IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 10, October 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 10, October 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0910006 |

Management of Electronic Health Care Records using Blockchain with a Brief study of Decentralization, Scalability, Cryptography and Smart Contracts

Pratiksha Shirsath, Abhishek Shinde, Aditi Chougule, Vishwajeet Sawant

UG Student, Dept. of I.T., Pimpri Chinchwad College of Engineering, Savitribai Phule Pune University, Pune, India

UG Student, Dept. of I.T., Pimpri Chinchwad College of Engineering, Savitribai Phule Pune University, Pune, India

UG Student, Dept. of I.T., Pimpri Chinchwad College of Engineering, Savitribai Phule Pune University, Pune, India

UG Student, Dept. of I.T., Pimpri Chinchwad College of Engineering, Savitribai Phule Pune University, Pune, India

ABSTRACT: The Healthcare ecosystem is a vast and complex network of interdependent members. These members do not have a joint system to manage the data of patients and their records. Solutions are being provided to the many shortcomings such as sharing and accessing medical records as well as providing security and privacy to the records with the help of blockchain. Blockchain is one of the key technologies in the digital reformation of the healthcare sector and it has been researched to have immense potential ahead. It is transforming the way existing medical systems and enterprises have operated in the last few decades. Digitalization and decentralization provide a modern and secure system to the healthcare ecosystem. Here we present a Ledger-based architecture that supports decentralization, scalability, privacy, and secure access to digital healthcare records. In this paper, we propose a solution on how healthcare records can be managed with the help of blockchain. This work presents an electronic healthcare record (EHR) for medical data management and to streamline complex medical procedures. Another purpose of this paper is to indicate the developing use of blockchain in healthcare and to show blockchain research's challenges and possible directions.

KEYWORDS: Electronic Health Record (EHR), Blockchain, Healthcare, Decentralization, Cryptography, Scalability, Smart Contracts.

I. INTRODUCTION

Blockchain is an application model which integrates a peer-to-peer transmission with distributed data storage and consensus mechanisms. It also includes digital encryption technologies, algorithms, and other digital age technologies. It implements decentralization, warrants security, and enhances scalability. The data that is stored in the blockchain is said to be persistent and cannot be changed easily. Blockchain is Decentralized and an open ledger. No separate entity or organization handles the transactions. Blockchain provides us with a peer-reviewed network. This will in turn remove the requirement of 'third party authorization' as everyone in the network will authorize the transactions themselves. An electronic healthcare record is a digital version of a patient's chart and records. It contains information about the patient's medical and treatment history. These records not only contain the treatment information but also help in the betterment of the quality of the care process. EHR's help in easily sharing information with other providers and organizations that are involved in the patient's care. It will additionally help in conducting health research, reduce health care charges and improve patient safety. With the growing advancement in blockchain, EHR systems are an effective method to share patients' records among different hospitals. However, retrieving patients' scattered data is still a challenge. Our aim is to build a blockchain system in the healthcare sector to access patients' data easily in the form of EHRs without relying on a centralized supervisory system.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 10, October 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0910006 |

II. METHODOLOGY

A. BLOCKCHAIN

The blockchain system is a decentralized, peer-reviewed system where there is no central authority on which we have to be dependent. In the healthcare sector blockchain can be used in maintaining electronic health care records. With blockchain, we can protect the integrity, confidentiality, and availability of EHR's. Using cryptographic technologies confidentiality of data can be ensured. Data Integrity is maintained in EHR's with chronological hashes on an immutable ledger and with its availability of information. The first thing about this system is that we move from centralized to decentralized ensuring there is no central authority who will handle our data. Since the data will be handled by all the nodes in the blockchain it can be validated by all. With the consensus protocol, we can make sure that every new block that is connected to the blockchain is valid. Using various cryptographic algorithms, the security and confidentiality of data stored in blocks are achieved. Further with the use of hashing, the integrity of information in the blocks is maintained. User authentication and transaction verifications are done with the use of digital signatures. The healthcare ecosystem is very vast and produces large amounts of data each day. For such large amounts of data to run smoothly on the blockchain, the system should be highly scalable. It should be able to achieve higher Transactions Per Second(TPS) compared to the existing systems either by modifying its Consensus protocols or by using Side Chains or Off-chains.State channels are a type of Off-Chain that can be used to reduce the scalability issue by using Crypto contracts. A Smart Contract is a self-executing contract that specifies the terms of an agreement between the people involved in the contract. It is written in lines of code that are agreed upon by all anonymous parties present in the blockchain. This removes the need for a central authority or legal system.

B. ELECTRONIC HEALTH RECORD

With new tech like EHR, there has been a significant change in the health care sector, but still, it has some problems like different hospitals use different software of EHR which in turn lead to interoperability which is the ability to connect different information systems in a coordinated manner across the organizational bounds. The information available at one location may not be accessible at another location, this, in turn, would result in a waste of time, money, and resources as the other location might have to conduct tests on a patient that already had been done. In the current scenario, the problem faced while usage of EHRs is the patient's access. They do not have complete immediate right of entry to their EHR. We can also observe that the providers of healthcare do not ask for the consent of the patient in case of transfers which implies that patients do not have any idea who all are accessing their records. But if the patients have this access then they won't have to worry about who is accessing their health records and if someone is making changes to their EHRs are valid or not. Our proposed system is used for sharing medical records that do not depend on any third party and no single party has absolute power to affect the processing. This shows that blockchain is an emerging technology in the healthcare field. In this way, blockchain can be efficiently used in the EHR's to enhance the reliability and security of clinical systems.

C. DECENTRALIZATION

Decentralization is the transfer of authority from a single central entity to the other entities in a distributed manner.
It helps in the distribution of information and prevents it from remaining at a single point so that the information can be handled by many trusted servers.
General Comparison: In a centralized system the control stays with a central authority while in a decentralized system the control is shared among the users. Centralized systems are more prone to hacks and data leaks as they have a single authority. This leads to the possibility of failure of the system. A decentralized system allows the users to keep their profile anonymous and hence provides anonymity.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 10, October 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0910006 |

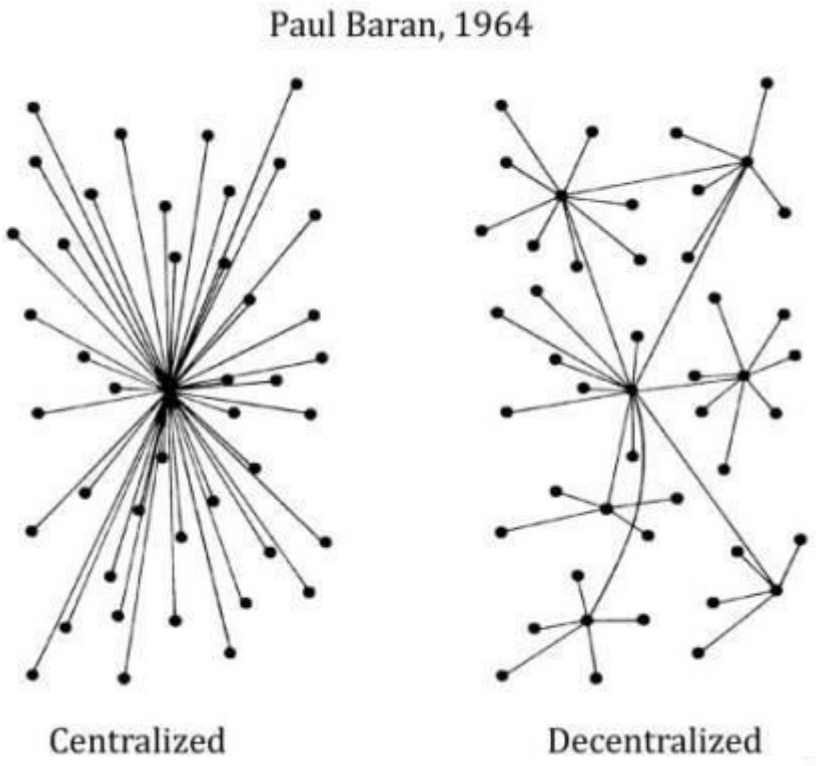

Fig 1: Centralized and Decentralized [10]

A Blockchain-based decentralized model offers the patient's to constraining access to their private data and concerned healthcare officials hence maintaining the transparency of the records. The patients have control over what happens to their EHR. This proposed system can give authority to the healthcare providers to look into a patient's exclusive record, allowing them to make the right call and let the participants enroll their systems into the value chain network without being worried about security and privacy concerns.

The proposed system will enable the patients to grant permission to access their data, and therefore reduce the possibilities of information piracy. It additionally guarantees more accurate identification of illness and making them aware about their tending history. For medical practitioners from completely different establishments that are ceded the permission to access, the proposed model will suggest better detection and medical action. The insurance firms will profit immensely by utilization of the projected model. Insurance providers can use this system to identify malpractices and to handle claims by connecting clients and insurance firms.

D. CRYPTOGRAPHY

Cryptography is the research and process of converting ordinary text into a secret or unidentifiable value. It is only readable to people having access to it. This is used to provide secure communication between two entities using the concepts of encryption. The first step in the process of cryptography is Encryption.

It uses an algorithm and a key to convert plain text input into ciphertext. Encryption can be done in two ways using either Asymmetric Key Cryptography or Symmetric Key Cryptography. In symmetric-key cryptography, the patient's data is encrypted using an adequate symmetric key and transferred to the EHR system with their approval. This same symmetric key is required to decrypt the data when it is accessed. This is a very secure and fast algorithm. The limitation of this method is it requires sharing of keys and if it's compromised it will cause more damage. Advanced Encryption Standard(AES) is one of the most secure and widely used symmetric-key encryption systems. In asymmetric key cryptography, we use multiple keys. The patients' data is encrypted using a public key that can be accessible by anyone. The data can only be decrypted using a private key which is present only with the person who needs access to the data i.e. Patient and if needed associated medical help. The advantage of using this method is that it doesn't involve sharing the key. It is comparatively slow. and due to the public keys not being authenticated can cause frauds. There is also a risk of loss of private keys, which is irrecoverable. A famous example of asymmetric key cryptography is the RSA algorithm.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 10, October 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0910006 |

The second step in cryptography is the conversion of the ciphertext into its corresponding hash value with the help of a hashing function. A hashing function is used to map data of some arbitrary size into fixed-size values. Hash values are the values we are returned by a hash function. Hashing is used for maintaining the integrity of the information. Some common hash algorithms include Message-Digest Algorithm 5 (MD5) and Secure Hashing Algorithm(SHA-2 and SHA-3).

The last step in the Encryption process is providing a digital signature to the block which already has a hash value and session block. Digital signatures are implemented following the signature schemes present. These are used to verify the authenticity of the related transactions by validating the signature. The Digital Signature Algorithm is a standard for digital signatures which is based on the mathematical concepts of discrete logarithmic problems.

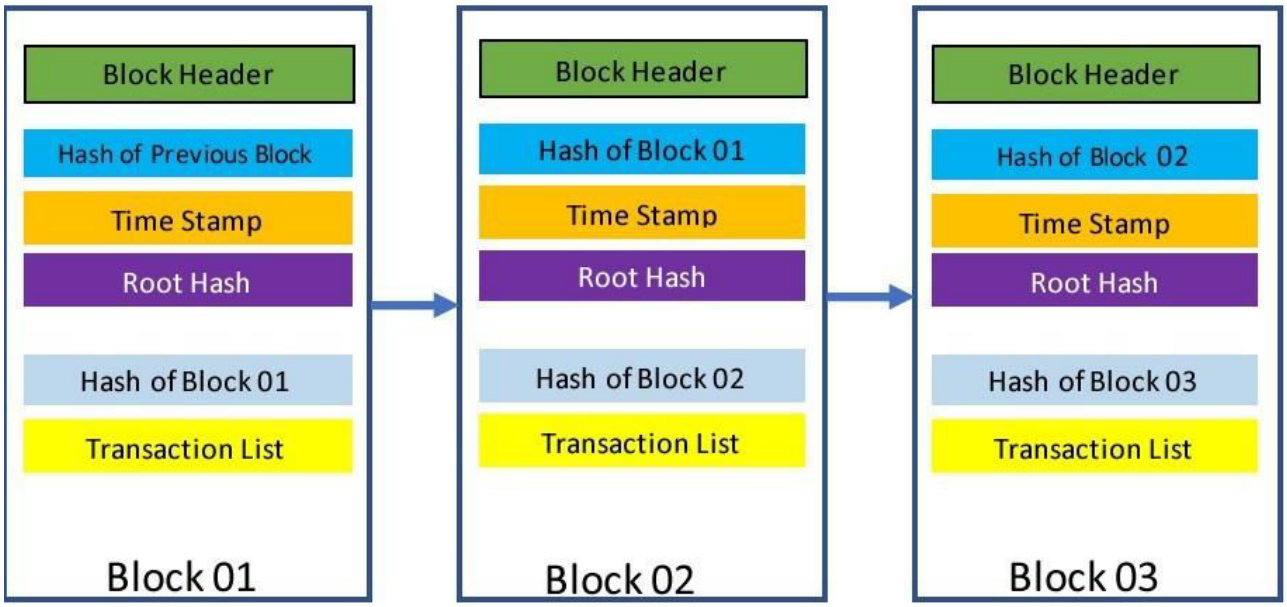

Fig 2: Structure of Information Block [4]

In a blockchain, the blocks contain all the data information of the entire network. The header of the block has the metadata and the body of the block contains all the transaction data. The block header consists of the previous block hash, the Merkle root, and the timestamp. The body of the block will have a list of all the transactions. Each block in the blockchain is identified by a hash value. Each block accesses its previous blocks or parent blocks' hash which is present in the block header. This linking of hashes by a block with its parent block creates a chain. A change in the parent hash will cause a change in the child hash and so on. This causes a cascading effect. No information in the block can be changed as they would also have to change all subsequent parent blocks which is an impossible task to do. The timestamp is used to prove the existence of a block of data. Merkle root is the outcome hash of all nodes in a Merkle tree.

E. SCALABILITY

Scalability refers to the system's capability to handle a growing amount of work, performing a large number of transactions per second without hindrance. In the healthcare sector, the number of patients increases day by day and hence the amount of data.

With this, the problem of scalability arose. This also happens to EHR systems as the patients data is increasing rapidly. In a fully decentralized blockchain, the issue of scalability becomes a dispute as the ledgers present on all nodes should be updated at the same time when any transaction takes place. Also the founder of Ethereum, Vitalik Buterin stated the problem of Scalability Trilemma.

This problem states that from the 3 main components of blockchain i.e. i)Decentralization ii)Security iii)Scalability we can implement almost 2 components in the blockchain. Transaction term in blockchain refers to an event that takes place and is recorded in the blockchain. Transactions in EHR are like adding patients' data to the block, appending the

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 10, October 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0910006 |

new tests or operations results to the block keeping it updated. In existing blockchain systems like Bitcoin and Ethereum, they provide a highly secure and fully decentralized network, but those systems are not scalable.

Mentioned are few blockchain scalability issues: block size, response time, and high transaction fees. Scalability issues arise due to limited block size as with growing patients data the block size increases limiting it to a point in the future. Also the current consensus protocols, every node in the network sequentially validates the transaction before it being published. For a blockchain to operate fast it has performed many operations per second, and with the growing users this rate should keep up with the pace. When a new block is added or some transaction takes place it usually takes a lot of time and huge computation energy is spent which leads to long waiting time and high fees for every transaction. All blockchain supporters recognize the importance of improving scalability for blockchain to be applied in the mainstream; however, the best method to resolve the scalability challenge and what the trade-offs should be are still up for debate. Scalability issues can be reduced either by changing the existing consensus protocols or by implementing sidechains or off-chains.

Consensus Protocols used by existing blockchains are :

1. Proof of Work (POW) is a consensus protocol used by bitcoin. In this nodes have to spend a significant amount of computing power i.e electricity before they can add the block to the chain. This is probably the best way to ensure that the network is secure but also according to the scalability trilemma this will never compete in speed as Bitcoin prioritizes security and decentralization over speed.

2. Proof of Stake(POS) is a consensus protocol used by Ethereum. This algorithm on the Ethereum blockchain is called Casper and replaces miners with validators who stake their funds to bet on correct blocks being appended to the blockchain. POS has its issues but it promises to limit energy consumption and speed challenges of the current blockchain.

On the other we have the following blockchain which tried to reduce scalability issue by altering their consensus protocols :

1) EOS is a blockchain that chooses security and speed over decentralization. It uses a consensus protocol called Delegated Proof of Stake(DPOS). According to DPOS, any EOS holder can vote for 21 block producers who are later incentivized to enforce the rules to prevent double-spending and drive the network forward. With this, they can achieve higher speed and can consume less energy as compared to POW and POS.

2) Stellar blockchain uses the Stellar consensus mechanism. In it, each node gathers a cluster of trusted validator nodes called a Quorum Slice. The cluster then builds a network of trust and limits the energy requirements of blockchain, which in turn increases the TPS.

Other solutions can be :

I. Sidechain is a secondary blockchain, connected via a two-way link originally made to lower the cost and increase the speed of transactions between two or more parties. Sidechains can be used to perform tasks on them, reducing the load on the parent chain by checking if the transactions to be done are valid or not and then implementing it on the main chain. But as side chains are a type of blockchain they need to have their own consensus protocol.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 10, October 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0910006 |

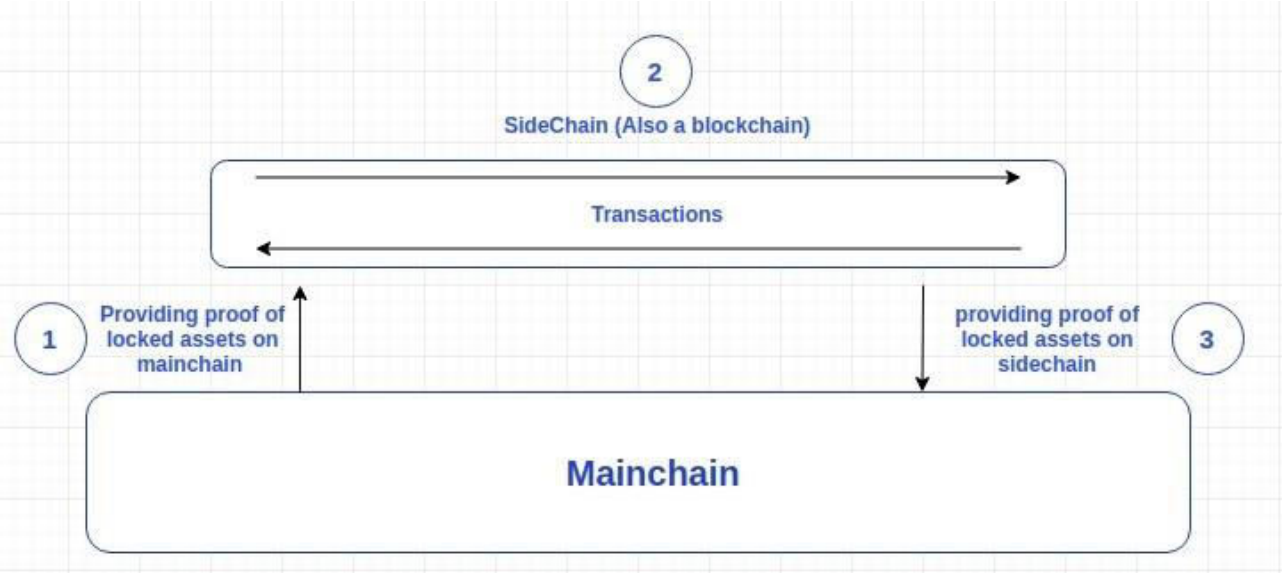

Fig 3: Sidechain [12]

Offchains solutions as the name suggests implies that the entire computation process is performed in a on-blockchain environment without increased risk. As compared to on-chain transactions the off-chain transactions consume less time and energy, entail lower fees, and achieve greater anonymity.By comparing the on-chain and off-chain transactions it will be more clear why we should use off-chain transactions in EHR's. In an on-chain operation, transactions are authenticated and validated by an appropriate number of participants, saving the details of transactions done on the said block and then broadcasts the updated information to the whole blockchain network, which makes it irreversible. To reverse a deal we need at least 51% network hashing power to an agreement.

II. Off-chains can be implemented in multiple ways :

1) Two parties can agree upon some transfer agreement.

2) There can be a guarantor who is a 3rd Party agent, who guarantees to be honest and honor the transaction. PayPal work on this method.

III. State channels are a type of off-chains that perform computations outside the main-blockchain network. To ensure security and compliance with the rules, a part of the blockchain is locked by a Smart Contract that requires participants to reach 100% consensus to update this part of the blockchain. When they fully agree the state is then transferred back to the blockchain and the state channel is closed. In this sense, the blockchain is used purely as a settlement layer to process the final transaction, which helps to lift the burden from the parent ecosystem. By using state channels we can 1) Increase transaction capacity 2) Lower the transaction fees and 3) Process information more quickly.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 10, October 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0910006 |

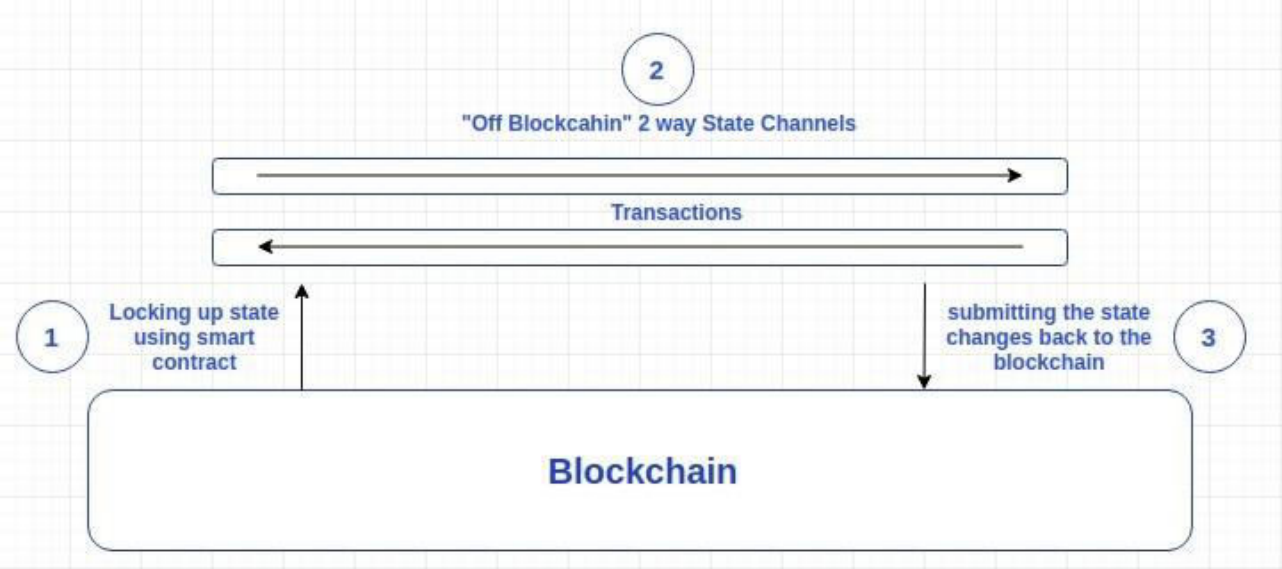

Fig 4: Two-way state channel [12]

Examples of existing solutions:

1. Lightning network where off-chain computations work in a very similar way where a trusted verifiable system executes computations outside of a blockchain. This pertains primarily to operations that would be extremely expensive on the blockchain

2. Plasma is also a similar solution, with the series of smart contracts running on top of the existing blockchain which ensures reliability, the validity of those plasma chains. Plasma blockchain does not reveal block data to the root chain .Rather it only provides the root chain with block header hashes , which is enough to determine block validity. In case of any presence of fraud on the parent chain , the block is rolled back and the block creator penalized.

3. Ethereum sharding breaks the network into smaller blockchains to distribute the computational load.

Advantages of Off-chain Transactions:

1. They can be executed instantly as compared to on-chain transactions which sometimes take many days to execute as it depends on the network load and the transactions ahead of it in the queue that is waiting to be confirmed.

2. Off-chain transactions charge less transaction or no transaction fees in some cases, as no operation happens on the parent chain. But in the case of on-chain transactions, they charge high transaction fees.

3. As in off-chains the details of the block on which transaction takes place, is not publicly broadcasted, the anonymity of the user is maintained, and with it security also.

As the idea of using blockchain in health care is not new, still some issues need to be resolved or reduced. The combination of off-chains and blockchains would favor EHR's because at any given time multiple patient transactions are occurring. Using off-chains fewer transactions would be sent to the parent chain, each patient's transaction would take place anonymously and hence users can perform a large number of transactions.

F. SMART CONTRACTS

A crypto contract is an automated contract which specifies the terms of the agreement between the two concerned entities. The language which is designed for writing smart contracts is Solidity. A layer of logic and computation is added to the trust infrastructure supported by the blockchain with the use of Smart Contracts. Any transaction in Ethereum includes a transfer of ethers that requires fees or gas points to be specified. Miners are paid fees for security, validation, and implementation of smart contracts. With crypto contracts, various agreements and verified transactions can be accomplished without the need for any legal system or external enforcement mechanism among anonymous parties.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 10, October 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0910006 |

Smart contracts are used to create a representation of existing medical records stored in the individual network on the nodes. Better interaction between doctor and patient is possible because of smart contracts. Data transactions are signed with the patient's or doctors' private keys. The data ownership and viewership permissions shared by members in peer-to-peer private networks are represented in the block contents of a system.

Smart contracts along with Distributed ledger technology solve various challenges in the healthcare system. DLT is a decentralized database that is managed by multiple members across multiple nodes. Blockchain is a type of DLT where the transactions are stored with an unchangeable digital signature. Multiple transactions are grouped into blocks and the new block added contains the hash of the previous one, linking them together, hence proving why distributed ledgers are referred to as Blockchains.

The smart contracts contain three types of blocks in managing healthcare records:

1. Patient-defined permission: which will allow doctors to access or share patient information or health data.
2. Clinical metadata: All the required information for accessing the stored data files are in clinical metadata.
3. The patient attaches his private data directly to the chain (self-collected health data)

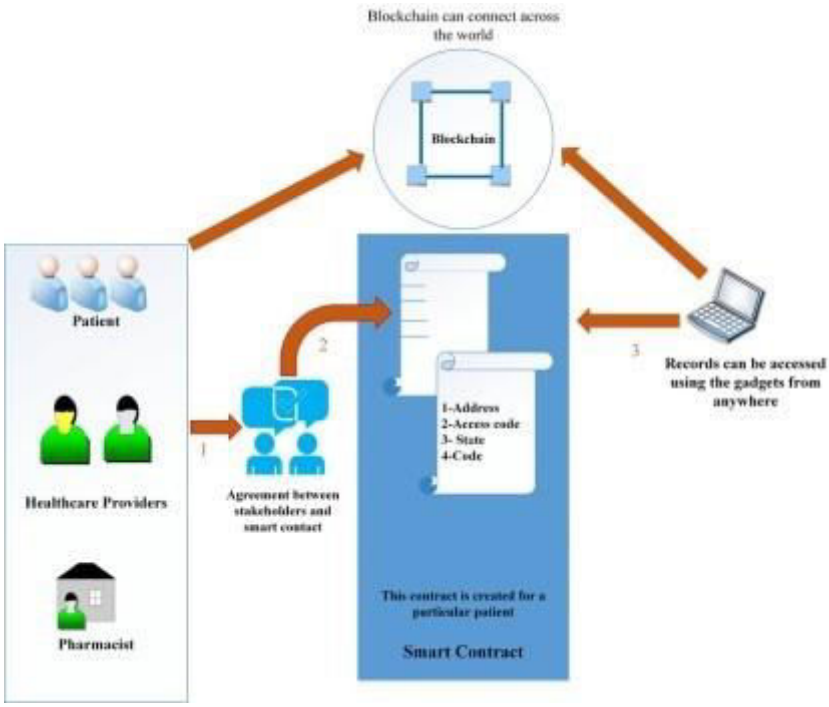

Fig 5: Smart contract for healthcare scenario [5]

Users of this healthcare ecosystem are doctors, patients, and pharmaceutical companies. They can send / store patient's medical records through this system. All these records along with the medical transactions are sent for verification to the blockchain network. These verifications are carried out with the help of distributed ledger and smart contracts. Once verified they are sent back to the blockchain network. These records can be accessed using gadgets from anywhere.

In a blockchain network, cryptocurrency is awarded to the network nodes for their help in providing the decentralized system with the data integrity. Users have to pay the price for the operator's incentive for performing computations and storing data. We can not openly distribute health information in a public blockchain. A partly centralized and partly decentralized approach is a possible step towards decentralization.

Growth in research can be achieved if patients could give access to their health data from a health data ecosystem by the usage of smart contracts. It can be promoted by multicenter research centers by the generation of smart contracts for

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 10, October 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0910006 |

the particular study. The EHR could suggest some possible studies from the clinical trial register and enlist them for the concerned patients in their health records. Authorization can be given by the patient simply by approving and signing the smart contract for the study. The analysts thus get admittance to the radiological data, clinical data, etc of the patient. For study population acquisition we can have a foundational change because a global decentralized EHR system would also include patients from developing countries. All hospitals would be able to participate in these multicenter studies nationally and internationally because an EHR will provide the infrastructure to make it possible. All study related management tasks are predetermined by the study protocol which is managed by the smart contract system. Managing studies by smart contract will lead us to a new way of research funding. The partaking centers can give study tailored research fundings by the significant clinical study backed by a research foundation.

The pharmaceutical industry is another application in healthcare, where Smart Contracts can be written for different produced medication batches. Medications of patients can be identified through the connected side chain from the pharmaceutical company to the EHR. All batches are personalized to the treated patients which are conciliated by a smart contract. When the batch cannot be verified in the blockchain, then the batch must stop the distribution because that batch is considered a fraud batch. This complication can be resolved by a fraud-solving smart contract by notifying the client and the supplier.

III. CONCLUSION AND FUTURE WORK

Our blockchain-based Electronic Healthcare Management System (EHR) shows how decentralized principles can be used in the medical, pharmaceutical industry. Managing complex medical procedures and the enormous amount of data is possible with the help of blockchain. By providing interoperability and accessibility to the system using blockchain technology and smart contracts we signify an inventive approach for data management. This system permits the sharing of patient data and their incentives to make the system user-friendly for medical researchers. We have implemented a system for managing and maintaining huge chunks of data based on demand from a medical perspective. Blockchain technology ensures privacy, security, and atomic control of access to EHR. The main objective behind using blockchain technology is to improve the healthcare process and patient satisfaction. Using smart contracts in blockchain technology the transaction cost is reduced because it removes intermediaries or third parties and reduces administrative burdens. Blockchain efforts also focus on improving the collection and sharing of patient's data with an authorized person like patients, researchers, and sub-processors of data. This will help patients to share their medical records freely and very securely with their respective doctors or hospitals. This will resolve the current issues faced by the healthcare system which includes data silos, problems related to networks based on older protocols, difficulties in an unstructured collection of data, lack of data security, high administrative expenses and unexamined privacy issues.

REFERENCES

1. Dara Tith and Joong-Sun Lee, "Application of Blockchain to Maintaining Patient Records in Electronic Health Record for Enhanced Privacy, Scalability, and Availability" Institute of Innovative Research, Tokyo Institute of Technology pp.5 - 6,2019.
2. A. Shahnaz, U. Qamar and A. Khalid, "Using Blockchain for Electronic Health Records," in IEEE Access, vol. 7, pp. 147782 -147795, 2019.
3. Javaid Iqbal Zahid, Dr. Alex Ferworn, Dr. Fatima Hussain Ryerson University, Department of Computer Science IEEE Internet Policy Newsletter, March 2018.
4. Guha, Paramita. (2016). Comparative Study of Different Cryptographic Algorithms. International Journal of Emerging Trends & Technology in Computer Science.
5. Kumar, Tanesh & Ramani, Vidhya & Ahmad, Ijaz & Braeken, An & Harjula, Erkki & Ylianttila, Mika. (2018). Blockchain Utilization in Healthcare: Key Requirements and Challenges.
6. Chauhan, Anamika & Malviya, Om & Verma, Madhav & Singh Mor, Tejinder. (2018). Blockchain and Scalability. 122-128. 10.1109/QRS-C.2018.00034.
7. Jamal N. Al-Karaki (2019), Amjad Gawanmeh DASS-CARE: A Decentralized, Accessible, Scalable, and Secure Healthcare Framework using Blockchain,Computer Networks Center, Balqa Applied University, Salt, Jordan
8. T. Mikula and R. H. Jacobsen, "Identity and Access Management with Blockchain in Electronic Healthcare Records," 2018 21st Euromicro Conference on Digital System Design (DSD), 2018, pp. 699-706
9. Al Omar, M.Z.A. Bhuiyan, A. Basu et al., Privacy-friendly platform for healthcare data in cloud based on blockchain environment, Future Generation Computer Systems (2019)

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 10, October 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0910006 |

10. P. Baran, "On Distributed Communications Networks," in IEEE Transactions on Communications Systems, vol. 12, no. 1, pp. 1-9, March 1964, doi: 10.1109/TCOM.1964.1088883.
11. Alyssa Donawa, Inema Orukari, (2020) “Scaling Blockchains to Support Electronic Health Records for Hospital Systems”,University of Kentucky
12. Vaibhav Saini, “A complete comparison of the two scaling methods.” (2018) https://hackernoon.com/difference-between-sidechains-and -state-channels-2f5dfbd10707

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 7.542

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details