BlockchainHub - Research #34

Research PoS Casper

04.01.2017 17:24 - didi

Status:	In Progress	
Priority:	Normal	
Assignee:		

Description

Philosophy:
Avoid wasted energy (1 BCT transaction is now ~ 100 kWH).
Cypherpunk spirit: defense easier then attack
Cooperative game theory
Vitalik's PoS Design Philosophy

Problems to solve:
Nothing at Stake problem
Bribing attack / Long range attack

Basic strategy:

- *validators* (nodes signing blocks) need to make security deposits
- validator signatures are relevant only as long as the deposit is in place
- Severe (asymmetric) punishments of misbehaviour make cooperative behaviour the winning economic strategy (Slasher)

Tendermint favours consistency over availability (CAP theorem).
It adds only finalized blocks.
Gives an incentive to form 2/3 cartels which censor outsiders.
At the same time 1/3 cartels can prevent consensus to form.

PoW blockchains have an incentive for 50+ % miner cartels.

Important difference: introduction of some subjectivity (client not always online probably needs to get current state of validators out of band)

Building of censoring cartels* is avoided by enforcing cooperative behaviour. If a validator gets offline, everybody is punished.

Traditional consensus protocols (favouring consistency over availability) require a *Byzantine quorum* in order to make decisions.
Contradicts the following definition of *decentralized*:

> A protocol is decentralized only if it can fully recover from the permanent removal of all but one of its nodes.

Casper keeps the basic principle of Ghost (comparing branches by weight, not height). Weight here is determined by number of validator signatures (weighted by the validator's deposit).
Validators are punished for going offline. All other validators are punished too.

Weak subjectivity is a concept introduced by Vitalik here. It deals with the fact that a PoS powered chain can't be verified based on the genesis block alone (unlike validator deposits were locked forever, which isn't realistic). This clients also need to rely on later states. This can e.g. be checkpoints (e.g. in the form of a block hash) hardcoded in the client. A *revert limit* helps client not always online to sync without out-of-band verification. *Exponential subjective scoring* is an alternative based on probabilities instead of hard limits.

Consensus by bet is explained here. It's designed for pushing consensus convergence.

Links:
Devcon 1 talk about casper
Series of blog posts The history of Casper.
Oct 2014 Blog post by Vitalik (this post includes a discussion with Tendermint creator Jae Kwon.
Universal Hash Time (linked timestamping on the Blockchain)

History

#1 - 06.02.2017 23:15 - didi

TODO: check
https://medium.com/@VitalikButerin/parametrizing-casper-the-decentralization-finality-time-overhead-tradeoff-3f2011672735#.5mp2ytus8