BITCOIN-A DIGITAL CRYPTOCURRENCY BASED ON PEER-TO-PEER NETWORK

Abhishek Jha[1], Dr. B. Indira Reddy[2]
Science and Technology, Hyderabad, 501301, India.

Abstract : We all are living in a digital world and becomes a part of it our most of the work is done with the help of digital systems. The current scenario of digital payment related to Cryptocurrency market is based on Bitcoin and various Cryptocurrency related to that and Bitcoin has its unique feature and if we apply Blockchain Technology it gives us more security which can be implemented on Bitcoin a digital Cryptocurrency market. In this paper I provided a detail review based on Bitcoin Cryptocurrency and Blockchain Technology.

IndexTerms **- Bitcoin, Blockchain, Merkle Tree, Smart Contracts, Consensus.**

I. INTRODUCTION

Bitcoin is introduced in 2009 an unidentified programmer or a group of expert or skillful people an assumed name called Satoshi Nakamoto developed by them. It follows a peer to peer digital cash system where whole work is performed in decentralization manner there are no central controller authority and servers, this concept shows the peer to peer network sharing of file.The Bitcoins solve various types of problems while doing payment through network that is two time spending the money. The decentralized platform provides the network like Bitcoin every single person who is participated in that particular network has to keep the record of balances and transaction of each participant needs to do this work. The concept of Blockchain has the capability to perform this task, it has a public ledger which helps in identifying the transaction happened within the network, available to everyone and this is the reason every person which is in the network can see their account details. The single transaction is a file structure that contains of sender's and recipients public keys in the form of wallet address and amount of coins which is transferred. The transaction is to signed by the sender by using the private key, this is called as basic cryptography technique and the transaction is broadcast first. The Cryptocurrency networks miners can assure transactions by solving cryptographic related problems, mark the as authorized and communicate them over the network. Next is the each node of the networks adds it to its database. If the transactions is confirmed it cannot be change further and immutable and miner gets a prize with the transaction.

Limitations of Bitcoins:

There are various digital currencies in the market which is having their own limitations and Bitcoins is also parts of them.So following are the limitations of Bitcoins are explained below:

a) Bitcoins does not approve in worldwide:

Bitcoins are not widely accepted in the worldwide and very less number of online platform accept Bitcoins as a currency for online business that makes us not feasible to totally depend on Bitcoins as a currency. The government also paying attention and gives awareness among the people to not use Bitcoins as a currency due to there is a chance of illegal use for various criminal activities.

b) Wallets get misplaced:

Hard drive contains lots of important information's and if it gets crashed due to any reason and virus corrupt the data then this will result in Bitcoins get damage. We cannot do anything to get back it. The coins which are used will be permanently waif in the system.This will affect the Bitcoins shareholder due to damage of Bitcoins and the coins that the investor earned will also be permanently destroyed.

c) Bitcoins assessment varies:

Bitcoins value changes regularly time to time according to the necessity. The cost of the Bitcoin accepting sites are not consistent sometimes it creates a lot of dilemma if anyone wants the money back. Suppose the a product cost is decided initially 10 Bitcoins and after a week if anyone wants to return the product back and wants the money back then the person doesn't get the same amount as they earlier paid before from online payment platform. It becomes sometimes injustice when the same product price gets devaluation and the amount of money gets calculated according to the current scenario.

d) Buyer protection is not considered:

When any items are purchased with the help of Bitcoins in return the retailer doesn't give the same product we can't do anything to reverse the whole transaction process.

e) Liability of unrecognized technological Fault:

There are various issues which are not known regarding Bitcoins system due to which the current technological world the hacker can gain advantage due to the particular system which leads to cost the destruction of whole Bitcoins based economy.

f) Lack of physical identity of Bitcoins:

Bitcoins doesn't contain any physical existence and cannot be used as a physical stock and this becomes important to change it into other valid currencies which are available in the market. There are some Bitcoins Card which is used for purchasing the products but the wallet information which is put forward and the particular system is not having agreement to that Bitcoins and this becomes not feasible to every systems to support all type of Bitcoins cards until and unless a worldwide system is purposed to handle all the type of Bitcoins cards.

g) Lack of central authority policy of Bitcoins:

The policies which are implemented regarding the use of Bitcoins is undefined means there is not a single central institution who can take the responsibilities about Bitcoins and this result in deciding a decent value for any Bitcoin becomes a great challenge. Suppose a huge number of online retailers and the value of Bitcoin decreases day by day, this will affect large amount of Bitcoins user very badly who are investor of money in Bitcoins.The decentralization of Bitcoins becomes both a bane and boon.

What is Blockchain?

A Blockchain is a decentralized distributed databases system in which data is shared among several system linking to a sequence of chain of blocks called ledger and the digital data get stored in all the blocks and all the work which is done is agreed upon a peer-to-peer network. The each and every block holds batches of transaction. Blockchain removes the double spending problems which mean the chances of any digital data in the form of currency the person who uses particular digital currency will make the same currency use repeatedly by sending it to the online payment merchant which becomes a risk earlier.

A block holds a collection of true number of transactions that uses hashing technique and cryptograph logic into the Merkle tree. The each and every block is hashed with a particular hash algorithm in the Blockchain. The number of all the blocks contains the previous hash values in the chain in this starting block is known as genesis block which doesn't store any previous hash data. This is the distributed ledger that is open to anyone (publically).The distributed ledger is a database which will continuously shared the data in a prescribed order over the network distributed among the multiple websites. Once the data is recorded it is very difficult to change it. If hacker attacks on one block then the hash code of that block will also changed and it is no longer the same block. This leads to mismatch of the hash number with the next block hash number. But it is not enough to safe the information of the data because computer can able to calculate the number of hash values per second. At the time when a new block is attach to the Blockchain this is distributed among Peer-to-Peer through the network. In Peer-to-Peer the details of the data has been checked by the member who is connected to that particular network and confirms it then only a new block is attached to the chain of ledger of Blockchain this is known as proof of work. This follows a decentralized method in which the whole work is distributed to each other.

Genesis Block

Block Z+1 Hash=@3$ l Previous Hash=q#1 Y	Block Z Hash=q#7Y Previous Hash=1z^A	Block Z-1 Hash=1z^A Previous Hash=0000

Fig: Architecture of a Blockchain contains secure Cryptographic Hash Values generated during transactions in Bitcoins .

In this above figure the first Block contain zero previous Hash value it means the Block is known as Genesis Block. The next Blocks contain the hash value of previous Block along with its own hash value. The Block represent Z-1 shows that previous Block, Block Z means current Block and Block Z+1 means the following Blocks. The Hash value of Bitcoins is used to perform the online transactions.

Generally Blockchain is of two types:

A) Public Blockchain:

Public Blockchain process in a way that anyone can join in this chain to add new block and access the transaction of each block according to this there are no restrictions is imposed to the participant in making the Blockchain.

B) Private Blockchain:

In private Blockchain there are several restrictions is imposed according to their privacy issue regarding the access of data in the blocks, reading transactions details adding new blocks to the chain. This is helpful for industries, government institution, e-commerce business etc.

Merkle tree in Blockchain:

Merkle trees are an important element of Blockchain technology. The Merkle tree follows a design which makes the information stored in a broad amount of data can be verified. The trees are build by frequently by hashing them in the form of combinations of different nodes until and unless we don't get the only one single hash left that is also recognized as Root Hash or Merkle Root. All of them are build from the downside-up and the hashing of particular transaction called as Transaction ID's.The tree containing leaf is known as leaf node which is a hash of transactional data and tree containing non leaf node is known as hash of its previous hash code. Merkle trees are generally a binary tree structure that makes it to use the even number of leaf node necessary suppose that the number of transaction is odd then the last hash value gets replicate to develop an even number of nodes in a particular Merkle tree.

Different versions in Blockchain:

Blockchain 1.0:

In this the concept of digital currency was introduced and the deployment of distributed blocks of ledger technique is used, the Cryptocurrency which is used in this version is Bitcoin and this is also known as digital currency of the Internet, a digital currency payment system.

Blockchain 2.0:

In this the concept of smart contracts was introduced the contracts are basically a program is implemented in the system which will follow all the terms and conditions needed to follow during purchase of property, business contracts in another word it is also called as consensus between an authorized persons.The main feature of this version is it makes the Blockchain technology best in the form of trustworthy system and makes hacker proof such as smart contracts used in Blockchain. The smart contracts makes cost of any agreement between them becomes feasible along with the authentication between different parties, provide best detection platform related to any type of scam and the contracts are transparent. The most outstanding in this field is Ehereum Blockchain which generally deals with deployment of the smart contracts.

Blockchain 3.0:

In this the concept of decentralization of an applications peer-to-peer network is introduced in a Blockchain. In comparison with traditional application facilitates in which backend coding is processing in centralize servers. A Decentralized application works on a frontend coding platform and user interaction with the system is written in any language which makes to call its backend programming, like a traditional application. But a Decentralize application has its own frontend introduced on decentralize storage platform such as Ethereums Swarm.

Blockchain 4.0:

In this the concept of the Blockchain becomes usable in an industry. The Industry 4.0 deals with limited terms computerized, enterprise resource planning(ERP) which is used to record the employee details regarding the attendance, salary details etc and also the integration of different execution systems. The demands of present industry is to protect the data along with its privacy and trustworthy. Blockchain stands all the perspective of Industry needs. Blockchain business process all the machines safety steps and placing all the independent replacement parts to reach. Blockchain are used in many things which boost up the Industry that is supply chain management, approval plans regarding the advancement of Industry, financial payment transaction reports, IOT in collection of data, health management and service management can be allow by Blockchain technology. The first framework for Blockchain 4.0 is unbright.io framework that helps in business integration in any Industry.

II. LITERATURE REVIEW

Satoshi Nakamoto.[1] In this paper, the author suggested that the digital signatures cannot give the solution for two time spending problem in this the author purposed a peer-to-peer network using proof of work to store a public history of all the transaction that will become computational and occupies the whole CPU process due to true nodes occupies a bulk of CPU power and it becomes impractical to the attacker to change anything in the node.

Ghassan O. Karame, Elli Androulaki, Srdjan Capkun.[2] In this paper, the authors break down the security of utilizing Bitcoin for quick payment, where the quick payment is likewise doesn't sheltered by performing double-spending assault against quick payment in Bitcoin. The author additionally give the arrangement space for double-spending assault by demonstrating the work giving a thought of double-spending alarms in the system would establish a first critical advance towards effectively distinguishing double-spending.

Christian Decker and Roger Wattenhofert.[3] In this paper, the authors investigate the issue in Bitcoin because of data gets spread while synchronization record duplicacy, the reliance on the blocks are very little reliable and it delay the transactions, when expansive blocks get duplicate gradually in the system it enables the attacker. The author demonstrates estimations demonstrate that a solitary hub actualizing these progressions diminishes the quantity of Blockchain duplicacy in the system by over 50%.

Malte Moser, Rainer Bohme, Dominic Breuker.[4] In this paper, the authors give a first orderly record of chances and impediments of against unlawful tax prevention in Bitcoin, the decentralized cryptographic digital currency proliferation on the Internet, similar to it follows in KYC rule.

Jega Anish Dev.[5] In this paper, the author says about a strategies for performing Bitcoin mining on not comparable equipment which results in relevantly quicker mining by consolidated use of figuring components inside machines in mining systems, both illicit and lawful.

Yu Zhang, Jiangtao Wen.[6] In this article, the authors first propose an Internet Of Things related to online platform business model, they all again design a many aspect in conventional electronic business models and the transaction is done based on smart property and do payment data on the IOT with the help of peer-to-peer deal based on the Blockchain smart contract and script.

Guy Zyskind, Oz Nathan, Alex Sandy Pentland.[7] In this paper, the authors portray a decentralized individual information the board framework that promise clients acquire and supervision their information. They all arrange a meeting that converts a Blockchain into an industrialize access-control supervisor that doesn't need trust in an outsider. Not at all like Bitcoin, exchanges in our framework are not carefully money related, they are utilized to convey guidelines, for example, putting away, questioning and sharing information.

Alireza Beikverdi, JooSeok Song.[8] In this paper, authors present the centralization aspect in Bitcoin's mining which establish conditions of centralization in all systems. In this paper it is mentioned, so as to carry Bitcoin as an appropriated & decentralize system, mining the process in the center motor of mining so that all the exchange check happened ought to be obvious to client.

Jay Kishigami, Shigeru Fujimura, Hiroki Watanabe, Atsushi Nakadaira and Akihiko Akutsu.[9] In this paper, the authors built up a Blockchain-based advanced substance appropriation framework and decentralize & pear-to-pear validation system could be treated as the perfect authority to the board instrument.

Giuseppe Di Battista, Valentino Di Donato, Maurizio Patrignani, Maurizio Pizzonia, Vincenzo Roselli, and Roberto Tamassia.[10] In this paper, the authors displayed BitConeView, a framework for the visual examination the Bitcoins streams in Blockchain. This apparatus helps in recognizing the blending procedure and examples in Bitcoin.

Shigeru Fujimura, Hiroki Watanabe, Atsushi Nakadaira and Akihiko Akutsu, Jay (Junichi) Kishigami.[11] In this paper, the authors propose an idea for another rights the board framework dependent on the Blockchain technology, which is celebrated for supporting the unwavering quality of the Bitcoin. The author elucidate issues that happen when they apply the Blockchain innovation to the rights the executives system, and they likewise portray their preliminary usage.

Wei-Tek Tsai, Robert Blower, Yan Zhu, Lian Yu.[12] In this paper, authors portrays issues identified with utilizing Blockchains for money related applications. Money related frameworks need high turnout, below idleness, large unwavering quality, large security & protection, & exacting administrative implementation, yet the current Blockchain has less throughput, large dormancy, low security, & deprived a thorough administrative structure.

Xiwei Xu, Cesare Pautasso, Liming Zhu, Vincent Gramoli, Alexander Ponomarev and Shiping Chen.[13] In this paper, authors give bases to help the design choice if to utilize a decentralize Blockchain rather than another programming answers, such as customary share information stockpiling. Moreover, they investigate explicit ramifications of utilizing the Blockchain as a product connector including configuration exchange offs in regards to quality characteristics.

Jose G. Faisca, Jose Q. Rogado.[14] In this paper, the authors portray so as to give individual cloud interoperability, they propose a start to finish validation system dependent on JSON Web Tokens (JWT) and the Blockchain. JWTs are an institutionalized holder arrangement to encode individual cloud and customer related data security utilizing claims. The conveyed, undeletable,

unchanging, and irreversible nature of the Blockchain has proper qualities for appropriated certification stockpiling and decentralized character the executives.

Brendan Benshoof, Andrew Rosen, Anu G. Bourgeois, Robert W. Harrison.[15] In this paper, the authors present Distributed Decentralized Domain Name Service (DNS), a framework to supplant the present best dimension DNS framework and declaration authorities, offering expanded versatility, security and heartiness Decentralized Domain Name Service depends on disseminated hash value table & uses a space name possession framework dependent on the Bitcoin Blockchain.

Feng Tian.[16] In this paper, the author consider the use and advancement circumstance of Radio Frequency Identification (RFID) and Blockchain innovation first time, and afterward they dissect points of interest & detriments of utilizing RFID and Blockchain innovation in structure the agri-food production network discernibility framework; at long last, they exhibit the structure procedure of this framework. It can understand the detectability with confided in data in the whole agri-food store network, which would successfully ensure the food security, by social affair, exchanging and sharing the valid information of agri-food underway, preparing, warehousing, dispersion and selling links.

Ahmed Kosba, Andrew Miller, Elaine Shi, Zikai Wen, Charalampos Papamanthou.[17] In this paper, authors present Hawk, a decentralized smart contract framework that doesn't stored money related exchanges free on the Blockchain, consequently holding value-based protection from the general visibility's. A Hawk software engineer can belong to a private smart contract in a natural way without accomplish cryptography & our compiler accordingly develops a proficient cryptography meeting where lawful binding collections associate with the Blockchain, take advantage of cryptographic natives, for example, zero-learning proofs.

Yan Zhu, Ruiqi Guo, Guohua Gan, Wei-Tek Tsai.[18] In this paper, the authors proposes another framework for definite affirmation of exchanges in a block. Supplanting unique mark, another Interactive Incontestable Signature (IIS) plot is utilized among merchant & proprietor to affirm an exchange. By this mark, the merchant can guarantee the proprietor that an exchange will incorporated into the Blockchain in non-revocation action. The plan is turned out to be secure for proprietors uncountable and merchant's disagreement.

Affan Yasin, Lin Liu.[19] In this paper, the authors essential goal of this paper is to propose an efficient structure for collecting on the web character and notoriety data, to give an all encompassing way to deal with individual online conduct appraisals.

Jun Zou, Yan Wang, Mehmet A. Orgun.[20] In this paper, the authors proposes an inventive administration contract the board conspire that encourages the checking of the execution of an administration contract in a distributed domain, motivated by the idea of Blockchain in Bitcoin.

III. CONCLUSION

Bitcoin is a Cryptocurrency which has its own demand and become crucial part in digital currency in the form of transaction and other Cryptocurrency is also growing in their demands like Ethereum Blockchain which is used for making smart contracts and it is widely used now a day many applications developed based on solidity language.

REFERENCES

[1] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic" .2008

[2] Ghassan O. Karame, Elli Androulaki, Srdjan Capkun, "Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin".Conference on Computer and Communication Security.2012

[3] Christian Decker and Roger Wattenhofert, "Information Propagation in the Bitcoin Network", IEEE P2P Proceedings.2013

[4] Malte Moser, Rainer Bohme, Dominic Breuker, "An Inquiry into money Laundering Tools in the Bitcoin Ecosystem", IEEE APWG eCrime Researchers Summit.2013

[5] Jega Anish Dev, "Bitcoin mining acceleration and performance quantification", IEEE 27th Canadian Conference on Electrical and Computer Engineering (CCECE).2014

[6] Yu Zhang, Jiangtao Wen, "An IOT Electric Business Model Based on the protocol of Bitcoin", IEEE 18th International Conference on Intelligence in Next Generation Networks.2015

[7] Guy Zyskind, Oz Nathan, Alex Sandy Pentland, "Decentralizing Privacy: Using Blockchain to protect personal data", IEEE Security and Privacy Workshops.2015

[8] Alireza Beikverdi, JooSeok Song, "Trend of centralization in Bitcoin's Distributed Network", IEEE/ACIS 16th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD).2015

[9] Jay Kishigami, Shigeru Fujimura, Hiroki Watanabe, Atsushi Nakadaira and Akihiko Akutsu, "The Blockchain Based Digital Content Distribution System", IEEE Fifth International Conference on Big Data and Cloud Computing.2015

[10] Giuseppe Di Battista, Valentino Di Donato, Maurizio Patrignani, Maurizio Pizzonia, Vincenzo Roselli, and Roberto Tamassia, "BitConeView: Visualization of Flows in the Bitcoin Transaction Graph", IEEE Symposium on Visualization for Cyber Security (VizSec).2015

[11] Shigeru Fujimura, Hiroki Watanabe, Atsushi Nakadaira and Akihiko Akutsu, Jay (Junichi) Kishigami, "BRIGHT: A Concept for a Decentralized Rights Management System Based on Blockchain", IEEE 5th International Conference on Consumer Electronics - Berlin (ICCE-Berlin).2015

[12] Wei-Tek Tsai & Robert Blower, Yan Zhu, Lian Yu, "A system view of Financial Blockchains", IEEE Symposium on Service-Oriented System Engineering (SOSE).2016

[13] Xiwei Xu, Cesare Pautasso, Liming Zhu, Vincent Gramoli, Alexander Ponomarev, Shiping Chen, "The Blockchain as a software connector", 13th Working IEEE/IFIP Conference on Software Architecture (WICSA).2016

[14] Jose G. Faisca, Jose Q. Rogado, "Personal Cloud Interoperability Fully Decentralized Identity Management", IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM).2016

[15] Brendan Benshoof Andrew Rosen Anu G. Bourgeois Robert W. Harrison, "Distributed Decentralized Domain Name Service", IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW).2016

[16] Feng Tian, "An Agri-food Supply Chain Traceability System for China Based on RFID & Blockchain Technology", IEEE 13th International Conference on Service Systems and Service Management (ICSSSM).2016

[17] Ahmed Kosba, Andrew Miller, Elaine Shi, Zikai Wen, Charalampos Papamanthou, "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smarts Contracts", IEEE Symposium on Security and Privacy (SP).2016
[18] Yan Zhu, Ruiqi Guo, Guohua Gan, Wei-Tek Tsai, "Interactive Incontestable Signature for Transactions Confirmation in Bitcoin Blockchain", IEEE 40th Annual Computer Software and Applications Conference (COMPSAC).2016
[19] Affan Yasin, Lin Liu, "An Online Identity & Smart Contract Management System", IEEE 40th Annual Computer Software and Applications Conference (COMPSAC).2016
[20] Jun Zou, Yan Wang, Mehmet A. Orgun, "A Dispute Arbitration Protocol Based on a Peer-to-Peer Service Contract Management Scheme", 2016 IEEE International Conference on Web Services (ICWS) .2016.