Zero-Con

POC - Proof of Consensus

Reduced risk consensus proposal for cryptographic assets

Concept by: equ1miner

First Draft

Date: August 17, 2019

Table of contents:

1.1 – Definition of Consensus Mechanism [con·sen·sus (/kənˈsensəs/): a general agreement]
The consensus mechanism is a protocol to create an irrefutable system of agreement between nodes on a distributed network to prevent exploitation and irregularities.

1.2– POW (Proof of Work)
Proof of work is a consensus protocol introduced by Bitcoin. The process is referred to as mining and block generation comes in the form of solving a mathematical problem.

1.3– POS (Proof of Stake)
Proof of stake is the consensus algorithm used by cryptocurrencies to validate blocks and provide consensus. The mechanism was made public in 2011 and the first cryptocurrency to implement it was Peercoin in 2012. In a proof of stake system, the creator of the next block is usually determined semi-randomly in by preset factors such as how much cryptocurrency a user is holding or, the availability of the node, how long they have been holding the cryptographic currency or UTXO or other factors.

1.4 – DPOS (Delegated Proof of Stake)
Holders can delegate stake to nodes to attain real-time voting and reputation to achieve consensus.

1.5 – Table of Advantages and Disadvantages

Mechanism	Advantages (Possible)	Disadvantages (Possible)
POW (Proof of Work)	• You do not have to "buy-in" from existing holders • Reward is a result in the computational energy delivered • Blockchain is created by physical energy inputs • Participants are rewarded with new coins instead of early holders or investors	• Environmentally unfriendly • Changes in hashrate or solution rate can have unpredictable effects on the network • Re-organization of blocks can occur resulting in the possibility to reverse transactions • Market dumping to cover mining costs
POS (Proof of Stake)	• Energy efficiency • Security • Increased copies of blockchain • Byzantine Fault Tolerance	• Rewards large holders • Low availability can occur • Stakers often provide little benefit to network health
DPOW (Delegated Proof of Stake)	• Energy efficiency • Security • Byzantine Fault Torrance • Faster transaction validation	• Nodes may not pay delegates • Centralization of nodes can occur

1.7 Masternodes
Masternodes, introduced by Dash, are full nodes that operate on a bonded collateral in order to provide high availability open port copies of the blockchain for validation. Masternodes can have additional functions such as transaction locking (InstantSend) and coin mixing on some blockchains.

2.1– Problem with our current consensus methods.

Current consensus methods have many problems

- Energy waste
- Rewards for founders and coin holders
- Block Re-organization
- Hash-rate Abuse
- Chain freezes
- POW ASIC abuse
- POS Fake Stake attacks
- Transaction invalidation
- Rewarding few users
- Un-necessarily high number of supporting nodes
- Low number of supporting nodes
- Centralization
- Governance systems allowing account freezing

2.2 – Current Hybrid Solutions and issue

The current hybrid solutions are designed to balance POW and POS in order to maintain a balance of energy input and holding value between users. With hybrid consensus systems is POW is used to generate the block and stake holders are rewarded for their network support or holdings. The fatal flaw in this system is the reward is decreased to the miners and thus less energy is required to produce a block reducing the security. As less energy is required to secure the network the network may become more vulnerable to double spends, inconsistent block times. Blockchains could invest in hash power to reduce reliability of block productions of their competitors or execute other mischievous exploits.

3.1 -- Zero-Con Proposal (Concept)

Zero-con offers a hybrid consensus system with the benefit of both POW and POS without the drawback of either system. There is no doubt POW, aka mining is an important element in blockchain technology. Mining brings community interest to a blockchain and in some ways creates a sporty competitive atmosphere. POS further brings another valuable element for investors and early adopters as well as decreases energy waste addressing environmental concerns. The Zero-Con proposal (Concept) is create a robust solution that strengthens the blockchain by adding diversity. The goal is to increase security and reliability.

3.2 – POS as the primary consensus mechanism 20% of reward

During the years 2018 and 2019 it became very clear that POS was much more reliable for new blockchains and POW brought more excitement and attention. POS is arguably far more secure as block reorgs and block timing is consistent. The Zero-Con Proposal thus will build upon POS (Masternode) as the primary consensus.

As an example Phore blockchain is the most forked version of this type of consensus called MN-POS (Masternode – Proof of Stake) and can be referenced here https://github.com/phoreproject/Phore

Zerocoin currently has a 120 and the consensus mechanism will have to be adjusted to 120seconds.

3.3 – POW as a mandatory secondary requirement for block creation 80% of reward

The POS consensus mechanism will require the inclusion of a POW transaction. The timing for the difficulty of a POW transaction will be 50seconds. In order for a POS block to be mined the masternode/zeronode must wait until a pool submits a POW solution as a POW solution transaction to the network. The value of the POW solution transaction will not be determined until the POS block is mined.

3.4 – How will multiple POW transactions be handled

In the case that only 1 POS transaction is in the MEMPOOL at the time of a POS block creation the block will only contain 1 POW transaction. Mining pools will build a second POW transaction be solving a second problem on top of the first POW transaction to be included in the POS generated block. Should a second solution be presented a third POW transaction will be attempted to be mined and added to the mempool to a maximum of 6 POW transactions. The POS mined block will include the POW reward as shown in the table.

Number of POW TX	MN-POS REWARD	POW REWARD per TX
1	20%	80%
2	20%	40% + 40%
3	20%	26.66666667%* + 26.66666666% + 26.66666666%
4	20%	20% + 20% + 20% + 20%
5	20%	16% + 16% + 16% + 16% + 16%
6	20%	13.33333334%* + 13.33333333% + 13.33333333% + 13.33333333% + 13.33333333% + 13.33333333%

* the first tx will contain the extra amount

3.5 – Consensus abuse cases and abuse reduction solutions

ABUSE PROBLEM	SOLUTION
Pool creates POW transaction solution and withholds it until the next block	POW solutions will not be valid on the next block. The first POW transaction will be built upon the hash of the previous block. The second POW transaction will be built upon the first on in the mempool.
Pool creates POW transaction solution and withholds it so another pool can no mine on top.	POW transactions will be time-stamped and POS nodes will generate consensus according to non-negotiable rules. The POW-TX submitted to the mempool with the earliest timestamp is accepted. It is in the best interest for the pool to get the POW-TX in the mempool to secure the solution.
High hash attack	After 8 POW-TX are created no more will be accepted and miners cannot add additional POW-TX. The next block will increase in difficulty by 50% if 8 solutions are created. Higher hash rate will not generate more rewards and miners will be rewarded based on their % of network.
Low hash drop attack	For example, the network has 100ksols and drops to 10ksols a 10x drop the POW could take up to 10 minutes to mine. The pow difficulty will adjust down quickly based. 12 POW-TX are expected every 10 minutes if only 1 is made the difficulty will drop by 50%

3.6 – This consensus method requires further review and extensive testing for fringe cases. This proposal solves the most pending issues including double-spend attacks, POW attacks, inconsistent POW as POW reward is reduced, multiple network abuse cases while removing many risk factors cryptocurrencies currently have while maintaining community participation and POW rewards and mining interest.

The implementation of this Zero-Con proposal in the Zerocoin (ZER) cryptocurrency would not only make Zerocoin (ZER) unique but become a true leader in blockchain development.