Ethereum Centralization Debate Rages on After Much-Hyped Upgrade

Some crypto watchers turn to industry measure to weigh change
Nakamoto Coefficient for blockchain has shrunk after the Merge

By Olga Kharif

September 23, 2022 at 4:00 AM EDT Updated on September 23, 2022 at 7:09 AM EDT

From Crypto

The high-profile upgrade of the world’s most commercially important crypto network was supposed to make it less centralized and vulnerable to attack. A little more than a week after the enhancement, industry observers fear it may have the exact opposite effect.

Crypto enthusiasts are poring over an obscure indicator birthed during the early days of crypto, dubbed the Nakamoto Coefficient, to evaluate the consequences of the ‘Merge’. The event replaced Ethereum’s power-hungry computers called miners with so-called validators that pledge Ether tokens as security so they can profit from ordering network transactions.

Under the old proof-of-work format, 51% of miners would have needed to join together for a successful attack on the blockchain. Now, only about a third of validators need to join forces to gain control, according to Leland Lee, who helped formulate the indicator, which is named after Bitcoin’s supposed anonymous creator, Satoshi Nakamoto.

The metric tracks the minimum number of participants in various important network support roles—code developers, parties ordering transactions, wallets and so on -- that would have to collude or be compromised to take over a blockchain. The higher its coefficient value, the more decentralized a blockchain is. The Nakamoto Coefficient was proposed in 2017 by Lee, now head of platform and investor at Galaxy Digital, and venture capitalist and former Coinbase Global Inc. Chief Technology Officer Balaji S. Srinivasan.

“The safety threshold for classical consensus protocols, including the protocol used in Ethereum 2, can be no higher than 33%,” Emin Gun Sirer, creator of the rival Avalanche blockchain and a former Cornell University professor, said in an email. “We know for certain that an attacker who controls 34% of the state can cause safety failures, including double-spends. The actual threshold for the Ethereum protocol is likely to be lower than 33%, because of the way validators are divided into slots.”
Alex Stokes, a researcher at the Ethereum Foundation, which supports the blockchain, said that a 33% or 34% attack “refers to the theoretical worst-case scenario.” That isn’t realistic given how geographically distributed Ethereum’s community is, he said. An attacker could also end up losing his entire stake of coins, something that few may want to risk. A more realistic threshold to pull off an attack that could wrestle control of the blockchain and potentially alter the code is 66% of validators, Stokes said.

Even so, Lee estimates 34% should be the threshold when considering Ethereum’s Nakamoto Coefficient. Before the upgrade, between three and five mining pools would have had to collude to be able to double-spend the same coin, for example. Currently, two validator addresses -- Lido and Coinbase -- control about 43% of Ethereum validator pools, according to block explorer Beaconcha.in.

“Ethereum is much more centralized than it was a week ago,” Lee said.

That’s a potentially troubling development as regulators circle Ether. Back in 2018, a US Securities and Exchange Commission official said Ether wasn’t a security thanks in part to the network’s “decentralized structure.” Now that structure may have been upended. SEC Chairman Gary Gensler said last week, without specifically referring to Ethereum by name, that proof-of-stake systems could fall under his agency’s securities rules.

That could have huge implications, not just for Ether investors, but also Ethereum users, who usually have to buy the tokens to use many of the network’s applications. Ethereum hosts nearly 3,500 decentralized apps and millions of users.
Merge Letdown
Ether has slumped since software upgrade

![Chart showing Ether price fluctuations]

Source: Bloomberg

READ MORE:

Now That Ethereum's Merge Happened, What's Next?

Ethereum Faces 'Blockchain Trilemma' as 'Merge' Mania Cools

Why Ethereum's Merge Means Crypto That's Much Greener: QuickTake

Lee pointed out that the Nakamoto Coefficient is just one of many ways to measure decentralization. The top two mining pools ordered transactions in 43% of blocks in the two weeks leading up to the Merge. In a few days since, the two big validator addresses -- Lido and Coinbase -- have ordered transactions in 42% of the blocks, according to researcher Chainalysis. That would suggest that centralization has decreased slightly. Because Lido is a decentralized organization, controlled by its members and comprised of thousands of independently-owned nodes, it's less likely to become an attack vector, some argue. Other observers see it differently.

“The Nakamoto Coefficient of Ethereum post-Merge is embarrassingly low,” said Kyle Samani, co-founder of Multicoin Capital, which owns Sol, a native coin of Solana, which competes with Ethereum. It's “the worst of all major chains.”
Ethereum’s proof-of-stake system also has another weak point, said Campbell Harvey, a finance professor at Duke University. Newly created entities called builders are packaging transactions into blocks and relaying them to validators. Currently, one relay, by Flashbots, handles more than 80% of all builder-made transactions, according to tracker Mevboost.org. Flashbots is also a builder, which accounts for the lion’s share of builder-built blocks.

“The world has gotten more complicated after proof-of-stake,” Lee said. “Quantifying what Nakamoto Coefficient was was much easier.”