

Cutting-Edge Consensus Algorithms in the Blockchain Industry

As a field of computing and as an industry, blockchain technology has moved far beyond that of Bitcoin, not just in magnitude but in sophistication. While Bitcoin did (and to an extent still does) a fantastic job of introducing blockchain and decentralization to the public, it only scratches the surface of what is possible within the field. This is because Bitcoin's consensus algorithm, Proof of Work, is becoming outdated. The system works well, but it is hugely inefficient in terms of electricity usage, cost of mining tools, and scalability. Since Bitcoin's creation, the industry has moved much further and expanded its horizons towards other consensus algorithms such as Proof of Stake, the second most popular mechanism after Proof of Work. Newcomers to crypto and blockchain might initially think that these are the only two ways of building and maintaining a blockchain, but they would be wrong. Here are three cutting-edge consensus algorithms which every blockchain enthusiast should examine.

Velas - AI-Enhanced Delegated Proof of Stake

The team behind [Velas](#) created their own consensus algorithm which allowed them to use artificial intuition (a subset of artificial intelligence) to run their blockchain. Their algorithm is known as AI-Enhanced Delegated Proof of Stake. As the name suggests, it is a variation on Proof of Stake but its differences are striking. Rather than relying solely on human intervention, Velas uses AI neural networks to determine which blocks should be added to the blockchain, when block rewards should be unlocked, and how fast or slow the blockchain should run. The idea behind this is that humans are too error-prone to safely run a blockchain alone, and that employing a pre-trained and knowledgeable system to handle some of the work makes the ecosystem more secure and robust.

Cosmos - Byzantine Fault-Tolerance

[Cosmos](#) is a project which is trying to enable individual blockchains to communicate with each other. It does this through the use of Byzantine Fault Tolerant consensus protocols which facilitate easy integration. Protocols like this are necessary for creating larger and more magnificent blockchains because they are able to combat the problems of trustworthiness and miscommunication. To understand why this is not possible with other traditional consensus algorithms it is best to read up on the [Byzantine Generals' Problem](#), an age-old issue within computer science which is unfortunately too complex for the scope of this discussion.

Grin - Cuckatoo Cycle + Proof of Work

[Grin](#) is a privacy-based cryptocurrency which promises security of information as well as scalability. It runs on the [MimbleWimble](#) protocol, which is essentially a Proof of Work consensus algorithm with some fundamental changes. Instead of using the Hashcash framework which most Proof of Work cryptocurrencies including Bitcoin use, the team developed their own; known as the Cuckatoo Cycle. It uses less processing power, and offers faster transaction speeds. If this version of Proof of Work is shown to be successful and

scalable, it could become the norm within the crypto industry as it is similar enough to the Hashcash variant that Bitcoin uses to be easily understood. Plus it is mining-friendly, and while that might not seem all too important, bear in mind that miners have a huge influence on which technologies gain prominence.

These three projects are only the tip of the iceberg when it comes to innovation within the blockchain industry. There are many, many more developers out in the ecosystem who are exploring the limits of the technology and producing cutting-edge solutions. Sometimes it can be complex to understand exactly what these innovations are due to the use of technical language, but for anybody who is truly interested in what blockchains are capable of, it is certainly worth learning.