Name: Fast difficulty in PoW consensus explainer

Category: Consensus

Paper title: '*Fast Difficulty Adjustment in Proof-of-Work Consensus*'

Authors: Juan Garay, Aggelos Kiayias, Yu Shen

Paper: https://eprint.iacr.org/2026/1116.pdf

Fast difficulty adjustment in proof-of-work consensus mechanisms explainer

Proof-of-Work (PoW) blockchains regularly adjust the level of difficulty, meaning the computing power required to add a new block to the chain. This is done so the network can produce blocks at a steady rate and remain secure, even as the number of active participants rises and falls. When participation changes quickly, the network can be either over- or under-secured for a long period of time between these adjustments.

Think of it like a call center that adjusts the staffing levels based on the volume of calls, but one that only reviews the workload at regular intervals. If there is a surge in call volume, the center is understaffed for a long period of time before the next review happens.

What the research unlocks

Research co-authored by IOG's Aggelos Kiayias, alongside Juan Garay and Yu Shen, asks whether the speed of adjustment can be made **fast**: namely, the ability to recalibrate in a fixed, short window, rather than needing that window to stretch out over time. Prior work, including the Bitcoin blockchain protocol, required that window to be at least proportional to the security parameter length. This new research proposes a way to shorten this to the lowest asymptotic limit. A novel PoW protocol is proposed that can adjust its difficulty level on a short schedule, holding steady no matter how the participation rate changes, and mathematically guaranteed to work. Formally, the adjustment can take place in constant time independent of the security parameter.

How it works

The key is how participants settle on a difficulty level. Rather than everyone agreeing on an exact level to stay in sync, an average estimate is used. Specifically, this protocol runs several blockchains in parallel and has each participant estimate difficulty from data across all of them, then throws out the highest and lowest estimates before settling on a number that only has to be approximately correct. This approach ensures that everyone's version is close enough to work together, even though the difficulty levels are not identical. Most importantly, no consensus on the estimate is required. This enables participants to progress fast without being held back to verify that everyone has reached a common understanding of the correct difficulty level.

Why it is secure, not just fast

Speed alone is one factor, but not at the cost of security. In a short adjustment window, it is possible for one participant, or even an attacker, to look far more active than everyone else purely by chance, which could otherwise be used to throw off the next difficulty calculation. The researchers prove that even though participants only approximately agree, difficulty estimates stay reliably close together, adjustment after adjustment, keeping the network stable throughout.

What this enables

A faster, secure way to adjust difficulty isn't the end goal, it's a building block. This protocol also supports a consensus mechanism and a full ledger system that can confirm transactions quickly, even while the number of participants is changing rapidly. For the first time in proof of work based protocol it is possible to have fast settlement paired with fast difficulty adjustment as well.

Learn more

More details on this concept of fast difficulty adjustment in a new PoW protocol can be found in the research paper '*Fast Difficulty Adjustment in Proof-of-Work Consensus*' by Juan Garay, Aggelos Kiayias, and Yu Shen.