Block Chain Based Health Care System

Dr.D.Shanthi [a], Dr. M Trupthi [b]

[a] Associate Professor, Sreyas Institute of Engineering and Technology
[b] Associate Professor, Chaitanya Bharathi Institute of Technology
email: [a]drshanthicse@gmail.com, [b]trupthijan@gmail.com

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 4 June 2021

Abstract: The use of block chains means that parties who don't trust each other must maintain a shared ledger of data. According to their submissions, the parties agree on the states, their values, and the facts of the matter are the same. and tedious and gratifying to maintain a grip on the basics of the technology and to offer is keeping pace. Healthcare data is more common in the world today than it was even a decade ago, as cloud computing becomes ubiquitous It is absolutely critical that data for patient use be secure and protected. Information and data security is important for almost all organizations, whether in business or in private use. You may find it difficult to track down the majority of this data in the event it falls into the wrong hands, however sensitive, in nature. information can be erased because of disasters, for example, but information loss to hackers or malware is more devastating. When each page of a ledger contains a transaction, the page acts as a block in the block-chain technology If that block or the page following it has the same effect, the next one that is created will as well. That is to say, when a block is found, it connects to the next block in the sequence, and when it connects to the end, it generates a secure code. Using system data will be a vital to getting access to healthcare information. This is implemented using the block concept and the cryptographic technique of key-based encryption Usesends the hash tables with a validating copies, and cross-checking them with each other to quickly discover which one has been tampered with is critical because they are on millions of nodes Establishing a database for healthcare system data If you add more healthcare data to the system would have to store it securely.

Keywords: Block, Block-chain technology, ledger, cryptography, hashing, Health care.

1. Introduction

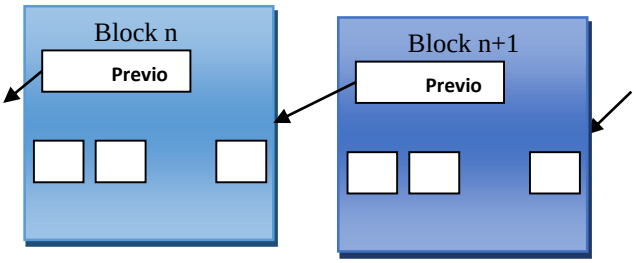

Figure 1: Simplified representation of Block chain

In contrast to the Blockchain, a peer-to-to-peer (P2P) network was initially used to make the block chain distributed. Newly, block chain has seen a surge in popularity because it is useful for many different applications other than currency such as the transfer of non-monetary asset and for smart contract operations. The world is strongly leaning towards block chain technologies due to the popularity of Bitcoin's own blockchain. Distributed ledger technology is best understood as an append-only data structure. The log of multiple blocks demonstrates agreement about an ordered information set of transactions.

A blockchain is a system which maintains a permanent record of each transaction or data modification made to a file and transmits them to every party that needs to see them. In the more specific case of a block chain, it is defined as a shared, permanent ledger that uses blocks to track peer-to-to-peer transactions. Block chain is a database, but it does not hold data on one central server, like a traditional database does. There is a constant stream of public data, but it is accessible only to those who have permission to look at. This is a visual representation of how data is stored in a decentralized and centralized. Each participant has a private key and an openly accessible public address. A connection to an entity can be established using the public key, but identification is made only in one direction with the private key. To unlock someone's personal identity on the block, it is necessary to have the private key.

In the summer of 2008, Satoshi wrote about the Block-chain for the world; however, it was fully developed in the spring of 2009, when Bitcoin, a digital currency, was invented. The concept was found to be the distributed ledger, which allows you to implement transactions using block-chain technology. Blockchain has come to represent a disruptive technology in industries including healthcare, retail, finance, and more recently the food

industry. According to Gartner, the analysis of their client, there has gone up by four times since August of last year.

A public ledger of digital events which has been shared across a wide network of parties not validated by a central authority is called a blockchain. It stores information in nonvolatile blocks that can't be tampered with. a blockchain is a public ledger which contains sequential records of transactions which are sequentially linked in blocks protected by secure cryptography the block chain is a network of digital data and transactions that goes across many nodes, one that isn't centralized. Each block [is] a chapter in a sequence that occurs after another, joined sequentially to form a chain. The data part of a block is comprised of one or more transactions, with one block generally consisting of several consecutive transactions. It uses a cryptographic approach and produces a set of data that verifies the identity and ensures the integrity of the message.

2.Data Structure of Block chain

Figure 1.2 shows a summary of the data structure of Block chain. Block chain consists of multiple blocks, each of which has information of block ID, previous block ID, and multiple transaction contents. A block is linked to its previous block via the previous block ID, and this relationship continues to the first block. A block ID is created as a hashed value of data included in the block, and it affects all the successive blocks. Thus, if a block content is altered, all the successive block IDs should be changed accordingly. This means that the tamper resistance of Block chain is very high because an attacker needs to alter the entire successive block IDs even when it tampers with only one transaction in a block.

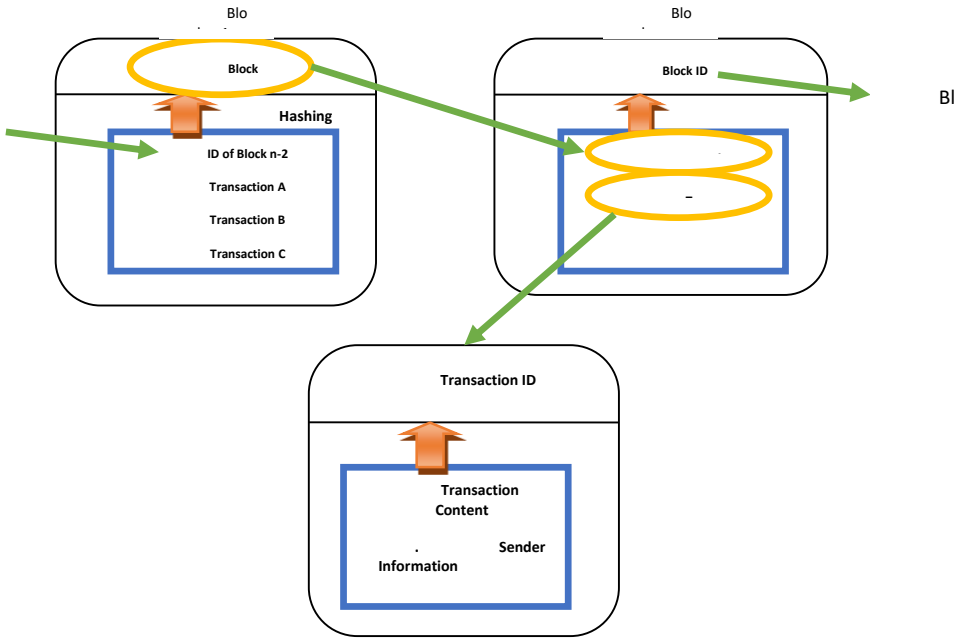

Figure 2: Data structure Block chain

The lower half of the figure shows an overview of the data structure of a transaction. Each transaction has transaction ID and transaction contents. The transaction contents include information of the sender, receiver, amount of remittance, and so on. The transaction ID is a hashed value of the transaction contents. A write query in Block chain appends a new block to the last block in Block chain. It does not update nor delete any blocks including transaction contents, transaction ID, and block ID.

3.Technical view of Block chain

Cryptography is used in the Bitcoin's original block chain to secure it. in this context, the replicated database serves as a record of currency transfers among participants in the crypto-currency network. blockchain transactions do not need not just be for digital currency changes; they can apply to any digital asset state that happens on top of it, too. In the first generations of blockchains, only cryptocurrency transactions took place. New-generation blockchains enable a wider range of digital assets to be recorded and include assets as well. Even if many people use the terms “block chain” and “blockchain” interchangeably, in Bitcoin the block chain is different. From a purely practical perspective, the main issue with block validation is that there is no central authority for this process.

blocks: A block chain consists of two classes: blocks and transactions.

So who use electronic digital signatures?

a collaborative communication network of peers This network has been built with the intention of authenticating transactions and to participate in the process of consensus.

To grasp the nature of the name block, we must think of transactions in the context of being recognized and signed. transactions are bundled and submitted to network nodes that must vouch for them every time a block is verified, it is published to the blockchain and broadcast to all network participants The chain of all blocks is a timestamp and a pointer to the first block, therefore it is a timestamp chain. The decentralized consensus network says that it delivers transactional security across the board. Every time a new information is confirmed, each node registers it in the chain and adds a new block to its own database, it authorizes the solution. Blocks obey the embedded database protocol rules; if there is no single source of truth, the blockchain will maintain that. In a distributed architecture, one central database is established by a single entity, whereas in a block chain architecture, every node has a replicated local database. Even if two separate blocks may temporarily form in the network circulation for a short time, the consensus protocol allows for quick and fluid recovery when they eventually converge. He identifies various types of consensus mechanisms

Different types of consensus mechanism are as follows:

A. Proof-of-work: It is the mechanism used by Bitcoin and is based on nodes competing to a computationally hard problem solution. network use is a significant issue

It is a combination of consensus and Byzantine fault tolerance.

[Proof-of-of-stake protocols] employ a disincentive incentive system to prevent nodes from deviating from the consensus To protect the integrity of the network, validators are required to bet a predefined amount of digital asset on the outcome of the protocol's decision making process. As far as determining a single point of agreement on the state of the network, the consensus protocol works, but also secures the block immutability. Once a block has been cryptographically verified, it is impossible to break the integrity of the entire blockchain. Public-key cryptography and digital signatures ensure immutability throughout the combination. broadband is obtained from a network unconditional action The six fundamental blocks of the bitcoin network

Two main types of block chain can be used in this project:

Permissionless: Anyone can join the network and receive permissionless authentication. Bitcoin and Ethereum are perhaps the best known examples of alternative digital currencies.

It is on a permissiveness basis to a select group of participants. The ripple payment system is a good example of a decentralized systems. There is no mandatory cost in permissionless networks, and thus, the reward in such systems is given to nodes based on the number of validated blocks. In the new generation permissioned block chains, incentives are typically not necessary. Both nodes and participants must be verified for enterprise-oriented solutions to succeed

Cryptographic key pair of block chain

Information concealment For block chain security, cryptography is used. By connecting to the blockchain, people or network, they generate a cryptographic key pair:

an individual key This information should be kept private and not disclosed since it is needed to sign transactions and access cryptographic currencies.

Account public key: the account address of which this is associated with it may be employed to track down the entity that originates a transaction A digital signature protocol is used in block chains to provide non-repudability and authenticity, to guarantee that only the entity with a key can be part of the account participates in transactions. Medical records information management Fact-finding in the Creative sector

Patients are an ever-increasing concern for healthcare administrators, so they have to contend with more and more data on a regular basis. Because of all the year-to-to-year increases in the volume of data, healthcare facilities must work harder to ensure that data is secure.

Industry, Efficacy (implementation of Creative standards) The block chain protects data better than traditional encryption. Nowadays, claims and medical records can be better managed by the new technologies Block chain serves as a way to secure data ownership without any intermediation.

While many believe that disintermediation is a positive advancement, there are a number of benefits associated with the use of a blockchain in the healthcare industry.

Credible examples of the block chain concept in healthcare include the following:

Authenticity, legal traceability

research is essential in order to protect patient privacy.

collaboration/ collaboration

To effectively do we have to have a block-based healthcare system

One of the major advantages of the block chain technology in healthcare is that it is highly decentralized. Since the data remains physical, even when stored in a database, meaning that it is still existing in a collection of bits and bytes. Anyone who has access to the computer has the capability of damaging the database. Block chain distributes trust -which eliminates the need for a central administrator. All users have the ability to store information and make transactions using this application. Since healthcare involves the handling of private patient information, block chain can assist in facilitating that in a secure manner. The decentralized, chain-based approach of Blockstack offers security, scalability, and privacy all in one action. It's a brilliant concept- but it won't address the problems with data management. We mean it would be an evolutionary, one where step-by-by-step rather than suddenly.

4.Literature Survey

Title: Consortium Block chain for Secure Energy Trading in Industrial Internet of Things

Author and Year: Zhetao Li, Jiawen Kang, Rong Yu - 2018 IEEE

Description: In various contexts, the term "Peer-to-to-Peer" has been used, e.g., microgrids, renewable energy harvesting, and P2P networks. Unfortunately, the untrustworthy and nontransparent energy markets do pose a common threat to security and privacy. Block chain addresses the security issues by providing a secure energy trading system. An energetic trust chain can be used in most aspects of P2P energy trading. Instead of fixing transaction rate limiting, which was due to transaction delays on the energy chain, the author has resorted to a credit- based payment system. The Stacberg game is applied for credit-based loans. A three-dimensional system of analysis and a robust results are put to the energy chain and the concept of pay-for-for-performance. androgenous material.[1]

Title: Block chain: A Panacea for Healthcare Cloud-Based Data Security and Privacy??

Author and Year: essay Contest Finalist This paper examines a shifting model in healthcare that observes rising data and services in the cloud, especially convenience (such as having all of one's medical records at the fingertips in real-time) (e.g. economics of healthcare data management). There are, however, shortcomings in the application of conventional primitives and access models to cloud-based environments. This paper considers how healthcare records could be secured using the Block Chain technology. There is a large amount of information being created, stored, and accessed within the healthcare industry, and that much of it is also disseminated. Most data is created during the time the CT or CT imaging is performed, and then it needs to be shared with the radiologist and the doctor. Thus, the results will be collected and stored in the hospital, and made available to other members of the network at a later time. It is apparent that technology can contribute significantly to the quality of care by optimizing personnel, equipment, etc. For example, data contained in paper is expensive to keep, difficult to archive, and may be necessary to access. This, as you know, is the case because individuals working in the learning process find it difficult to view others as workers, unless they are contributing to something of value.

Title: Enabling Localized Peer-to-Peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Block chains

Author and Year: Kang, R. Yu, X. Huang - 2016 IEEE

Description: Peer-to-to-peer (P2P2P) electricity model for providing locally-generated electricity for plug-in hybrid vehicles (PHEVs) has been described in this paper. Modeling does just what traditional systems do in another way: It provides incentives for people to unplug their plug-in hybrids to help balance the region's overall electricity use. Since transaction security and anonymity are significant problems, consortium block chain technologies are inapplicable for most general use, though. the Block-consortium electricity trading method is used to demonstrate detailed transactions in a localized P2P market as well as double-auctionalgorithm iterative solution is utilized to maximize social benefit in the electricity trading Used PETCOWS analysis shows that

transaction and privacy protection are each improved. Real maps for Texas have demonstrated that double auction will also maximizes social welfare without jeopardizing privacy for PHEV owners. Dads never read the latest sci-fi or comic books; they only remember the books from the days when they were being seen as entertaining, successful and really nerdy, with dust jackets removed and insides read.

Title: Peer to Peer Energy Trading with Electric Vehicles

Author and Year: R. Alvaro-Hermana, J. Fraile-Ardanuy - 2016 IEEE

Description: This paper presents a novel power sharing system that reduces the strain on the electric vehicle systems while at work. Also, this trading method is mutually beneficial for all those who are in the process of trading. An artificial population is assigned daily activities and a trip pattern to be calculated using all that data (Belgium). These drivers may be initially limited to three groups; for those who have a full day's charge at their disposal, this question deals with the two groups who aren't. These last customers have the option to take into account grid electricity pricing and their mobility constraints to customize their energy costs of operation. Finally, when all available offer/need information about vehicles in the parking areas are taken into consideration, an aggregator can produce an optimal per-vehicle and per-time price offer for the supply of renewable energy. This allows customers to benefit from excess renewable energy while driving. By applying the trading, this driver's bill will be reduced by 71 in one minute and one zone.

Title: Bitcoin: A Peer-to-Peer Electronic Cash System

Author and Year: Satoshi Nakamoto - 2009 IEEE

Description: It's quite a delicate task to allow both security and operational staffs the flexibility needed to assess the potential consequences of each proposed new changes to procedures, design, and security design policy on the application of current policies and procedures for making future changes more secure. There is a proposal for a purely peer-to-peer version of electronic cash that does not require the use of a financial institution. The majority of the benefits are lost if the transaction must be locked down with a trusted third party like digital signatures. There is no doubt that the most significant chain in the chain of events. In the absence of enough cooperating nodes, an attacker's chain will be split into multiple parts, each of which will outpace the others, as a majority of the CPU power is always controlled by non-colluding nodes. It does not need much of a framework to get running. Messages are not authenticated. Every node does the best it can to find a proof-of-of-work, and messages are no more verifiable after they are seen by other nodes. Litigation [v.t.] the word coined in 1601 to describe court actions of exposing, questioning, and opposing unlawful, invalid, unenforceable, invalid, or unauthorized patents.

Title: Bitcoin:Security and privacy in decentralized energy trading through multi- signatures, block chain and anonymous messaging streams

Author and Year: N. Z. Aitzhan - 2016 IEEE

Description: Transactional security is studied in this paper by N. Z. Z. Aitzhan and D. Svetinovic presents as well as long-standing They've created a testbed for decentralized energy trading with block technology, multi-signature signatures, and encrypted messages to establish transactions without exposing private data. On June 3, 1920, he was first knighted; on that date he finally broke his silence and became a member of the Army Officers Club, although many believe that it was because he found the Miss America Pageant insulting

Title: Bitcoin:Nrgcoin: Virtual currency for trading of renewable energy in smart grids

Author and Year: M. Mihaylov, S. Jurado - 2014 IEEE

Description: Michael Mihovray, Van de Bello, A. A. Avellana, and K. Van Moffaert presented a computerized currency, known as "Nergium" sustainable electricity system producers in the Smart Grid trades are referenced on the open market, with an estimation of its replacement cost already embedded in the system. Because of this, it uses various favorable circumstances compared to cash, it is similar to Bit-coin, however it is unlike Bit-coin in that it's process of being made by infusing computational energy. Additionally, they exchange one view of the universe for a better one based on efficient and renewable power production in the renewable energy grid network

Title: Bitter to better-how to make bitcoin a better currency

Author and Year: Barber et a - 2012 Springer)

Description: Bit-coin has lured a large numbers of investors, say investors in the creative industry, as a result of being unconnected to the stock market. In contrast to e-money, they look at Bit-coin through a top-to-bottom study to comprehend why it has acquired massive acceptance.

Block chain:

Block chain is an emerging technology for distributed and transactional data sharing across a large network of un-trusted participants. In today's life health care system storage data increasing more. Patient data is more important it should be more secure and accessible from anywhere. Here need is to store data securely.

It can be used in some business processes in the retail sector to benefit the customers and the retailers to a great extent.

Healthcare application.

Transportation data.

5.Mathematical Model

We are using healthcare data along with block chain to provide security and privacy. Purpose will secure the patient's drug data, patient's personal data and data related to disease along with doctors data and admin's information. Thus this data related to health care would be taken as transaction in nodes of block chain thus after processing with private and public key, all Authenticated user are to access the healthcare data securely.

Model:

Figure 3: Mathematical model basic framework

U= User of the system

S - System -{I, P, O, Fc, Sc} Where

I- Input

P- Process

O- Output

Fc- Failure case Sc- Success Case

I- {T1,T2,T3,T4}

Where

{T1,T2,T3,T4}- Transaction of healthcare data in .text extension file.

P- {Fc, Hc}

Where

Fc- File is encrypted using advanced encryption standard Algorithm

Hc- Hash value is created for each transaction in block using Standard Hashing Algorithm

Where

Fc - {Pt, Pk, De} Where

Pt- Transaction data in terms of Plain Text

Pk- Private key is generated

De- HealthCare data Encrypted

O - File has been Encrypted and successfully stored.

Sc - It is success case when file of healthcare data stored successfully on network

FC - It is failure case when nodes containing all the transactions are not connected to Network.

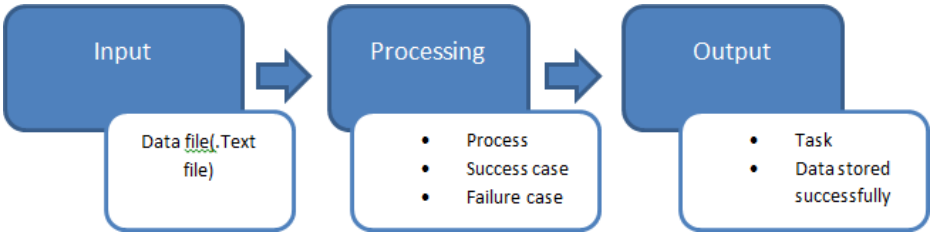

Figure 4: Process Inflow

6.Methodology

This section covers system architecture and flow of the system.

6.1.System Architecture:

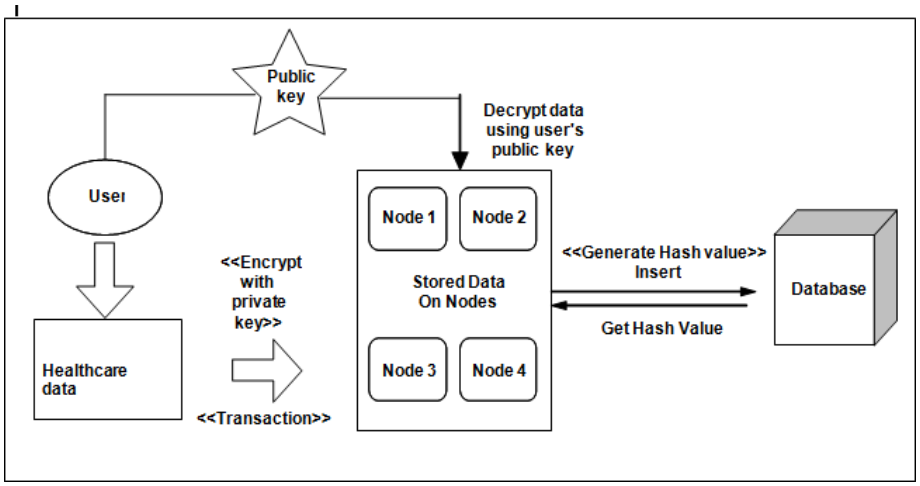

Figure 6: System Architecture

The foundation of an application is based on data, so the integrity of the data is critical. a set of data is generated by the digital signature of the identity and the signer's integrity that identifies it. to ensure that the information comes from the owner and that a certificate's digital signature is valid, the user verifies the signature with the owner's public key Hash is generated for every time a transaction is made in the network and each node, along with its subsequent block, making it possible for health care information to be distributed to the users. In the majority of cases, key-based cryptography is to verify the source of the information is genuine.

There is a large amount of information being created, stored, and accessed within the healthcare industry, and that much of it is also disseminated. In the example, the data will need to be sent to the radiologist, the equipment (computerized tomography and computerized axial tomography) creates it. Thus, the results will be collected and stored in the hospital, and made available to other members of the network at a later time. It is apparent that technology can contribute significantly to the quality of care by optimizing personnel, equipment, etc. Intellectual property captured in paper form is hard to archive, and on hand when needed. Health challenges may result in decisions that are not always correct due to complete information, expensive due to missing information, and international trips to get better information (at increased cost and inconvenience for patients). It is in an industry like this that maintaining security, privacy, and keeping private healthcare data safe are critical. We understand how important it is to implement a sound and secure data management system

for security, this uses a chain concept of blocks and a digital signature Storing the hash tables with data in the blockchain also ensures that other similar copies are immediately identified, as outdated. To secure the entire node, Encryption is applied, and the Doctor app can return it.

6.2.Algorithm and Datasets:

6.2.1.Advanced encryption standard

AES: 128bits (Advanced Encryption Standard). It's an equally simple algorithm. For many years, it had the capability of translating plain text into encrypted text The application of this algorithm is necessitated by DES's failings. As opposed to 64-bit key search attacks, the 56 bit secret key should be considered insecure, as well. blocks of 128 bits were required Rij created it. With this encryption key, the data owner key is being used to encipher the data

Input: 128 bit ,192 bit,256 bit input in terms if 0 and 1 Process: 10/12/14,rounds for-128 bit ,192 bit,256 bit input Hard Disk: 20 GB

State block: Xor (i/p)

Final round: 10,12,14

Each round consists: sub byte, shift byte, mix columns, add round key Output: cipher text(128 bit)

6.2.2.Secure hash algorithm (SHA)

The foundation of an application is based on data, so the integrity of the data is critical. a set of data is generated by the digital signature of the identity and the signer's integrity that identifies it. to ensure that the information comes from the owner and that a certificate's digital signature is valid, the user verifies the signature with the owner's public key Hash is generated for every time a transaction is made in the network and each node, along with its subsequent block, making it possible for health care information to be distributed to the users. In the majority of cases, key-based cryptography is to verify the source of the information is genuine.

There is a large amount of information being created, stored, and accessed within the healthcare industry, and that much of it is also disseminated. In the example, the data will need to be sent to the radiologist, the equipment (computerized tomography and computerized axial tomography) creates it.

7.Conclusion:

The results will be collected and stored in the hospital, and made available to other members of the network at a later time. It is apparent that technology can contribute significantly to the quality of care by optimizing personnel, equipment, etc. Intellectual property captured in paper form is hard to archive, and on hand when needed. Health challenges may result in decisions that are not always correct due to complete information, expensive due to missing information, and international trips to get better information (at increased cost and inconvenience for patients). It is in an industry like this that maintaining security, privacy, and keeping private healthcare data safe are critical. We understand how important it is to implement a sound and secure data management system for security, this uses a chain concept of blocks and a digital signature Storing the hash tables with data in the blockchain also ensures that other similar copies are immediately identified, as outdated. To secure the entire node, Encryption is applied, and the Doctor app can return it

References

1. Zhetao Li, Jiawen Kang, Rong Yu. Consortium Block chain for Secure Energy Trading in Industrial Internet of Things,14, Aug. 2018. 2015 IEEE. ISBN 978-1- 4503-3747-2/15/10. [Online]. Available:http://dx.doi.org/10.1109/TII.2017. 2786307
2. Christian Esposito, Alfredo De Santis. Block chain: A Panacea for Health- care Cloud-Based Data Security and Privacy?, Feb. 2018, INSPEC Accession Number: 17683528. [Online]. Available:http://dx.doi.org/10.1109/MCC.2018. 011791712
3. Kang, R. Yu, X. Huang. Enabling Localized Peer-to-Peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Block chains,Dec. 2017.Copyright 2017 IEEE. INSPEC Accession Number: 17466402. [Online].
4. Available:http://dx.doi.org/10.1109/TII.2017.2709784
5. R. Alvaro-Hermana, J. Fraile-Ardanuy. Peer to Peer Energy Trading with Elec- tric Vehicles, Fall 2016. INSPEC Accession Number: 16157249 . [Online]. Avail- able:http://dx.doi.org/10.1109/MITS.2016.2573178
6. Gareth W. PetersEmail, Efstathios Panayi. Understanding modern banking ledgers through block chain technologies: Future of transaction processing and smart contracts on the internet of mone,18 Nov. 2015 . [Online]. Available:http:
7. //dx.doi.org/10.2139/ssrn.2692487

8. Satoshi Nakamotoi. Bitcoin: A Peer-to-Peer Electronic Cash System,2009 . [On- line]. Available:http://www.bitcoin.org/bitcoin.pdf
9. N. Z. Aitzhan. Bitcoin:Security and privacy in decentralized energy trading through multi-signatures, block chain and anonymous messaging streamse,Oct. 2018 . [Online]. Available:http://dx.doi.org/10.1109/TDSC.2016.2616861
10. M. Mihaylov, S. Jurado. Bitcoin:Nrgcoin: Virtual currency for trading of renew- able energy in smart grids,21 July 2014. ISBN: 978-1-4799-6095-8. [Online]. Avail- able:http://dx.doi.org/10.1109/EEM.2014.6861213
11. Barber et a. Bitter to better-how to make bitcoin a better currency,A.D. Keromytis (Ed.): FC 2012, LNCS 7397, pp. 399414, 2012.c International Financial Cryp- tography Association 2012. [Online]. Available:https://link.springer.com/ chapter/10.1007/978-3-642-32946-3_29
12.