# [ PDF Database Document ] - BTCC Cryptocurrency Exchange

Original:
https://www.btcc.com/en-US/academy/crypto-basics/a-brief-glance-at-proof-of-work

**A Brief Glance at Proof-of-Work**

## What is Proof-of-Work?

**Proof-of-work is the blockchain-based algorithm that secures many cryptocurrencies, including Bitcoin and Ethereum.**

Proof-of-work is the algorithm that secures many cryptocurrencies, including Bitcoin and Ethereum. Most digital currencies have a central entity or leader keeping track of every user and how much money they have. But there's no such leader in charge of cryptocurrencies like Bitcoin. Proof-of-work is needed to make the online currency work without a company or government running the show.

More specifically proof-of-work solves the "double-spending problem," which is trickier to solve without a leader in charge. If users can double-spend their coins, this inflates the overall supply, debasing everyone else's coins and making the currency unpredictable and worthless.

Double-spending is an issue for online transactions because digital actions are very easy to replicate, which is what makes it trivial to copy and paste a file or send an email to more than one person.

Proof-of-work makes doubling digital money very, very hard. It's much what it sounds like: "proof" that someone has done a significant amount of computations.

# How does Proof-of-Work Work?

Bitcoin is a blockchain, which is a shared ledger that contains a history of every Bitcoin transaction that ever took place. This blockchain, as the name suggests, is composed of blocks. Each block has the most recent transactions stored in it.

Proof-of-work is a necessary part of adding new blocks to the Bitcoin blockchain. Blocks are summoned to life by miners, the players in the ecosystem who execute proof-of-work**.** A new block is accepted by the network each time a miner comes up with a new winning proof-of-work, which happens roughly every 10 minutes.

Finding the winning proof-of-work is so difficult the only way to provide the work miners need to win bitcoin is with expensive, specialized computers. Miners will earn bitcoin if they guess a matching computation. The more computations they churn out, the more bitcoin they are likely to earn.

What computations are the miners making exactly? In Bitcoin, miners spit out so-called “hash,” which turns an input into a random-looking string of letters and numbers.

The goal of the miners is to create a hash matching Bitcoin’s current “target.” They must create a hash with enough zeroes in front. The probability of getting several zeros in a row is very low. But miners across the world are making trillions of such computations a second, so it takes them about 10 minutes on average to hit this target.

Whoever reaches the goal first wins a batch of bitcoin cryptocurrency. Then the Bitcoin protocol creates a new value that miners must hash, and miners start the race for finding the winning proof-of-work all over again.

***Read more:*** ***Proof-of-Work FAQ***