A Review of “Bitcoin -A Peer-to-Peer Electronic Cash System” by Satoshi Nakamoto

JRMDB Karunarathne

The University of Colombo, School of Computing,

***Abstract*— This review discusses the Bitcoin whitepaper[1], the background why such a paper was needed, its strengths and weaknesses and its effect on humanity.**

***Keywords*— Bitcoin, Block Chain, Electronic Cash, Review**

I. Introduction

By 2008 the United States was facing ‘the great recession’ which had severe effects on the economy, quality of life and poverty levels of the average American. This led to distrust in the banking system which had failed the public and the world needed a transaction system which did not rely on banks. Thus a person under the pseudo name Satoshi Nakamoto published the Bitcoin Whitepaper in 2008. Bitcoin officially started as an electronic currency when Nakamoto mined the starting block of blockchain in 2009.

II. Paper Discussion

The Bitcoin whitepaper consists of 12 sections. The first 4 sections discuss the need for a peer-to-peer electronic currency based on cryptography rather than blind trust in the banking system and the theory behind Bitcoin.

Nakamoto argues that an electronic coin is nothing more than a chain of signatures based on commonly known cryptographic principles. To confirm the ownership and to transfer these coins cryptographic signatures will be used. Nakamoto also argues that if all transactions are public this electronic cash system will not need a mint, a central authority and will also be a solution to the double-spending problem.

Nakamoto then discusses the problems that could arise when deploying a public ledger. All nodes, the participants of the blockchain must agree on a single history. For that Nakamoto proposes a timestamp server to identify which transactions were made first. Similar transactions will be bundled and hashed over the previous transactions recursively thus giving birth to the blockchain. To implement a reliable blockchain, Nakamoto proposes a proof of work system where nodes should do a rigorous number of calculations that are hard to do but easy to prove. Only the nodes who do the required amount of transactions will be able to add a block to the blockchain and these nodes will be rewarded and that's when coins will be issued. Nakamoto argues that the longest chain should be accepted as the correct blockchain as it contains the most amount of proof of work and in the Calculations section of the whitepaper Nakamoto mathematically proves that for a fraduelent party creating a fake blockchain is comptuationally impossible.

In the sections to follow Nakamoto discusses the network of the blockchain, how the miners should be rewarded, how to save disk space once the blockchain grows, how simple transactions are done, the divisibility of Bitcoin and the privacy offered by Bitcoin. Nakamoto also mentions that as long as the majority of the nodes are honest nodes Bitcoin will not fail.

III. Analysis

The Bitcoin whitepaper was published by Satoshi Nakamoto, whose true identity is still unknown and this paper was published on the cryptography mailing list of metzdown.com[2]. This paper provides a solution to an existing problem and is presented with proof that it will work and how to maintain the blockchain. The paper has a good flow and is well audience specifically written. The paper yet has several weaknesses like no mention of future work and Nakamoto does not clearly discuss macro transactions which was a major motivation behind the paper.

IV. Conclusion

The Bitcoin whitepaper is inarguably one of the most controversial, effective and practical publications of all time. This paper is considered the Bible of all cryptocurrencies. This paper has paved the way for a high-functioning breed of crypto currencies resulting in private and efficient transactions and also adverse effects like the boost of crime on the dark web and bad environmental impacts.

References

[1] S. Nakamoto, *Bitcoin.org*, 2022. [Online]. Available: https://bitcoin.org/bitcoin.pdf. [Accessed: 12- Jul- 2022]

[2] "cryptography Info Page", *Metzdowd.com*, 2022. [Online]. Available: https://www.metzdowd.com/mailman/listinfo/cryptography. [Accessed: 12- Jul- 2022]