International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 04 | Apr 2020 www.irjet.net p-ISSN: 2395-0072

Blockchain in Healthcare

Nithin Revanna

Masters in Information Technology in Networking and Cyber Security, Macquarie University, Sydney, Australia

---

Abstract - *Blockchain innovation has demonstrated its extensive versatility as of late as an assortment of market areas looked for methods for combining its abilities into their tasks. The ramifications of the decentralized web are for sure radical in that it empowers us to make automated services, disintermediate existing occupants, and engage people to set up their own safe systems of trade driving them in new ways. While up until this point, the money related administrations have rose to prominence, a few undertakings in other administration related zones, for example, healthcare services demonstrate this is starting to change. Different starting stages for blockchain development in the healthcare services providers are the focal point of this report. This paper summarizes blockchain and following explanation of its structure, underlying process, Proof of Work, Proof of Stake and recent advancements specifically in the healthcare domain. Also, the current problems in the healthcare is highlighted and ways of resolving this problem is deeply discussed. Blockchain has given us the opportunity to build modern, efficient and patient centric systems. The prospects of patient's compounding data are invaluable. This massively boosts the healthcare domain and indeed revolutionizes it. Thus, blockchain brings trust, interoperability and security which helps a lot in the way medical industry is going to work in the future)*

***Key Words*: Blockchain, consensus, ledger, miners, healthcare, patient.**

1.INTRODUCTION

Digital databases have been around for some time now, yet as of not long ago they've been intended to concentrate data on one PC or inside an association. As an innovation, at its most essential level, the blockchain can be comprehended as another sort of database. Decentralization character is what that makes this database diverse.

As Melanie Swan writes in her book [1], Initially, there were the centralized computer and (PC) standards, and afterward the Internet changed everything. Mobile and person to person communication or social networking has been the latest worldview. The current rising worldview during the current decade could be the connected worlds of computing depending on blockchain cryptography.

The first ever blockchain was conceptualized in 2008 by Satoshi Nakamoto. It was later termed as Bitcoin, a shared electronic money framework. The blockchain concept served as a foundation in 2009 for the digital currency, bitcoin, recording all the transactions in an open ledger.

It was in the later stages when the concept of blockchain was separated from bitcoin. This was a great revelation as a vast number of implementations of blockchain was found out from the usage as bitcoin in digital currency field. The underlining innovation had an increasingly broad application past digital currencies in its ability to work as a distributed ledger, tracking and recording the trading of any types of significant worth. The bitcoin configuration was a motivation for different applications, and it has assumed a significant job as a large-scale proof of concept inside only a couple of years.

The second generation blockchains today serve as a platform for building applications by network developers, basically the beginning of its progression towards distributed virtual computers. Advancement of the Ethereum platform made this technically conceivable. Vitalik Buterin founded Ethereum in 2013, who describes it as a decentralized blockchain based distributed computer platform for building applications [2]. The framework went live right around two years after the fact, and it's been very fruitful drawing a large and dedicated group of developers, supporters, and organizations.

Blockchain is basically an open, digital ledger that records transactions among individuals or companies through a network without any middlemen. The decentralized structure of blockchain enables trust between two parties as it eliminates any dependency on third parties or centralized institutions. Unprecedented, but blockchain is hugely relevant in an age of globalization and a new set of 21st century challenges that require mass collaboration

1.1 Structure of Blockchain

Blockchain can be termed as a distributed highly secure database. It is a series of blocks interlinked with one another such that each block will have information of its previous block. This block can be referred to as a record or a transaction for which a hash is generated for each entry.

A single block or a node can store the timestamp, unique hash value, the original data and the hash value of the previous node. As depicted in the Fig. 1, usually the principal block is known as the Genesis block and does not contain any previous hash values. Each insertion of data to the block is encrypted and is allotted with a unique value called the hash.

In the network cluster there are special computers termed as mining computers whose job is to mainly do the following:

- Approve the current transaction.
- Add them to the block.

• Communicate the finished block with all the other nodes so that every block has a duplicate of the updated database.

Here we are eliminating any centralized component to check whether the alterations made to the databases is true. This structure ensures highest level of security by preventing any infiltration of data that may occur in the middle of any transactions.

The validation is reliant on a distributed consensus algorithm. To add an entry into the blockchain database, each computer must agree on the new entry and no other computer can make any adjustment without others agreeing. After this is complete, the permanent record is added. This interlinking of blocks goes on to innumerous extent with connection being made in the same chain in a linear chronological order with each addition

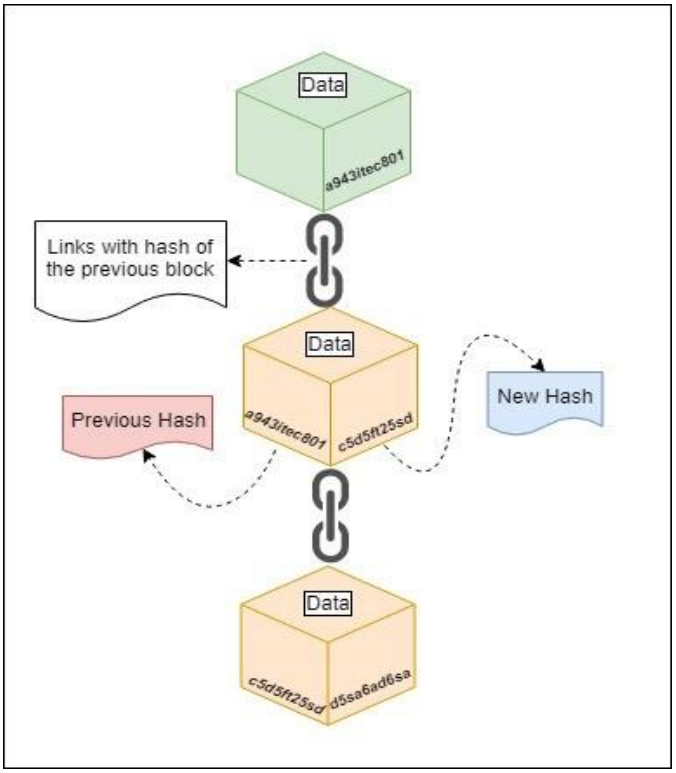

Fig -1: Structure of Blockchain

Transactions are immutable as there is always a dependency created between two consecutive blocks because each block comprises a hash value of its preceding block. All the blocks are tightly interlinked with each other. So, if one block is changed, then it is easily identifiable and thus is tamper-proof.

1.2 Advancements of Blockchain

The first generation blockchains work with point of view being only databases, nevertheless the technology is currently progressing to come to be far more superior than it is. Because the second generation by now delivers the ability to carry out any computer code on the blockchain. The system is evolving to become a globally distributed cloud computing infrastructure. Yet blockchain remains noticeably a work in progress once seen from this perspective, blockchain technology runs to form a permanent and reliable database. This makes blockchain's shoot ball for the storage of transactions that entails great risk as it holds responsibility of handling the database with highest security. These encrypted distributed records are known as distributed ledgers which holds a replicated and shared digital data, synchronized, and spread globally across multiple sites, countries, or organizations being supported by a distributed network of computers. Such ledgers are used for any type of asset records like financial transactions or the army unit. This may consist of physical properties like cars, homes or even the digital assets like currencies, patents, digital identity, health care information or every type of useful data facilitating the replace of large amount of confidential data within each company with one distributed database that is trusted and made available to all the groups engaged in this respect. The blockchain permits trust between organizations which will generally not confide in each other.

The outcomes significantly improve our capability for collaboration between organizations or between individuals peer to peer without dependency on third parties, centralized institutions. Likewise, they result in complete transparency and numerous different efficiencies. Many centralized organizations that may be internally optimized, however the whole hierarchical space in the middle of them is extremely inefficient with huge amounts of border contact, redundancy, arbitrage and resources squandered on rivalries. By enabling these trusted inter-organizational networks, these ledgers empowered the formation of organization and coordinated effort where beforehand there was none, for example, a cross sector supply chains or for various healthcare service providers to work together around the patient's needs

2. UNDERLYING BLOCKCHAIN

2.1 The Process

A blockchain may be considered as a progression of blocks of information that are securely tied together. New blocks are shaped as participants insert new data or modify the existing data. These blocks are encrypted and are allocated with a unique hash value that represents the data inside that block. This hashing is based on a standard algorithm being kept running over the block's data to compress it into a hash.

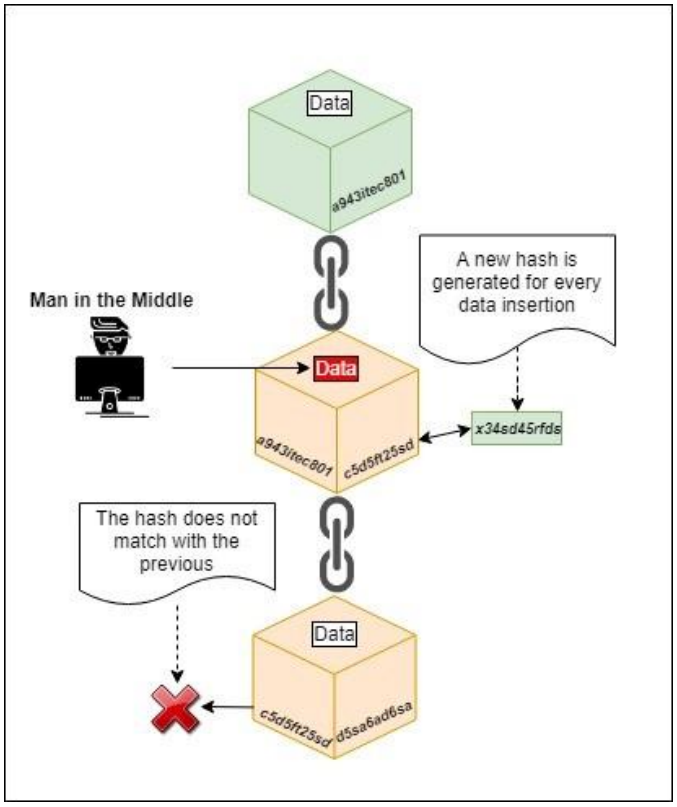

Fig -2: Immutable transaction

Regardless of how enormous the record or what data is contained; it is compressed into a 64-character secure hash. The file's integrity can be confirmed by recalculating the hash value but not vice versa. The data contained within blocks cannot be recreated and is encrypted.

All newly created blocks, following the first block are encrypted and chained to their respective previous one. In this way, once recorded, the data in some random block cannot be altered thereafter without changing all subsequent blocks along with the hash pointer that links to the past block. Also, each block typically holds a timestamp that helps us to recognize any data modifications at any time. The hashing and chain structure of the blocks make them efficiently resistant to any alteration of their data, making them immutable and incorruptible records.

2.2 Blockchain Security Method

Blockchain security methods employ public key cryptography. The blockchain uses addresses through which assets, say bitcoins can be virtually located. These addresses are comprised of "private key" and "public key". A public key can be generated with the help of hashing algorithms like SHA256 which outputs a series of random numbers. The obtained output represents the blockchain asset's address that can be shared over the network. This public key helps to only virtually locate the asset or transaction but cannot initiate any transaction. For example, bank account number can be shared with someone who can just send you money but will not be able to access your bank account and initiate any transaction from within. Unlike the public key which is shared, the address also holds a private key which is likely to be a secret or a password kind of thing that provides access to the owner to their digital assets or ways to generally interface with their corresponding data which corresponds to account password in the bank account example mentioned previously. As a whole, public key is associated with the private key so that anyone can make an encrypted transaction to the public key address, but that encrypted message must be decrypted with the private key that corresponds to that public key. In such a manner effective security just requires keeping the private key secured.

Also, the blockchain is a distributed system meaning there it does not involve any centralized organization that maintains and verifies the database entries. This database is rather kept up by an enormous number of computers that are motivated to give resources required for processing by acquiring some form of tokens in return, but these computer nodes in the network themselves cannot be trusted individually. But the system provides a mechanism where the dispersed parties do not have to trust each other for creating consensus, instead they just need to rely on the mechanism by which their consensus has been arrived down. The transaction validation task can be taken up by any node or computer connected to the blockchain network and a duplicate of the latest blockchain is automatically downloaded. When entries are made to the database, these changes or progressions are automatically reflected across the blockchain network.

2.3 Proof of Work

Proof of Work (PoW) is an algorithm in blockchain platform that confirms the transactions and produces new blocks to the chain. Before the new block is added to the chain it is verified by a group of people, known as miners. Miners are required to crack a computational puzzle, known as the proof of work problem, for which they must compete among themselves. This process is called mining and the first miner to solve the PoW problem will be rewarded.

Advantages:

- Protects against DDOS attacks- As the POW task requires high computing capacity, so as the effective attack also.

Disadvantages:

- Useless calculations- Mining involves lot of processing power required to solve the complicated mathematical puzzle, resulting in huge expenditures.
- 51% attack- Also known as majority attack occurs when majority of miners acquire majority control over the hash rate. The attack may result to mining monopoly and the double spending problem where they can reverse transactions.

2.4 Proof of Stake

In contrast to PoW where miners race, Proof of Stake (PoS) is a pseudo random election process of nodes for the transaction validation. PoS algorithm elects the node based on their wealth or stake. This process is named as staking. In simple words, more the number of coins an individual hold, more the chances of that staker being elected for the transaction validation task. The proof of stake system usually uses transaction fees as a reward.

Advantages:

- Improves scalability by keeping the entire network occupied in the validation process.
- Less energy consumption compared to PoW.
- Prevents 51% attack.

Disadvantages:

- Less decentralized network i.e. staking helps the rich get richer.
- Nothing at Stake (NoS) problem.

3. BLOCKCHAIN APPLICATION IN HEALTHCARE SECTOR

3.1 Problems in Healthcare

Despite of what state a patient is in, the doctor must run a progression of tests even if doctors from another hospital have effectively done so. This situation is a result of failure in retrieving the patient's data from another hospital, causing loss of time, patient's money, and putting the patient's life in danger. The absence of interoperability is acquiring us a major issue in healthcare organizations.

3.2 Blockchain scenario in Healthcare

Imagine we have a system like a ledger which holds patients' details including their past medical history. Now if the ledger is made accessible for the doctors or pharmacists of healthcare service providers, only upon the consent of the patient. Now comes the blockchain [3].

The whole process can be divided into 5 steps

1. Healthcare service providers collect information from the patient

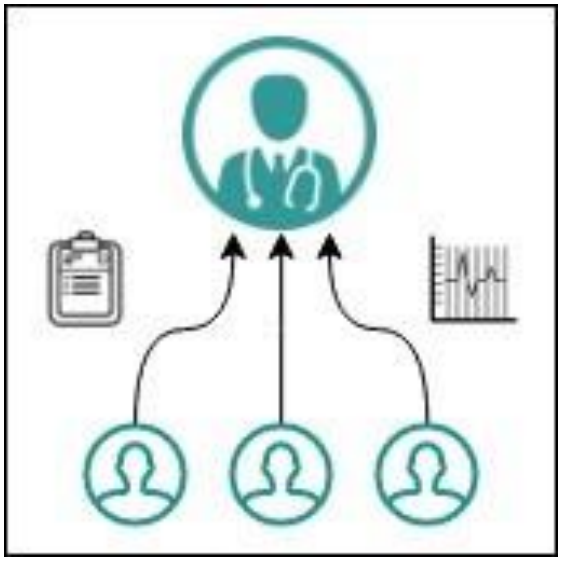

Fig -3: Information Collection

2. The data is then stored in existing database

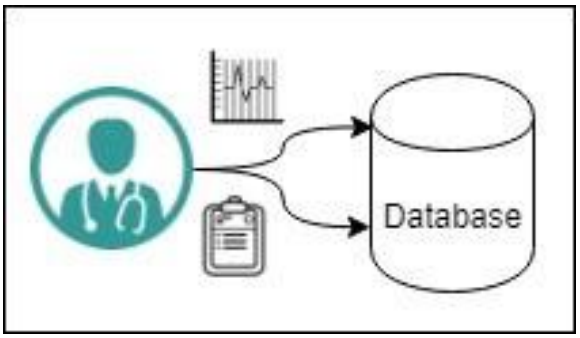

Fig -4: Database Storage

3. Creates a hash from each source redirecting to the blockchain

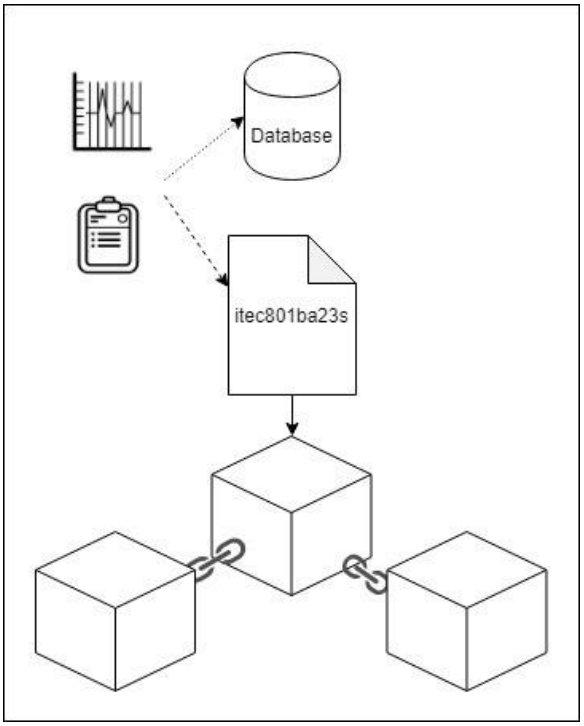

Fig -5: Hashing Algorithm

4. The patient decides who can access his medical records

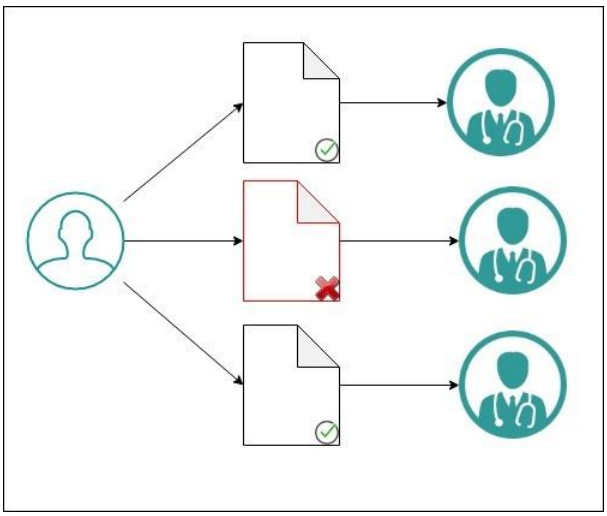

Fig -6: Records Retrieval

5. The healthcare stakeholders can gain access to the data by querying the blockchain

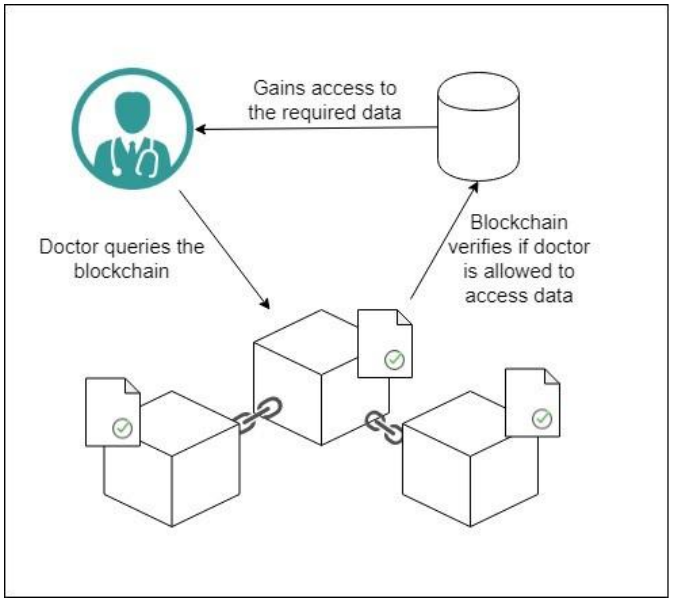

Fig -7: Blockchain Construction

For example, let's consider a patient diary where it says that patient y undergoes this kind of surgery when he/she went to that hospital. The content of the information cannot be seen because of the privacy rules; however, you can see what kind of documents have been produced.

We manage and create access to the sensitive information through smart contracts.

Smart contracts are contracts that are written as code into the blockchain. These contracts employ event-driven architecture i.e. the contract automatically starts executing as a reaction to a triggered event. For instance, here in this case, when a doctor asks for permission to access the information, if the patient gave consent, the contract automatically executes and makes the data available to the doctor [3].

Blockchain and smart contracts provide two big advantages. First, this implementation is patient-centered as the patient authorizes his medical records. Though the patient cannot alter everything or delete things upon his wish, he at least decides who is permitted to access his details or medical history. This solves the trust issue in the healthcare sector. Second, the blockchain can act like a catalogue that lists all the medical records of the patient and all his medical history. That way the next time you visit the doctor, instead of having him do all the tests again, he will just have to look into the database, under patient's consent, for the required information [4] [5].

Table -1: Pros and Cons of blockchain in medical field

Sl. No.	*Pros*	*Cons*
1.	Blockchain helps assemble patient history all in one	A comprehensive version of patients' history would be

Sl. No.	*Pros*	*Cons*
	place.	always preferred.
2.	Blockchain could help making medical records accessible faster to the physicians during any case of emergency.	The easy access to any medical records will always tend to encourage the insider privacy breaches.
3.	The full-information catalog provided by blockchain will allow multiple points of care to take action in concert for that patient instead of the regular stereotypical manner.	The whole Blockchain reputation was based upon Bitcoin & many people in healthcare will struggle to see the correlation and will equate it with privacy risk.
4.	The doctor, the customer, the hospital, the pharmacy and other relevant participants work on the same data set.	The management of data is still not streamlined as it has too many vulnerabilities for attackers to exploit.
5.	Provides cost efficient maintainence of patient information while speeding up the access to therapy.	It is not easy to work with legacy systems and introduce blockchain.

3.3 Blockchain in Pharmaceutical supply chain

Drug manufacturing process is a sensitive production process management where reputational and liability issues are related. According to World Health Organization (WHO), fake drugs is an increasingly worldwide hazardous issue with rising percentage from 10 percent across the world and 30 percent in developing countries, regardless of various regulations (e.g. Drug Supply Chain Act (DSCSA)) struggling to preserve integrity of the drug supply chain [6] [7]. The counterfeit drugs may cause adverse health issues because of their off-base ingredients' dosage or contaminated way of production [7].

Blockchain implementation in this area enables us to track the drug pathway from its source to destination. This is achieved through timestamping of the medicines. Timestamps helps in product identification, tracing, and verification providing the product's owner, place and time of origin. Blockchain records any change in proprietorship and the components of every product, making it accessible to everybody. This approach was employed to purely fight the manufacturing and supply of counterfeit drugs [7].

4. CONSTRAINTS OF BLOCKCHAIN

Although blockchain has great potential, it faces many constraints, limiting for the wide usage, some of major challenges includes

Scalability: With increasing transactions the blockchain storing becomes colossal. Transaction on each node to validate on the blockchain as they have to examine if the source of the current transaction is unspent or not. There are constraints such as restriction of block size and time interval used for generating a new block, for example Bitcoin blockchain can process verging 7 transactions per second
As total transactions count is swiftly increasing with addition of new block, for every few seconds, the volume of transactions is likewise an existing constraint with blockchain
Lack of Inducement and Desireless to Adopt: Creating a large network of connected nodes is creating a major monetarily driven challenge

Usability: The concept of Blockchain transaction is unfamiliar with most of the people, for example in medical records sharing, patients have to manage their key pairs in order to provide cryptographic signature.

Secure Identification: In health care sectors, there is a need to tie patients' identification to their care records across different healthcare providers which is critical and non-trivial.

Performance: For Bitcoin network, Mining is used for support which consumes energy to a great extent, this high energy consumption degrades the performance of the network and not suitable for mass adoption. Speed is measured by TPS transaction per second. The bitcoin network theoretical maximum capacity is up to seven transactions per second. While the Theorem, blockchain as of 2018 can handle about 15 transactions per second.

Standardization Challenges: For the deployment in healthcare applications, suitable standards must be expounded by standardization bodies. For example, in case of healthcare information stored on the blockchain, information such as what data, size and format to be sent to blockchain as to be clear. Thus, it must be well defined what medical data is stored on or off the blockchain.

Cost: It does not cost a huge amount to run the network to pay the miners for upholding the ledger. large transactions such as transferring money but making a small transaction by purchasing a tea could not be done by maximum blockchains. They simply can't in their present form, they deal with a very large amounts of small transactions such as will be required to enable high volume machine to machine exchanges. It would prove too expensive to operate these kinds of economies that involve many small exchanges

5. POSSILE IMPACT OF BLOCKCHAIN IN THE NEAR FUTURE

Recent study shows that over seven hundred cryptocurrencies are listed and different kinds of blockchains appear. This Blockchain is used in various fields such as stock marketing, medical field and with the benefits of blockchain it can be extended to other fields also

As the Block chain has storage and performance issues combined with big data it can be categorized as data analytics and data management, for storing the important data in distributed and securely data management is used. Blockchain can also be used to validate data, for instance a blockchain used to store health information of patients can protect information from tampering and it is hard to steal private information.

In data analytics, Transaction on blockchain can be used for big data analytics this helps the developer to visualize the pattern/trend in transaction. Other emerging technology can be combined to take a new technology architype. Combing data analytics with data vacation and IOT and cloud utilization, with the proper utilization of cloud and big data we can construct a distributed global cloud computer where in storing the data can be eased by using a cloud and large number of transaction can be handled with the help of big data.

Blockchain applications are mostly used in financial domain such as Bitcoin, this technology can be extended in different field, for example storing the user reputation on a blockchain, the upcoming startups can make use of blockchain to improve performance. A smart contract can be implemented with blockchain, in blockchain smart contract is fragment that could be executed by developers(miners) automatically

Although future in the healthcare sector seems to be promising, the practicality of the healthcare using blockchain is untested. But the features blockchain promises to add would help in improving the current healthcare system quality and services. It would empower the patients to take more control of their medical data and handle their overall health condition. So that it they can measure accurately their overall healthcare

6. CONCLUSION

To date, we have had an internet patched onto the side of an economy operated through the many centralized organizations of the industrial age, creating a strong contradiction between the underlying technology and the institutional arrangements. The distributed web will work to transform this by merging information networks and economic organization as the flow of information and economic value becomes one. This will greatly reduce our dependency on centralized organizations, expanding markets. As systems of organization, the global market economy will become available to the many through small distributed peer-to-peer interactions, running through web protocols as the decentralized Internet takes us a step further into the network economy.

REFERENCES

[1] Wood, G., 2014. Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper, 151(2014), pp.1-32.

[2] Kumar, Tanesh, et al. "Blockchain Utilization in Healthcare: Key Requirements and Challenges." 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom). IEEE, 2018.

[3] Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J. and Amaba, B., 2017, June. Blockchain technology innovations. In 2017 IEEE Technology & Engineering Management Conference (TEMSCON) (pp. 137-141). IEEE.

[4] Mettler, M., 2016, September. Blockchain technology in healthcare: The revolution starts here. In 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom) (pp. 1-3). IEEE.

[5] World Health Organization, "Growing threat from counterfeit medicines, "Bulletin of the World Health Organization, vol. 88, no.4, pp. 241-320, April 2010.

[6] Kassab, M.H., DeFranco, J., Malas, T., Laplante, P. and Neto, V.V.G., 2019. Exploring Research in Blockchain for Healthcare and a Roadmap for the Future. IEEE Transactions on Emerging Topics in Computing.