A Review Paper on "Blockchain and Cryptocurrency Based Transaction Systems"

Sanjay Singh Rajpurohit[1], Talha Khan[2]
[1, 2]*Department of Information Technology, SSIPMT, Raipur (C.G), India*

***Abstract*—This paper provides a comprehensive and details of the current technological state of the Blockchain technology. The review outlines in details what is required for the Blockchain technology to function in development of cryptocurrency and the required factors for success. Conclusively, it is noted that the Blockchain technology in its current state still has way to go before the technology will reach a state considered sufficient for mainstream adoption.**

Keywords: Blockchain

I. INTRODUCTION

The theory of decentralized crypto-currencies (e.g. Bitcoin) have gained rapid recognition, often associated with statements such as a glimpse into our future. While the Bitcoin technology has been extensively studied, we believe that the concept of the Blockchain provides a new perspective on the already existing literature by looking at the various appliances of the underlying technology in a socio-economical setting prior to its previous literary focus within finance and economics.

While Blockchain represents a novel application on cryptography and information technology, researchers still lack to find the tipping point for the technology. Researchers agree that the Blockchain technology has certain features that is well applied within the financial industry, but still lacks to find the appropriate use of large scale Blockchain usage within modern society.

However, technologies such as automation, computing, robots and ultimately the Internet have been contributing immensely to progression and wealth of economies andcultures and thus expect that the Blockchain technology will provide further contributions.

II. OBJECTIVE

The goal of this paper is to conduct a literature review of the current literary landscape. We will look at the Blockchain technology andanalyzeprior literature in order to identify gaps in the current literature. Motivated by its technical and mathematical nature, previous research has focused exclusively on aspects of the technological infrastructure such as security, anonymity, scalability.

Due to the novelty of concepts and the underlying technologies, we provide a new overview on recent developments and related literature in this paper and strive to explore the related concepts in the literature. Through exploration of the concepts, we dive into the Blockchains utilization as a technological platform for an upcoming ecosystem of applications and software and look at the theoretical features of the technology as a foundation for this paper.

Thus, we seek to enhance the understanding of the technology in other contexts throughout the literature and explore the current contributions to the literature. This study has implications for both researchers and practitioners. For researchers we seek to identify a new branch of research that focuses on enablement of the Blockchain as a platform-centric technology for ecosystems to flourish.

III. SUMMARY

Transferring money online has always relied on banking systems to verify and authorize. This makes consumer information available to 3rd parties, while slowing down the transaction speed. The overhead for using a bank increases the transaction cost and limits the amount of money to be sent. Using cryptographic digital signatures to verify a publicly distributed ledger over a decentralized, peer-to-peer network, removes the need and expense of trusting financial institutions. The chain of distributed ledger is verified using Proof-of-Work algorithms to ensure double-spending doesn't occur.

IV. MECHANICS

A ledger, or record of credits and debits, is stored on a block where each transaction is given a timestamp and hashtag. These ledgers are made public, while being secured from tampering using cryptographic keys. The block is authenticated over a distributed network of independent nodes, validating receipts and timestamps to prevent double-spending. The network of peer nodes uses computational power to read and validate the accuracy of each recorded transaction and add new ones as they appear, in a process called mining.

When a transaction receives a hash with certain characteristics, a new block is created. The main (root) hash from the previous verified block is recorded with the new block, creating a chain of distributed ledgers. When a new

block is created, the validating node is granted ownership of the block. These blocks can be transferred using the cryptographic keys as digital signatures, giving the semblance of a currency. Any balance remaining on the ledger, after a transaction, is kept by the block owner as a transaction fee.

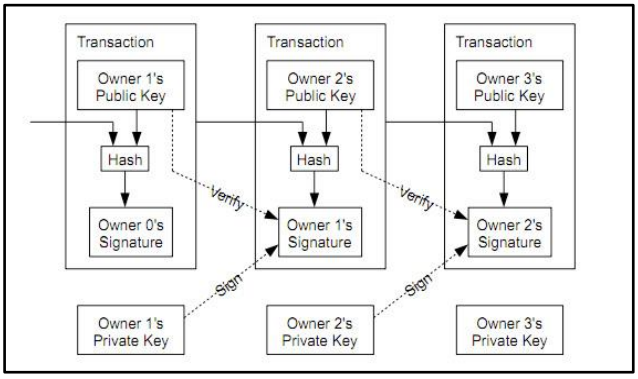

Fig. 1 Mechanisms involved in a transaction

The peer-to-peer network of miners validates the entire chain with each transaction. In order to function as a currency, however, transfer authentication must be processed quickly. In order to accomplish this, every transaction is verified by the network, but once consensus is reached, only the root node of previous blocks must be re-read. Block transactions must also allow for multiple inputs and outputs, increasing the memory requirements. Using a root hash system, based on a Merkel Tree model, stores only necessary information, reducing the data each node must validate.

V. SECURITY

The peer-to-peer network creates new blocks in the blockchain based on transaction verification. This occurs at randomly generated intervals, making it difficult to spoof. Since each block is re-authenticated by every node in the network, a hacker would have to recreate the entire chain in order to fool the network. Otherwise, nodes will detect the change and reject the fake block. If consensus is not reached across the network, the block is not authenticated.

VI. CONCLUSION

Bitcoin is a cryptographic currency for making electronic payments over a peer-to-peer network of decentralized nodes. This network records timestamped transactions using Proof-of-Work to verify accuracy, then publicly distributes the ledger in an ongoing chain. This revolution in exchanging value will bring a new paradigm in finance and payment systems. The use-cases for a secure public ledger are just being explored, but the blockchain is already changing how we think of money.

REFERENCES

[1]. Satoshi Nakamoto,"Bitcoin: A Peer-to-Peer Electronic Cash System", https://bitcoin.org/bitcoin.pdf, 1998
[2]. W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998
[3]. A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.