There was once a deeply influential white paper from Satoshi Nakamoto. The ideas introduced there would go on to energize the cryptocurrency community. A brief summary of that white paper is presented below.

Money can be stored on your computer. In fact, any computer file can be used as a unit of currency. For instance, you could make a Word file called "1 dollar.docx" and treat it as a real dollar bill. The problem is that no one would want to use it. That is because you can get away with making as many "1 dollar" documents as you wish.

If we used a trusted third party, like a bank, then the above problem with duplicating money would not exist because banks were widely regarded as being reliable.

So, could we find a way to store money on computers that people would want to use and that didn't rely on a third party such as a bank? This had been a difficult problem for some time. What Satoshi did was to give a solution to this in a whitepaper that introduced Bitcoin to the world.

Overview of Whitepaper

In the whitepaper, Satoshi described how to use certain data structures to represent past transactions. These transactions are stored into ledgers. Satoshi then proposed to widely broadcast these ledgers and to make them harder to fabricate.

To widely broadcast these ledgers, you need to transmit them so that they can be stored across entire networks of computers. To make fabrication impractical, Satoshi: (1) stacked stored transactions on top of one another; (2) had these networks favor ledgers with the most transactions; and (3) made the process of such stacking very computationally intensive.

The idea is that if a group of crooks tried to fabricate some transaction, they would have difficulties because their ledger would be short on transaction history compared to other, well established, ledgers in the network.

Proof of Work

Satoshi made the process of such stacking computationally intensive by introducing a protocol known as Proof of Work. It involves pitting computers in the network against one another in various computing contests.

Proof of Work ensures that transactions in the ledger worked on by the largest number of computers on the network are recognized faster than transactions in the other ledgers. Therefore, ledgers with the longest transaction history are secure from fraudulent groups.

In the whitepaper, Satoshi also introduced systems of incentives, including one for participants in the network to support Proof of Work. This is useful because with incentives, enough people are incentivized to improve the reliability of the network.

At some point, Satoshi left without a trace. To this day, no one knows who this individual was. It is not even known if Satoshi represented one person. We are now left with an interesting idea, a cryptocurrency market that is exploring these ideas and their implications.