The Problem With Bitcoin

Everybody Wins

Willem L. Middelkoop
Dec. 9, 2024

A few days ago the value of a single Bitcoin briefly surpassed $100K, a milestone that seemed unimaginable just some years ago. I wonder how durable the ever growing love for Bitcoin is. Let's have a closer look at the mechanisms underpinning the world's most famous cryptocurrency.

Bitcoin's Brilliance

Described in a paper, Bitcoin was introduced in 2009 by an anonymous entity known as Satoshi Nakamoto. In this paper an alternative for a cash system with central control (e.g. a central bank) is given using software that runs on multiple computers (or peers) owned by different organisations and people.

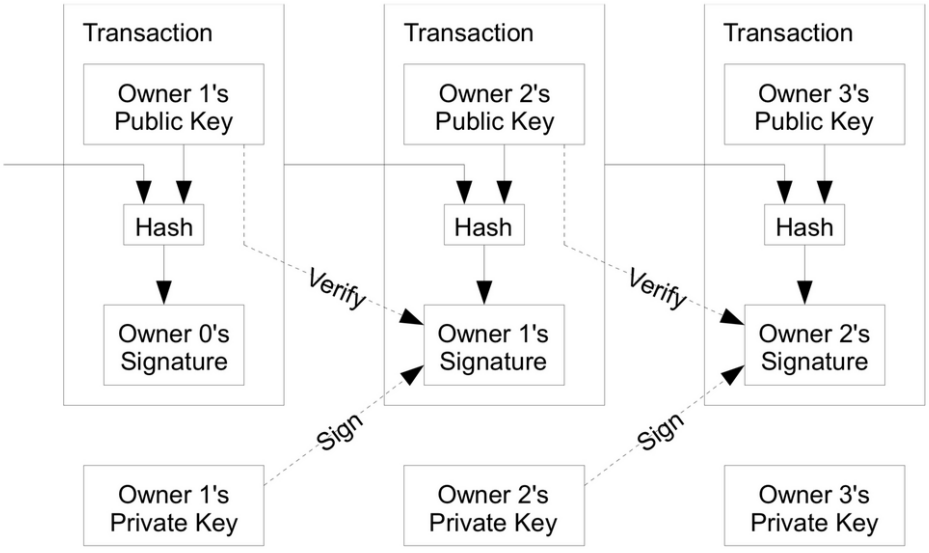
Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Abstract from Satoshi Nakamoto's original paper (2009)

Each peer in the network is able to track *all* transactions using cryptographic signing. Transactions are signed subsequently where the output of preceding transactions form the cryptographic input for new ones: forming a chain, the blockchain.



The blockchain principle visualised: output from previous transactions form the cryptographic input for new ones

Over time, Bitcoin has grown from a niche technology to a widely recognised financial asset. As of 2024, over 52 million unique Bitcoin addresses hold balances, highlighting its expanding adoption globally. Bitcoin's value, initially negligible at its 2009 launch,

set a new 'all time high' at $100,000 in December 2024, though it remains volatile. The cryptocurrency has gained traction as both a speculative asset and a financial tool, especially in regions with unstable currencies or limited banking access.

2009-2024: Bitcoin's rise in value is hard to ignore

While I appreciate the underlying cryptographic technology as an alternative for fiat money, I do think that the thought of Bitcoin's value going go up indefinitely is problematic. As long as prices go up, everybody is a winner - but it requires a (nearly) constant influx of new money. Where will Bitcoin's price stabilise? Nobody really knows!

Tulip Mania

In a way Bitcoin's current price rising reminds me of the Dutch Tulip Mania, a financial phenomenon in the Dutch Golden Age (1630s), which is often described as one of the first recorded economic bubbles. It revolved around the speculative trading of tulip bulbs, which became highly sought after. During the height of Tulip Mania, many investors operated under the assumption that tulip prices would continue to increase due to the strong demand and limited supply of rare bulbs, much like today's view on Bitcoin. This belief was fuelled by stories of extraordinary profits and the rapid rise in prices. However, when confidence in the market faltered in 1637, prices collapsed sharply, leading to financial losses for many speculators.

Yesteryear's speculative trading: The Dutch Tulip Mania

Dependency on Exchanges

Bitcoin's role as a "store of value" is fundamentally tied to the ability to exchange it for fiat currencies, as its widespread use in everyday transactions is limited. Unlike cash, Bitcoin is not universally accepted for direct purchases, necessitating reliance on exchanges to convert it into spendable forms of capital.

This reliance introduces bottlenecks, as exchanges are subject to increasing regulatory scrutiny, particularly through stringent "Know Your Customer" (KYC) and anti-money laundering (AML) procedures. These regulations add layers of centralised oversight and reduce the pseudonymous nature originally associated with Bitcoin. As a result, while Bitcoin itself operates on a decentralised network, its practical use remains partially constrained by centralised infrastructure.

A sudden shift in sentiment about Bitcoin's value could lead to a mass sell-off, overwhelming exchanges with "cash-out" requests. This raises concerns about whether exchanges hold sufficient fiat reserves to honour withdrawals.

Conclusion

As long as Bitcoin's price is rising everybody will be happy, but I suspect there is a limit to its growth. Will Bitcoin's price eventually stabilise or will it drop sharply once the influx of new money stops? Be careful with exposing yourself to this volatility, nobody really knows what the peak valuation of Bitcoin will be or when it will be reached!

Disclaimer: This is not financial advice, please do your own research.