上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

A Survey of PoS-like Consenses

Log Creative

April 10th, 2024

1 PPC

1.1 Description

Peercoin (PPC) [1] is the first to introduce the Proof-of-Stake (PoS) mechanism into the blockchain system in 2012. "Stake" here means the "coin age", i.e., currency amount × holding period.

In coin-stake transactions, each stakeholder is required to send coins to himself, which is used to generate a PPC block and obtain partial revenue. The cost of gaining revenue is the consumption of coin age. The PPC block requires participants to look for random numbers (nonce) to make the hash value of the block header meet the target difficulty. The target difficulty is inversely proportional to the coin age consumed in coin-stake:

$$H(H(B_{\text{prev}}, A, t)) \leq balance(A)m \tag{1}$$

The more coin age accumulated by participants, the lower the bookkeeping difficulty, and the greater the probability of generating blocks.

1.2 Advantages

It alleviates the energy and cost waste problem of PoW mining. Compared with Bitcoins based on PoW (Proof-of-Work), the opportunity in PPC only depends on the user's deposit in the system and the time of saving the currency.

There is less motivation for the adversary to attack. The cost of getting a large sum of coins in the PoS system is higher than that of mastering most of the computing power in the PoW system, since time is counted. Besides, once the block is generated, the coin age will be immediately cleared (by the action of sending coins to himself), which also guarantees that an attacker cannot continue the attack.

1.3 Disadvantages

Less active chain. PoS encourages the behavior of hoarding. And since the coin age will also accumulate when the node is offline, the node may prefer not to go online.

Nothing-at-stake attack. It is "nearly" costless to execute PoS protocol. With the aim of getting a reward, nodes start supporting several branches of the chain. They can simply put their money in all chains without any fear of repercussion at all. No matter what happens, they will always win and have nothing to lose.

2 DPoS

2.1 Description

DPoS (Delegated Proof of Stake) [2] introduces two roles called witness and delegate, both of which have multiple members. DPoS mechanism is similar to the decision of the board of directors in the real world. Stakeholders with more than 51% stakes can vote for the N witnesses and delegates. As shown in Figure 1, the delegates are responsible for voting and the witnesses just need to be their follower nodes. The system calculates a certain number of delegates with the most votes based on the stakes of stakeholders, and the delegate takes turns to generate the block in a prescribed order.

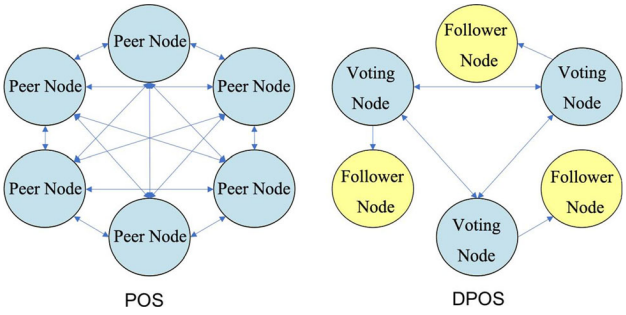

Figure 1 Node differences between PoS and DPoS

2.2 Advantages

Speed up the transaction. The node does not have to wait for confirmation of a considerable number of untrusted nodes after the transaction is initiated, but only the delegate needs to verify the transaction.

Make the chain active. Since the block is signed by the delegates in turn, if a delegate is offline and misses signing the block, he will face the risk of being replaced by other candidate delegates. Therefore, the delegate must guarantee sufficient online time for the profit.

2.3 Disadvantages

Centralization. With only a few delegates holding a considerable amount of power, this further makes DPoS vulnerable to vote buying.

Nothing-at-stack attack exists. This verification is still not computationally intensive and the parties can easily misbehave by voting for all blocks. This could be improved by another version of the DPoS protocol, where the node has to pay a price to become a delegate, such as paying a deposit to a security account [3].

3 FFG

3.1 Description

The first version of Casper, the Friendly-Finality-Gadget (FFG) [4] takes on the form of a hybrid PoW/PoS system based on BFT consensus theory. Casper FFG overlays an existing roof PoW blockchain, providing additional protections against block reversions.

In the simple version of Casper, there is a fixed set of validators and a proposal mechanism, which produces child blocks of existing blocks, forming an ever-growing block tree. In the case of network latency or deliberate attacks, the proposal mechanism will inevitably occasionally produce multiple children of the same parent. Casper's job is to choose a single child from each parent. Casper only considers the subtree of checkpoints forming the checkpoint tree, as shown in Figure 2, where the dotted lines represent 99 blocks. A supermajority link colored in pink is an ordered pair of checkpoints such that at least $\frac{2}{3}$ of validators (by deposit) have published votes.

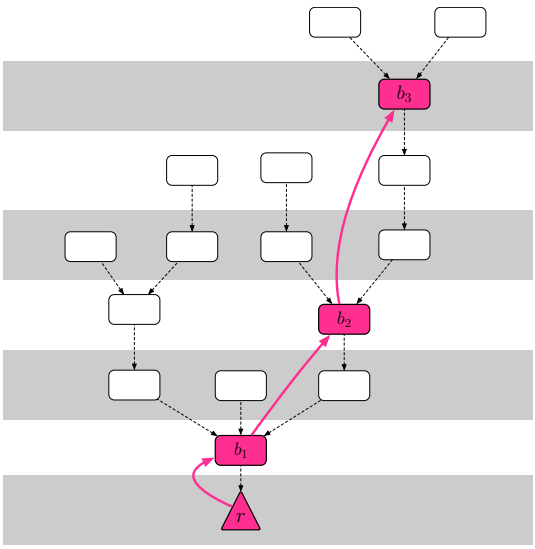

Figure 2 Block tree with height and supermajority links in FFG

The most notable property of Casper is that it is impossible for any two conflicting checkpoints to be finalized unless $\frac{1}{3}$ of the validators violate one of the two Casper Commandments/slashing conditions shown in Figure 3. If a validator violates the conditions, their entire deposit is forfeited, with a minor "finder's fee" provided to the individual who submitted the evidence transaction.

FFG is more complicated than standard PoW designs. The fork choice rule is: Follow the chain containing the justified checkpoint of the greatest height. FFG also enables dynamic validator sets to prevent the attack

An individual validator v must NOT publish two distinct votes	
$\langle v; s_1; t_1; \mathrm{h}(s_1); \mathrm{h}(t_1)\rangle$	$\langle v; s_2; t_2; \mathrm{h}(s_2); \mathrm{h}(t_2)\rangle$
such that either: I. $\mathrm{h}(t_1) = \mathrm{h}(t_2)$. Equivalently, a validator must not publish two distinct votes for the same target height. or II. $\mathrm{h}(s_1) < \mathrm{h}(s_2) < \mathrm{h}(t_2) < \mathrm{h}(t_1)$. Equivalently, a validator must not vote within the span of its other votes.	

Figure 3 The two Casper Commandments.

of two conflicting checkpoints to both be finalized without any validator getting slashed.

FFG introduces several new features that BFT algorithms do not necessarily support: accountability, dynamic validators, defenses, and modular overlay.

3.2 Advantages

Plausible liveness. This means that, no matter what has occurred in the past, if at least two-thirds of validators follow the protocol, it's always possible to finalize a new checkpoint without any validator violating a slashing condition.

Robust to attacks. For "nothing-at-stake" attacks, FFG introduces the betting mechanism. For long-range attacks, the node must regularly update the latest blocks and forbid revert blocks that have been finalized. For catastrophic crashes, Casper FFG introduces the "Inactivity Leak."

3.3 Disadvantages

51% attack. A wholly compromised block proposal mechanism will prevent Casper from finalizing new blocks. The problem that Casper does not wholly solve, particularly related to 51% attacks, can still be corrected using user-activated soft forks.

Parallel voting. This contract version of Casper FFG was later deprecated. [5] In the contract version, it is assumed that the votes can be processed in parallel, but there are many intermediate states in calculating the voting reward. The order of voting processing will affect the final state, which means that the parallelization will make the consensus unreachable. This is fixed by Ethereum 2.0, which integrates Casper FFG with other optimization proposals (such as sharding) [6].

References

[1] K. Sunny and N. Scott, "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake," Tech. Rep., 2012. [Online]. Available: https://bitcoin.peryaudo.org/vendor/peercoin-paper.pdf.

[2] L. Daniel, "Delegated Proof of Stake (DPoS)," BitShares Blockchain Foundation, Tech. Rep., 2014. [Online]. Available: https://how.bitshares.works/en/master/technology/dpos.html.

[3] S. Fabian and L. Daniel, "Bitshares 2.0: Financialsmart contract platform," Cryptonomex, Tech. Rep., 2015. [Online]. Available: https://www.weusecoins.com/assets/pdf/library/Bitshares%20Financial%20Platform.pdf.

[4] V. Buterin and V. Griffith, "Casper the friendly finality gadget," Oct. 2017. DOI: 10.48550/ARXIV.1710.09437. arXiv: 1710.09437 [cs.CR].

[5] D. Ryan, *Why not EIP-1011 (Hybrid Casper FFG)?* 2018. [Online]. Available: https://notes.ethereum.org/@djrtwo/rJDrKoBOQ?type=view.

[6] vbuterin, *Serenity design rationale*, 2022. [Online]. Available: https://notes.ethereum.org/@vbuterin/serenity_design_rationale?type=view.