IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 7, June 2022
Impact Factor: 6.252

Bitcoin -Digital Currency Wallet

Mrs. Sonal Sanjay Jogdand[1], Prof. M. S. Malkar[2], Mrs. S. P. Chattar[3]
Lecturer, Department of Computer Engineering[1,3]
Head of Department, Department of Computer Engineering[2]
Pimpri Chinchwad Polytechnic, Pune, Maharashtra, India

Abstract:*Crypto currencies have imitative as important financial software systems. They depend on a secure distributed, public, digital ledger that records all the transactions. Mining is a most essential part of systems. Mining keeps number of records of past transactions to the distributed ledger known as Blockchain. Using the Blockchain technology customers have to make secure, robust consensus for each transaction. Mining also introduces capital in the form of new units of currency. Crypto currencies do not have a central Management to handle transactions because they were designed as peer to-peer systems. They rely on miners to validate transactions.Bitcoin became the first decentralized cryptocurrency come into the market in 2009 these use a decentralized control which is related to the use of bitcoin's transaction database.Bitcoin generation and transactions are based on hashes and asymmetric encryption algorithms.*

Keywords: Cryptocurrency, Blockchain, Bitcoin, Ledger, etc.

I. INTROUDUCTION

A Cryptocurrency is a peer-to-peer digital exchange system.In the digital exchange system cryptography technique is used to generate and distribute currency units. This process requires distributed verification of transactions without an administration or central authority. Transaction verification confirms transaction amounts, and check whether the customer have it owns the currency, or they are trying to spend while ensuring that currency units are not spent twice. This verification process is called mining. Cryptocurrencies use a variety of mining technologies, according to their particular requirements.

Cryptocurrency is a digital currency in which cryptography techniques are used to control the creation of units of currency and verify the transfer of funds. Cryptocurrency system is Decentralized i.e., operates independent of any central authority or individuals. In the cryptocurrency transaction the supply of money is regulated by software and the agreement of users of the system. Thecryptocurrency transaction is based on peer-to-peer transaction.

Table 1: Difference between Conventional currency and cryptocurrency

	Conventional Currency	Cryptocurrency
Type	Real	Virtual
Intermediates	Yes	No(peer to peer)
Portability	Yes(except heavy cash)	Highly portable
Durable	Moderate	Highly durable
Acceptance	National	Global(throughout the internet)
Secure	Moderate	High
Sovereign (Government issued)	Yes	No
Decentralized	No(Central bank control)	Yes

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 7, June 2022
Impact Factor: 6.252

Table2: Evolution of cryptocurrency

Year	Name	Description
2009	Bitcoin	First cryptocurrency and used SHA-256 as hashing function.
April 2011	Namecoin	Decentralized DNS
Oct 2011	Litecoin	First successful Scrypt cryptocurrency
2012	Peercoin	First use of POW and POS function
Early 2014	Monero	Uses cryptoNote protocol.2G of cryptocurrency.
2015	Capricoin	Improved and more user friendly

1.1 Bitcoin

Bitcoin is virtual cryptocurrency.Bitcoin used in all over the world as a payment system It is the first decentralized digital currency, because this system works without a central bank or single administrator. The network is peer-to-peer and transactions take place between users directly, without an intermediary. These transactions are verified by network nodes through the use of cryptography and recorded in a public distributed ledger called a blockchain. Bitcoin was invented by an unknown person or group of people under the name Satoshi Nakamoto and released as open-source software in 2009.

The technology used to summarize the Bitcoin is as follows:

1. Blockchain
2. Bitcoin mining process
3. Bitcoin Transaction process

1) Blockchain:A blockchain is a continuously growing list of records, called blocks.Blocks are linked and securedusing cryptography. Each block typically contains a cryptographic hash of the previous block,atimestampandtransaction data. The modification of the data possible in a blockchain. It is "an open, distributed ledger that can record transactions between two customers efficiently and in a verifiable and permanent way".For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network for inter-node communication and validating new blocks. Once recorded, the data in any given block cannot be altered posterior without the alteration of all subsequent blocks.

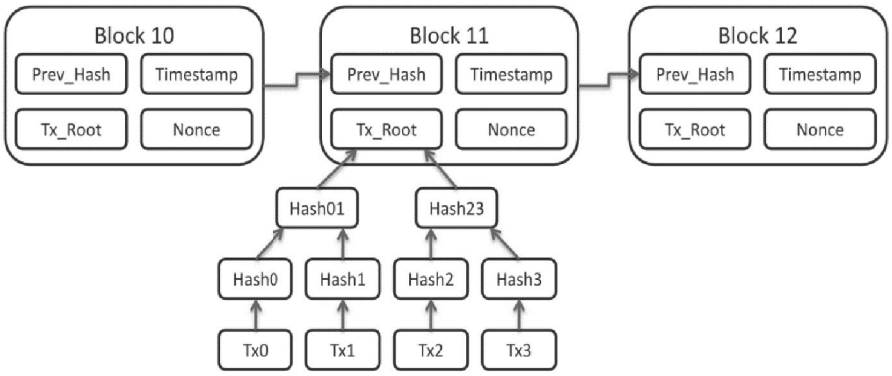

Figure 1: Blockchain Creation Structure

Blocks are data structures whose purpose is to bundle sets of transactions and be distributed to all nodes in the network. Blocks are created by miners.Blocks contain a block header, which is the metadata that helps verify the validity of a block.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 7, June 2022
Impact Factor: 6.252

Typical block metadata contains:

- previous block header hash - the reference this block's parent block
- merkle root hash - a cryptographic hash of all of the transactions included in this block
- time - the time that this block was created
- nonce ("number used once") - a random value that the creator of a block is allowed to manipulate however they so choose.

Hash Function

SHA-256 is a cryptographic hash functions designed by the NSA (National Security Agency). SHA stands for Secure Hash Algorithm. Cryptographic hash functions are mathematical operations run on digital data; by comparing the computed "hash" (the output from execution of the algorithm) to a known and expected hash value, a person can determine the data's integrity.

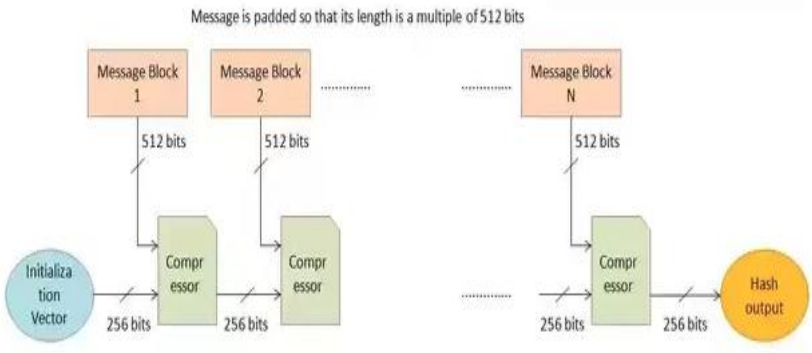

Figure 2: Workings of SHA-256 Hash Function

a. The SHA-256 function takes an input message of any size and produces a fixed size output – 256 bits.
b. The message is broken into blocks of 512 bits each and it is also padded to make sure the overall message size is a multiple of 512 bits.
c. An initialization vector, as defined by SHA-256, is passed as input to the first compressor.
d. Each compressor will use binary operations such as AND, XOR etc. to compress the input message into 256 bits.

Hash Pointer

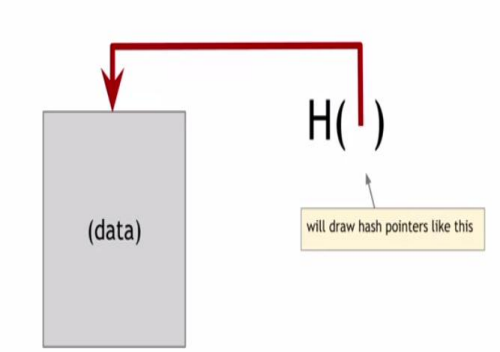

Figure 3: Hash Pointer

a. A Hash Pointer is a type of data structure which stores both the address and hash of a data.
b. So given a Hash Pointer, you can access the data stored in that address, compute its hash and verify the computed hash against the hash present in the Hash Pointer.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 7, June 2022
Impact Factor: 6.252

Merkle Root

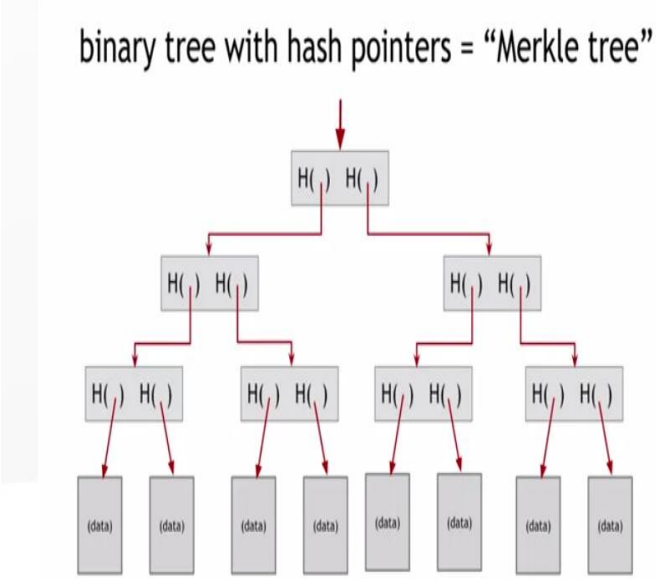

Figure 4: Merkle Tree

Another useful data structure using hash pointers is a binary tree. We can build a binary tree with hash pointers. Suppose we have a bunch of data blocks which we'll draw across the bottom down. We have to take consecutive pairs of these data blocks and for these two data blocks we're going to build a data structure here that has two hash pointers, one to each of these blocks, and similarly all the way across. Then go another level up and this block will contain a hash pointer of these two children down.And so on, all the way back up to the root of the tree.

Bitcoin Mining

Bitcoin mining is the process of verifying Bitcoin transactionsand recording themon to Bitcoin's public ledger of past transactions or blockchain. This ledger of past transactions is called the block chain as it is a chain of blocks. The block chain serves to confirm transactions to the rest of the network as having taken place.

Mining Bitcoin in Six easy steps

1. Join the network, listen for transaction
   a. Validate all proposed transaction.
2. Listen for new blocks, maintain the blockchain
   a. Validate it, when a new block is proposed.
3. Collect a new valid block.
4. Find the nonce to make your block valid.
5. Hope everybody accepts your new block.
6. Profit.

Validation of Block

First join the network, and becoming a Bitcoin node. After that listen for all of the transactions that people are broadcasting. Then we have to validate them, you listen for new blocks that people have found, you maintain a view of the current block chain. The other miners accept your block, that they validate it and start mining on the topof it, and that they don't accept some competitor's block instead. And if all that happens in step 6 you finally get to profit,Miners perform this validation step.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 7, June 2022
Impact Factor: 6.252

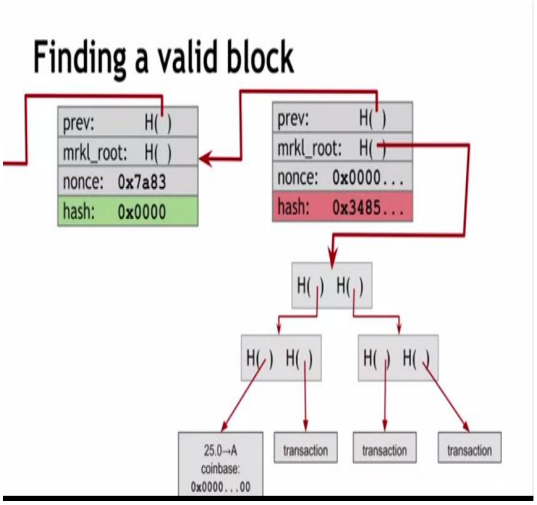

Figure 5: Validation of Block

Bitcoin Transaction

The following diagram gives a streamlined view of how transactions are signed and linked together. Consider the middle transaction, moving bitcoins from address B to address C. The contents of the transaction (including the hash of the previous transaction) are hashed and signed with B's private key. In addition, B's public key is included in the transaction. By performing several steps, anyone can validate that the transaction is authorized by B. First, B's public key must correspond to B's address in the previous transaction, proving the public key is valid.

Next, B's signature of the transaction can be verified using the B's public key in the transaction. These steps ensure that the transaction is valid and authorized by B. One unexpected part of Bitcoin is that B's public key isn't made public until it is used in a transaction.

With this system, bitcoins are passed from address to address through a chain of transactions. Each step in the chain can be verified to ensure that bitcoins are being spent validly. Note that transactions can have multiple inputs and outputs in general, so the chain branches out into a tree.

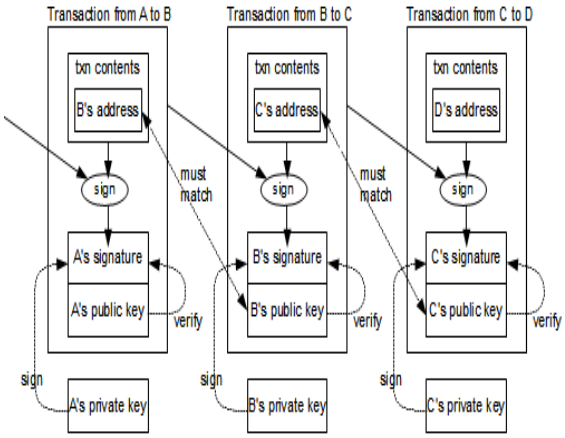

Figure 6: Bitcoin Transaction

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 7, June 2022
Impact Factor: 6.252

II. LITURATURE SURVEY

Paper 1: Mukhopadhyay, Ujan, et al. "A brief survey of cryptocurrency systems." Privacy, Security and Trust (PST), 2016 14th Annual Conference on. IEEE, 2016.

This paper explores the brief survey of cryptocurrency like Bitcoin, Litecoin, Peercoin, Ethereum, Ripple, Namecoin, Auroracoin, Blackcoin, Dash, Decred, and Permacoin. TheseCryptocurrencies are the most interesting, widely used, and with the greatest capital and transaction rates. This paper discusses about the Hash function.

SHA 256: SHA 2 is a set of Secure Hash Functions that has six algorithms, which produce digests (results) that are of different bit lengths. SHA 256, produces a digest of 256bits. SHA 256 satisfies the requirement of unidirectional hashes. Also, the same input will always produce the same digest. SHA 256 pads input to convert its length to a multiple of 512 bits. Then, it divides the input into blocks of 512 bits each. The compression function permutes and compresses the input block answer is a combination of bitwise logical operators, such as AND, OR, XOR, Complement, etc. In Figure Ch and Ma are the block wise logical operators using XOR functions.

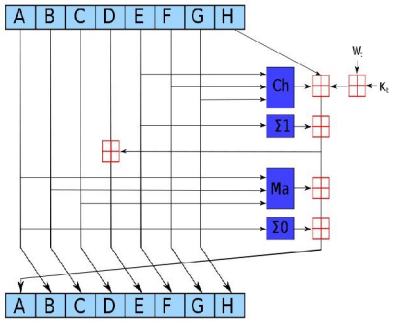

Figure 7: Round function of SHA-256

Paper 2: Bayu Adhi Tama, Bruno Joachim Kweka, Youngho Park, Kyung-Hyune Rhee, "A Critical Review of Blockchain and Its Current Applications" International Conference on Electrical Engineering and Computer Science (ICECOS) 2017.

This paper explores about Blockchain Technology.

Blockchain is a type of distributed ledger (data structure) which contains information about transactions or events. It is replicated and shared among the participants in the network.

The size of chain increases since blocks are added to the previous block using a hash function. A cryptographic hash function is used to produce a hash. For instance, Bitcoin uses SHA-256, whilst Litecoin and Primecoin use Scrypt and Cunningham chain, respectively. In addition, it enables us to simply verify the input mapping to a given hash value. It would not be feasible for two different inputs having the same hash. Each node keeps a complete replica of the entire ledger.

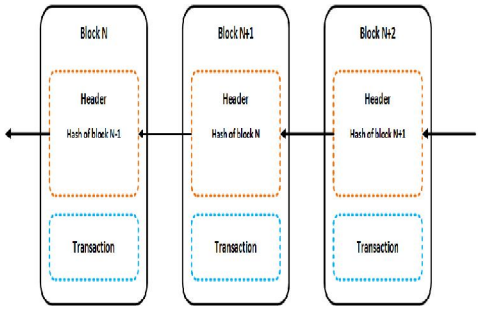

Figure 8: A chain of blocks-blockchain in Bitcoin

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 7, June 2022
Impact Factor: 6.252

Paper 3: Satoshi Nakamoto "Bitcoin:A peer-to-peer Electronics Cash System".
This paper discusses about the transaction of bitcoin. This paper explores about the transaction of the bitcoin.They proposed a system for electronic transaction without relying on trust.They started with usual framework of coins made from digital signature,which provides a strong control of ownership.
It also explores about the Timestamp server.
A timestamp server works by taking a hash of block of items to be time stamped and widely publishing the hash. The timestamp proves that the data must have existed at a time in order to get into the hash. Each timestamp includes the previous timestamp in its hash forming a chain with each additional timestamp reinforcing the ones before it.

III. CONCLUSION

Thus,i have studied the Bitcoin as a cryptocurrency. As per the study I have observed that Bitcoin is a revolutionary currency system which can work in parallel or even replace the existing forms of currencies in the future. Bitcoin can be used as a reliable alternative for fast cashless payments.Bitcoin joins a number of crypto currencies in presenting an alternative to banking-mediated online commerce. A cryptocurrency is a money-exchange protocol that uses cryptography to ensure transaction security, privacy, and the creation of units of exchange. The ideal cryptocurrency is secure, anonymous, and free from duplication, portable and two-way, and divisible. Indeed, the most pressing concern of a digital currency is to protect transactions from hackers who could steal or modify information, and also ensuring that each transaction has its source and destination authenticated.

REFERENCES

[1] Mukhopadhyay, Ujan, et al. "A brief survey of cryptocurrency systems." Privacy, Security and Trust (PST), 2016 14th Annual Conference on. IEEE, 2016.
[2] Bayu Adhi Tama, Bruno Joachim Kweka, Youngho Park, Kyung-Hyune Rhee, "A Critical Review of Blockchain and Its Current Applications" International Conference on Electrical Engineering and Computer Science (ICECOS) 2017.
[3] Satoshi Nakamoto "Bitcoin:A peer-to-peer Electronics Cash System".
[4] www.slideshare.net/CoinDesk/state-of-bitcoin-and-blockchain-2016-57577869/118-Source_Bitcoin_ and_Blockchain_Thought
[5] https://www.coursera.org/learn/cryptocurrency/lecture/0htpQ/the-task-of-bitcoin-miners
[6] Matthew D. Sleiman, Adrian P. Lauf, Roman Yampolskiy, "Bitcoin Message Data Insertion on a Proof-of-Work".
[7] Matthew D. Sleiman, Adrian P. Lauf, RomanYampolskiy, "Bitcoin Message:Cryptocurrency System" 2015 International Conference on Cyberworlds.