

What is Delegated Proof-of-Stake?

Educational Series

October 2, 2018

Overview

- Delegated proof-of-stake (DPoS) is a consensus mechanism used in blockchain based networks to determine who the validator of each block will be and reach on a consensus on what data should be added to the chain.
- It was invented in 2013 by Dan Larimer, who was attempting to solve the issues that plagued Bitcoin's proof-of-work system. He originally invented DPoS to power a cryptocurrency called BitShares. He later refined the consensus mechanism for his second project, Steem, and is now continuing to refine it for EOS.
- Delegated proof-of-stake can be thought of as a technological democracy that is a digital version of an organizational hierarchy. A DPoS system has a certain number of delegates that secure the network by validating transactions and blocks, and these delegates are voted into position by the token holders.

How does it work?

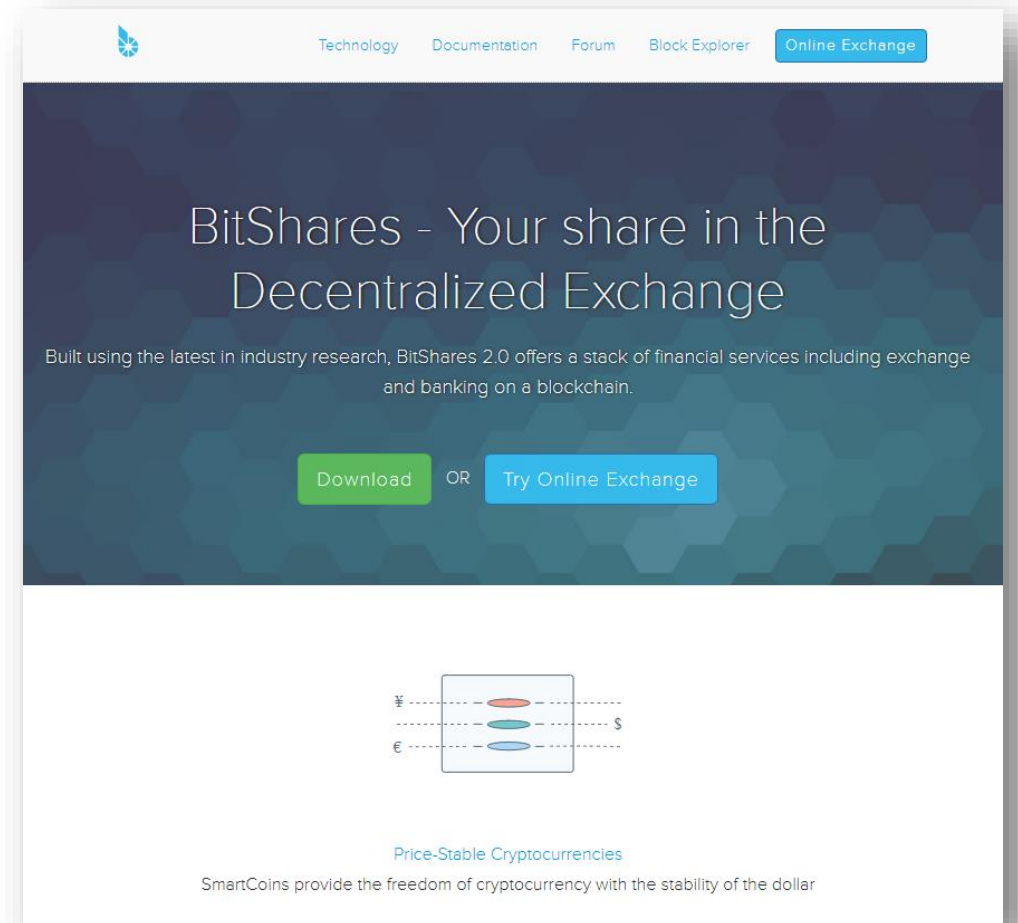
- Delegates' responsibilities include ensuring their node is always running, collecting transactions and building them into blocks, signing and broadcasting blocks to validate the transactions, and resolving consensus issues that may arise in the network.
- For most DPoS chains, voting for delegates is accessible to all token holders in the network, and voting power is directly proportional to the number of tokens held by a certain account. Users can also delegate their voting power to another user who will vote on their behalf.
- Votes are dynamic and can be changed, meaning delegates can be voted in or out at any time. The threat of loss of income and reputation provides incentive for delegates to act honestly and keep the network secure. Delegates are responsible for distributing the block rewards they receive to their voters in a proportional manner based on voting power.

How does it work? (continued)

- Unlike traditional proof-of-stake, delegates are not required to have a large stake in the network, but they must compete for votes from token holders.
- DPoS systems sacrifice some decentralization by limiting who is allowed to validate blocks of transactions, but in turn gain efficiency as less work is required to reach consensus on the network.

Implementations - BitShares

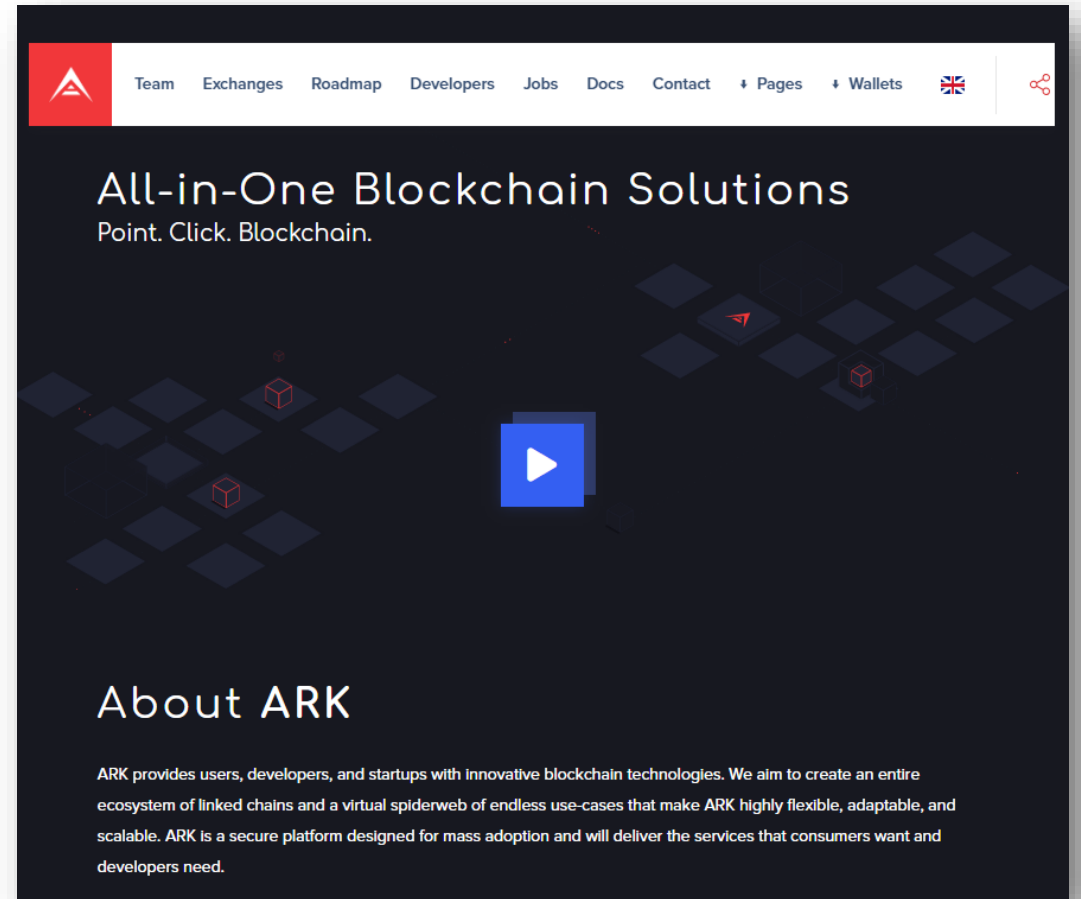
- The first known implementation of delegated proof-of-stake.
- At the initial release, there was a set amount of 101 voted-in delegates (called witnesses), although now the number is dynamic. For example, if a majority of shareholders vote for 50 witnesses, then 50 will be used, and the minimum possible witness count is 11.
- The BitShares blockchain can reach 100,000 TPS and the average block confirmation time is 3 seconds.



The screenshot shows the BitShares website homepage. At the top, there is a navigation bar with links for Technology, Documentation, Forum, Block Explorer, and Online Exchange. The main heading reads "BitShares - Your share in the Decentralized Exchange". Below this, a sub-heading states: "Built using the latest in industry research, BitShares 2.0 offers a stack of financial services including exchange and banking on a blockchain." Two buttons are present: "Download" (green) and "Try Online Exchange" (blue), separated by "OR". Below the buttons is a diagram showing three price-stable cryptocurrencies: one with a red oval, one with a teal oval, and one with a blue oval, each between horizontal dashed lines representing price levels. The currencies are labeled with symbols: ¥, €, and \$. Below the diagram, the text reads "Price-Stable Cryptocurrencies" and "SmartCoins provide the freedom of cryptocurrency with the stability of the dollar".

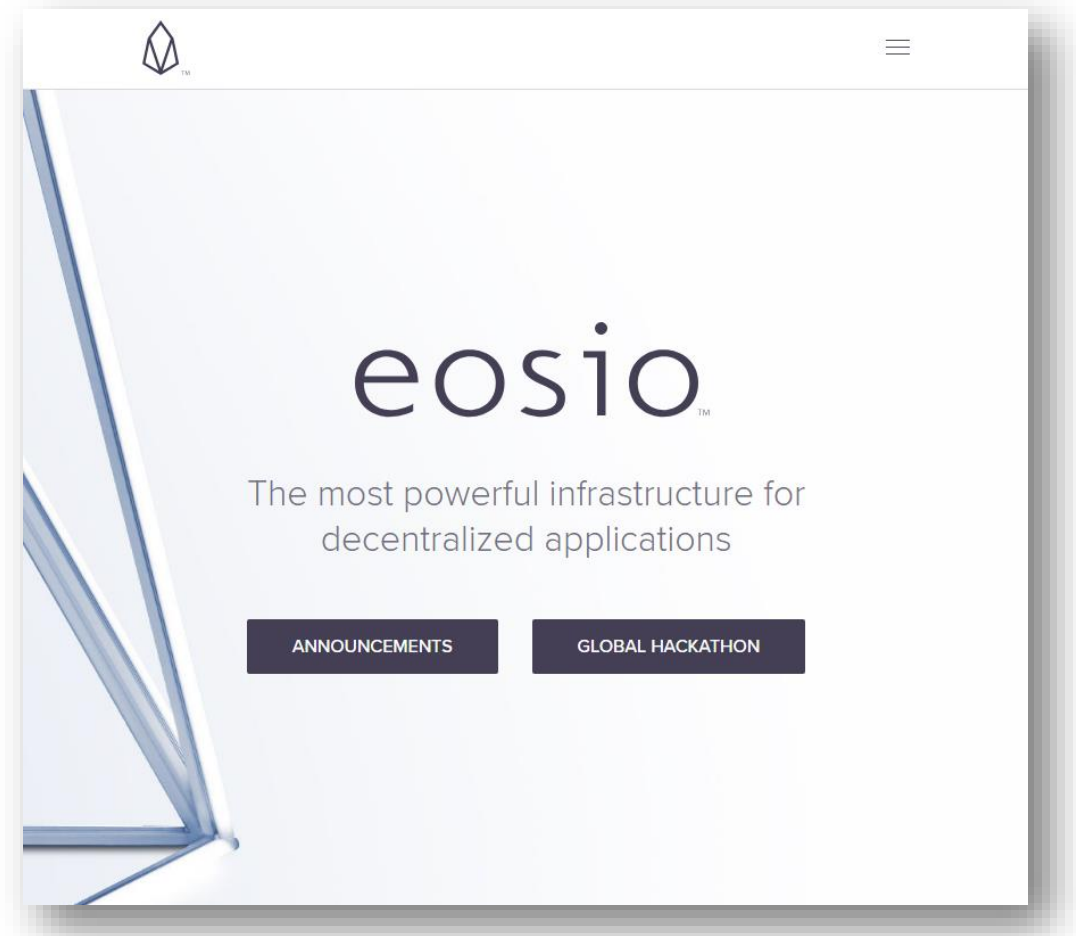
Implementations - Ark

- The Ark blockchain uses DPoS and has the delegate number fixed at 51. This was done to maximize efficiency in the network, allowing the average block time to hover between 5 and 8 seconds.
- The cost to vote is fixed at 1 ARK, and votes can be withdrawn or changed at any time although the fee cannot be recovered.
- Most ARK delegates provide a dividend rate of 7-9% per year to their voters.



Implementations - EOS

- Dan Larimer was the creator of DPoS and BitShares, and he is now working as the CTO of Block.one, the core team of EOS.
- EOS utilizes a DPoS consensus mechanism with 21 delegates, although the top 72 delegates by votes are considered “standby block producers” that still earn dividends.
- Anyone can become a delegate for EOS, there is no voting fee, and the voting rate is around 40% of token holders. EOS averages a 0.5 second block time and has the potential to support over 3,000 TPS.



Benefits

- **Speed:** As less nodes are needed to confirm the blocks, DPoS consensus mechanisms allow for higher throughput, meaning it can process more transactions in a given amount of time.
- **Less energy usage:** As there are no miners required for DPoS, it's far more energy efficient and has less of an impact on the environment over time. For most DPoS chains, users don't need expensive hardware to run a node.
- **Incentives for honesty:** Delegates have an incentive to maintain the role, and any malicious act would risk getting voted out.

Weaknesses

- **Centralization:** By limiting the number of people who can act as block validators, blockchains that utilize DPoS are inherently more centralized than blockchains that allow anyone to become a block validator. This could theoretically make it easier to organize a 51% attack if delegates combine their power.
- **Concentrated voting power:** Users that hold large amounts of tokens will have significantly more voting power and thus more influence in deciding delegates. They will also receive more dividends over time, meaning they will continue to grow voting power faster than users with smaller stakes.
- **Required participation:** A DPoS-based blockchain will only work efficiently and securely if token holders participate in the voting process. Just like a real-world democracy, low participation rates will cause centralization of power and the system will not work as intended.

CrushCrypto