Proof-of-Work FAQ

Original:
https://www.btcc.com/en-US/academy/crypto-basics/proof-of-work-faq

Why do Miners Follow the Rules?

Miners earn bitcoin rewards for every block for which they find the solution. This is what drives them to mine in the first place.

This monetary reward also drives them to follow the rules – not double-spending their money, for instance. Say Alfred the Miner finds a winning hash for a block. If Alfred submits the solution with the block but breaks rules within the block – say, spends coins more than once – the rest of the Bitcoin network will reject Alfred's block. Alfred will lose all the bitcoin he should have won. The threat of losing the bitcoin rewards keeps miners honest.

[Download App for Android](#)   [Download App for iOS](#)

Why is Proof-of-Work Needed?

The goal of proof-of-work is to prevent users from printing extra coins they didn't earn, or double-spending. If users were able to spend their coins more than once, it would effectively make the currency worthless.

In most digital currencies, this problem is easy to solve. The bank that is in charge of the system keeps track of how much money each person has. If Alice sends Bob $1, then the bank deducts $1 from Alice and gives $1 to Bob.

But in cryptocurrency there isn't such an entity. Proof-of-work provides a solution.

Who Invented Proof-of-Work?

Bitcoin creator Satoshi Nakamoto invented proof-of-work to get Bitcoin off the ground. No one knows who Nakamoto is, or whether the name is an alias.

[Download App for Android](#)   [Download App for iOS](#)

What are the Downsides of Proof-of-Work?

There are at least a few problems with proof-of-work:

- **High energy use**: Bitcoin uses as much energy as all of Switzerlandbecause of proof-of-work. And its energy use is increasing as more miners join the hunt for bitcoins, though some of this is powered by renewable energy.

- **51% attacks**: If one mining entity is able to accumulate 51% of Bitcoin's mining hashrate, it can then flout the rules temporarily, double-spending coins and blocking transactions.

- **Mining centralization**: Proof-of-work is all about creating a currency without one single

entity in charge. That said, in practice the system is somewhat centralized, with just three mining pools controlling almost 50%of Bitcoin's computational power. Developers are attempting to at least alleviate this issue, however.

Why does More Mining Power Mean More Security?

The more computational power being poured into securing Bitcoin, the more resources a potential attacker needs to amass in order to successfully attack Bitcoin.
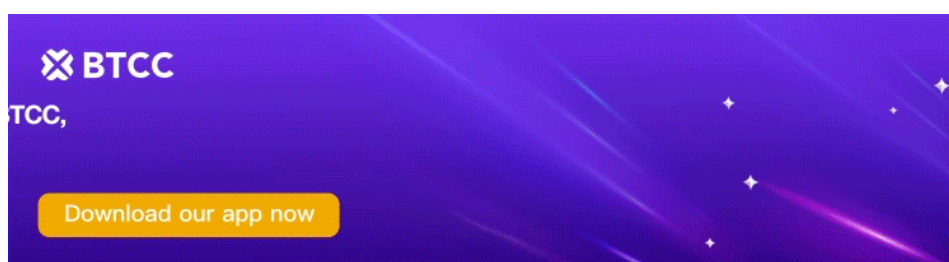
Which Cryptocurrencies Use Proof-of-Work?

Most cryptocurrencies use proof-of-work, though some are experimenting with other ways of securing their networks. The most popular cryptocurrencies tapping proof-of-work include:

- Bitcoin
- Ethereum
- Bitcoin Cash
- Litecoin
- Monero