



BLOCKCHAIN: AN ANALYSIS ON NEXT-GENERATION INTERNET

Mr. Atul Kumar Verma

Assistant Professor, Computer Science Engineering
Poornima College of Engineering
Jaipur, India

Mr. Arpit Garg

Student, Computer Science Engineering
Poornima College of Engineering
Jaipur, India

Abstract: The blockchain is a peer to peer technology that protects the integrity of a digital piece of information. It can serve as a digital decentralized distributed ledger that can record sharing of information between two parties in a permanent way. All the information is stored in a network of personal computers. Each computer has memory records called blocks and each block has a time stamp and a link to the previous block as a hash pointer. All the records are secured using cryptography. Timestamp keeps the track of creation of the record. Once the record is created no one can manipulate the records, not even the owner. It keeps the proof and exact time at which that data exists. A hash function is a mathematical algorithm and algorithm is made in such a way that it is a one-way function that means the process cannot be rolled back. Next generation of the Internet will be using in FITS.

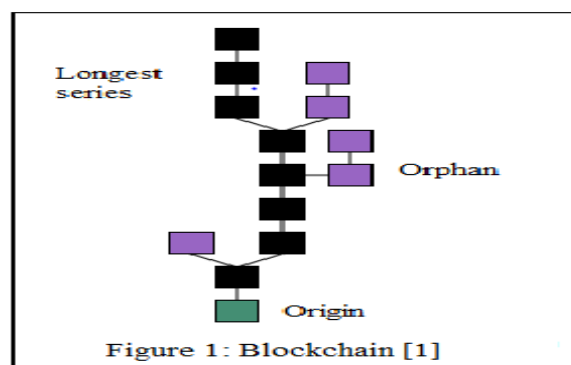
Keywords: Hash pointer, Time Stamp, Hash function, Cryptography, FITS.

I. INTRODUCTION

The blockchain is one of the emerging area of research in the field of computer science. Blockchain is a peer to peer technology which is digitalized decentralized and distributed. In today's world all the process like transactions etc. are maintained through a centralized system. Blockchain removes the concept of the centralized system. In blockchain a network is present in that network many personal computers relate to each other. Each computer has its own set of data records called block. There are few terms related with each block. First each block is linked and secured using cryptography and each block is linked to its previous block through hash pointer and time stamp is present which maintain the record of exact creation time of the record.

Algorithms of hash functions are created in such a way that once the process is executed it cannot be revert. Once the record is made it cannot be alter, if there is need to make changes in the record then all the subsequent blocks are needed to be altered and all the process information will be stored with exact details.

Blockchain uses the distributed open ledger. In distributed open ledger all the data are replicated among several computers present far from each other and all the information is synchronized and shared among all the computers present in the network. A peer to peer network is maintained and algorithms are used to share and replicate the data among various computers.



II. DISTRIBUTED OPEN LEDGER

In the distributed open ledger every computer which is present in that network have copy of the ledger with the property that all the ledger is synchronized with each other. A ledger is basically a collection of data and that ledger is distributed among all the computers and sharable. If any process executes it will be first broadcast so that every computer present in that network can analyze that process and according to it ledger is modified and this ledger is open to all means all the computers present in that network is able to see any process going in that network. An advance algorithm is used so that all the ledgers must be synchronized and share data between each other. Miners are the special nodes that holds the ledgers. A unique key is present with each miner which is used to validate the process[2].

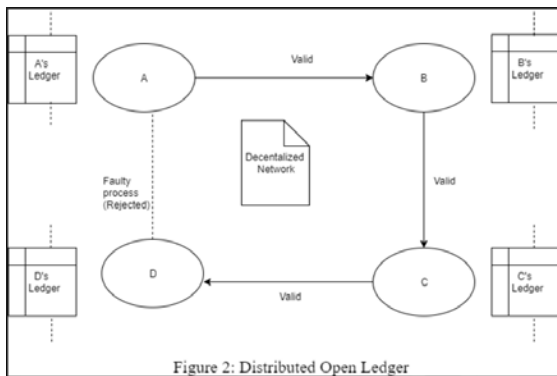


Figure 2: Distributed Open Ledger

III. CHARACTERISTICS OF BLOCKCHAIN

Blockchain is called next generation of internet. There are various problems that are solved by block chain. The main problem is Double Spending Problem. In double spending problem same resources are used for more than one process so it is impossible to spend the same resources on the different process using this blockchain technology. One application of blockchain is Bitcoin. Considering the double spending problem about bitcoin. Bitcoin was the first protocol which claim to solve this problem. Double spending means uses the same bitcoin more than once. The bitcoin network which is based on blockchain protects against double spend by verification of each transaction using Proof of Work mechanism.

Blockchain is successful whenever there is a condition of FITS is needed [3]. In FITS F stands for Fraud protection whenever there is requirement to protect any process against any fraud blockchain can be used. As blockchain is nearly impossible to hack, for hacking the blockchain hacker must hack all the computers present in the blockchain and alter all the ledgers which requires very large amount of computational powers which is nearly impossible. I stand for intermediaries which means there is no centralized network present so the process will take less time and less resources are required. T stands for throughput. Throughput stand for number of processes that can be performed in a second. Throughput value is increasing day by day till now maximum value recorded is nearly about 400,000 transactions/sec. S stand for stable data. Once the data are stored in ledger it is not possible to alter the data. To alter the data there is requirement to alter all the ledgers present in that network and data are managed properly and have stability.

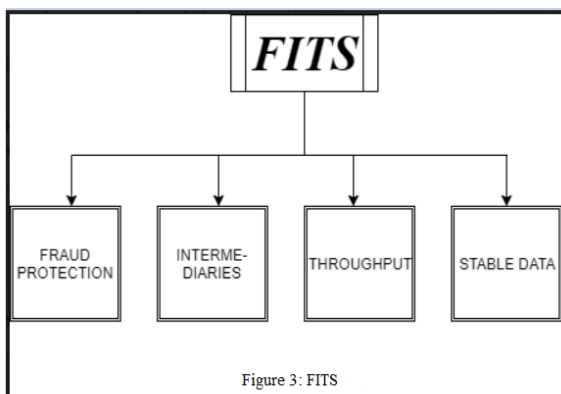


Figure 3: FITS

IV. IMPACT ON INDUSTRIES

There are many companies that start using blockchain. Everledgers uses blockchain to protect valuable assets. It reduces risk, theft, trafficking and fraud. Nasdaq and Citi announce pioneer blockchain and global banking integration. Six major banks decided to make their own single cryptocurrency including Barclays, HSBC, Credit Suisse etc. Microsoft is working on Ethereum blockchain. There are different sites which uses blockchain like Steemit which is social media platform and dTube which is online video player [4].

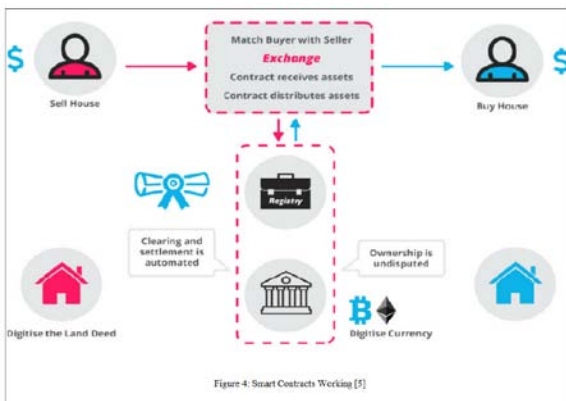
Blockchain provides a way to record and transfer data that is transparent, safe, auditable, and resistant to outrages. There are several industries which will badly impact by blockchain. As the blockchain is democratic, decentralized and secure compare to present technology used. There are many industries in present which is already disrupted like Banking. Presently, all the banking information like transactions details, timing etc. are maintained by a centralized system which act as an intermediate and charged transactions fees from the customers. By using blockchain there is no intermediate present and transaction can be successfully done using peer to peer network with very less amount of transaction charges with in very less period. It will able to provide the banking services to all over the world where bans are still not present. It allows anyone to send money to anyone instantly with very low transaction fees. Banks also started using blockchain to improve their efficiency. IBM predicts that 15% of the banks will be using blockchain till the end of 2017.

Blockchain is hackproof. All the data present in the blockchain is verified and secured using cryptography and resistant to unauthorized access. With blockchain technology all the processes are broadcasted and is visible to all the computers present in that network so all the processes in blockchain are properly documented and transparent and distributed. It maintains a proper chain. All the processes can be monitored from anywhere making it more secure. Blockchain can be used for copyright and major other issues. Its helps in fair-trade of any product with authentication. Blockchain can be used with integration with cloud which prevents data loss, data hack and human error problems. Blockchain technology can be further used in many different fields like cab booking. In the cab booking system there will be no centralized system and travelers and direct can directly connected without any middle man. Blockchain can monitor the charity process. Voting system, blockchain must be used in voting system so that only original votes are counted and all the process is transparent and hack proof and provide unbiased results. Dubai is aiming to put all its government document on blockchain by 2020. It also helps in universal basic income. Blockchain can help hospitals to maintain and store data and share them with only authorized doctors and patients. Smart contracts can be used to solve licensing issues with their respective creators. Smart contracts give the trust to both service providers and service users.

V. SMART CONTRACTS

As blockchain is peer to peer technology and there is no centralized system there must be some method for verification and maintaining authenticity and this done by

smart contracts. Smart contracts are just a protocol which allow exchange of services without any middle man. The contract between service providers and service users is represented by the code present in blockchain, both are anonymous but their contract is present in public ledger. A contract executed itself according to the coded conditions. Regulators uses the blockchain to understand the market and maintain the privacy of any individual. Smart contracts are autonomous means there is no requirement of any middleman and it also prevents the data from middle man. Backup is always present as the ledger is open to all so if one miner lost any data it will always be present on some other miner. Smart contracts use the cryptography to make our data safe and make our data hackproof. Smart contracts use the advance algorithmic codes to automate task and help to reduce time. It reduces the intermediate transaction cost. It also helps to avoid the errors which occur while manually performing a task. It reduces the requirement of legal authority and their role will be managed through smart contracts. There is no chance of any confusion and there is never need of any litigation. autonomous execution capacities of smart contracts extend the transactional security assurance of blockchain into situations where complex, evolving context transitions are required.



VI. APPLICATIONS

1. Digital currency: Allows instant transaction without any centralized network.
2. Distributed cloud storage: Anyone on the internet can store your data at a pre-agreed price. Hashing and having the data in multiple locations are the keys to securing it.
3. Digital Identity: All the identities are secured and efficient to use.
4. Digital Voting: Blockchain ensures that the vote was successfully transmitted while remaining anonymous to the rest of the world.
5. Assets Management: Ledgers reduces the errors by encrypting the data and prevent from the intermediaries.
6. Insurance: Blockchain provides risk-free and transparent mechanism for insurance claim.
7. Government: Few nations government decided to put all its data on blockchain to reduce fraud and make their data stable.

Blockchain is the emerging technology and its advantages are uncountable. As each process is verified before performing the transaction this

gives the back support to blockchain to change the future of the market.

VII. ADVANTAGES

1. All the processes are transparent and can be view from any computer present in that network reduces the fraud possibility.
2. Problem of redundancy is removed. All the processes are stored on a distributed network so helps to protect integrity and authenticity.
3. Low cost: As it is decentralized and no intermediate is present it reduces the middle man cost.
4. Less time: Blockchain is peer to peer technology with no centralized system helps to save time.
5. Data present in the blockchain is hack proof and cannot be altered once created which makes our data more secure. Altering any unit of information on the blockchain would mean using a huge amount of computing power to override the entire network.
6. Highly advance protocols and algorithms are used to protect our data.
7. One can trust that transactions will be executed exactly as the protocol removing the needs for a trusted third party.
8. Blockchain data is complete, consistent, accurate, timely and widely available.
9. Low risk and increase customer satisfaction in every field.
10. Blockchain may help to set a basic common income.

VIII. DISADVANTAGES

1. Blockchain always uses cryptography which required mining system which need large energy consumption.
2. Every blockchain must be digitally signed using a public-private cryptography scheme.
3. There is lack of privacy using blockchain. All the process is anonymous but can be seen by anyone present in that network.
4. Blockchain is a unique data structure, it cannot solve world's all problems.
5. There is lack of scalability. None of the different platforms have anywhere near the throughput capacity to become a financial platform for the whole world. [6]

IX. CONCLUSION

This paper presents a review on blockchain and working of blockchain. Many terms which are related to blockchain and all the industries which are getting affected or will get affected by blockchain are discussed. Various applications of blockchains with working principle of blockchain and future scope are mentioned. Blockchain is very challenging field which is increasing at highest rate possible yet it is in a critical phase of its development. Future of the internet or next generation internet depends upon the advancement of the blockchain. Highly advance algorithms and protocols

will be used to make blockchain a stable network. All the advantages and disadvantages of blockchain are presented. Despite of some disadvantages blockchain will be the future and advancement in technology can overcome the disadvantages. Blockchain reduces the human error, cost and time by removing the intermediaries.

X. REFERENCES

- [1] Blockchain: Wiki en.wikipedia.org/wiki/Blockchain.
- [2] Youtube: youtube.com/watch?v=93E_GzvpMA0..
- [3] Youtube: youtube.com/watch?v=sDNN0uH2Z3o..
- [4] Youtube: youtube.com/watch?v=G3psxs3gyf8.
- [5] Blockgeeks: blockgeeks.com/guides/smart-contracts.
- [6] Quora: quora.com/limitation-of-blockchain-technology.