MIT Technology Review 04 maart 2022

Why Ethereum is switching to proof of stake and how it will work

One of the world's biggest blockchains is testing a new way to approve transactions. The move has been many years in the making but doesn't come without risks.

By Amy Castorarchive page

The market for NFTs—tokens that represent digital art, music, videos, and the like—soared last year to $44 billion. This brought a lot of attention to Ethereum, the blockchain network where most NFTs are bought and sold. It also brought a lot of attention to something else: the massive energy wastefulness of cryptocurrency mining.

Blockchains don't have a central gatekeeper, like a bank, to verify transactions. Instead, both Bitcoin and Ethereum, the two largest cryptocurrencies, rely on a consensus mechanism called "proof of work" to maintain a time-ordered ledger of transactions. Crypto miners are at the core of that process.

Decentralization comes at a hefty cost. In the case of proof of work, that cost is computing power. Proof of work pits miners against each other, as they compete to solve a difficult math problem. Any miner who solves the problem first, updates the ledger by appending a new block to the chain, and gets newly minted coins in return. This requires an enormous amount of computing power and, thus, electricity.

Ethereum uses 113 terawatt-hours per year—as much power as the Netherlands, according to Digiconomist. A single Ethereum transaction can consume as much power as an average US household uses in more than a week. Bitcoin's energy consumption is even worse.

The blockchain system has daunting technical problems to fix. But first, its disciples need to figure out how to govern themselves.

Right now the world is facing a power crunch, which is partly why China banned crypto mining last year, and why countries like Kosovo and Kazakhstan, where the miners scattered off to, are pushing miners out and cutting off their electricity. These countries need the power to keep their businesses running and their homes warm.

Not only does proof of work waste electricity, it generates electronic waste as well. Specialized computer servers used for crypto mining often become obsolete in 1.5 years, and they end up in landfills.

Ethereum's mechanism has other drawbacks—it's tediously slow, averaging 15 transactions per minute. And it doesn't scale. CryptoKitties, a game where players breed and trade cartoon cats, caused a transaction pileup on the network in 2017.

With all the money venture capital firms are shoveling into Web3—a futuristic model where apps will all run on decentralized blockchains, much of it powered by Ethereum itself—now is a good time for Ethereum to disassociate from proof-of-work mining. And that's the game plan.

Sometime in the first half of 2022, in a dramatic event termed "The Merge," Ethereum plans to transition its entire network to a different consensus mechanism: proof of stake, which it promises will use 99% less energy, allow the network to scale, and process 1,000 transactions per minute.

Of course, Ethereum's move to proof of stake has been six months away for years now. "[We thought] it would take one year to [implement] POS … but it actually [has] taken around six years," Ethereum's founder, Vitalik Buterin, told Fortune in May 2021. That's because building such a model is complex.

What is proof of work?

Bitcoin was the first blockchain. Its creator wanted to do away with the control that third parties, often big banks or states, exerted over financial systems.

In a blockchain where participants maintain a shared ledger, Bitcoin's creator needed to find a way to keep people from trying to game the system and spend the same coins twice. Proof of work was a clever kludge—it wasn't perfect, but it worked well enough.

By demanding a significant upfront investment, "proof of something" keeps bad actors from setting up large numbers of seemingly independent virtual nodes and using them to gain influence over the network. Essentially, you have to pay to play.

But it's an approach that's fraught with complications, given platforms' whims and proliferating scams.

In Bitcoin's proof of work, that investment is hardware. Roughly every 10 minutes, Bitcoin miners compete to solve a puzzle. The winner appends the next block to the chain and claims new bitcoins in the form of the block reward. But finding the solution is like trying to win a lottery. You have to guess over and over until you get lucky. The more powerful the computer, the more guesses you can make.

Sprawling server farms around the globe are dedicated entirely to just that, throwing out trillions of guesses a second. And the larger the mining operation, the larger their cost savings, and thus, the greater their market share. This works against the concept of decentralization. Any system that uses proof of work will naturally re-centralize.

In the case of Bitcoin, this ended up putting a handful of big companies in control of the network.

Since early on in Bitcoin's history, though, crypto enthusiasts have searched for other consensus mechanisms that can preserve some degree of decentralization—and aren't as wasteful and destructive to the planet as proof of work.

How proof of stake works

Proof of stake, first proposed on an online forum called BitcoinTalk on July 11, 2011, has been one of the more popular alternatives. In fact, it was supposed to be the mechanism securing Ethereum from the start, according to the white paper that initially described the new blockchain in 2013. But as Buterin noted in 2014, developing such a system was "so non-trivial that some even consider it

impossible.” So Ethereum launched with a proof-of-work model instead, and set to work developing a proof-of-stake algorithm.

Proof of stake does away with miners and replaces them with “validators.” Instead of investing in energy-intensive computer farms, you invest in the native coins of the system. To become a validator and to win the block rewards, you lock up—or stake—your tokens in a smart contract, a bit of computer code that runs on the blockchain. When you send cryptocurrency to the smart contract’s wallet address, the contract holds that currency, sort of like depositing money in a vault.

In the proof-of-stake system Ethereum is slowly moving to, you put up 32 ether—currently worth $100,000—to become a validator. If you don’t have that kind of spare change on hand, and not many people do, you can join a staking service where participants serve as validators jointly.

An algorithm selects from a pool of validators based on the amount of funds they have locked up. The more you stake, the greater your chance of “winning the lottery.” If you’re chosen and your block is accepted by a committee of “attestors”—a group of validators randomly chosen by an algorithm—you are awarded newly minted ether.

Ethereum’s proponents claim that a key advantage proof of stake offers over proof of work is an economic incentive to play by the rules. If a node validates bad transactions or blocks, the validators face “slashing,” which means all their ether are “burned.” (When coins are burned, they are sent to an unusable wallet address where nobody has access to the key, rendering them effectively useless forever.)

Proponents also claim that proof of stake is more secure than proof of work. To attack a proof-of-work chain, you must have more than half the computing power in the network. In contrast, with proof of stake, you must control more than half the coins in the system. As with proof of work, this is difficult but not impossible to achieve.

Ethereum’s proof-of-stake system is already being tested on the Beacon Chain, launched on December 1, 2020. So far 9,500,000 ETH ($37 billion, in current value) has been staked there. The plan is to merge it with the main Ethereum chain in the next few months.

A risky move

None of this comes without risks. Ethereum’s switch to proof of stake is an enormous undertaking. Thousands of existing smart contracts operate on the Ethereum chain, with billions of dollars in assets at stake.

And though staking is not as directly damaging to the planet as warehouses full of computer systems, critics point out that proof of stake is no more effective than proof of work at maintaining decentralization. Those who stake the most money make the most money.

Proof of stake also hasn’t been proven on the scale that proof-of-work platforms have. Bitcoin has been around for over a decade. Several other chains use proof of stake—Algorand, Cardano, Tezos—but these are tiny projects compared with Ethereum. So new vulnerabilities could surface once the new system is in wide release.

At Ethereum’s annual developer conference, its founder tells us why his technology can only be truly decentralized if it stops depending on him.

As Ethereum transitions to its new protocol, another risk is that a group of disgruntled miners could decide to create a competing chain. All of the smart contracts, coins, and NFTs that exist on the current chain would be automatically duplicated on the forked, or copied chain.

Something similar happened in 2016, after Ethereum developers rolled back the blockchain to erase a massive hack. Some community members were so upset they kept mining the original chain, resulting in two Ethereums—Ethereum Classic and what we have today. If it happens again, the success (and mining power) behind any competing version of Ethereum will depend on the value of its coin in the open markets.

Ethereum needs to move to proof of stake so it doesn't further exacerbate the environmental horrors of Bitcoin. The question is, will its new system fulfill all the promises made for proof of stake? And how decentralized will it really be? If a public blockchain isn't decentralized, what is the point of proof of anything? You end up doing all that work—consuming vast amounts of energy or staking all those coins—for nothing other than maintaining an illusion.

by Amy Castor