A computer scientist explains proof-of-stake for cryptocurrencies, NFTs and metaverse transactions

September 13 2022, by Scott Ruoti

Credit: Pixabay/CC0 Public Domain

Proof-of-stake is a mechanism for achieving consensus on a blockchain. Blockchain is a technology that records transactions that can't be deleted or altered. It's a decentralized database, or ledger, that is under no one person or organization's control. Since no one controls the database, consensus mechanisms, such as proof-of-stake, are needed to coordinate the operation of blockchain-based systems.

While Bitcoin popularized the technology, blockchain is now a part of many different systems, enabling interesting applications such as decentralized finance platforms and non-fungible tokens, or NFTs.

The first widely commercialized blockchain consensus mechanism was proof-of-work, which enables users to reach consensus by solving complex mathematical problems. For solving these problems, users are commonly provided stake in the system. This process, dubbed mining, requires large amounts of computing power. Proof-of-stake is an alternative that consumes far less energy.

At its core, blockchain technology provides three important properties:

1. Decentralized governance and operation—the people using the system get to collectively decide how to govern and operate the system.
2. Verifiable state—anyone using the system can validate the correctness of the system, with each user being able to ensure that the system is currently working as expected and has been since its inception.
3. Resilience to data loss—even if some users lose their copy of system data, whether through negligence or cyberattack, that data can be recovered from other users in a verifiable manner.

The first property, decentralized governance and operation, is the property that controls how much energy is needed to run a blockchain system.

Voting in blockchain systems

Blockchain systems use voting to decentralize governance and operation. While the exact mechanisms for how voting and consensus are achieved differ in each blockchain system, at a high level, blockchain systems allow each user to vote on how the system should work, and whether any given operation—accepting a new block into the chain, for example—should be approved.

Traditionally, voting requires that the identity of the people casting ballots can be known and verified to ensure that only eligible people vote and do so only once. Some blockchain systems allow users to present a digital ID to prove their identity, enabling voting with negligible energy usage.

However, in most blockchain systems, users are anonymous and have no digital ID that can prove their identity. What, then, stops an individual from pretending to be many individuals and casting many votes? There are several different approaches, but the most used is proof-of-work.

In proof-of-work, users get votes based on the amount of computational power they have in proportion to other users. They demonstrate their ownership of this computational power by solving difficult mathematical problems. If one user can solve twice as many problems as another user, they have twice the computational power as other users and get twice as many votes.

However, solving these mathematical problems is extremely energy intensive, leading to complaints that proof-of-work is not sustainable.

Proof-of-stake

To address the energy consumption of proof-of-work, another way to validate users is needed. Proof-of-stake is one such method. In proof-of-stake, users validate their identities by demonstrating ownership of some asset on the blockchain. For example, in Bitcoin, this would be ownership of bitcoins, and in Ethereum, it is ownership of Ether.

Though this does require users to temporarily lock their assets in the blockchain for a period of time, it is far more efficient because it requires negligible energy expenditure. By the company's estimation, moving from proof-of-work to proof-of-stake will reduce Ethereum's energy consumption by 99.95%.

Ethereum's 'Merge'

This improved energy efficiency is why many blockchain systems intend to transition away from proof-of-work to proof-of-stake. Ethereum plans to make this change during the week of Sept. 15, 2022. This is known as the Merge. During this merge, operations will shift from being voted on using proof-of-work to being voted on using proof-of-stake. At the completion of the merge, only proof-of-stake will be used to vote on transactions.

The hope is that this will set up Ethereum to be sustainable for the foreseeable future.

Provided by The Conversation

Citation: A computer scientist explains proof-of-stake for cryptocurrencies, NFTs and metaverse transactions (2022, September 13) retrieved 20 April 2024 from https://techxplore.com/news/2022-09-scientist-proof-of-stake-cryptocurrencies-nfts-metaverse.html