Casper the Friendly Finality Gadget

Over the past few years there has been considerable research into “proof of stake” (PoS) based blockchain consensus algorithms. In a PoS system, a blockchain appends and agrees on new blocks through a process where anyone who holds coins inside of the system can participate, and the influence an agent has is proportional to the number of coins (or “stake”) it holds. This is a vastly more efficient alternative to proof of work (PoW) “mining” and enables blockchains to operate without mining’s high hardware and electricity costs.

Casper introduces several new features that BFT algorithms do not necessarily support:

- Accountability. If a validator violates a rule, we can detect the violation and know which validator violated the rule. Accountability allows us to penalize malfeasant validators, solving the “nothing at stake” problem that plagues chain-based PoS.
- Dynamic validators. We introduce a safe way for the validator set to change over time.
- Defenses. We introduce defenses against long range revision attacks as well as attacks where more than $\frac{1}{3}$ of validators drop offline, at the cost of a very weak tradeoff synchronicity assumption.
- Modular overlay. Casper’s design as an overlay makes it easier to implement as an upgrade to an existing proof of work chain.

Casper remains imperfect. For example, a wholly compromised block proposal mechanism will prevent Casper from finalizing new blocks. Casper is a PoS-based strict security improvement to almost any PoW chain. The problems that Casper does not wholly solve, particularly related to 51% attacks, can still be corrected using user-activated soft forks. Future developments will undoubtedly improve Casper’s security and reduce the need for user-activated soft forks.