Research/Readings 2: Blockchain Ecosystem

Find a blockchain project (that is not using Proof of Work), write a report summarizing what the project is about and explain how the consensus is different from PoW (between 500-1000 words, sources should be cited and referenced)

Proof of Activity – A Hybrid Approach

(730 words)

In Dec 2014, 4 authors including Litecoin creator Charlie Lee, published a recommendation paper in the ACM SIGMETRICS Performance Evaluation Review newsletter[1]. The authors recommended Proof of Activity (POA), combining Proof of Work (POW) and Proof of Stake (POS), as a hybrid approach to cryptocurrency mining. The abstract in the paper stated,

*"**We propose a new protocol for a cryptocurrency, that builds upon the Bitcoin protocol by combining its Proof of Work component with a Proof of Stake type of system. Our Proof of Activity protocol offers good security against possibly practical attacks on Bitcoin and has a relatively low penalty in terms of network communication and storage space.**"*

POW and POS are both designed to prevent 51% attacks, a malicious action in which one control majority of the mining power in the distributed network and then disapproved any invalid transactions in the blockchain. There is also a potential problem called the "tragedy of the commons" in Bitcoin which uses POW, where miners begin to act only in their own self-interests, ruining the otherwise secure system. It has been theorized that this can occur for Bitcoin once the mining rewards are gone after all the 21 million coins have been mined, or potentially even sooner as rewards become increasingly smaller and miners are basically only receiving transaction fees.

How does it work?

As suggested in the 2014 paper, POA combines these mechanisms into a single 2 step-process:

1. Using POW, miners first compete to be the first in solving the puzzle to find the block then earn the reward. The difference is that the blocks being mined do not contain transactions but are simply templates with header information and the mining reward

address. The greater percentage of the network's total computing power a miner has, the greater the probability that they will find a block[2].

2. Once this nearly "blank" block is mined, the system switches into POS protocol, to validate/sign the new block. The header information is used to select a random group of validators to sign the block. These stakeholders and the larger the stake a validator hold, the greater the chance they will be selected to sign the new block. Once all the chosen validators sign the block, it becomes an actual part of the blockchain. If the block remains unsigned by some of the chosen validators after a given time, it is discarded as incomplete and the next winning block is used. Validators are once again chosen and this will continue until a winning block is signed by all the chosen validators. The network fees are split between the wining miner and the validators who signed the block.

Is POA better?

It has been criticized that POA still requires a fairly large amount of resources for mining phase. It has also been suggested that there is nothing preventing a validator from double signing[3].

POA makes the mining process more secure against a 51% attack. An attacker would theoretically need to have both 51% or more of the network's total mining power and 51% or more of the coins stalked in the network in order to pull off the attack successfully[4].

Who uses POA?

Decred and Espers are the 2 coins that are currently using a variation of the hybrid POA i.e. a hybrid of the hybrid. In terms of market pricing, Decred (DCR) has much better performance compared to Espers (ESP) and seems to have further development in support of smart contracts, atomic swaps and lightning network[3].

Decred indicated that the reason a hybrid POA approach is used in their mining system is to ensure that a small group cannot dominate the flow of transactions or make changes without the input of the community. For POW, miners only receive 60% of the block reward while

POS received 30%. The remaining 10% goes into the Decred Treasury and the how the treasury uses the reward is decided by proposal and voting of the stakeholder community[5].

Espers developed a custom difficulty retarget algorithms called Terminal Velocity RateX (VRX) to allow proper shuffling of the time span between either POW or POS so that blocks are generated at a consistent pace[6].

Summary

In conclusion, only 2 coins to date have chosen the use of POA indicate that it is either difficult to implement or it doesn't provide enough benefits to outweigh the downsides.

1. Iddo Bentov, Charles Lee, Alex Mizrahi, Meni Rosenfeld, “Proof of Activity: Extending Bitcoin’s Proof of Work via Proof of Stake [Extended Abstract]”, ACM SIGMETRICS Performance Evaluation Review Vol. 42, No.3, “https://dl.acm.org/doi/10.1145/2695533.2695545”, Dec 2014.

2. Jake Frankenfield, “Proof of Activity (Cryptocurrency)”, “https://www.investopedia.com/terms/p/proof-activity-cryptocurrency.asp”, 25 Jun, 2019

3. Steve Walters, “Proof of Activity Explained: A Hybrid Consensus Algorithm”, “https://www.coinbureau.com/blockchain/proof-of-activity-explained-hybrid-consensus-algorithm/” 6 Apr, 2018.

4. Shobhit Seth, “Proof-of-activity (PoA)”, “https://golden.com/wiki/Proof-of-activity_(PoA)-BWK8BAG”, 4 Apr, 2018.

5. Jon Creasy, “3 Things You Need to Know About Decred”, “https://medium.com/decred/3-things-you-need-to-know-about-decred-649aac41dc4”, 13 Mar, 2017.

6. The CryptoCoderz Team, “ESPERS, A CryptoCoderz Team Project White Paper”, “https://espers.io/download/Espers-White-Paper-v1-Final.pdf”, Ver 1.0 Release, 20 Feb, 2018