# Migration from POW to POS for Ethereum

Prashant B., Makrant I., Mansi M.

2019

Abstract

Block-chain is rapidly evolving. There are continuous enhancements. In order to validate transactions algorithm is used. The traditional approach of Proof of Work (POW) is where miners are incentivized to compete with each other to complete transactions. Alternate system is proof of stake (POS) where in the validators lock up some of their tokens and thus replace the role of miners. Generation three block chain, which are the latest and fastest ones are mostly Proof of Stake (POS). Hence the POW systems seek to leverage the POS properties in order to attain higher speed and scalability. The paper discusses the approach with Ethereum has taken to migrate from the current POW protocol to POS protocol. The concept of Caster is focused as implementation. Casper further has two subtypes of approaches know as Friendly Finality Gadget (FFG) and Correct by Construction (CBC). The paper discusses on safety guard over these algorithms.

Keywords: Block-chain, Ethereum, Casper, Proof-of-work, Proof-Of-Stake, node, Decentralized Application.

## 1 Introduction

Block-chains are making their presence felt across the world. Their adoption is widely increasing due to the technology involved. The two widely and well-established block-chain types are Proof of Work and the other is Proof of Stake. Proof of Work is the primitive block-chain type wherein the miners have the system is setup such that each node needs to be up and running hence high-performance pressure on the node. Part of mining process, POW consumes lots of energy. For example expensive and heavy hardware is needed. Resultantly lots of electricity is consumed leading to higher costs. Mining difficulty increases with time, leading to higher cost and slower

transaction speed and transaction fees. Most of above issues are resolved by POS systems.

This paper presents an approach for POW to POS conversion and adding a safety guard to it during its conversion for effective and smooth transition. We highlight Ethereum, a prominent block chain that is focused on not just transfer of assets but also for programming money. Ethereum block chain is established in hierarchically structure wherein transactions are matched. There are nodes which uses antennas in them and transfer the data. They also help in enhancing the communication depending on their sizes. Ethereum is presently setup for Proof of Work. There are deliberations ongoing to take the Proof of Stake route.

## 2 Phases of POW to POS Migration

Casper is simply the name of Ethereum's approach to solve the proof of work and proof of stake problem. At the moment Ethereum relies on the proof of work concept for consensus. But in the past, they made it really clear that at some point in the future they have to migrate to proof of stake protocol.

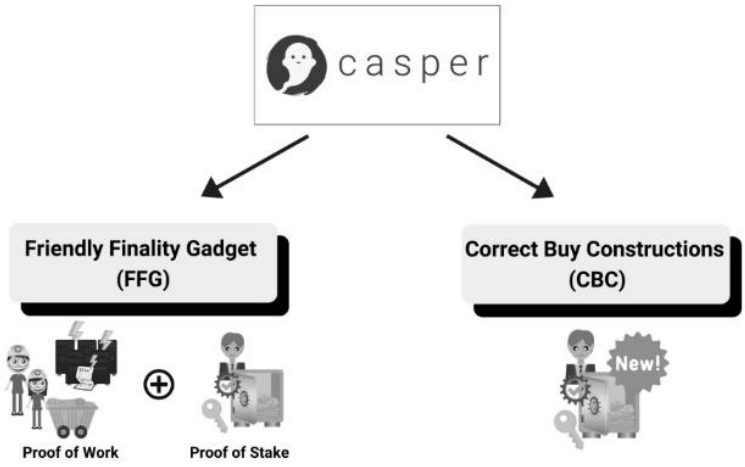


*Fig 1 Casper sub types*

Consider the above figure, there are two types of Casper implementation. The first one is Friendly Finality Gadget (FFG) the other one is Correct Buy Constructions (CBC).

## 2.1 Friendly Finality Gadget (FFG)

The first phase of Casper is Friendly Finality Gadget, that is, FFG. This approach is provided by Vitalik B.

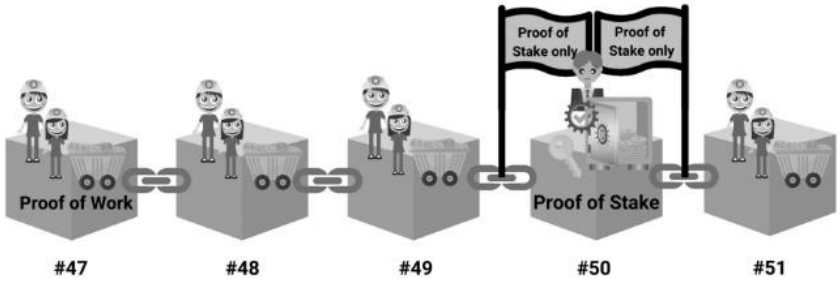


*Fig 2 Casper Friendly Finality Gadget ie FFG*

Casper Friendly Finality Gadget, that is, FFG is the approach Ethereum is taking forward as a mechanism to transition from POW to POS. Since this is a combination of two protocols (POS, POW), this is also known as a hybrid answer. Here the Proof of Work occurs from the first to the forty nine block. However each of the subsequent fiftieth block, POS occurs. POS takes place via voting. Once the set of fifty transactions complete, these are captured to the ledger and marked as permanent. In this way there is both POS and POW protocol. However it is not possible to ride on two horses all the time. With the eventual goal being the transition away from POW, POS would be the focus.

## 2.2 Casper CBC

Correct by Construction approach is provided by Vlad. Zamfir. For majority purposes, a sixty six percent agreement helps to provide consensus. This helps to protect against the remaining 33% attack. Above approach helps to

provide little incentive for collusion as network attack can lead to the attackers losing deposit.

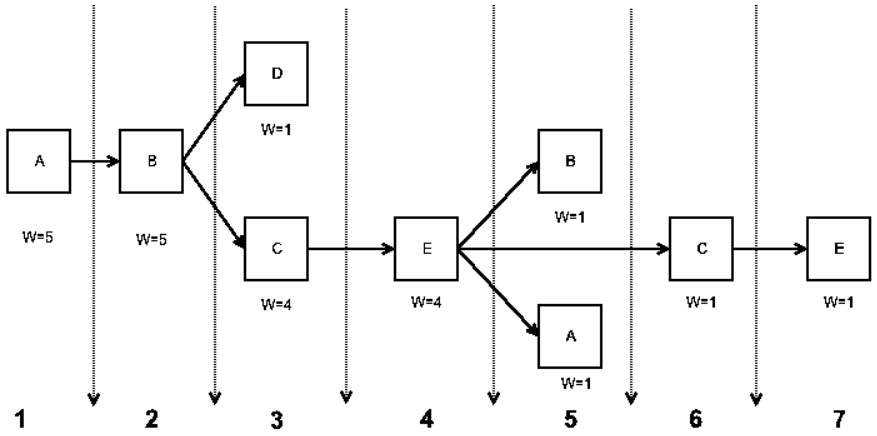


*Fig 3 Casper Correct by Construction (CBC)*

Consider above figure. There exists five nodes A, B , C, D and E. Starting block 1 is validated by node A. Let's give this a weightage of points 5. Next block is validated by block B, having 5 points. Now we observe a fork at node B resulting into blocks validated by blocks C,D. Thus we come across two paths A-B-D and A-B-C-E. At point D, the weightage is one point as there is no other block validator. At point C and point E the weightage is four points. The path size is A-B-C-E giving size four. Since the weightage at point C is greater than node D, we path A-B-C-E is selected over A-B-D.

The risk of minority chain taking over does not exist. Consider a scenario where node D generates faster blocks. However since it is on minority chain, it cannot generate more than 51% attack. The concept of finality is further reinforced as the validators have knowledge to validate the correct chain.

# 3 Potential issues with Casper

There are some issues with the current Casper implementation. They are mentioned below:

- Issue with single jurisdiction having validator nodes:

  If the same jurisdiction has all the validators. Then the network suffers from a single point of failure. As all the nodes in a given location can be forced to be turned off. If during the staking period all the validators are in the same location, a law is passed against Ethereum all the nodes would be forced to shut down. Then the entire network would shut down. In the case of POW that cannot happen as the miners can spring up a machine and start mining from where they left off. This would also invalidate the peer to peer consensus mechanism.
- Affects neutrality of a protocol:

  In a peer to peer protocol, the miners, nodes, client wallets are independent of the protocol. In case of Casper the validators are tied to their status. The ordinary nodes are forced to accept the status of the other nodes. This can result in vector attacks made in the system.
- Coupling of stakeholder risk takes place.

  The actions of a bad node validator can affect the profitability of a good node validator as the validators are tightly coupled. The high-status validator can start producing bad blocks. They will be disincentivized. So they would not produce bad blocks. The assumption made is that the nodes are rationale and should be responsible for doing so. The reasons for producing bad blocks could be bugs, hacker compromising the network, etc. Such checks have not been made by the network in the Casper implementation.
- Problem of new Stakeholders being elected:

  As per Casper, new validators must be approved by old validator. There ae many possible ways this can be attacked. If the old validator assigns his votes to the new validator and his votes are hacked. The new validators address is hacked. The new validators can be malicious to the network etc.

# 4 Potential Benefits of Casper

- PoW is extremely expensive due to mining. There is high electric expense due to mining. Casper helps to save upon this thigh use of electricity.

- Token supply can be curtailed and burnt as there is lesser incentive to issue more tokens. This puts less pressure on the system.
- Mining operating can lead to centralization. POS can setup options that can help dissuade mining cartels that can hurt the network.
- Incentive model of Casper helps ensures the bad actors are kept in check. Resultantly the miners serve to look to the benefit of the chain, not just their interest.
- At times there is collusion observed among the miners. Checks in place part of Casper can help control this.
- Casper has provision to fight censorship. Casper helps to level the field wherein the one third and two third members do not end up fighting

# 5 Enhancement to Casper

Casper is in the nascent development phase and has a long road ahead. There is no track record of the efficiency and security. When Eth validation system is impacted, Casper will suffer from block finalization. Currently Casper's phase 1 implementation does not provide protection from attack above fifty-one percentage. Phase1 also does not provide formal specifications to handle attacks

ETH has always been POW. There has never been POS development and hence adoption of POS for Ethereum is no track record.

However, we have never seen the adoption of the protocol at this level before.

The algorithm to overcome weakness:

Create a mutex at the fiftieth block such that all the transactions within mutex will ensure there will be a lock placed on all the transactions due to which the finality can be achieved with a safeguard.

# 6 Conclusion

There are many researches ongoing to overcome the limitations of POW and moving to POS. Casper seems to be a good fit for performing this as this is done in two stages that is partial transition to POS and subsequently full transition to POS. Since change is incremented into two main steps, these can

be thus controlled in better way. Feedback from first stage can be used and leveraged in second phase.
As Casper faces issues with block finalization, a safeguard can be placed so that block finalization takes place at layer2. This is common to both POS and POW. As safety guard is provided at layer2, the network is more secured and protected from hacks and attacks.

# 7 References


Buterin, Vitalik. "A next-generation smart contract and decentralized application platform." *white paper* 3 (2014): 37.

Dannen, Chris. *Introducing Ethereum and Solidity*. Berkeley: Apress, 2017

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

Park, Daejun, Yi Zhang, Manasvi Saxena, Philip Daian, and Grigore Roşu. "A formal verification tool for ethereum vm bytecode." In *Proceedings of the 2018 26th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*, pp. 912-915. ACM, 2018.

Tikhomirov, Sergei. "Ethereum: state of knowledge and research perspectives." In *International Symposium on Foundations and Practice of Security*, pp. 206-221. Springer, Cham, 2017.

Zamfir, Vlad. "Introducing Casper “the friendly ghost”." *Ethereum Blog URL: https://blog. ethereum. org/2015/08/01/introducing-casper-friendly-ghost* (2015).

Antonopoulos, Andreas M., and Gavin Wood. *Mastering ethereum: building smart contracts and dapps*. O'Reilly Media, 2018.

Buterin, Vitalik, Daniel Reijsbergen, Stefanos Leonardos, and Georgios Piliouras. "Incentives in Ethereum's Hybrid Casper Protocol." *arXiv preprint arXiv:1903.04205* (2019).

Buterin, V. "Ethereum 2.0 spec–Casper and sharding, 2018." *Available [online].[Accessed: 30-10-2018]*.

Dale, Oliver. "Beginner's Guide to Ethereum Casper Hardfork: What You Need to Know." *Blockonomi (blog). November* 7 (2017).

Rosic, A. "What is Ethereum Casper Protocol? Crash Course." (2017).

Zamfir, V. "Introducing casper “the friendly ghost”," Ethereum Blog, 2015."

Mohanty, Debajani. "Ethereum: What lies ahead." In *Ethereum for Architects and Developers*, pp. 245-258. Apress, Berkeley, CA, 2018.

Deshmukh, Amit A., Mansi Mohan, Raj Shah, and Prateeksha Runwal. "Analysis of Broadband Proximity Fed Gap-coupled C-shaped Microstrip Antennas."

Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).

Wood, Gavin. "Polkadot: Vision for a heterogeneous multi-chain framework." *White Paper* (2016).

Zamfir, Vlad. "Casper the friendly ghost: A correct by construction blockchain consensus protocol." *White paper: https://github. com/ethereum/research/blob/master/papers/caspertfg/caspertfg. pdf* (2017).

Buterin, Vitalik. "Incentives in casper the friendly finality gadget." (2017).

Hertig, Alyssa. "Where's casper? inside ethereum's race to reinvent its blockchain." (2017).

Saleh, Fahad. "Blockchain without waste: Proof-of-stake." *Available at SSRN 3183935* (2019).

Tikhomirov, Sergei. "Ethereum: state of knowledge and research perspectives." In *International Symposium on Foundations and Practice of Security*, pp. 206-221. Springer, Cham, 2017.

Aung, Yu Nandar, and Thitinan Tantidham. "Review of Ethereum: Smart home case study." In *2017 2nd International Conference on Information Technology (INCIT)*, pp. 1-4. IEEE, 2017.

Siim, Janno. "Proof-of-stake." In *Research Seminar in Cryptography*. 2017.

Chepurnoy, Alexander. "Interactive proof-of-stake." *arXiv preprint arXiv:1601.00275* (2016).

Zheng, Zibin, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. "An overview of blockchain technology: Architecture, consensus, and future trends." In *2017 IEEE International Congress on Big Data (BigData Congress)*, pp. 557-564. IEEE, 2017.

Deeshmukh, Amit A., Mansi Mohan, A. Amrita, and K. P. Ray. "Broadband Proximity Fed Equilateral Traingular Microstrip Antenna." In *2012 International Conference on Advances in Computing and Communications*, pp. 263-266. IEEE, 2012.

Bartoletti, Massimo, Stefano Lande, and Alessandro Sebastian Podda. "A Proof-of-Stake protocol for consensus on Bitcoin subchains." In *International Conference on Financial Cryptography and Data Security*, pp. 568-584. Springer, Cham, 2017.

Moindrot, Olivier, and Charles Bournhonesque. "Proof of Stake Made Simple with Casper." *ICME, Stanford University* (2017).

Iyengar, Makrant M., and Mansi M. Iyengar. "SEMANTIC MATCHING USING ONTOLOGY IN MULTILINGUAL ENVIRONMENT (WITH GUI & IMPLEMENTATION)." *International Journal of Global Technology Initiatives* 2, no. 1 (2013): B20-B27.

Duong, Tuyet, Alexander Chepurnoy, Lei Fan, and Hong-Sheng Zhou. "Twinscoin: A cryptocurrency via proof-of-work and proof-of-stake." In *Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts*, pp. 1-13. ACM, 2018.

Atzei, Nicola, Massimo Bartoletti, and Tiziana Cimoli. "A survey of attacks on Ethereum smart contracts (sok)." In *International Conference on Principles of Security and Trust*, pp. 164-186. Springer, Berlin, Heidelberg, 2017.

Gencer, Adem Efe, Soumya Basu, Ittay Eyal, Robbert Van Renesse, and Emin Gün Sirer. "Decentralization in bitcoin and Ethereum networks." *arXiv preprint arXiv:1801.03998* (2018).

Bogner, Andreas, Mathieu Chanson, and Arne Meeuw. "A decentralised sharing app running a smart contract on the Ethereum block-chain." In *Proceedings of the 6th International Conference on the Internet of Things*, pp. 177-178. ACM, 2016.

Hildenbrandt, Everett, Manasvi Saxena, Xiaoran Zhu, Nishant Rodrigues, Philip Daian, Dwight Guth, and Grigore Rosu. *Kevm: A complete semantics of the Ethereum virtual machine*. 2017.

G. Hall, M. Mansi, and I. Makrant. "Novel method for handling Ethereum attack." arXiv preprint arXiv:1909.12934 (2019).

Antonopoulos, Andreas M., and Gavin Wood. *Mastering Ethereum: building smart contracts and dapps*. O'Reilly Media, 2018.

Jentzsch, Christoph. "Decentralized autonomous organization to automate governance." *White paper, November* (2016).

Swan, Melanie. "Block-chain thinking: The brain as a dac (decentralized autonomous organization)." In *Texas Bitcoin Conference*, pp. 27-29. Chicago, 2015.

Chohan, Usman W. "The decentralized autonomous organization and governance issues." *Available at SSRN 3082055* (2017).

Wood, Gavin. "Ethereum: A secure decentralised generalised transaction ledger." *Ethereum project yellow paper* 151, no. 2014 (2014): 1-32.

Buterin, Vitalik. "A next-generation smart contract and decentralized application platform." *white paper* 3 (2014): 37.

Clack, Christopher D., Vikram A. Bakshi, and Lee Braine. "Smart contract templates: foundations, design landscape and research directions." *arXiv preprint arXiv:1608.00771* (2016).