International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 05 | May - 2021 ISSN: 2582-3930

Research Paper on Bitcoin -The future

Aansumol Yohannan , *Keraleeya Samajam*
Dombivli's Model College,Dombivli east,Mumbai ,Maharashtra,India

***Abstract*—Blockchain technology has created a new wave of disruption similar to the way internet did .One of the beautiful usecases of blockchain technology is Bitcoin. Bitcoin is a cryptocurrency that is enabled by the unde rlying technology called blockchain. Satoshi Nakamoto invented a cryptocurrency called Bitcoin. Satoshi Nakamoto, is a pseudonymous name.Cryptocurreny is a digitalized or virtual currency that can be secured by cryptography.As bitcoin's underlying technology is blockchain,Its main feature is being decentralized.It made its appearance back in 2009.Bitcoin is one of the most successful cryptocurrency due to its featues like anonymity and decentralization.Although bitcoin has always been questionable.Lets learn more about bitcoin and blockchain through this research paper.**

Keywords—**mining, decentralization, TCP/IP,Blockchain.**

I. INTRODUCTION

Inorder to understand bitcoin it is essential to know about its underlying technology that is blockchain. When the Internet was made accessible to public (WWW) in the early 1990s, it was supposed to be more open , peer-to- peer and decentralized.Thats why it was built atop the open and decentralized TCP/IP. Whenever a new technology, especially the revolutionary ones comes in to there are two probabilities either they fade away on their own, or they create such an impact that they become the accepted norm.Internet was such a thing it got accepted by the world. People adapted to the WWW revolution and leveraged the benefits it had to offer in every possible way. As a result, the it started shaping up in a way that might not have been the exact way it was imagined. Initially when internet came in to picture,it was made with an intention to be decentralized, But as we are aware now that is not the case. Many new technologies and businesses started to build on top of it and it became what it is today—more centralized. s. Blockchain is believed to be the component that completes the Internet puzzle and makes it more open, more accessible, and more reliable.

Blockchain is a system of records to transact value (not just money!) in a peer-to-peer fashion. What it means is that there is no need for a trusted intermediary such as banks, brokers, or other escrow services to serve as a trusted third party.Thus bitcoin came in the picture. Just the way TCP/IP was designed to achieve an open system, blockchain technology was designed to enable true decentralization. In an effort to do so, the creators of Bitcoin has open-sourced it so it could inspire many decentralized applications, It is just an another layer on top of the Internet and can coexist with other Internet technologies.

Ideally now when we transact we always need a third party trusted source like banks in between. Bitcoin is a currency which doesn't need any trusted third party intermediary

II. BLOCKCHAIN TECHNOLOGY

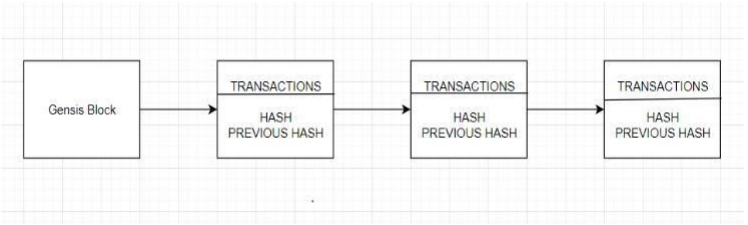


Fig. 1. Blockchain data structure

The blockchain data structure as we can see in the above image is a back-linked list of blocks of transactions. It can be stored as a flat file or in a simple database. every block is a collection of transactions, hence the name blockchain Each block is identifiable by a hash, generated using the SHA256 cryptographic hash algorithm on the header of the block. links back to the previous block in the chain. What it means is that every block header will contain the hash of the previous block so that no one can alter any transaction in the previous block. So, given the latest block makes it feasible to access all the previous blocks in a blockchain.

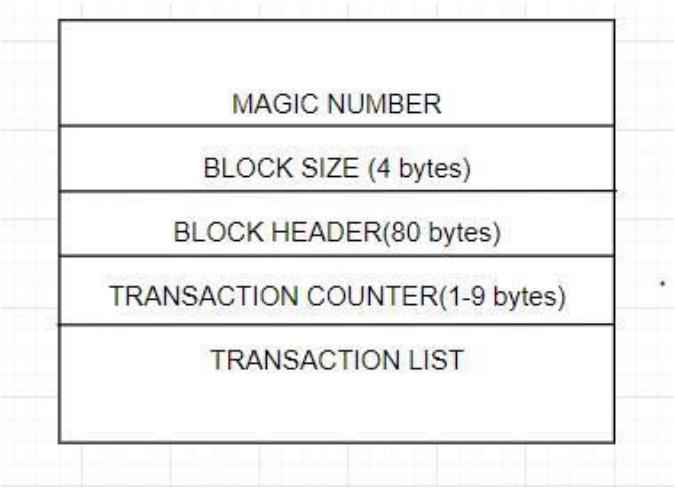
History Of Money

Money is primarily the medium of exchange for exchanging value, that is anything of value.In olden days there was nothing like currency.There was barter system .For example is rice in exchange of wheat .Now the question arises what if the person exchanging is not wanting rice as exchange instead would need oranges.In this case exchange is not possible.So they can find someone who needs rice and can provide what the other person needed.But it was difficult to always find such a person .So they decided to commoditize system of value exchange, Eventually, better techniques were found to be used where banking system started. fiat currency" was introduced by the governments as legal tender. This was purely trust based, in the sense that people had to trust the government. Fiat currency does not have any intrinsic value, it is just backed by the government. Today, the money that we know of is all fiat currencies. So, the value of money today depends on the stability and performance of the governments. This was the state of banking systems.In these centralized systems ,the cost of transactions, time taken for a transaction to settle and many such issues were caused due to centralization .This problem could be solved digital currency backed by computing power which is decentralized. Bitcoins are designed to enable electronic payments between two parties based on cryptographic proof.
It is decentralized in every aspect—technical, logical, as well as political. Anyone having good computing power can participate in mining and generate new Bitcoins.

III. BITCOIN.

Bitcoin mining is the process by which new bitcoins are created . It is performed using very sophisticated computers that can solve extremely complex math problems. n. Since Bitcoins are generated in such manner by a competitive and decentralized process called "mining," they are at a fixed rate with an upper cap of 21 million Bitcoins in total that means bitcoin can ever exist is this number , this makes Bitcoin a scarce resource.

There is a ledger which maintains identies of participants anonymously and respective records of all the genuine transactions executed between network participants.This ledger database is an append-only database so it cannot be changed or altered.That means that every entry in it is a permanent entry. Any new entry on it gets reflected on all copies of the databases hosted on different nodes. There is no need for trusted third parties to serve as intermediaries to in order to verify, secure, and settle the transactions.
Bitcoin like any other blockchain has the same structure.



.Fig 2.Block structure of bitcoin blockchain

Bitcoin uses merkle tree. The Merkle tree is a tree data structure of the hash of the transactions, Bitcoin uses public-key cryptography, peer-to-peer networking, and proof-of-work to process and verify payments

There are also certain security issues due to anonymity some people may use bitcoin for wrong purposes as well.

!V. RESEARCH METHODOLOGY

This research is based on the secondary data from small group online research finding that is existing paper and thesis. to understand the basics of blockchain technology and bitcoin.

V. ACKNOWLEDGEMENT

I would like to thank Keraleeya Samajam's Model College for providing me with an opportunity to present this research paper. And also, I would also like to thank Divya Ma'am and teaching staff for assistance and comments that greatly improved the manuscript.

VI.CONCLUSION

Adopting Internet has changed the way people did business. It removed friction from creation and distribution of information. This also has paved the way for new markets, more opportunities, and possibilities. Similarly, blockchain is here today to take the Internet to a whole new level. Bitcoin is just one cryptocurrency application of blockchain, and the possibilities are limitless. Bitcoin can be the future.As it is cedentralized . Bitocin uses the Usual framework of coins made from digital signatures, which provides strong control of ownership, a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power.

IV.REFERENCE

[1] Beginning blockchain: by Bikramaditya Singhal Gautam Dhameja Priyansu Sekhar Panda
[2] Bitcoin: A Peer-to-Peer Electronic Cash System Satoshi Nakamoto-www.bitcoin.org