2021 2nd International Conference on Computer Communication and Network Security (CCNS) | 978-1-6654-2711-1/21/$31.00 ©2021 IEEE | DOI: 10.1109/CCNS53852.2021.00020

Development in Consensus Protocols: From PoW to PoS to DPoS

Jingwen Pan[*, †]
University of Wisconsin–Madison
Henan, China
jpan82@wisc.edu

Zhaoyi Song[*, †]
Auburn University
Tianjin, China
zzs0034@auburn.edu

Wangze Hao[*, †]
Shandong Experimental high school
Shandong, China
245084268@qq.com

[†]These authors are contributed equally

***Abstract*—Consensus protocols are the essential algorithms to achieve overall network reliability in the distributed system. As the representative of the distributed system, the blockchain applies its specific consensus algorithm to ensure security and consistency in the system. The three main consensus algorithms in the blockchain system now are Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of Stake (DPoS). The development process of consensus algorithms illustrates the trend of consensus protocols in the blockchain. This paper analyzes the development of three representative consensus protocols: PoW, PoS, and DPoS. Then we compare the advantages and disadvantages of them and discusses the future direction of consensus protocols.**

Keywords- Consensus Protocols, Blockchain, Proof-of-Work, Proof-of-Stake, Delegated-Proof-of-Stake

I. Introduction

The traditional information system is centralized, and its network is controlled by authoritative centralized nodes. In contrast, the distributed system can execute tasks on the different nodes in the network and achieve point-to-point information transmission. To reach the consensus in different nodes, the distributed system adopts the consensus protocol, which is a procedure that can ensure every node in the distributed system achieve an agreement. Through applying appropriate consensus protocols in different scenarios, achieving the reliability of the whole network is possible. As one of the most important applications of distributed systems, the blockchain was introduced by Satoshi Nakamoto in the white paper of Bitcoin, and it has received extensive attention in recent years [1]. The blockchain is a system that applies distributed public ledger to ensures that the transactions cannot be maliciously tampered with [2]. As a distributed network, the blockchain system contains both the nodes which work as servers and the malicious nodes which are the block to the consensus. As a result, the blockchain system needs consensus protocols to prevent the consensus from being attack by malicious nodes [3].

The consensus protocols are crucial to the blockchain, and they have been experienced intense development. In the past years, various consensus protocols have emerged, such as Proof-of-Work (PoW), Proof-of-Stake (PoS), Delegated-Proof-of-Stake (DPoS), Proof-of-Existence (PoE), etc. Different kinds of consensus protocols have their own characteristics, strengths, and weaknesses. The researches of the development process and defects of available consensus protocols can be helpful to design more efficient, secure, and reliable consensus algorithms in the future.

This paper analyzes the development of three representative consensus protocols: PoW, PoS, and DPoS in section 2. Then we compare the advantages and disadvantages of PoW, PoS, and DPoS in section 3. After that, section 4 discusses the development trends of consensus protocols in the future. Finally, the conclusion is given in section 5.

II. Development of Three Main Consensus Algorithms

A. *Byzantine Generals Problem (BGP) and Byzantine Fault-tolerance (BFT)*

The distributed system has a peer-to-peer network, and there is no central authority. So, the distributed system needs to reach a consensus between different nodes and prevent the attack from the malicious nodes. In 1982, Lamport et al. summarized this problem as the Byzantine Generals Problem (BGP) [4]. In the Byzantine Generals Problem, a Byzantine command general leads the army to surround an emery city. The army is divided into several parts which which a lieutenant individually leads. The general will send the order attack or retreat to lieutenants, and they can only communicate by messages. However, the general or lieutenants can be disloyal, and the traitors will send a misleading message to others to destroy achieving a consensus. All loyal generals should execute the same plan of action to reach a consensus, and the traitors fail to mislead the loyal generals to the wrong plan.

The disloyal general or lieutenant in BGP represent the malicious node in the distributed network. Lamport et al. early proposed several solutions to this problem [4]. If the disloyal generals are less than one-third of the loyal generals, the loyal generals can reach a consensus called Byzantine Fault Tolerance (BFT). And another solution is to apply the unforgeable message signatures to handle the situation that the traitors are more than one-third of the loyal generals. In 1999, Castro and Liskov proposed Practical Byzantine Fault Tolerance (PBFT), a BFT algorithm with higher response speed, practicability, and consistency than the previous BFT protocols [5]. After PBFT, some other BFT protocols were introduced, such as Q/U [6] and RBFT [7]. The BFT protocols allow nodes in the distributed network to reach a consensus with the presence of unreliable nodes.

B. *PoW (Proof of Work)*

PoW is the consensus protocol based on computational power. The competition of computational power is to compute a hash function to find a nonce that meets the requirement. After

978-1-6654-2711-1/21/$31.00 ©2021 IEEE
DOI 10.1109/CCNS53852.2021.00020

the verification, the miner who first obtains the correct answer will have the right to create a new block and earn the reward. The flow of PoW in the blockchain system is presented in Fig. 1. PoW is used in Bitcoin [1] and Ethereum 1.0 [8]. PoW can help reach the consensus of creating a new block and avoid the public ledger have tampered with.

The difficulty in PoW decides how many times computation of the hash puzzle the node needs to generate a new legal block [1]. The difficulty of the hash puzzle of creating a new block is controlled depending on the average number of blocks per hour. If the new block is generated too low, the difficulty will decrease. If the new block is generated too fast, the difficulty will increase. The control of difficulty can ensure the speed of generating a new block keeps in ten minutes.

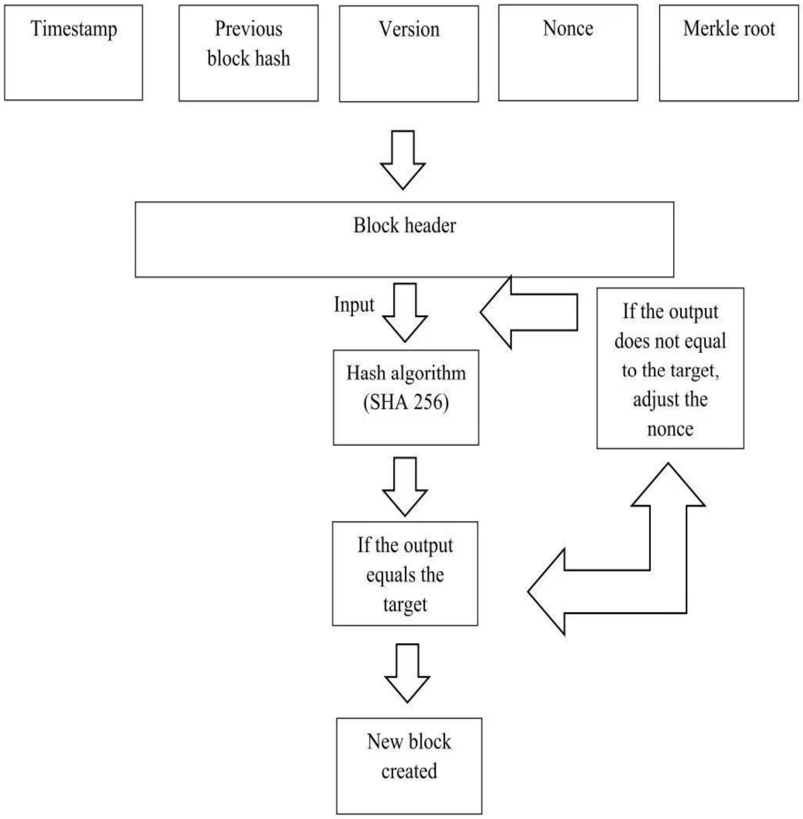

Figure 1. Flow of PoW

C. *PoS(Proof of Stake)*

- principle

In order to solve the problem that Pow consumes too much energy, the concept of PoS is proposed. In PoS, the amount of stake represents the probability of being selected as a validator. If the validators successfully verify valid transactions, they will receive transaction fees as a reward, and if they pass a fraudulent transaction, their stake will be deducted as a penalty. Therefore, the stake of validators must exceed all transaction fees to encourage them to maintain the blockchain. Then, the validators vote for the blocks they consider legal, and the voting power is proportional to the amount of stake. By analogy, new validators and new blocks are continuously produced. The flow of PoS is presented in Fig.2.

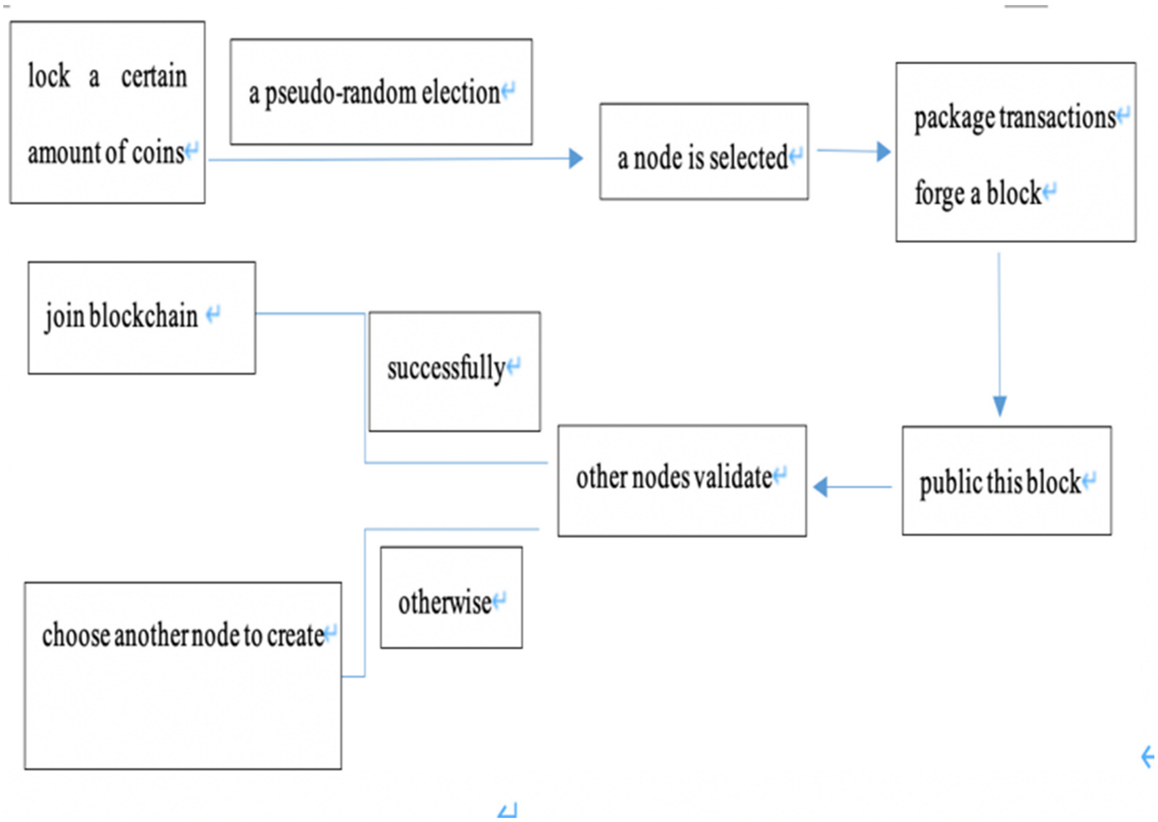

Figure 2. Flow of PoS

- Three scenarios in PoS

Peercoin PoS.: The first PoS based currency was PeerCoin [9] Peercoin proposes the concept of "Coinage". Coinage is equal to the number of tokens multiplied by the time of the pledge of the token. The basic principle of Peercoin is to consume Coinage to gain the right to create new blocks. Its mining formula is H (H (Bprev), A, t) ≤balance (A) m×Age. H (Bprev) represents the hash operation of the last block, t is the timestamp, balance (A) is the tokens that are pledged, m is the pre-defined value, and Age is the pledge time. Adding timestamp prevents nodes from counting future hash values. The difficulty of mining is inversely proportional to Coinage. The bigger the Coinage, the easier it is to mine.

Pure PoS: The pure PoS form could be seen in Nextcoin[10]. In this platform, the more stakes a node has, the greater the probability that it will be selected as a validator. In pure PoS, nodes do not need to perform hash calculations. They are selected as validators through a verifiable random number generation function. After a node is selected as a validator, the node verifies the transaction information and packages them into the block. Then, broadcast it, and other nodes verify the block. Upon successful verification, the node will have a rewarding fee. But this consensus is vulnerable to nothing at stake attack.

New PoS: Ethereum is designed a full PoS protocol which has a mechanism called Casper [11]. The Casper Consensus was originally a combination of PoW and PoS. For example, first, produce blocks in PoS, and use BFT (Byzantine fault-tolerant) algorithms to check blocks after a certain number of blocks. Or first, produce blocks in PoW, and then use PoS to confirm consensus. Later Casper transformed into a pure PoS consensus. But what makes it different from NextCoin is that Casper uses a Slasher mechanism. It solves nothing at stake attack. During the voting process, once a node is found to have a malicious forking behavior, the token of that node will be confiscated

D. Delegated Proof of Stake

- principle

A round in a DPoS blockchain with N block producers/witnesses follows a round robin order as follows: N block producers get elected from the pool of witnesses' candidates. The kth block producer signs the kth block until k=N. A block is finalized when it is voted on by (2/3+1) of block producers. In case of two chains, the longest chain rule is followed. Block added cannot be reversed. The flow of DPoS is presented in Fig. 3.

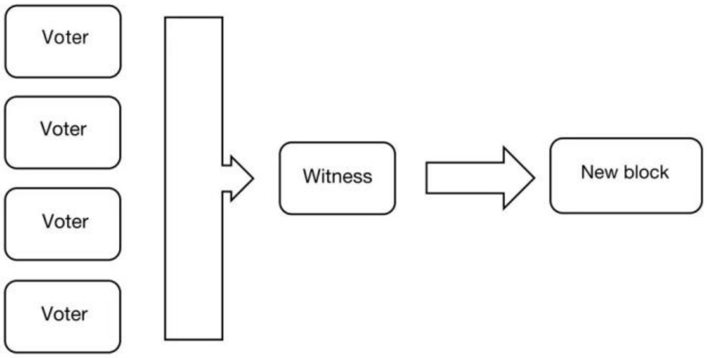

Figure 3. Flow of DPoS

- Elements

Witnesses: Witnesses are people who verify transactions to create blocks, who are the main part of DPoS. If a witness verifies all transactions in a block, a reward would be given to them, usually shared with the ones who had voted for this witness. Instead, suppose a witness fails to verify all transactions in the given time. In this case, the block is missed, the transactions are left unverified till the next witness verify it, and the witness will get all the rewards added together. This process is called stolen. The number of witnesses in the top tier is usually in the range of 21-101. Witnesses can prevent specific transactions from being included in the block, but they cannot change information about any transaction.

Voting is a continuous process that results in each witness in the top tier always being replaced by another who gets more votes, which means more trusted. As the number of applicants for witness grows, competition grows, and reputation becomes much more critical for each witness to remain competitive. Since the witnesses hold more power, they also take more risks and they are threatening to its loss of income, locking of stake, and reputation score. A certain part of the witnesses' stake will be locked if they act maliciously or try to attack blockchain.

Delegates: Users in DPoS systems also vote for a group of delegates who supervise blockchain governance. They do not play a role in transaction control, but they can change the size of a block or the amount of reward a witness should be paid in return for validating a block through voting.

Block validators: Block validators are people who verify whether the blocks created by witnesses follow the consensus rules. Any user is able to run a block validator and verify the network without incentive.

III. Comparison

This section analyzes the three main consensus protocols PoW, PoS, and DPoS in terms of energy consumption, security, operating speed, decentralization, scalability, and reward mechanism. The comparison results are summarized in Table I.

- Energy consumption

As the classic consensus protocol in the blockchain system, PoW reaches the consensus in the blockchain through the competition of computational power. The process of PoW needs specialized machines that consume large amounts of power. The later consensus protocols PoS and DPoS solve the energy problem in PoW. In PoS, proportional to the amount of stake is the voting power. In DPoS, electors will choose their delegates to vote for generating and verifying the new blocks. Both PoS and DPoS do not need the calculating machine and avoid excessive waste of energy. PoS and DPoS improve the disadvantage of high energy use in PoW.

- Security

The consensus protocols should ensure the nodes in the blockchain network can reach a consensus and guarantee the blockchain system's security. The existing consensus protocols are facing certain security problems. In PoW, the transaction records of block i are a part of the header of block i+1. Every transaction is recorded in the ledger. So, it is hard to spend the money more than once, which prevents double-spending. PoW applies computational power as the voting rights, and it is vulnerable to the 51% attack, which can happen when the attackers equal or more than 50% of the computational power. In PoS, the cost of 51% attack is huge. Since PoS is based on the amount of stake, if attackers plan to use the 51% attack, they need to buy a large number of tokens until they control 51% of the cryptocurrency. With the purchase of a substantial quantity of cryptocurrency in the market, the price of the coins will be raised, and meanwhile, the cost of 51% attack is also largely increased. So, launching the 51% attack in PoS is riskier than in PoW. But PoS face the danger of long-range attack. In the long-range attack, adversaries try to make their chain be longer than the main chain to change the transaction records on the ledger for their purposes. The attackers can forge the timestamps or hack the private key from others to make the length of their chain exceeds the length of the main chain [9]. In DPoS, since the blockchain is protected by voting the witness, it can effectively defend against double-spending attacks. However, the voting system negatively influences the decentralization of DPoS. The voting power of small stakeholders is not equal to the big stakeholders. The big stakeholders can hold more than 51% percent of the voting power. So DPoS is vulnerable to the 51% attack and long-range attack [10].

- Operating speed

An effective consensus protocol should be practical for application. Except for the energy consumption and security, the operating speed of the consensus algorithm should also be considered. Since PoW is based on the computational power to solve a difficult hush puzzle, the speed of generating a new block and processing a transaction is slow. Compared to PoW, the processing speed of PoS and DPoS is much faster. In PoS, since the miners do not need to spend time and energy on computation, generating a new block is fast. In DPoS, the shareholders will vote the witness for validating transactions and delegates for proposing advice to develop the network community. This system increases the efficiency of the whole network. DPoS is more efficient than PoW and PoSEnergy consumption

As the classic consensus protocol in the blockchain system, PoW reaches the consensus in the blockchain through the competition of computational power. The process of PoW needs specialized machines that consume large amounts of power. The later consensus protocols PoS and DPoS solve the energy problem in PoW. In PoS, proportional to the amount of stake is the voting power. In DPoS, electors will choose their delegates to vote for generating and verifying the new blocks. Both PoS and DPoS do not need the calculating machine and avoid excessive waste of energy. PoS and DPoS improve the disadvantage of high energy use in PoW.

TABLE I. COMPARISON OF POW, POS, AND DPOS

Property	**Energy consumption**	**Security**	**Operating speed**	**Decentralization**	**Scalability**	**Reward mechanism**
PoW	High	Vulnerable to 51% attack	Slow	Face the problem of mining centralization	Not fast confirmation speed	The miner who successfully mined a new block can earn the reward of a coin
PoS	Low	Vulnerable to long range attack	Fast	Face the problem of the monopoly of property	Fast confirmation speed	The participate in validating the next block can receive a reward if the block is successfully created
DPoS	Low	Vulnerable to the 51% attack and long range attack	Fast	**The voters who have much more property may influence the voting**	Fast confirmation speed	The delegates will receive the reward when every new block generated

- Decentralization

One of the most remarkable characters of the distributed system is decentralization. In PoW, anyone can freely access or leave the node, which helps keep the decentralization of the network. However, in PoW, some miners increase their competitive power by gathering their computational power in a pool, which brings the problem of mining centralization. Although PoS avoid the centralization of computing power, it has the monopoly problem of property. Some nodes are holding a large number of stakes, and as long as their coins exceed 51%, the centralization degree of the system is negatively influenced. DPoS have a better decentralization degree than PoW since small shareholders can also vote for witnesses as the other big shareholders. And the witness will be reelected for each new block. The transactions in DPoS are not entirely dependent on computing power or property hold. But the voters who have much more property than others can also influence the voting.

- Scalability

PoW has thousands of nodes, which ensures its good scalability [11]. In the early period, its scalability can guarantee the confirmation speed of transactions in Bitcoin to be fast enough. But with the increase of transactions, PoW shows its shortcoming in scalability. The initial block size is 1Mb, which is small to contains thousands of transactions. And it causes the long confirmation time of the transaction in Bitcoin. PoS mitigates this problem and its confirmation time of transaction is much shorter than PoW. In DPoS, the confirmation speed of transactions is also faster than PoW.

- Reward mechanism

The reward mechanism is also an essential part of the consensus protocols. It directly influences the practicality of the consensus protocols. In PoW, the miner who is successfully mining a new block can earn the reward of the coin. But the reward will change with the number of new blocks. For example, in Bitcoin, the amount of the reward halves every 210,000 blocks [1]. In PoS, the participate in validating the next block can receive a reward if the block is successfully created. It is similar to the reward in PoW, but there is no need for complicated computation in PoS. And in DPoS, the delegates will receive the reward when every new block is successfully generated and shared with owners based on the amount of currency they hold. If the block fails to be created, the reward will be transferred to the next block.

IV. DISCUSSION

With the development of consensus protocols, the new protocols can mitigate or solve the problems from former protocols. For example, PoS and DPoS solve the energy use problem of PoW. However, the advanced consensus protocols still face their own challenge. For instance, PoS can effectively prevent the 51% attack, but it is vulnerable to the long range attack. Good consensus protocols should consider several aspects: energy consumption, security, operating speed, decentralization, scalability, and reward mechanism. The future development process of consensus protocols should pay attention to them.

The consensus algorithms in the future will have several characters. Firstly, future consensus protocols will be energy-saving. From PoS and DPoS, the consensus protocols abandon the proof way, which will consume much energy, and turn to a more environmental-friendly approach.

Secondly, from PoW to PoS to DPoS, the security of consensus protocols keeps increasing. But they still have specific security problems. For instance, PoS mitigate the 51% attack, which is harmful to PoW, but PoS is also vulnerable to the long range attack. Future consensus algorithms need to avoid 51% attack, long range attack, and other existing attacks.

Thirdly, future consensus protocols should think about the problem of centralization. In both PoW and PoS, although they have tried different voting approaches centralization still exists. Even though in DPoS, the people who control huge property may also influence the voting. It is important to ensure the decentralization in the blockchain system to make the network be truly distributed.

Fourthly, good scalability is essential to the practicality and sustainability of consensus protocols. The blockchain system is popular nowadays, and its transactions also increase accordingly. The future consensus algorithm should keep developing its scalability to increase efficiency and reliability.

Fifthly, the reward mechanism should be designed to help increase the security, decentralization, and scalability of the blockchain system. The reward mechanism of the future consensus algorithm should attract users, ensure decentralization, and keep the system's fairness.

V. CONCLUSION

The blockchain system received wide attention in the recent years. Since the blockchain system is a distributed network, it needs consensus protocols to ensure that the whole system can achieve a consensus between different nodes. But some unreliable nodes destroy the processing of reaching consensus and the security of the network. The consensus protocols should guarantee the blockchain's security and consider other characters such as energy use, decentralization, scalability, reward mechanism, etc. PoW, PoS, and DPoS are three representative protocols. Their development process provides valuable experience and reflection to the later consensus protocols. The development of consensus algorithms in the distributed system should learn from the formal cases and combine their advantages.

REFERENCES

[1] Nakamoto, S.: 'Bitcoin: A Peer-to-Peer Electronic Cash System', 2008

[2] Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W., and Qijun, C.: 'A review on consensus algorithm of blockchain', in Editor (Ed.)^ (Eds.): 'Book A review on consensus algorithm of blockchain' (2017, edn.), pp. 2567-2572

[3] Shijie Zhang, J.-H.L.: 'Analysis of the main consensus protocols of blockchain', 2019

[4] Lamport, L., Shostak, R., and Pease, M.: 'The Byzantine Generals Problem', 1982, 4, (3 %J ACM Trans. Program. Lang. Syst.), pp. 382–401

[5] M. Castro, B.L.: 'Practical Byzantine Fault Tolerance', OSDI, 1999, 99

[6] Abd-El-Malek, M., Ganger, G.R., Goodson, G.R., Reiter, M.K., and Wylie, J.J.: 'Fault-scalable Byzantine fault-tolerant services'. Proc. Proceedings of the twentieth ACM symposium on Operating systems principles, Brighton, United Kingdom2005 pp. Pages

[7] Cowling, J., Myers, D., Liskov, B., Rodrigues, R., and Shrira, L.: 'HQ replication: a hybrid quorum protocol for byzantine fault tolerance'. Proc. Proceedings of the 7th symposium on Operating systems design and implementation, Seattle, Washington2006 pp. Pages

[8] Wood, D.: 'ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER', in Editor (Ed.)^(Eds.): 'Book ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER' (2014, edn.), pp.

[9] Sunny King and Scott Nadal. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. peercoin.net, 2013.

[10] Nxt wiki, "Whitepaper: Nxt," 2016 [Online]. https://nxtwiki.org/wiki/Whitepaper:Nxt.

[11] V. Buterin. Ethereum 2.0 spec – Casper and sharding, 2018.

[12] Delegated Proof Of Stake (DPoS) – GeeksforGeeks
https://www.geeksforgeeks.org/delegated-proof-of-stake/