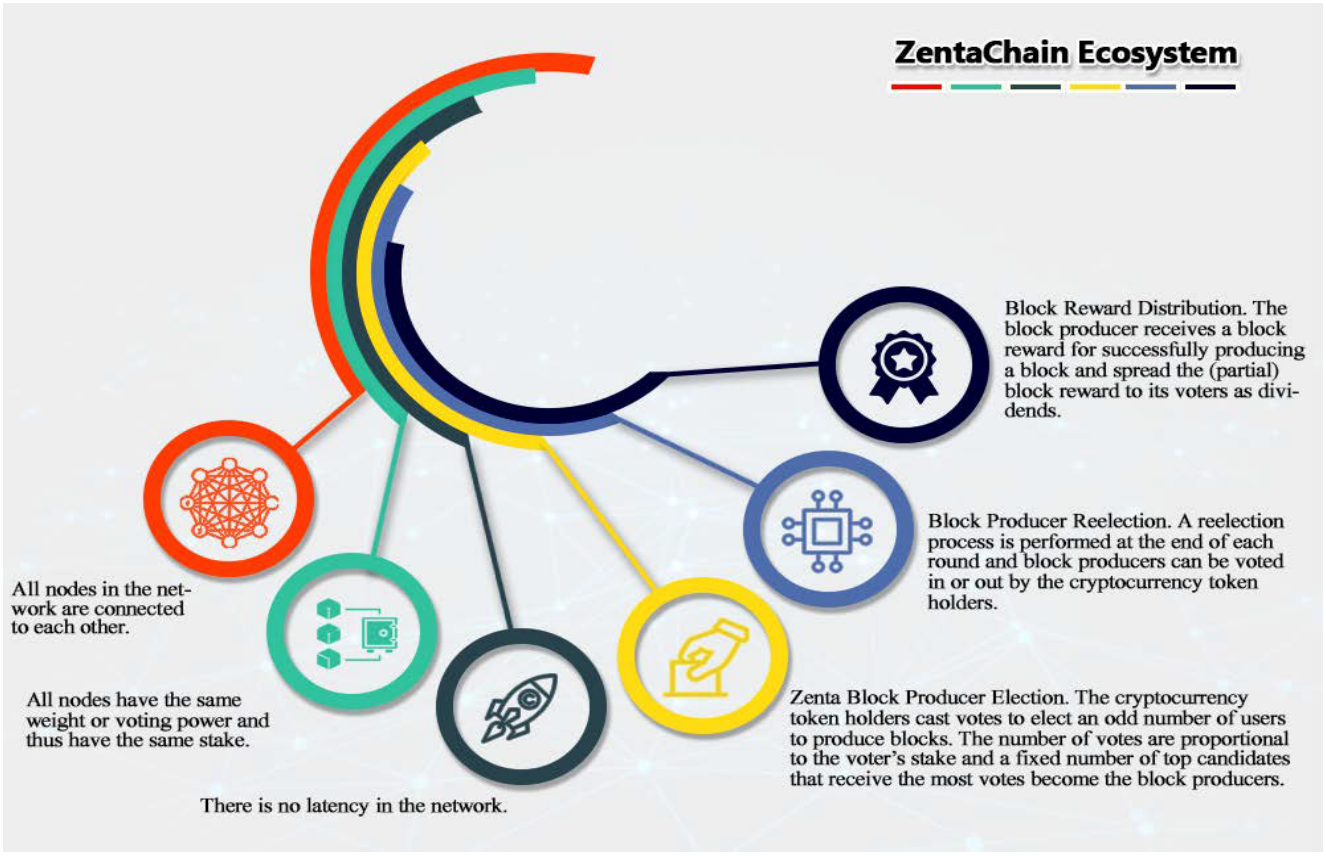
Zenta Token a Dpos Algorithm

INTRODUCTION Delegated Proof of Stake (DPoS) is a robust and flexible blockchain consensus mechanism invented by Larimer in 2014, which leverages the voting power of the stakeholder to resolve consensus issue in a fair and democratic. DPoS was first applied by Larimer to power the blockchain project BitShares .

In the decentralized system of blockchain, all network resources, computing resources, and storage resources are provided by users themselves, and each node is both a consumer of the service and a provider of the service. Elections and the generation of new blocks require CPU time, electricity, and network resources. If there is no incentive mechanism, no users are willing to participate, so for each job, such as elections and the generation of new blocks, the provision of each resource, it provides a certain amount of tokens as rewards. At the same time, in order to encourage all nodes to participate together and maintain the safe operation of the blockchain system, an equity mechanism is needed as compensation and incentive for participants. That is, through the means of economic balance, to prevent tampering the contents of the general ledger, Token has become an inevitable mechanism for issuing incentives. In addition, this incentive mechanism also encourages nodes to remain honest.

The Zenta token uses Dpos algorithm with the witness mechanism: to solve the centralization problem, each person holding shares votes, resulting in n-bit representatives(usually n=101), the value of n is decided by the number of nodes on the blockchain. The larger number of nodes, the larger the value of=n, and the: n node representatives share the same rights. Due to the decentralized voting mechanism, DPoS is more democratic than other systems. From a certain perspective, DPoS is a bit like a parliamentary system or a people's congress system. If the delegates are unable to perform their duties, they will be delisted and the network will select new supernodes to replace them. It is not always the node with the largest stake value to be the winner, because that will be easy to cause monopoly and manipulation. Multiplies the stake value of each node by a random number in the election, and prohibit re-election.



In DPOS, block producers are voted in and campaign for the privilege, perhaps offering something more, working harder. More concentrated and powerful hardware that allows the platform to scale is deployed in the service of the community. The voting makes the system agile. DPOS can respond to change more easily since change is not always a code change. Change, for some things, is only as far away as a vote. DPOS puts the community centre stage. It asks us to participate, requires us to pay attention. When B1 talks about aligning interests it is human interests that they are talking about, it is human interests that are being aligned. Not just the consensus algorithm's interests. You express your interests with your vote.

DPOS has certain properties that make it central to the decentralization of politics and governance. It is the only consensus algorithm that is socially disruptive in a good way!

Why DPOS is better than POS (Proof of Stake)?

DPoS is a better alternative to the more commonly known, Proof-of-stake (PoS) model, which requires miners to put up a stake in the required cryptocurrency before they are able to process transactions and add them to the blockchain. We can also define DPos like that; a consensus algorithm developed to secure a blockchain by ensuring representation of transactions within it. DPoS can be seen as the least centralized consensus protocol compared to all others as it is the most inclusive.

1)Delegated Proof of Stake (DPoS) is a newer consensus structure and It's somewhat similar to PoS but has different and more "democratic" features that make it more efficient and fair.

2)To add in the "proof of stake" part of DPoS, stakeholders have influence proportional to their stake in the system. DPoS is found to be more decentralized than other consensus systems because the threshold to enter is very low. Other alternatives generally "allow" anyone to enter, but most people are excluded from entering due to high costs/needs, and generally, a few pools or large miners produce all blocks on those systems.

4)The people you vote for are possibly the ones who will be deciding/shaping the future of the network as well. Just like a democracy, the system will work better and be more decentralized/ fair if more people participate and are informed.

5)When using PoS, it must vote among thousands of nodes in the election. The more nodes participating in the cluster, the slower the efficiency, the greater the pressure onnetwork traffic. DPoS gives an idea that these thousands of PoS nodes vote among through a mechanism to elect a number of nodes, then vote among these number of nodes, not all nodes in the network, to elect each bookkeeper. This mechanism can greatly improve the efficiency of elections. Consistent voting among dozens, up to hundreds of nodes can generally be done in seconds and reach consensus, so the can increase the consensus process to the second level.

6)As a variant of PoS, DPoS reduces network pressure by reducing the number of It is a typical divide-and-conquer strategy: divide all nodes into leaders and followers, and only inform the followers after reaching a consensus among the leaders. This mechanism can effectively reduce network pressure without increasing computing resources, and will have strong application value software implementation. Theoretically, It has no upper limit, hundreds of thousands of transactions per second.

This electoral system has the following advantages:

1)The larger the equity, the higher the probability of being elected, guarantees the stability of the system.

2)The small equity may also be elected, ensuring the fairness of the system.

3)Certain restrictions are placed on the big equities. Ensure that the system is not manipulated and monopolized.

4)Due to the token reward system, the election mechanism effectively prevents the rich from becoming richer. Through this real-time change of shareholder voting mechanism, this makes the whole system is more like a 24-hour uninterrupted shareholder meeting, and shareholders can change the company's organizational structure at any time by voting.

The efficiency of the Zenta token election algorithm:

If the number of people participating in the election is n, the number of rounds of the election process is n times. This process is called the first stage. When the voting is over, the initiator of the election broadcasts the election result to the whole network, inform each node about who is elected. When the information of the last node election result is successfully delivered to the initiator, this is considered as success of the election result broadcast, this process is called the second stage, and it needs to be cycled n times, until the election is completely finished, so the cost of the algorithm is to deliver the messages 2*n times. If there is any problem in the whole process, it can only be regarded as a failed election, and the election is invalid. Obviously, the election algorithm only needs to deliver messages and confirm elections. It does not require complicated calculations and can be completed within 1 second. It is much more efficient than bitcoin's PoW algorithm. Compare with the current bitcoin network, it takes about 10 minutes to generate a block. it takes an average of 6 rounds of confirmation, which is 60 minutes to confirm that a transaction really takes place. So the efficiency of election algorithm is greatly improved.

The Zenta DPoS consensus mechanism is used to implement the blockchain through two elections; first one, elect the representatives, then the generator of the block. The Zenta token election algorithm uses the improved A ring-based coordinator election algorithm as the consensus algorithm. Ensure the Decentralization of the whole process and the fairness prevents monopoly. The efficiency of the Zenta token whole algorithm is much higher than that of PoW, which reduces transaction costs. On the other hand, since the consensus algorithm proposed in this paper is the block generator elected by the whole Zentachain network nodes, there is another situation in realities, that is, when a node I initiates an election activity, and the election message has not arrived at all nodes of the entire network, it is possible that another node J initiates an election process without knowing the activities of node I, at the same time, two or more elections will be going on the whole network.

CONSENSUS ALGORITHM CHARACTERISTICS

Algorithm Name					
Property	***PoW***	***PoS***	***PBFT***[1]	***DPoS***	***Ripple***
Energy Saving	No	Partial	Yes	Partial	Yes
Tolerated power of adversary	< 25% computing power	<51% stake	< 33.3% replicas	< 51% validators	<20% faulty nodes

Fig (1)

TRANSACTIONS PER SECOND FOR SELECTED CRYPTOCURRENCIES

Scalability and Sharding: The theoretical maximum number of transactions per second (TPS) that a cryptocurrency can achieve is listed in this section. As shown in Table(Fig2), while the algorithm that underlies a cryptocurrency ultimately dictates the maximum TPS that can be achieved, there is still some variance between networks that use the same protocol.

Cryptocurrency Name	Protocol	TPS
Bitcoin	PoW	7
Ethereum	PoW	15
Ripple	RPCA	1500
Bitcoin Cash	PoW	60
Cardano	PoS	7
Stellar	SCP	1000
NEO	DBFT	10000
Litecoin	PoW	56
EOS	DPoS	~millions
NEM	PoI	4000

(Fig2)

ZENTA Token distribution is shown below:

Official Token Name: ZENTA
Token Symbol: ZENTA
Algorithm (Mainnet): DPOS
Blockchain: Ethereum - ERC20
Number of tokens (total supply): 260.514.201 ZENTA

Thank you Zentachain.io

CONTRIBUTORS

E-mail:Team@zentachain

Harun Kacemer
Daniel Wale
Göktas Polat

REFERENCES

S. Nakamoto, "Bitcoin: A Peer-to-peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf. [Accessed: 05-Feb-2018]

S. King, S. Nadal, "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake, "2012.[Online].Available:https://peercoin.net/assets/paper/peercoin-paper.pdf. [Accessed: 04-Feb-2018]

Yonatan Sompolinsky and Aviv Zohar, “Secure high-rate transaction processing in bitcoin,” In Financial Cryptography and Data Security, Springer, vol. 8975, July 2015, pp.507–527, doi:10.1007/978-3-662-47854-7_32

Juan Garay, Aggelos Kiayias, and Nikos Leonardos, “The bitcoin backbone protocol: Analysis and applications,” In Advances in Cryptology-EUROCRYPT 2015, Springer, vol.9057, 2015, pp.281–310, doi:10.1007/978-3-662-46803-6_10

Yoad Lewenberg, Yonatan Sompolinsky, and Aviv Zohar, “Inclusive block chain protocols,” In Financial Crypto, vol.8975, 2015, pp 528-547, doi:10.1007/978-3-662-47854-7_33.

BitShares. 2018.https://bitshares.org

