as Paxos and is better suited in real life implementation and comprehension. As mentioned, Raft algorithm cannot support byzantine nodes and can stand up to failure of 50 % of nodes [4].

III. Analysis and Comparison

In this Section we present a comparative study of the different consensus algorithms that we have discussed up to now in this paper. A detailed comparison of above discussed consensus algorithms in terms of characteristics and performance are presents in the following Table 2.

Table 2. Consensus algorithms in terms of characteristics and performance.

	PoW	PoS	DPoS	LPoS	PoA	PoI	PBFT and its variants	Paxos	Raft
Type of Blockchain	Permissionless	Permissioned and Permissionless	Permissioned and Permissionless	Permissioned and Permissionless	Permissioned and Permissionless	Consortium	Permissioned	Permissioned	Permissioned
Electing miners based on	Solving Difficulty hash	Stake owned	Stake owned	Leasing Stake	Solving Difficulty hash	High priority	Mathematical operation	Proposal Number	Randomized timers
Model of Trust	Un-trusted	Un-trusted	NA	NA	NA	NA	Semi-trusted	Semi-trusted	Semi-trusted
Transaction finality	Probabilistic	Probabilistic	NA	NA	NA	NA	Immediate	Immediate	Immediate
Decentralization structure	Strong	Strong	Strong	Strong	Strong	Strong	Weak	Weak	Weak
Properties of Distributed Consensus	Probabilistic	Probabilistic	Probabilistic	Probabilistic	Probabilistic	Probabilistic	Deterministic	Deterministic	Deterministic
Reward	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
control of acceptance of the adversary	Less than 25% computing power	Less than 51% stack	Less than 51% Validators	NA	50% of online stake	Less than 50% importance	Less than 33.3% replicas	NA	50% of nodes
Fees of Transaction	Yes, for all miners	Yes, for all miners	Yes, for all witnesse	NA	Yes, for miner and lucky stakeholders	Yes, for transaction partners	No	NO	No
Speed of Verification (Per Sec)	Greater than 100 sec	Less than 100 sec	Less than 100 sec	NA	NA	NA	Less than 10 sec	NA	Less than 10 sec
Throughput (transaction /Sec)	Less than 100	Less than 1000	Less than 1000	Not Found	NA	NA	Less than 2000	NA	Greater than 10000
Speed of Block Creation	Low	High	High	Not Found	High	High	High	High	NA
Consumption of Energy	High	Something less than PoW	Low	Low	Low	Low	Moderate	High	High
Scalability	Strong	Strong	Strong	Strong	Strong	Strong	Weak	Weak	Moderate
51% Attack	Yes	No	No	No	No	No	No	No	No
Double Spending	Yes	No	No	No	No	No	No	No	No
Crash fault tolerance	50%	50%	50%	Not Found	50%	50%	33%	50%	50%
Byzentine Fault Tolerance	50%	50%	50%	Not Found	50%	50%	33%	Not Found	Not Found

*NA=Not Available

IV. Conclusion

The Blockchain technology has a great future in many areas, not only in the field of cryptocurrencies but also in various ICT from various dimensions like as security and privacy of data in the field of IoT. In blockchain consensus algorithms has used as a key technology. Consensus algorithms have promised the stable operation in this technology. In consensus algorithm nodes agree on a certain value or transaction through the consensus protocol. Though, the research in this area is still in progress. In this paper, we presented some popular blockchain consensus algorithms and also presented their characteristics through comprehensive comparison and analysis. After analysis we conclude that, the permissioned blockchain offers strong throughput but it scarifies with decentralization and permission. In case of permissionless systems, transaction finality remains non-deterministic. We consider that the good consensus algorithm should be fault tolerance.

References

[1] B. K. Mohanta, D. Jena, S. S. Panda and S. Sobhanayak, Blockchain technology: A survey on applications and security privacy challenges, 2019. https://doi.org/10.1016/j.iot.2019.100107.

[2] S. Moin, A. Karim, Z. Safdar, K. Safdar, E. Ahmed and M. Imran, Securing IoTs in distributed blockchain: analysis, requirements and open issues, 2019. https://doi.org/10.1016/j.future.2019.05.023.

[3] S. Zhanga and J.-H. Lee, Analysis of the main consensus protocols of blockchain, https://doi.org/10.1016/j.icte.2019.08.001, 2019.

[4] S. S. Panda, B. K. Mohanta, U. Satapathy, D. Jena, D. Gountia and T. K. Patra, Study of Blockchain Based Decentralized Consensus Algorithms, TENCON 2019 - pp. 908-913, 2019.

[5] W. Wang, A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks, IEEE Access 7 (2019), 22328-22370.

[6] S. J. Alsunaidi and F. A. Alhaidari, A Survey of Consensus Algorithms for Blockchain Technology, 2019, ICCIS, pp. 1-6, 2019.

[7] S. Zoican, M. Vochin, R. Zoican and D. Galatchi, Blockchain and Consensus Algorithms in Internet of Things, ISETC, pp. 1-4, 2018.

[8] NEM, Technical Reference, 2018. [Online]. Available: https://nem.io/wp content/themes/nem/files/NEM_techRef.pdf. [Accessed: 15-Nov-2018].

[9] M. A. Khan and K. Salah, IoT security: Review, blockchain solutions, and open challenges, Futur. Gener. Comput. Syst. 82 (2018), 395-411.

[10] Q. He, N. Guan, M. Lv and W. Yi, On the consensus mechanisms of blockchain/DLT for internet of things, 13th International Symposium on Industrial Embedded Systems (SIES), IEEE, (2018), 1-10.

[11] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli and M. H. Rehmani, Applications of Blockchains in the Internet of Things: A comprehensive survey, IEEE Communications Surveys & Tutorials, 2018.

[12] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei and C. Qijun, A review on consensus algorithm of blockchain, ICSMC), (2007), 2567-2572.

[13] D. Larimer, Delegated proof-of-stake (dpos), Bitshare whitepaper.

[14] I. Bentov, C. Lee, A. Mizrahi and M. Rosenfeld, Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake, ACM SIGMETRICS Performance Evaluation Review, 42(3) (2014).

[15] S. Nakamoto et al., Bitcoin: A peer-to-peer electronic cash system, 2008.

[16] L. Lamport et al., Paxos made simple, ACM Sigact News 32(4) (2001), 18-25. https://docs.wavesplatform.com/en/blockchain/leasing#leasing-benefits-for-the-token-holder.