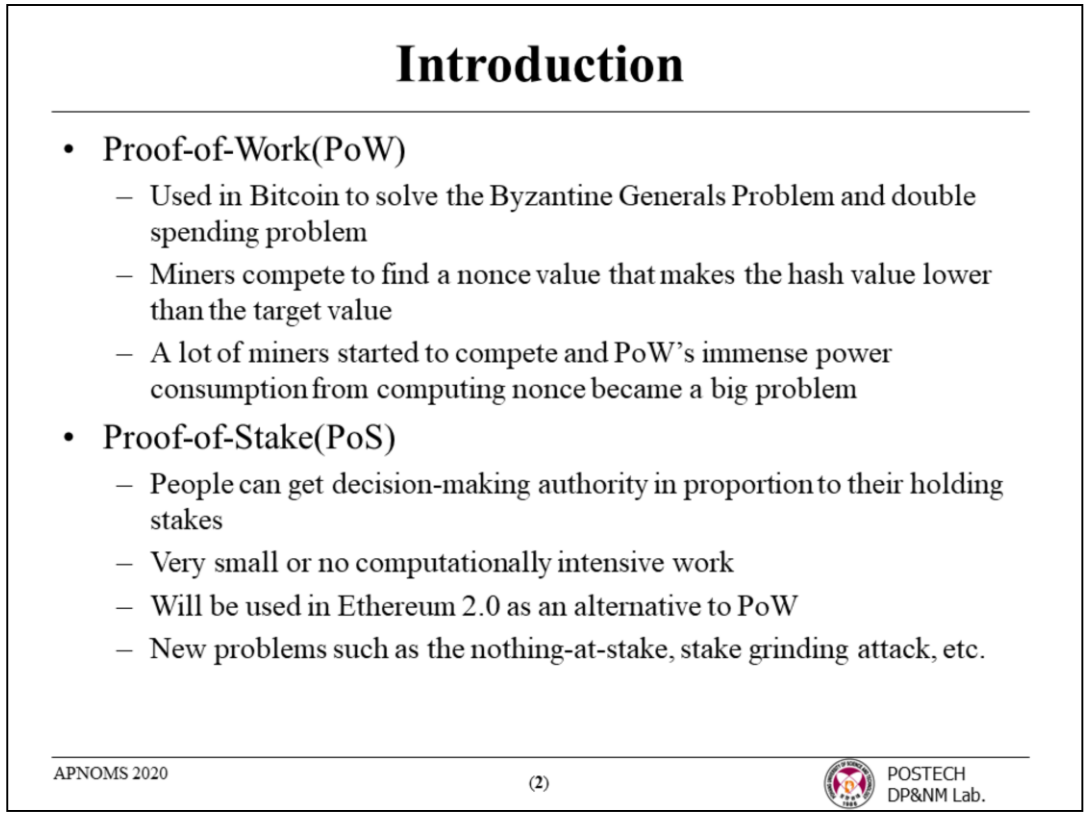
# A Survey of Proof-of-Stake Consensus Algorithms

Wonseok Choi and James Won-Ki Hong
DP&NM Lab.
Dept. of Computer Science and Engineering
POSTECH, Pohang Korea
Email: {ws4583, jwkhong}@postech.ac.kr
http://dpnm.postech.ac.kr/



Abstract

Since Bitcoin was launched, the blockchain technology and the cryptocurrencies have been in the spotlight. However, people also were interested in mining and earn money. The mining pools became larger and larger and since the Proof-of-Work (PoW) consensus protocol requires lots of computation for mining, immense power consumption became a big problem. Many alternative consensus protocols have been proposed to overcome the PoW's power consumption problem, and Proof-of-Stake (PoS) is one of them. Ethereum, the second most popular blockchain, next to Bitcoin, recently announced a transition from PoW to PoS. In this paper, we present a survey of PoS consensus algorithms. We have analyzed the major PoS consensus algorithms and classified them into three groups. We also examine its potential problems, especially about nothing-at-stake, long-range attack, and stake grinding attack. The algorithms are compared concerning their method and possible attacks. We hope that this paper will contribute in designing a better PoS consensus algorithm in the future.

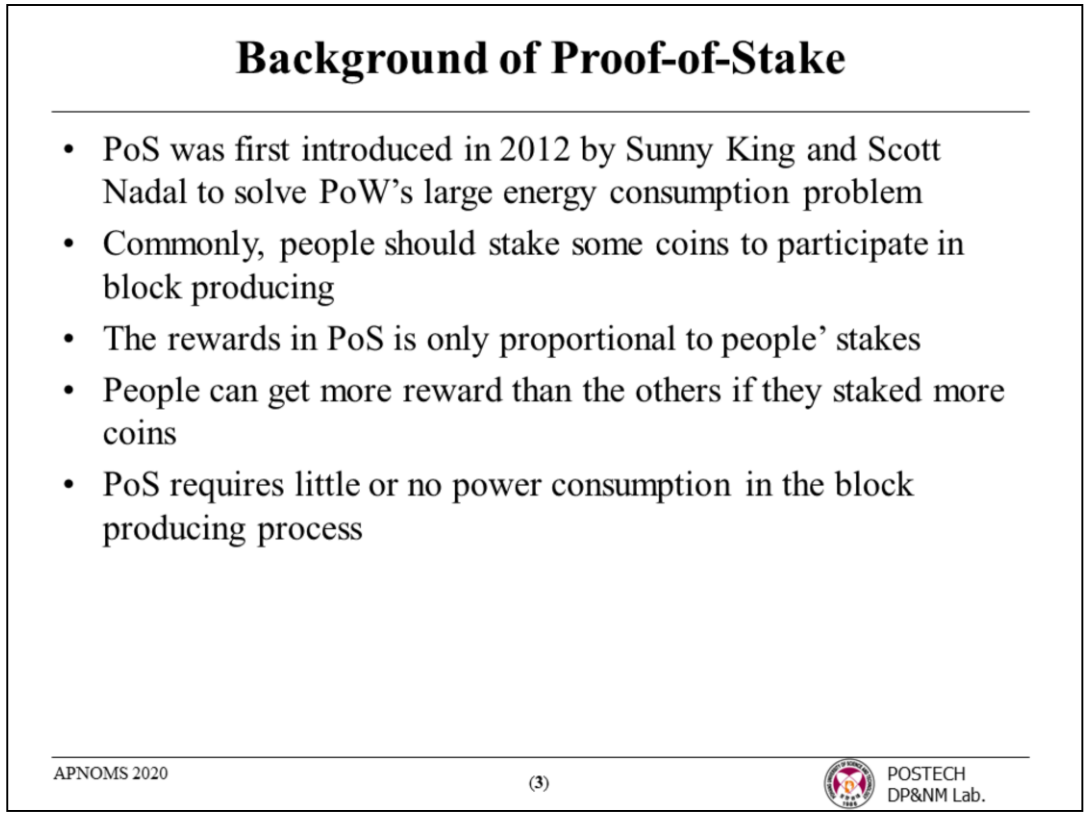



# 1. Introduction

Bitcoin [1] was invented in 2008 and its operation started in Jan, 2009 by Satoshi Nakamoto. In Bitcoin, to solve the Byzantine Generals Problem [2] and double spending[3] problem, Proof-of-Work (PoW) is used as its consensus algorithm. With PoW consensus algorithm, miners competeto find a nonce value that makes the hash value lower than the target value. A miner who finds the nonce satisfying thiscondition at first can produce a block and get a block reward. Since PoW could prevent 51% attack [4] effectively, it initially received positive reviews. However, over time, a lot of miners started to compete and PoW's immense power consumption from computing nonce became a big problem. Also, huge mining pools [5] began to emerge, and it caused centralization of the blockchain network as opposed to the initial goal.

Due to these problems, as an alternative, other proof-based consensus algorithms like Proof-of-Stake (PoS) [6], Proof-of-Storage [7], Proof-of-Reputation (PoR) [8], and other Byzantine Fault Tolerance [9] based consensus algorithms were introduced. Recently, one of the most popular blockchains, Ethereum [10] introduced its upgraded version, Ethereum 2.0[11]. One of the key changes is a transition from PoW to PoS to reduce electricity consumption and achieve decentralization. Normally, consensus algorithms that people can get decision-making authority in proportion to their holding stakes are called PoS. It was coming up as an alternative to PoW because very small or no computationally intensive work is required in PoS. However, new problems such as the nothing-at-stake[12] and the stake grinding attack [13] emerged, and still lots more research is underway to solve these problems.

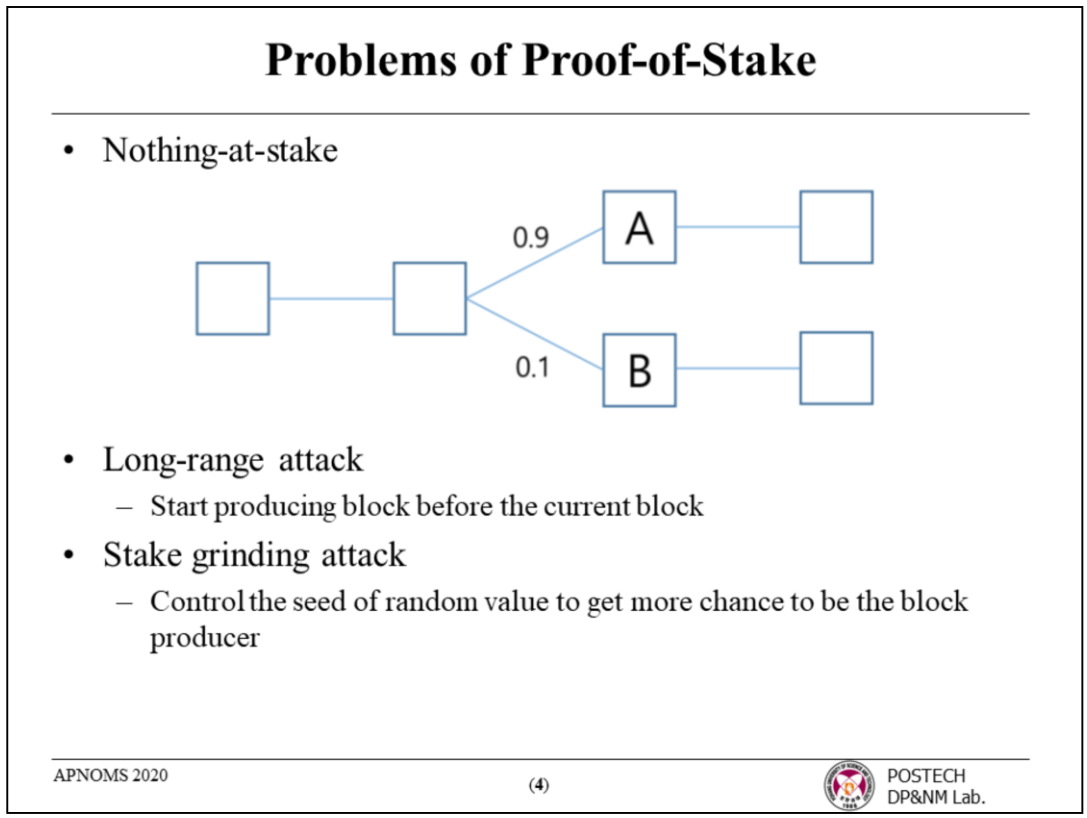
In this paper, we introduce PoS with its problems and explain some existing PoS consensus algorithms to suggest a better idea of PoS. In Section II we introduce the background of PoS and its main problems, nothing-at-stake, long-range attack [12] and stake grinding attack. In Section III, we analyze and compare some existing blockchains using PoS consensus algorithms, such as Peercoin, Nxt [14], Cardano, and Ethereum2.0. We conclude this paper in Section IV.




# 2. Proof-of-Stake

## 2.1 Background

PoS was first introduced in 2012 by Sunny King and Scott Nadal to solve PoW's large energy consumption problem [6]. Commonly, in PoS consensus algorithms, people should stake some coins to participate in block producing. There can be many differences following the detailed design of PoS, but people can get more rewards than the others if they staked more coins. In the block producing process, PoS requires little or no power consumption. In PoW, people can get more reward if they join a big mining pool, or have expensive equipment for mining. However, the rewards in PoS is only proportional to their stakes.

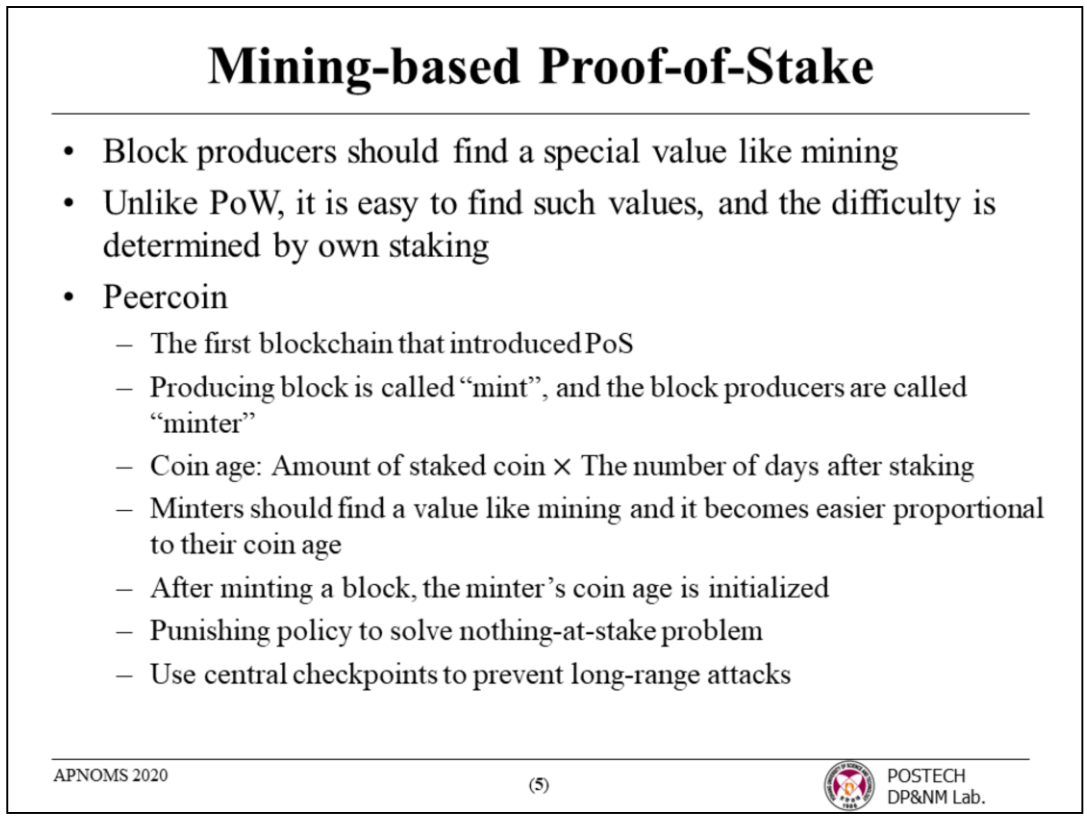



## 2.2 Problems

After PoS was suggested, new problems and security attacks have also emerged. One of the main problems is nothing-at-stake problem [12]. In Fig. 1, block A likely to be in the main chain with probability 90%, and block B likely to be in the main chain with probability 10% due to its speed or correctness or reliability, or any other reasons. In PoW, since it needs much time and many computations to mine a new block, and miners can't get any reward for mining a new block in the wrong chain, most of the miners will start mining after block A. This supports the longest chain rule because these miners' behaviors make the correct chain as the main chain. However, in PoS, people don't have any disadvantage to mine a new block in or vote for both chains. Therefore, this dishonest strategy is the best strategy for people to get the maximum reward and it makes it hard to find the correct chain. There can be two possible ways to solve this nothing-at-stake problem. One is to minimize the reward so that people can't have any incentives to do multiple mining or voting. The other one is just punishing them when they perform any malicious behaviors.

A long-range attack is also possible due to similar reason[12]. In a long-range attack, attackers start producing block before the current block. It can be even from the genesis block. In PoW, this attack doesn't make sense because the attackers are impossible to catch up with the current block. However, in PoS, producing a block doesn't take a long time and many computations, so they may catch up on the current block and start the double spending attack, or change the main chain. Long-range attacks can be prevented by using some checkpoints that make impossible to make other fork chains.

Grinding attack, also called stake grinding attack is to control the seed of random value to get more chance to be the block producer [13]. In PoS, the probability to be the block producer is proportional to stakes. This probability should rely on random values in the end, and it is very hard to create a real random value. Some PoS consensus algorithms use block headers, block creation time, and many other values as a seed of random value, and it means attackers may try to set or modify these values to get a random value that they want. Since this calculation is not that easy, it may not be practical in some cases. However, the possibility of this attack is not negligible. The grinding attacks can be prevented by introducing safe random value generation algorithms.



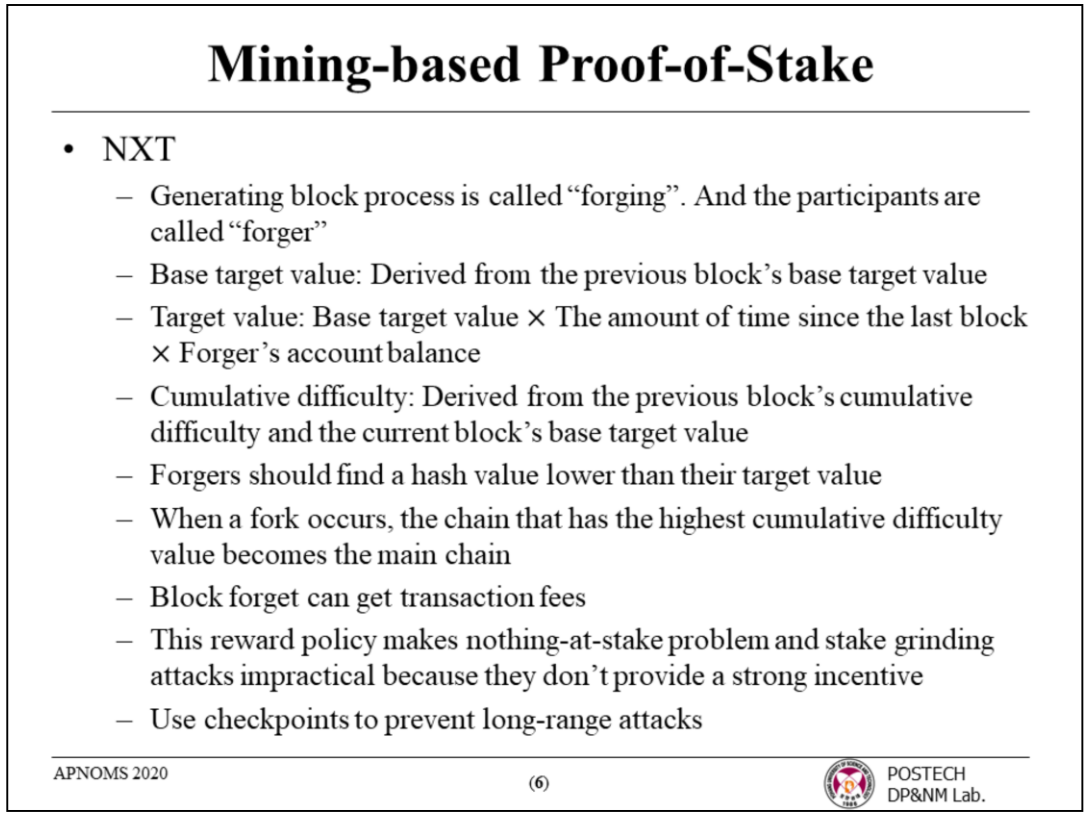

## 3. Proof-of-Stake Consensus Algorithms

### 3.1 Mining-based Proof-of-Stake

Mining-based PoS consensus algorithms are similar to PoW. In mining-based PoS, block producers should find a special value like mining. However, unlike PoW, it is easy to find such values, and the difficulty is determined by own staking.

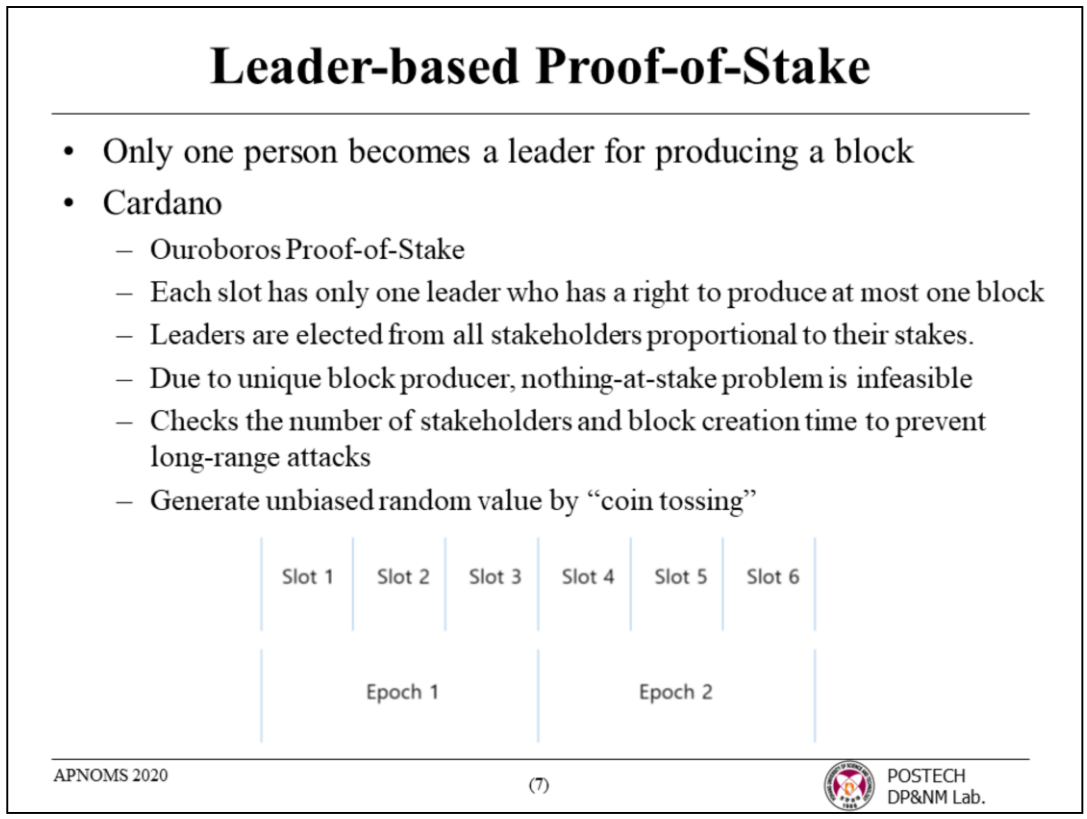
Peercoin [6] is called the first blockchain that introduced PoS. In Peercoin, producing block is called "mint", and the block producers are called "minter". Peercoin uses its unique idea, coin age, which is used to determine the minter. It can be derived from multiplying the amount of staked coins by the number of days holding those coins. People can participate in the block producing after 30 days of staking Peercoin. To mint a new block, minters should find a special hash value, and it becomes easier proportional to their coin age. In this approach, malicious attackers can increase their coin age by staking their coins for a long time. To prevent this problem, after ninety days, the number of days holding coins reaches its maximum. After mining a new block, the minter's coin age is initialized and the minter can get some reward proportional to the staked coins. When a fork occurs, the chain that has the most coin age becomes the main chain.

In Peercoin, punishing policy is used to solve nothing-at-stake problem. It used some central checkpoints to prevent long-range attacks and some other similar attacks, and it was criticized a lot due to its centralization. Peercoin developers say that the checkpoint system will be removed after the re-basing Peercoin. Stake grinding attacks can be possible in Peercoin by trying many parameters like block headers.




Similar to Peercoin, Nxt [14] also uses a mining-based PoS consensus algorithm. The difference is, Nxt only uses account balances. In Nxt, generating block process is called "forging". To participate in forging, forgers should have at least 1000 NXT and wait for 1440 blocks. After satisfying these requirements, the forger's account becomes active. Eachblock has its base target value, and it is derived from the previous block's base target value and the average block time for the last 3 blocks. Each forger has its target value. The target value is derived from the multiplication of the base target value, the amount of time since the last block, and the forger's account balance. Forgers should find a hash value lower than a target value to forge a block which means it becomes easier to forge a block if a forger has more coins. Each block also has a cumulative difficulty value that is derived from the previous block's cumulative difficulty value and the current block's base target value. The cumulative difficulty is used for the fork choice rule. When a fork occurs, the chain that has higher cumulative difficulty values becomes the main chain.

There is a total of one billion Nxt coins and they were allocated to initial users. Therefore, there is no additional reward for block forging, but only the transaction fees of that block. This policy makes the nothing-at-stake problem impractical because it doesn't provide a strong incentive. Nxt also prevents the long-range attacks by using a checkpoint 720blocks behind the current block. Since randomness for forging a block is dependent on the previous block, stake grinding attacks can be possible, but it is also not that practical due to the reward policy.



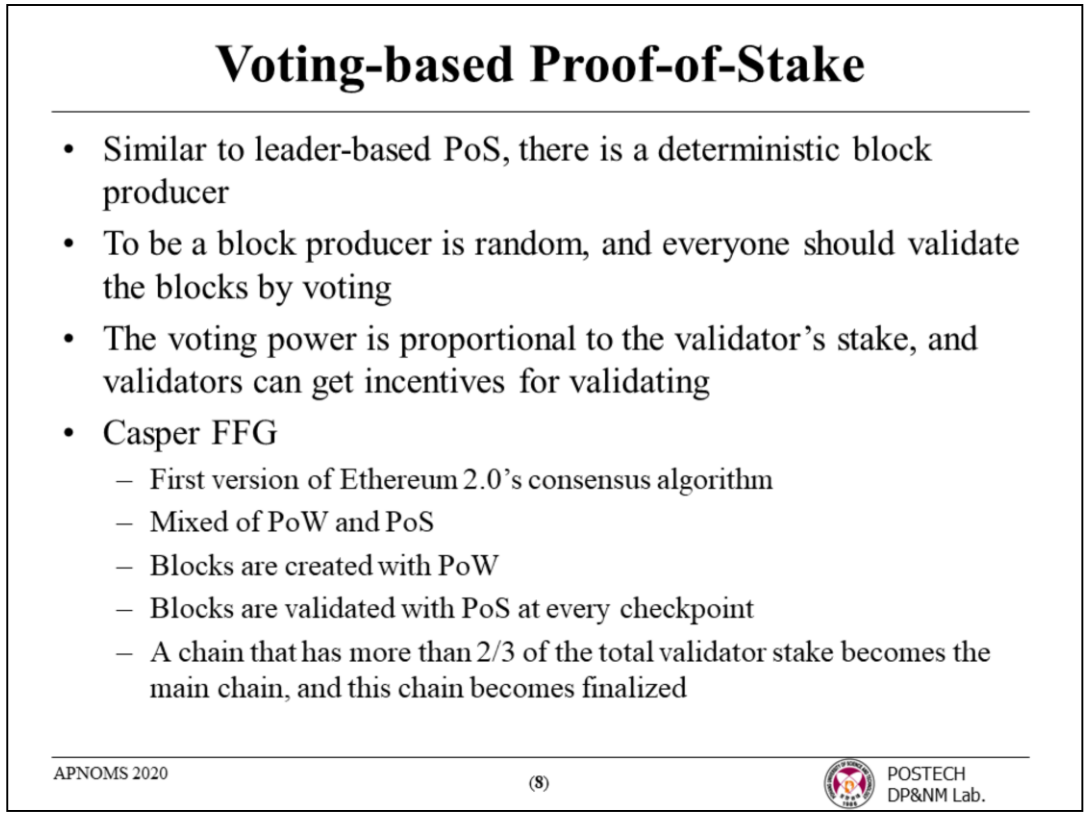

## 3.2 Leader-based Proof-of-Stake

In leader-based PoS consensus algorithms, only one person becomes a leader for producing a block by algorithms, unlike all people competes for producing a block and the first one's block is accepted. Ouroboros PoS [13] consensus algorithm uses this method.

Cardano, a blockchain and cryptocurrency project uses the Ouroboros PoS consensus algorithm. Real-time is divided into many epochs and there are many epochs in Ouroboros PoS. As in Fig.2, each epoch is also divided into some slots. Each slot has only one leader who has a right to produce at most one block. Leaders are elected from all stakeholders. This process is similar to a lottery, but the important thing is that the probability to be elected is proportional to the stakeholder's stake.

Ouroboros PoS uses a process called "coin tossing" for the leader election. In coin tossing, every elector generates specialrandom value and shares it by encrypted communication. Then, electors form a seed using from other random values. Since every elector can verify every other's random value, all electors get the same seed. Finally, electors select a slot leader using that seed. A seed indicates a coin in the blockchain, and the owner of the coin becomes a slot leader.

Since there is one unique slot leader agreed by every stakeholder, and they follow the longest chain rule, nothing-at-stake problem is infeasible in Ouroboros PoS. The long-range attacks are also prevented by Ouroboros PoS's protocol that checks the chains whether the majority of stakeholders are participating or not, and the blocks whether it is generated far ahead of time. Coin tossing protocol perfectly generates unbiased random value, so the stake grinding attacks are impossible, too.



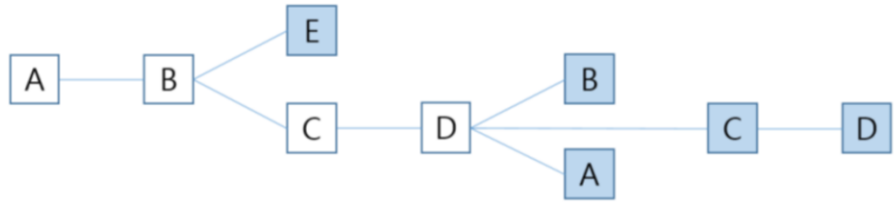

### 3.3 Voting-based Proof-of-Stake

Voting-based PoS is similar to leader-based PoS. There is also a deterministic block producer. The difference is, to be a block producer is completely random, and there is no advantage to produce a block. Instead, everyone should validate the blocks by voting, and the voting power is proportional to the validator's stake. Validators can get incentives for validating. This method is introduced in Ethereum 2.0.

There were many discussions to apply PoS in Ethereum2.0. Since the original Ethereum is using PoW, developers tried a mixed consensus algorithm of PoW and PoS at first.It was Casper FFG(friendly finality gadget) [15] by Vitalik Buterin. Casper FFG is similar to ordinary PoW, but it also has a PoS based validation and voting at every checkpoint. There are checkpoints at every specific number of blocks. Validators validate and vote a chain at every checkpoint, and they can't vote on multiple chains. A chain that has more than 2/3 of the total validator stake becomes the main chain. After this process, the blocks of the chain can't be reverted which is called finalized.

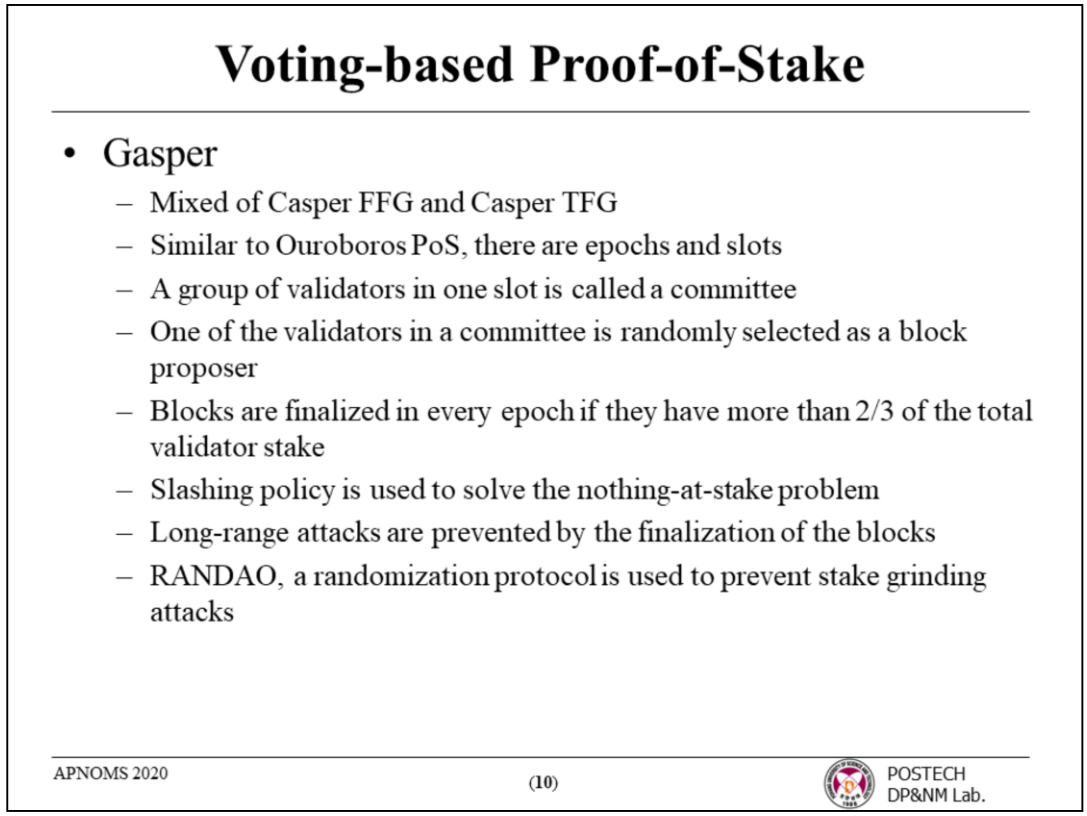
## Voting-based Proof-of-Stake

- Casper TFG(the friendly gadget)
  - LMD GHOST(latest message driven greedy heaviest observed subtree)
  - Similar to longest chain rule, but when there are many forks, a minority of malicious validators can't beat the majority in LMD GHOST rule






Casper CBC(correct by construction) [16] project is started to build a PoS consensus algorithm in Ethereum 2.0 at first, but the project is expanded to a study of overall consensus algorithms. Casper CBC was subdivided into many projects and the main project about PoS is done in Casper TFG(the friendly gadget) [17]. Casper TFG deals with a fork choice rule called LMD GHOST(latest message driven greedy heaviest observed subtree). LMD GHOST protocol decides the main chain based on validators' latest message that is weighted with their stakes. In Fig. 3, A, B, C, D, E are validators who making blocks. The latest messages are in blue. By LMD GHOST, A-B-C-D-C-D becomes the main chain. It seems like there is not that big difference longest chain rule, but when a fork occurs a lot, and a minority of validators are malicious, their attacks can succeed in the longest chain rule unlike they can't beat the majority in LMD GHOST.




Recently, a new version of Ethereum 2.0's PoS was suggested which is mixed with Casper FFG and Casper TFG[18]. It is used in Ethereum 2.0 testnet, now. In Gasper's PoS, there are epochs and slots similar to Ouroboros PoS's. In every epoch, every validator is randomly assigned to each slot. A group of validators in one slot is called a committee. One of the validators in a committee is randomly selected as a block proposer. There can be one or zero blocks in each slot. Other validators in a committee validate and vote to a block following the Hybrid LMD GHOST rule which is a slightly different version of LMD GHOST, and blocks are finalized in every epoch if they have more than 2/3 of the total validator stake.

In Ethereum 2.0, slashing policy is used to solve the nothing-at-stake problem. When a validator violates the rule, that is votes to more than one chain, or illegal chain, the validator is punished. The long-range attacks are prevented by the finalization of blocks. To prevent the stake grinding attacks, Ethereum 2.0 uses own randomization protocol called RANDAO [19]. In RANDAO, every participant submits a random value, and a unique random value is generated by submitted random values. In this case, a participant who submits last can see other's values and can control the random value. Therefore, a delay function that makes it impossible to check other's random value will be applied in Ethereum 2.0 later.

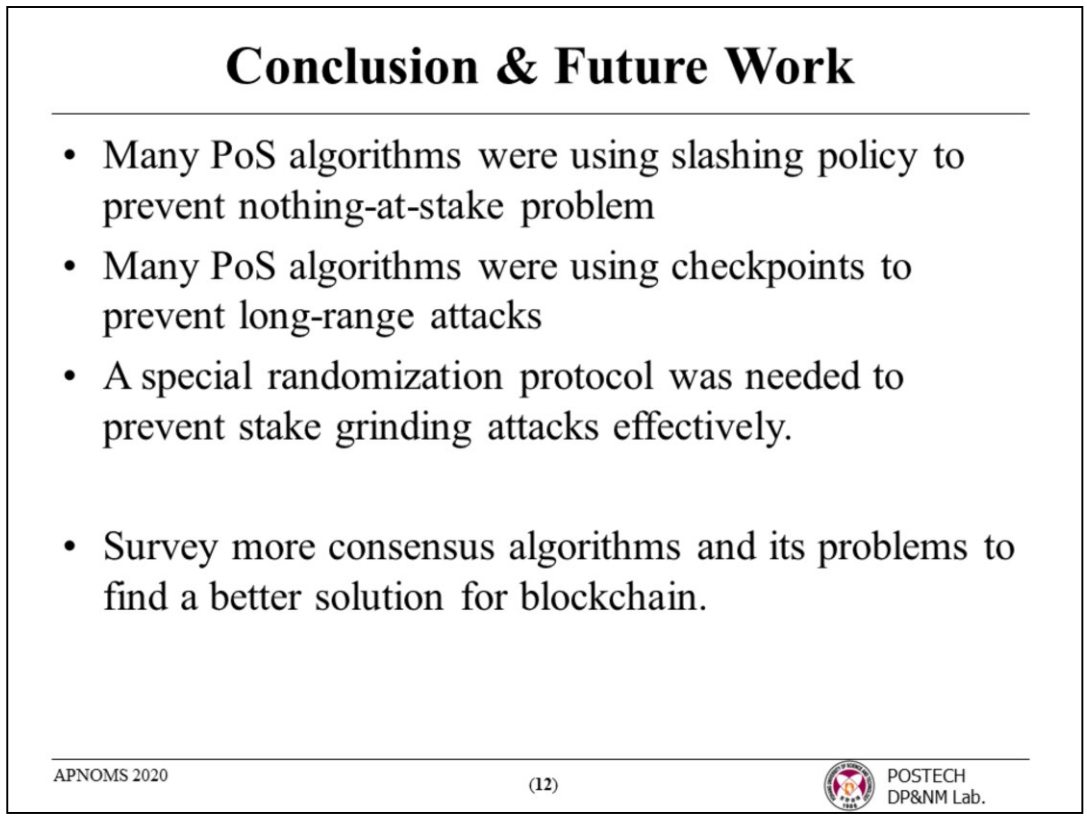
## Overall Comparison

| | Peercoin | Nxt | Cardano | Ethereum 2.0 |
|---|---|---|---|---|
| Type | Mining | Mining | Leader | Voting |
| Block Producer | Coin age | Balance | Balance | Random |
| Fork Choice Rule | Largest coin age | Largest cumulative difficulty | Longest chain | HLMD GHOST |
| Nothing-at-Stake | Punishment | Small reward | Deterministic leader | Punishment |
| Long-range Attack | Checkpoint | Checkpoint | Validation Protocol | Checkpoint |
| Stake Grinding Attack | | Small reward | Coin tossing | RANDAO |

APNOMS 2020 (11) POSTECH DP&NM Lab.

### 3.4 Overall Comparison

We introduced four PoS Consensus algorithms and grouped them with 3 types. A summary and comparison of them are in Table. Peercoin and Nxt are using mining-based PoS. Cardano is using leader-based PoS, and Ethereum 2.0 uses voting-based PoS. In Peercoin, block producers are selected based on coin age, while they are selected based on their balance in Nxt and Cardano. In Ethereum 2.0, they are randomly selected. Peercoin chooses a chain that has the largest coin age as a main chain. In Nxt, cumulative difficulty is used and Cardano uses longest chain rule. Ethereum 2.0 uses HLMD GHOST protocol. To solve nothing-at-stake problem, Peercoin and Ehtereum 2.0 uses slashing policy. In Nxt, nothing-at-stake problem is impractical due to low benefit, and in Cardano, it is impossible due to deterministic leader choice. To prevent long-range attacks, most blockchains use checkpoints and Cardano uses own validation protocol. To prevent stake grinding attacks, Nxt makes it impractical, and Cardano and Ethereum 2.0 use own randomization protocol.




## 4. Conclusion & Future Work

In this paper, we introduced PoS consensus algorithms, and its problems especially about nothing-at-stake, long-range attack, and stake grinding attack. We also introduced four existing PoS consensus algorithms and grouped them with mining-based PoS, leader-based PoS, and voting-based PoS. Then, we analyzed those algorithms concerning possible problems and attacks. Leader-based PoS, Ouroboros PoS consensus algorithm can prevent nothing-at-stake well due to its deterministic leader while other algorithms should consider the incentive or punishment. Most algorithms were using checkpoints to prevent long-range attacks. To prevent the stake grinding attacks effectively, a special randomization protocol was needed. Since we didn't introduce other vulnerabilities in PoS and other PoS consensus algorithms, there can be other pros and cons of each method. There also can be some tradeoffs between preventing a specific attack and another attack, so it is hard to say that an algorithm is superior to the others. However, people still study to make a more improved PoS consensus algorithm for safety and practicality. Our future work is to survey more consensus algorithms and its problems to find a better solution for blockchain.

# References


- [1] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system."
- URL: https://bitcoin.org/bitcoin.pdf (accessed: 25.05.2020) (2008).
- [2] Lamport, Leslie, Robert Shostak, and Marshall Pease. "The Byzantine Generals Problem." Concurrency: the Works of Leslie Lamport. 2019. 203-226.
- [3] Chohan, Usman W. "The double spending problem and cryptocurrencies." Available at SSRN 3090174 (2017).
- [4] Ye, Congcong, et al. "Analysis of security in blockchain: Case study in 51\%-attack detecting." 2018 5th International Conference on Dependable Systems and Their Applications (DSA). IEEE, 2018.
- [5] Eyal, Ittay, and Emin Gün Sirer. "Majority is not enough: Bitcoin mining is vulnerable." International conference on financial cryptography and data security. Springer, Berlin, Heidelberg, 2014.
- [6] King, Sunny, and Scott Nadal. "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake." [Online]. Available: https://decred.org/research/king2012.pdf (accessed:25.05.2020) (2012).
- [7] Ateniese, Giuseppe, Seny Kamara, and Jonathan Katz. "Proofs of storage from homomorphic identification protocols." International conference on the theory and application of cryptology and information security. Springer, Berlin, Heidelberg, 2009.
- [8] Gai, Fangyu, et al. "Proof of reputation: A reputation-based consensus protocol for peer-to-peer network." International Conference on Database Systems for Advanced Applications. Springer, Cham, 2018.
- [9] Castro, Miguel, and Barbara Liskov. "Practical Byzantine fault tolerance." OSDI. Vol. 99. No. 1999. 1999.
- [10] Wood, Gavin. "Ethereum: A secure decentralised generalised transaction ledger." Ethereum project yellow paper 151.2014 (2014): 1-32.
- [11] Buterin, Vitalik. "Ethereum 2.0 mauve paper." Ethereum Developer Conference. Vol. 2. [Online]. Available: https://cdn.hackaday.io/files/10879465447136/Mauve\%20Paper\%20Vitalik.pdf (accessed:25.05.2020) (2016).
- [12] Buterin, Vitalik. "On stake," [Online]. Available: https://blog.ethereum.org/2014/07/05/stake/(accessed:25.05.2020)(2014).
- [13] Kiayias, Aggelos, et al. "Ouroboros: A provably secure proof-of-stake blockchain protocol." Annual International Cryptology Conference. Springer, Cham, 2017.
- [14] Popov, Serguei. "A probabilistic analysis of the nxt forging algorithm." Ledger 1 (2016): 69-83.
- [15] Buterin, Vitalik, and Virgil Griffith. "Casper the friendly finality gadget." arXiv preprint arXiv:1710.09437 (2017).
- [16] Zamfir, V., et al. "Introducing the minimal CBC Casper family of consensus protocols." DRAFT v1. [Online]. Available: https://github.com/cbc-casper/cbc-casper-paper/blob/master/cbc-casper-paper-draft.pdf (accessed:25.05.2020) (2018).
- [17] Zamfir, Vlad. "Casper the friendly ghost: A correct by construction blockchain consensus protocol." Whitepaper [Online]. Available: https://github.com/ethereum/research/blob/master/papers/CasperTFG /CasperTFG.pdf (accessed:25.05.2020) (2015).
- [18] Buterin, Vitalik, et al. "Combining GHOST and Casper." arXiv preprint arXiv:2003.03052 (2020).
- [19] RANDAO: A DAO working as RNG of Ethereum. [Online]. Available: https://github.com/randao/randao (accessed:25.05.2020) (2019)





# References

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

URL: https://bitcoin.org/bitcoin.pdf (accessed: 25.05.2020) (2008).

[2] Lamport, Leslie, Robert Shostak, and Marshall Pease. "The Byzantine Generals Problem." Concurrency: the Works of Leslie Lamport. 2019. 203-226.

[3] Chohan, Usman W. "The double spending problem and cryptocurrencies." Available at SSRN 3090174 (2017).

[4] Ye, Congcong, et al. "Analysis of security in blockchain: Case study in 51\%-attack detecting." 2018 5th International Conference on Dependable Systems and Their Applications (DSA). IEEE, 2018.

[5] Eyal, Ittay, and Emin Gün Sirer. "Majority is not enough: Bitcoin mining is vulnerable." International conference on financial cryptography and data security. Springer, Berlin, Heidelberg, 2014.

[6] King, Sunny, and Scott Nadal. "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake." [Online]. Available: https://decred.org/research/king2012.pdf (accessed:25.05.2020) (2012).

[7] Ateniese, Giuseppe, Seny Kamara, and Jonathan Katz. "Proofs of storage from homomorphic identification protocols." International conference on the theory and application of cryptology and information security. Springer, Berlin, Heidelberg, 2009.

[8] Gai, Fangyu, et al. "Proof of reputation: A reputation-based consensus protocol for peer-to-peer network." International Conference on Database Systems for Advanced Applications. Springer, Cham, 2018.

[9] Castro, Miguel, and Barbara Liskov. "Practical Byzantine fault tolerance." OSDI. Vol. 99. No. 1999. 1999.

[10] Wood, Gavin. "Ethereum: A secure decentralised generalised transaction ledger." Ethereum project yellow paper 151.2014 (2014): 1-32.

[11] Buterin, Vitalik. "Ethereum 2.0 mauve paper." Ethereum Developer Conference. Vol. 2. [Online]. Available: https://cdn.hackaday.io/files/10879465447136/Mauve\%20Paper\%20Vitalik.pdf (accessed:25.05.2020) (2016).

[12] Buterin, Vitalik. "On stake," [Online]. Available: https://blog.ethereum.org/2014/07/05/stake/(accessed:25.05.2020)(2014).

[13] Kiayias, Aggelos, et al. "Ouroboros: A provably secure proof-of-stake blockchain protocol." Annual International Cryptology Conference. Springer, Cham, 2017.

[14] Popov, Serguei. "A probabilistic analysis of the nxt forging algorithm." Ledger 1 (2016): 69-83.

[15] Buterin, Vitalik, and Virgil Griffith. "Casper the friendly finality gadget." arXiv preprint arXiv:1710.09437 (2017).

[16] Zamfir, V., et al. "Introducing the minimal CBC Casper family of consensus protocols." DRAFT v1. [Online]. Available: https://github.com/cbc-casper/cbc-casper-paper/blob/master/cbc-casper-paper-draft.pdf (accessed:25.05.2020) (2018).

[17] Zamfir, Vlad. "Casper the friendly ghost: A correct by construction blockchain consensus protocol." Whitepaper [Online]. Available: https://github.com/ethereum/research/blob/master/papers/CasperTFG /CasperTFG.pdf (accessed:25.05.2020) (2015).

[18] Buterin, Vitalik, et al. "Combining GHOST and Casper." arXiv preprint arXiv:2003.03052 (2020).

[19] RANDAO: A DAO working as RNG of Ethereum. [Online]. Available: https://github.com/randao/randao (accessed:25.05.2020) (2019)