What Is the Nakamoto Consensus?

By

Decentralized Dog

Published on:
November 25, 2020

The Nakamoto Consensus gave birth to blockchain as we know it — what makes it so different from consensus mechanisms that came before it?

Table of Contents

The Nakamoto Consensus, as its name implies, was created by Satoshi Nakamoto, Bitcoin's pseudonymous founder, in the Bitcoin white paper.

It can be considered the solution to the Byzantine Generals Problem, a thought experiment that deals with a key question in computer science: is it possible to form a consensus in a computer network of independent, distributed nodes? — The Nakamoto Consensus says that yes, indeed it is.

The Nakamoto Consensus is a set of rules that verifies the authenticity of a blockchain network, using a combination of the proof-of-work consensus algorithm on a Byzantine Fault Tolerance (BFT) peer-to-peer network.

Prior to Satoshi's creation of the Nakamoto Consensus, Byzantine Fault Tolerance was used in peer-to-peer networks to maintain their authenticity for a variety of cryptography-related projects, and even some early forms of digital currency.

However, there were problems — in just a Byzantine Fault Tolerant system, the voting system for consensus requires a rotating election of leaders. If a leader acted maliciously, as leaders are known to do, then they could be removed from the network by a vote from the other nodes. In the case of Bitcoin (and for the idea of a digital currency in general) this individual removal of leaders through a voting process would pose a huge problem when it came to scaling.

Why Proof-of-Work Matters

Satoshi's addition to using BFT on a P2P network was to add the idea of a proof-of-work consensus mechanism, where nodes had to mine (along with other things we will explain below!) to create a fully trustless, decentralized network.

Proof-of-work, in simplest terms, is the idea that **miners** support the (Bitcoin) network with literal "work," i.e. their computing power. In more complex terms, PoW is when full nodes compete to mine "blocks" faster than other nodes — the fastest miner receives the block reward, thus creating new Bitcoin, as well as an incentive to keep participating in the network. In other words, it creates an environment where honest nodes thrive and malicious nodes are discouraged.

Proof-of-work blockchain technology also prevents the possibility of double spending, since the time-stamped blocks on the blockchain makes it immutable — the longest chain is the valid chain, since it is supported by the majority of the miners' computing power.

In the Nakamoto Consensus, there is no block selection "voting" process like in BFT-only networks; instead, the miners compete to solve a cryptographic puzzle, and the winner (and their new block) is then accepted as valid across the entire network of miners. The mining computation process is a little bit like a lottery: it's not possible to tell who will find the solution, meaning that miners have to be willing to honestly invest time and money in their participation to validate the next block.

Another aspect of the Nakamoto Consensus comes from Satoshi putting a hard cap on the amount of Bitcoin — there will only ever be a total of 21 million of the cryptocurrency in circulation. This creates artificial scarcity, which again adds to the incentives for miners to participate in the network.

The Nakamoto Consensus Beyond Bitcoin

Looking beyond **Bitcoin**, the Nakamoto Consensus created the foundation for the large blockchain and cryptocurrency community that exists today. By solving the Byzantine Generals Problem, Satoshi created a consensus model that can be used for almost an infinite number of use cases besides Bitcoin — blockchain's potential has reached industries ranging from banking, to real estate, to voting, and even to health care.

Tldr; the Nakamoto Consensus answers much more than just a computer science thought experiment: it has been shown to provide real world value.