Can I really trust the blockchain?

Different blockchains leverage certain techniques to validate that their blocks are to be trusted. What follows is a high-level overview of some of the common approaches.

Proof-of-Work (PoW) protocols task nodes with performing complex mathematical computations. This computation is typically referred to as “mining,” and can be extremely costly to perform—both in that it requires powerful machines, and those machines use up a ton of energy.

This process is effective because of the cost-benefit structure that mining imposes on participants. While mining for a solution is extremely difficult, verifying that a solution is correct is extremely easy. The first computer to solve for each solution is typically rewarded with the chain’s custom token, creating incentive for honest actors to participate. The more nodes that participate in the process, the more challenging the computation becomes, and the more difficult it becomes for those acting in bad faith.

Proof-of-Authority (PoA) is a more traditional concept, as an “authority node” awards different nodes the role of “validators,” which are then tasked with verifying transactions in blocks. This process introduces slightly more risk, as the authority node (and any individual validator) is at risk of an attack or failure, but it is a common solution for closed or permissioned blockchains.

Proof-of-Stake (PoS) is another algorithmic solution, but instead of requiring effort in the form of mining (like PoW), it determines a computer’s trustworthiness by its “stake” in the chain’s validity. To validate a new block, nodes must first invest their coins into the system. Nodes will lose their investment if they act in bad faith.

PoS is much quicker and more energy-efficient than a PoW protocol, but it is still imperfect. PoS is vulnerable to the “nothing at stake” problem, in which the investment is insufficient to act as a disincentive to bad behavior. This type of “pay to play” scheme is also a shortcoming for a blockchain that aspires to be truly open and democratic.

Raft is an historically relevant protocol that became popular because it is an easily understood and implemented variant of Paxos. In Raft, a node is designated as either a leader, a follower, or a candidate (in the event a leader is unavailable); and elections favor the most updated candidates. Leader nodes initiate and coordinate log replication through a regular “heartbeat” update. An example implementation is Quorum, JP Morgan’s Ethereum fork.

Experimental Protocols

SHAFT (GRANDPA) is an emerging scheme that ensures progressive finality in an adaptive way. Currently in use by Polkadot, SHAFT (GRANDPA) could dramatically reduce costs with its flexibility to partitioning, replicating, and distributing data.

Snowflake to Avalanche is a new framework of protocols that separate consensus from governance. Combining conventional gossip protocols with cycles of subsampling, Avalanche crowdsources truth, and can adapt to changing ecosystems.

Tendermint & Rhododendron are examples of a different group of protocols that—unlike the other examples included here—determine validity of each block before another block can be proposed.