Building A Cryptocurrency The Digital Coin Using Blockchain Technology

Prashil Raorane[1] Abhishek Tukrul[2] Gautham Mudaliar[3] Dr.J.W.Bakal[4].

[1,2,3]*Department of Information Technology, Shivajirao S. Jondhale College Of Engineering, Dombivali.*

[1]prashilraorane19@gmail.com

[2]gauthammudaliar13@gmail.com

[3]tukrulabhishek@gmail.com

[4]j.w.bakal@gmail.com

Abstract: *In the world of information technology, blockchain technology is a newcomer. Bitcoin as a cryptocurrency has gotten a lot of attention since it was one of the first implementations. They represent the very core of modern cryptocurrency development, along with blockchain implementation with a focus on smart contracts. The aim of this paper is to provide a brief overview of these topics.*

Keywords: *Bitcoin; blockchain; cryptocurrency; smart contracts*

1. Introduction

In the fields of computer science and information technology, block chain technology has begun to shape and define new dimensions. The need for a decentralised currency has been used more as a marketing tool. It was once a theoretical idea, but in the last decade, it has become a fact, thanks to the well-known paper of Bitcoin and blockchain technology were first introduced by Satoshi Nakamoto in 2008. Including the fact that controversies surrounding One thing is certain about Nakamoto's true identity: he created something innovative, and it is up to the users to determine what to do about it. Others will invest capital in those ideas or simply trade with the ups and downs of the market, while others will take advantage of this ability to create their own application for solving different societal problems. The market value of cryptocurrencies. We figured it would be useful to include a brief overview of blockchain and cryptocurrencies in this article.. The bulk of the crypto market capitalization is held by these two cryptocurrencies. Naturally, as with any modern technology, certain drawbacks and issues arose, which we also discussed.

2. **Literature Survey**

Title	An Analysis of Cryptocurrency and Their Functioning
Authors	Neha Soni
Year of Publishing	2020
Summary	Cryptocurrency is a digital currency which acquires cryptography to secure the transactions. It is designed to make payments anonymously and in more secured way. In this paper, I first explain the detailed meaning of cryptocurrency. Then some features of trade in cryptocurrency are discussed such as the technique include the zero involvement of any governmental authority and allowing users to store and trade anonymously. Next, I demonstrate the facts and functioning of blockchain technology. It is believed that block chain technique has potential to disrupt many industries such as finance, law, banking or accounting. For the explanation of this, I state some critic point of views for the use of cryptocurrencies. It also faces criticism for vulnerabilities of the infrastructure and volatility of exchange rates. Being the nature of anonymous, cryptocurrency becomes a host for money laundering, tax evasion and other illicit activities. After this, I bring to discuss the types of cryptocurrency.

Title	Bitcoin: A Peer-to-Peer Electronic Cash System
Authors	Satoshi Nakamoto
Year of Publishing	2008
Summary	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 hashbased proof-of-work, forming a record that cannot be changed without redoing the proof-ofwork. 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 proofof-work chain as proof of what happened while they were gone

Title	Transformation of crypto currency into global phenomenon
Authors	A. Manimuthu; R. Sreedharan V.; Dr. Rejikumar G.; D. Marwaha
Year of Publishing	2019
Summary	Bitcoin is a crypto-currency-based open-source technology that operates in the peer-to-peer grid as a private payment mechanism. Bitcoin works on sophisticated cryptography supported by a local community in a peer-to-peer network. This study reviews scholarly articles to understand how bitcoin is addressed in the literature. The study reports on the attributes of bitcoin through a systematic literature review. The paper is based on primary data from existing literature and secondary data from relevant case studies in the public domain. Unlike other currencies, Bitcoin seems to have faced many hurdles and with many applications in day-to-day life, created unique challenges for the end user community. When Bitcoin came into existence, it seemed to signal hope for a better future, but the growth of bitcoin is hard to predict. Bitcoin opens up an entirely new world for both practitioners and academicians. Further, this study presents an idea about the "potential" of bitcoin, highlights the prerequisites, needs, implications, and challenges faced by bitcoin in processing business transactions.

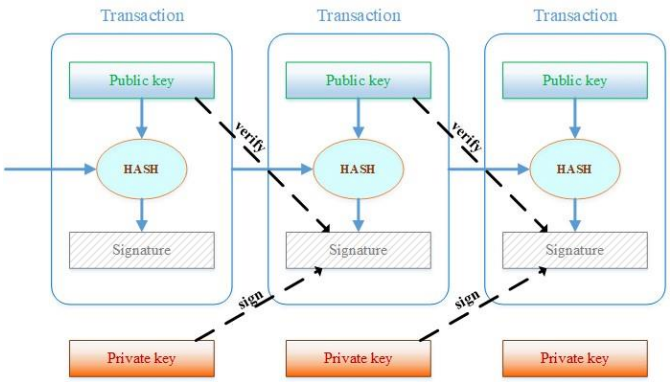
Title	Blockchain and Cryptocurrency Based Transaction Systems
Authors	Sanjay Singh Rajpurohit Talha Khan
Year of Publishing	2018
Summary	This paper provides a comprehensive and details of the current technological state of the Blockchain technology. The review outlines in details what is required for 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.

3. **Conceptual Overview**

3.1 Cryptocurrency essentials: -

Satoshi Nakamoto demonstrated a solution to the problems that digital currency implementation and usability faced, especially the double-spending problem, in his now-famous work. the issue. Although Nakamoto's true identity remains a mystery

He proposed a framework that uses a P2P distributed timestamp server as a generator of the computational proof of transaction chronological orders. The term "electronic coin" refers to a coin A digital signature chain is characterised as a series of digital signatures linked together. Every transaction is unique. a set of digitally signed hashes of the previous transaction and the next owner's public key The secret code The private key is used to sign the transaction, while the public key is used to verify it. As shown in Fig 1. the transaction is checked. The general population The key is held in the wallet and can be used in applications. hardware or through the internet



The Bitcoin ledger is a state transition system that consists of a state that displays the ownership status of all existing bitcoins and a state transition operation, which takes the form of a transaction. A new state is the product of the state change function. If the sender has enough bitcoins to make a transaction, this mechanism can result in state changes for both the sender and the receiver, or an error if the sender does not have enough bitcoins to make a transaction.

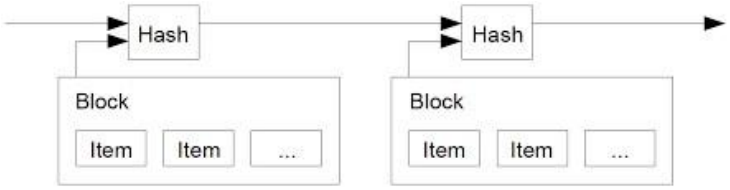
3.2 Transaction :-

Each transaction has a hash value that represents a transaction identifier as well as a collection of inputs and outputs. In the entire blockchain, each transaction output can only be used once as an input. Double-spending is caused by attempting to reference the same output twice, which is prohibited in the network. It's considered an unspent transaction output (UTXO), if the transaction's output hasn't been referenced before. and it is referred to as a spent transaction output if it has been referenced (STXO). A transaction may have up to two outputs and several inputs. Multiple inputs may be used to combine smaller quantities of coins being exchanged, with outputs being either a sum sent to the other party or change returned to the sender.

All transactions and ownerships in the Bitcoin network are recorded in the distributed ledger. This P2P network's nodes each hold a copy of the ledger record . If a user wishes to send a certain amount of coins to another, he can do so by publicly announcing the transaction, and the network will validate it is right. However, a user may try to game the system by sending several transactions of the same coin to different users (double-spending problem). Furthermore, a single user may create multiple instances to validate his original intent and thus launch a Sybil attack.

3.3 Timestamp Server:-

A timestamp server operates by taking a hash of a group of objects to be timestamped and widely disseminating it, such as in a newspaper or on Usenet . The timestamp proves that the data had to exist at the time in order to be included in the hash. Each timestamp hash contains the previous timestamp, creating a chain, with each subsequent timestamp reinforcing the previous ones.



3.4 Proof of work and blockchain :-

In a cryptocurrency network, these situations are avoided (or at least minimised) by requiring a proof-of-work from each node that verifies the transaction. To prove that they are legal members of the network, the nodes must perform some complex calculations. The scheme will remain consistent as long as the cumulative computing power of the honest nodes exceeds that of the attacker, and all legitimate transactions will take place.

A block is described by a collection of transactions, as well as the hash of the previous block and a nonce. A timestamp server generates a hash of a block and publishes it, demonstrating that the data contained within the block must have existed at the time of hashing. The timestamp server must ensure that the block's timestamp is greater than the previous block in the chain and less than two hours in the future. As seen in Fig. 2, these hashes are connected in a chain, which is referred to as a blockchain. The ability to track transactions back to any point in time is a key feature of the blockchain.

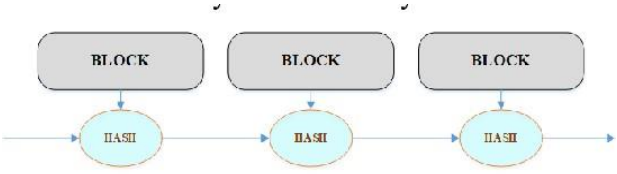
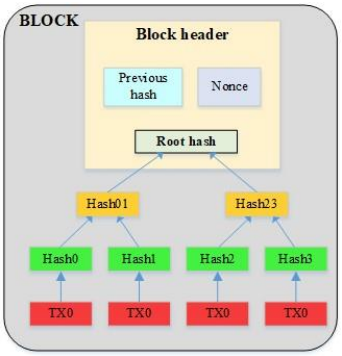


Figure 2. The blockchain scheme

Bitcoin uses a proof-of-work hashing scheme similar to Hashcash and is based on the SHA-256 hash algorithm. The proof-of-work is performed by incrementing a nonce in the block until a value is produced with the necessary number of zero bits at the block hash's

beginning. It is impossible to reverse it without repeating the calculations. If it is tampered with by a malicious attacker, all subsequent blocks will have invalid hashes. The rule is that the longest chain with majority agreement in the network is the right one, so if an attacker wants to alter a block, he'll need a lot of computing power to get around the majority.

A Merkle tree is used to hash the transactions inside a block. A Merkle tree is a binary tree with a large number of leaf nodes, each of which has a root that is a hash of its children. A Bitcoin block is depicted in Figure 4 as a Merkle tree of transaction hashes. The Merkle tree is critical for long-term maintainability because any inconsistency in the tree would represent anywhere in the chain. This is done to free up storage space on the nodes, which is needed to store the blockchain. The Bitcoin blockchain is currently 144.8 GB in size. The network discards all hashes in a tree except the root hash used in the block header after the transactions are inserted into a block and this block is checked. cryptocurrency implemented Simplified Payment Verification (SPV), which requires nodes to hold only a copy of the longest chain's block headers, rather than a complete record of transactions.



3.5 Network and mining:-

The first transaction in a block generates a new coin that belongs to the block's creator. Since there is no central authority issuing coins, this stimulates nodes to check transactions and brings coins into circulation. A coinbase transaction is the name for this type of transaction. The nodes have an opportunity to remain truthful with this strategy. The Bitcoin network is designed to generate one block every ten minutes or so. Since the computing power of the computer grows over time, the block time is kept relatively constant by gradually increasing the complexity of creating new blocks.

Fresh transactions are broadcast to all nodes at the start of the cryptocurrency network. Each node compiles transactions into a block and searches for proof-of-work, after which it broadcasts its block to the rest of the network. The network's nodes consider a block as legitimate only if all of the transactions within it are right and have not yet been spent. If

the network accepts the block, the chain is continued by generating a new block and inserting the hash of the previously inserted block.

Considering the essence of distributed decentralised networks, there are times when many nodes broadcast the same block almost simultaneously, but with likely different sets of transactions. This is referred to as a fork, and it results in the network's inconsistency. Essentially, there are many chains that stem from various blocks. This problem is solved by ensuring that the network still follows the longest chain. Gradually, the network will agree on the correct direction for the blockchain, and any chains created as a result of a fork will become invalid.

4. Conclusion

Digital coin most known and valuable cryptocurrencies. They are based on blockchain technology that is intended to promote a trust mechanism in a peer-to-peer networ based on the consensus of the majority of the nodes. We have shown in this paper a short chronological survey of the early stages of the digital money implementation,as well as the foundations of blockchain technology, and it’s most promising (or popular) implementations, In the past few years, there has been a rapid growth of numerous cryptocurrencies, hashing algorithms, and consensus agreements in the networks. Some of the cryptocurrencies worth mentioning are Ripple, Cardano, NEO, Stellar, Litecoin, EOS, IOTA, Dash, Monero, TRON, Qtum, Lisk, Tether, Stratis, Zcash,
Steem, Siacoin,Verge, Electroneum, Nxt, Dogecoin, and many more

5. Acknowledgement

With due respect and gratitude we take the opportunity to thank all those who helped us directly and indirectly. We feel pleasure in expressing our Heartfelt gratitude and vote of thanks to our guide Dr J.W.Bakal, who guided us in difficult situations. We would also like to thank our respected Head of Department Dr. Savita Sangam for providing unlimited access to all possible resources and encouragement

6. References

[1] *W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.*

[2] *H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In 20th Symposium on Information Theory in the Benelux, May 1999.*

[3] *S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In Journal of Cryptology, vol 3, no 2, pages 99-111, 1991.*

[4] *D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In Sequences II: Methods in Communication, Security and Computer Science, pages 329-334, 1993.*

[5] *S. Haber, W.S. Stornetta, "Secure names for bit-strings," In Proceedings of the 4th ACM Conference on Computer and Communications Security, pages 28-35, April 1997.*

[6] *A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.*

[7] *R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980.*

[8] *W. Feller, "An introduction to probability theory and its applications," 1957.*

[9] *N. Szabo, "Secure property titles with owner authority," 1998,*

[10] *D. Malkhi and M. Reiter, "Byzantine quorum systems," Distributed Computing, vol. 11, no. 4, pp. 203-213, 1998.*

[11] *J. Douceur, "The Sybil attack," in Proceedings of IPTPS '01 Revised Papers from the First International Workshop on Peer-to-Peer Systems, pp. 251-260, March 2002.*