Introduction

So what exactly is a cryptographic hash function?

To set the stage for a clearer understanding, I'll start by discussing Bitcoin, which is really now getting increasing acceptance .

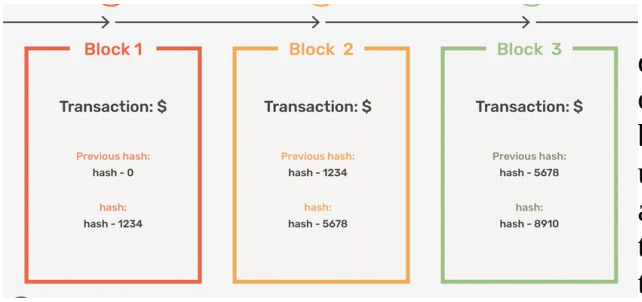
A decentralized digital money is bitcoin. It is a kind of money that is entirely digital and is seen as decentralized since it may be purchased, sold, or traded without the involvement of a middleman like a bank or the government. Because of this, it is said to function as a peer-to-peer system where people may transact with one another directly.

How can these people demonstrate their transactions, though, in the absence of a centralized controlling body?
How can we be certain that they paid for what they claimed to have?
Or, even better, how do we even know they had the money?

The is known as the double spending issue . It is the chance that virtual currency will be used more than once. This type of money is entirely virtual, making it difficult for anybody to simply manufacture copies of it and use it several times, even those who have the expertise and processing ability to do so. Traditional physical currencies can prevent this since they are difficult to duplicate. People may also more easily demonstrate its legitimacy and previous ownership. However, with relation to virtual currencies, this is not the case.

Fortunately, the Proof-of-Work was a solution created by Satoshi Nakamoto, the person who invented Bitcoin, in October 2008.

How does Proof-of-Work operate and what is it?



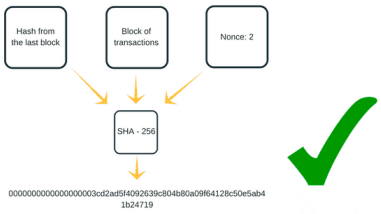
Bitcoin and other cryptocurrencies employ the consensus mechanism known as "Proof-of-Work" to confirm transactions. I need to establish the idea of a blockchain first before I can explain how this is utilized. Therefore, Bitcoin is based on what is known as blockchain technology, which is a public ledger that records every Bitcoin transaction that has ever taken place.

It is made up of a number of blocks, each of which contains the information mentioned above, a cryptographic hash of the block it extends or the prior transaction, and a timestamp indicating the moment the block was created.

So how do the blockchain and proof-of-work connect to one another?

Well, a block must first have a legitimate Proof-of-Work before it can be added to the blockchain, and this can only be done by resolving cryptographic puzzles. The process of mining bitcoins is known as mining, and the individuals who do it are known as miners.

The miner that creates a valid Proof-of-Work first will receive a free Bitcoin as a reward and recompense for the processing power that he or she used. Miners might be any network participants. However, it must be noted that only those with extremely powerful computing power are likely to solve these extremely complex cryptographic puzzles. This is especially true now that large Bitcoin mining farms have been established, equipped with pricey and quick computing resources, making mining more and more difficult and expensive.



But what exactly are these cryptographic issues?

A miner must create a hash that meets a precise criterion specified by the network protocol in order to locate a valid block. The hash of the previous block, the information about the set of transactions that will be added to the blockchain, and a nonce—a number that is only used once—must all be hashed. This nonce is iteratively increased within the block until its value provides the block's hash with the appropriate quantity of zero bits, also known as the target, as needed by the network protocol.

The SHA-256 hash algorithm is the one utilized by Bitcoin.
It is called Secure Hash Algorithm, or SHA; the 256 just denotes the length of the output string, which is 256 bits.