BLOCKCHAIN TECHNOLOGY – BASED ELECTRONIC HEALTH RECORD SYSTEM

[1]GUNREDDY LAHARI, [2]Dr,D. William Albert
[1]Research Scholar, [2]Professor
Department of CSE
Ashoka Womens engineering college, Kurnool, AP, India.

ABSTRACT

Years of heavy regulation and bureaucratic inefficiency have slowed innovation for Electronic Health Records (EHRs). We now face a critical need for such innovation, as personalization and data science prompt patients to engage in the details of their healthcare and restore agency over their medical data. We propose a novel, decentralized record management system to handle EHRs, using blockchain technology. Our system gives patients a comprehensive, immutable log and easy access to their medical information across providers and treatment sites. Leveraging unique blockchain properties, the project manages authentication, confidentiality, accountability and data sharing crucial considerations when handling sensitive information Blockchain technology is on the cusp of revolutionizing the way we handle healthcare data, in term of storage and utilization. The main goal is to empower patients to be the centre of their own health record so that, the patient doesn't have to rely on different institutions or hospitals they might visit. Blockchain technology and smart contracts provide an interesting and innovative way to keep track of Electronic Health Records (EHRs). This technology could help the patients to have better control of their own data. Health professionals and institutions, such as hospitals, could have access to patient's data owned by other institutions. We demonstrate how blockchain technologies can be used to handle EHR while improving the efficiency of operations through streamlining processes and transparency. A modular design integrates with providers' existing, local data storage solutions, facilitating interoperability and making our system convenient and adaptable. We incentivize medical stakeholders (researchers, public health authorities, etc.) to participate in the network as blockchain "miners". This provides them with access to aggregate, anonymized data as mining rewards, in return for sustaining and securing the network via Proof of Work. This enables the emergence of data economics, supplying big data to empower researchers while engaging patients and providers in the choice to release metadata.

This technology provides patients with an extensive, unaltered records and provides access to EHRs free from service providers and treatment websites. To guarantee the validity of EHRs encapsulated in block chain, we present an attribute based signature scheme with multiple authorities, in which a patient endorses a message according to the attribute while disclosing no information other than the evidence that he has attested to it. We propose an architecture to manage and share healthcare data among different organizations. The proposed work could significantly reduce the time needed to share patient data among different health organizations and reduce the overall cost.

Keywords –Electronic Health Records, Smart Contracts,

I. INTRODUCTION

1.1 What is Blockchain?

Blockchain is a digital-ledger-based technology developed to change the perspective of the digital transactions, or specifically, to replace them. Blockchain is defined as a distinct, decentralized distributed ledger that includes all transactions records related to participating members. Blockchain transactions are created and stored in chronological order, allowing digital assets (such as digital currency and digital data) to be tracked by participants without central record-keeping. One of the key features in blockchain is that participating nodes in the network will hold a copy of the full blockchain. All transactions on the blockchain must be approved because transactions are only valid under the consensus agreement of the participating members. In addition, all transactions are trackable, making fraudulent transactions impossible to bypass.

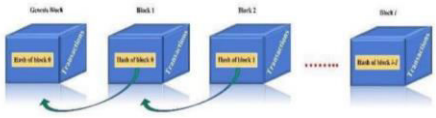

Figure 1.1: Blockchain Architecture.

1.2 Blockchain Technology & Its Dependencies

This technology was introduced by Nakamoto , for his popular work of digital currency or cryptocurrency, i.e., bitcoin. Nakamoto used blockchain technology to solve the double spending problem of bitcoin but soon this novel technology was being used in many other applications. Blockchain is a chain of blocks that are connected together and are continuously growing by storing transactions on the blocks. This platform uses a decentralized approach that allows the information to be distributed and that each piece of distributed information or commonly known as data have shared ownership. Blockchains holds batches of transactions that are hashed thus providing them security and they are managed by peer-to-peer networks. A blockchain has certain benefits such as security, anonymity, and integrity of data with no third party intervention. These benefits make it a reasonable choice to store patient's medical records on it, because the innovation of technology in the healthcare industry has made the security of patient's medical data a top priority.

A number of researchers have also identified that using blockchain technology in healthcare would be a feasible solution as explained earlier blockchain are formed together by a number of blocks connected together in a peer-to-peer network thus making a decentralized application. The header of these blocks contains hashes of previous blocks in them. A block contains three things in it which are data, hash of current block and hash of previous block. When a user (user A) wants to make a transaction to another user (user B) using blockchain, a new block is created to include the transaction. Each transaction is broadcasted across network nodes to verify it. If the new transaction is verified, the new block is added to the blockchain and distributed across network nodes so that other nodes will update their blockchain. Finally, the transaction is received by another user (user B).

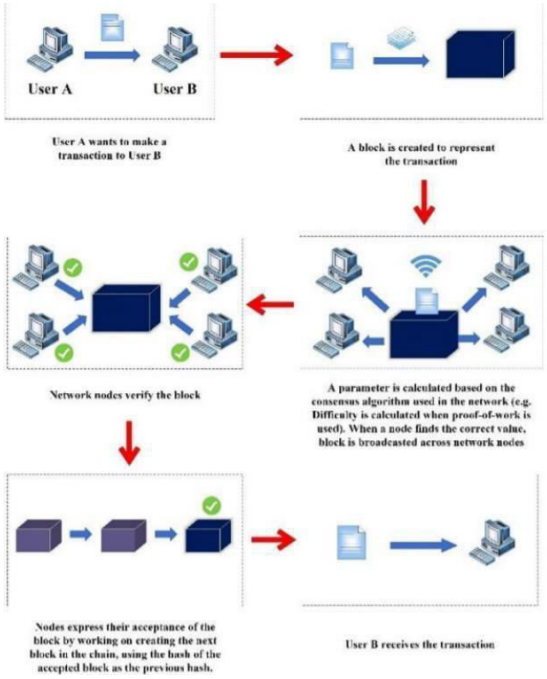

Figure 1.2: Blockchain Process.

Blockchain in Healthcare :

Blockchain technology has been merged and integrated with many types of applications such as Internet of Things (IoT), healthcare, real estate and food security. Among the different applications that use blockchain, healthcare is one of the most interesting fields in current blockchain-based research. This is because healthcare is one of the most regulated industries and blockchain can have a positive impact on the healthcare domain. Blockchain technology has led to tremendous solutions for traditional healthcare domain issues, such as providing a secure infrastructure and integrated private health records. Blockchain can be used to provide secure communication among stakeholders and deliver clinical reports efficiently. Blockchain allows sharing an Electronic Health Record (EHR) in a secure manner since blockchain technology can be extended as a standard for stakeholders. Using blockchain for EHR provides many advantages, such as preserving patient's privacy and improving quality of medical care. The need for patient-centric services and connecting disparate systems have triggered the usage of blockchain. Blockchain provides patients full control over their medical records. Patient information is very case-sensitive and must be stored and shared in a secure and confidential manner. Therefore, it is a prime target for malicious attacks, such as Denial of Service (DoS), Mining Attack, Storage Attack and Dropping Attack.

Blockchain technology was designed by Nakamoto, the basic idea was to have a cryptographically secured and a decentralized currency that would be helpful for financial transactions. Eventually, this idea of blockchain was being used in various other fields of life; healthcare sector also being one of them intends to use it. A number of researchers have carried out the research on this area, these research works focus on the fact that whether the idea of using blockchain for healthcare sector is feasible or not. They also identify the advantages, threats, problems or challenges associated by the usage of this technology. Some researchers also discussed the challenges that would be faced while actually implementing this on a larger scale.

II. LITERATURE SURVEY

2.1 Blockchain

Blockchain seems complicated, and it definitely can be, but its core concept is really quite simple. A blockchain is a type of database. To be able to understand blockchain, it

helps to first understand what a database actually is.

A database is a collection of information that is stored electronically on a computer system. Information, or data, in databases is typically structured in table format to allow for easier searching and filtering for specific information. What is the difference between someone using a spreadsheet to store information rather than a database?

Spreadsheets are designed for one person, or a small group of people, to store and access limited amounts of information. In contrast, a database is designed to house significantly larger amounts of information that can be accessed, filtered, and manipulated quickly and easily by any number of users at once.

Large databases achieve this by housing data on servers that are made of powerful computers. These servers can sometimes be built using hundreds or thousands of computers in order to have the computational power and storage capacity necessary for many users to access the database simultaneously. While a spreadsheet or database may be accessible to any number of people, it is often owned by a business and managed by an appointed individual that has complete control over how it works and the data within it.

Blockchains provide a mechanism through which mutually distrustful remote parties (nodes) can reach consensus on the state of a ledger of information. To trace the origins of these technologies, we start by identifying their essential elements informally. A blockchain is a distributed ledger comprising blocks (records) of information, including information about transactions between two or more parties. The blocks are cryptographically linked to create an immutable ledger. Nodes may append information to the ledger through invoking transactions.

An access policy determines who may read the information. A control policy determines who may participate in the evolution of the blockchain and how new blocks may be potentially appended to the blockchain. A consensus policy determines which state of the blockchain is valid, resolving disputes should conflicting possible continuations appear.

A Database list of records / transactions, like a ledger, that keeps growing as more entries are added; Which is Distributed Copies of the entire database are stored on multiple computers on a network, syncing within minutes / seconds; adjustably Transparent Records stored in the database may be made visible to

relevant stakeholders without risk of alteration; highly Secure Malicious actors (hackers) can no longer just attack one computer and change any records; and Immutable The mathematical algorithms make it impossible to change / delete any data once recorded and accepted

Blockchains leverage techniques from a field of mathematics and computer science, known as cryptography, to sign every transaction (e.g., the transfer of assets from one person to another) with a unique digital signature belonging to the user who initiated the transaction. These signatures are held privately but are verifiable publicly. This means that if a

user with identity A sends an asset to identity B, anybody can verify that the asset was sent by A, but cannot use A's signature for their own transactions. This cryptographic system creates accountability while preventing identity fraud: if you send assets or update information on a blockchain, you later cannot claim otherwise or shift the responsibility for the action. Blockchains also enable the creation of 'smart contracts', defined as self-executing contracts with the terms of the agreement between the buyer and seller directly written into lines of code.

The code and the agreements exist across a distributed, decentralized blockchain network. The code controls the execution, and transactions are trackable and irreversible.

Consensus Protocols Computer algorithms that define the modality of how the blockchain based system defines what is the correct updated state of the database. The simplest version of this would be a simple majority amongst nodes. Cryptography Method of protecting information and communications through the use of codes so that only the recipient can read it. In computer science, cryptography refers to secure communication techniques based on algorithms which transforms confidential messages (like email, credit card transactions, web browsing) in ways that are hard to decipher by third parties. Hashes Mathematical functions that convert data of indeterminate length to a 'fingerprint' of a fixed length.

It is astronomically unlikely for two different sets of data to have the same 'hash'. Merkle Tree Structure (also used in BitTorrent, Git, Bitcoin and Ethereum) that summarises data of all related transactions in a block by producing a digital fingerprint in the form of a hash (or a transaction ID) for each transaction and thereafter for every pair of transactions until only one unique ID/ hash is left (called the Root Hash/ Merkle Root). The structure is built from the bottom up from hashes/ Transaction IDs of individual transactions and tests whether a specific transaction is included in the block or not. It records transactions in a chronological order and can verify whether the record has been altered or tampered with, or whether the record has been branched or forked Mining Refers to the actions nodes take to authenticate transactions.

III. EXISTING SYSTEM

In the existing system the patient may lose control of the existing healthcare data, while the service provider usually maintains the primary stewardship. Patient access permissions to EHRs are very limited, and patients are typically unable to easily share these data with researchers or providers. Interoperability challenges between different providers, hospitals, research institutions, etc. add extra barriers to high-performance data sharing. Without coordinated data management and exchange, the health records are distributed instead of cohesive.

Disadvantages of the Existing System

• Patient has no control or knowledge about his health records.
• There is no proper communication between institutions.
• Databases are not reliable.
• The processes are slow, ineffective and defective.
• There is a lot of cons and swindles.

IV. PROPOSED SYSTEM

Electronic restorative statistics (EHRs) are basic but very responsive to innate information for finding and treat human services, which have to be as often as viable disseminated and shared amongst pals, as an example, medicinal services suppliers, insurance agencies, drug stores, analysts, sufferers' families, amongst others. This represents a noteworthy take a look at on preserving a patient's medicinal history splendid. Putting away and sharing records among various elements. In our system we have proposed the following methodology wherein the Patient has about 90% of the access of the system and rest is accessible to the Doctor. Doctor have the access to view the documents only. Patient only has the access to upload documents and modify them. As the Patient has most of the access which helps us to deal with the confidentiality of the documents.

The System which we have implemented is totally different from traditionally used medical record system in Hospitals. We have implemented Different types of software to setup our project, among which Ganache is the most vital one which deals with whole of our Ethereum Platform. We have eliminated the problem of storing large documents by using blockchain. Our system can be deployed from remote servers also.

Block chain is considered as a new technological revolution that was introduced. It is a peer-to-peer distributed ledger technology to record transactions, agreements, and sales. The benefits of the block chain technology are decentralized maintenance, data saving in the block-then-chain structure, secure transporting and accessing of data as well as anti-tamper and undeniable data security. Taking advantage of these distinguishing features above in an EHRs system, block chain enables the management of authentication, confidentiality, accountability and data sharing while handing information related to privacy, medical resource saving and facilitating for the patient, and making population.

Adavantages of Proposed System

- Providing accurate, up-to-date, and complete information about patients at the point of care.
- Enabling quick access to patient records for more coordinated, efficient care.
- Securely sharing electronic information with patients and other clinicians.
- Helping providers more effectively diagnose patients, reduce medical errors, and provide safer care.
- Improving patient and provider interaction and communication, as well as health care convenience.
- Enabling safer, more reliable prescribing.

V. SYSTEM ARCHITECTURE

Blockchain technology utilizes computer science technique such as (linked lists, distributed networking) as well as cryptographic primitives such as (hashing, digital signatures, public/private keys) mixed with financial concepts such as ledgers. In the blockchain technology, the centralized infrastructure is replaced with a distributed one. Blockchain software runs on thousands of nodes distributed across the entire network. When a new transaction arrives, it is distributed to all the network nodes, when all the nodes have reached a consensus to accept the new transaction into the common ledger, the transaction is added to the ledger. As

the name indicates, a blockchain is a chain of blocks that contain information. It contains:

5.1 Hash: used to uniquely identify a block. Even the smallest change of input (e.g., a single bit) will result in a completely different output. The blockchain technology takes a list of transactions and creates a hash "fingerprint" for the list. Anyone with the same list of transactions will generate the exact same fingerprint. If a single value in a transaction within the list changes, the fingerprint for that block changes. A block also contains the hash of the previous block.

5.2 Transaction: It is a recording of an assets (consist of documentation of specific healthcare services provided). An ID or a hash is generated for that specific transaction as a unique identifier. To validate the transaction, it is signed with a public/private key pair. Each transaction is assigned a block that cannot be altered unless the other blocks in the chain are altered. The transaction should include a digital signature of the contributor to trace the provenance of data. After the documents are stored in the blockchain, the patient would use a web-based or mobile application to view their blockchain contents and to grant or revoke access to specific parties.

5.3 Asymmetric-key Cryptography: (also referred to as public/private key cryptography). They are mathematically related to each other. The public key may be made public without reducing the security of the process. It is used by Health organizations and institutions on the blockchain to retrieve the encrypted data, but the private key must remain secret to retain its cryptographic protection of the data.

5.4 Address: It is a short, alphanumeric string derived from the user's public key. It uses a hash function, along with some additional data. Addresses are not secret and are shorter than the public keys. They are used to send and receive digital assets. They are generated by taking a public key, hashing it, and converting the hash to text.

Addresses represent the public-facing "identity" on a blockchain for a user. When a transaction is added to the blockchain, it is assigned an address. Users or Health organizations must prove possession of the address's corresponding private key. Thus,

when a transaction is digitally signed with the private key, the transaction can be verified with the public key on the blockchain.

5.5 Private Key Storage: It is stored on an external software commonly called a wallet. The wallet is a basic interface and method of access to the system. It can store private keys, public keys, and associated addresses. The wallet software can also calculate the total number of transactions a user may have. It contains the patient's identification to a blockchain. It could be a web-based or mobile application used by the patient to view their blockchain contents and to grant or revoke access to specific stakeholder.

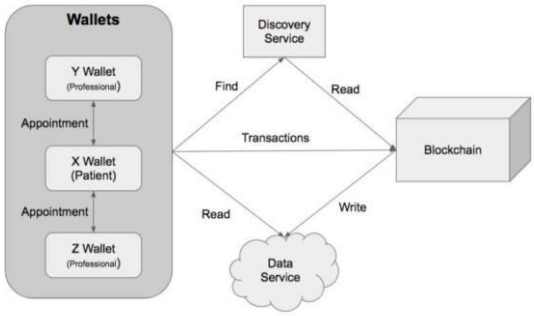

Figure 5.1: Proposed Architecture.

A ledger is a collection of transactions. In a healthcare context, transactions would consist of documentation of specific healthcare services provided. Healthcare providers, payers, and patients would encrypt the data. This information would be stored in the blockchain and could only be decrypted by parties who have the patient's private key. Thus, a ledger is a linked list of blocks where each block contains the patient's public key, the pointer to the previous transaction (hash of the previous block), the encrypted data(hash), and the provider's cryptographic signature. The blockchain ledger will be copied and distributed amongst every node within the network system.

A node is a computer in the healthcare network system. There is no central entity determining which node publishes the next block on the blockchain. Each node maintains a copy of the blockchain and may propose a new block to the other mining nodes. When a new transaction is submitted to a node, there is a mechanism (smart contract) to alert the rest of the network that a new transaction has arrived. The transaction will be added after the require consensus method have been met. This new block will be distributed across the system and all ledgers will be updated to include the new transaction. Invalid blocks will be detected and rejected. Whenever new users join the system, they receive a full copy of the blockchain, making loss or destruction of the ledger difficult.

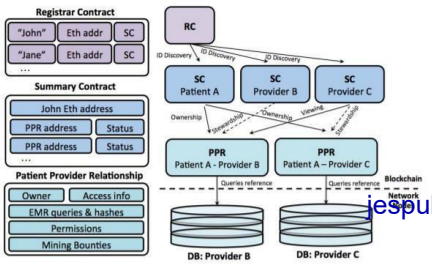

Figure 5.2: EHR system in Blockchain.

To automate and track certain state transitions such as (changing the viewership rights or creating a new record in the system), the blockchain technology uses "smart contracts. A smart contract is a computer program that is stored in the blockchain and can be executed in a virtual machine more specifically it is a computerized transaction protocol that executes the terms of a contract. It is activated automatically when a trigger event occurs." some examples include; the execution of a new transaction, the regulation of conflicts between transactions.

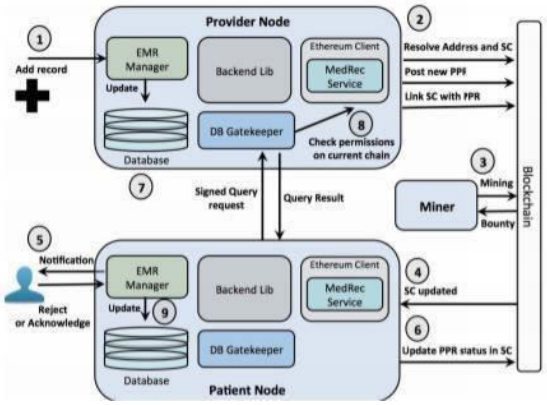

Figure 5.3: Provider adds a new Patient.

Registrar Contract (RC): This global contract maps participant identification strings to their Ethereum address identity (equivalent to a public key). We intentionally use strings rather than the cryptographic public key identities directly, allowing the use of already existing form of ID. Policies coded into the contract can regulate registering new identities or changing the mapping of existing ones. Identity registration can thus be restricted only to certified institutions. The RC also maps identity strings to an address on the blockchain, where a special contract described below, called the Summary Contract, can be found.

Patient-Provider Relationship Contract (PPR): A Patient-Provider Relationship Contract is issued between two nodes in the system when one node stores and manages medical records for the other. While we use the case of care provider and patient, this notion extends to any pairwise data stewardship interaction. The PPR defines an assortment of data pointers and associated access permissions that identify the records held by the care provider. Each pointer consists of a query string that, when executed on the provider's database, returns a subset of patient data.

Summary Contract (SC): This contract functions as a bread crumb trail for participants in the system to locate their medical record history. It holds a list of references to Patient Provider Relationship contracts (PPRs), representing all the participant's previous and current engagements with other nodes in the system. Patients, for instance, would have their SC populated with references to all care providers they have been engaged with. Providers, on the other hand, are likely to have references to patients they serve and third-parties with whom their patients have authorized data sharing

VI. IMPLEMENTATION

MULTI-AUTHORITY ABS SCHEME IN EHRs SYSTEM

We now describe the EHRs system model and detailed ABS construction in this section. The proposal is an ABS scheme with multiple authorities which can be applied in the healthcare with blockchain technology

6.1 MA-ABS FOR HEALTHCARE IN BLOCKCHAIN APPLICATION

Blockchain is considered as a new technological revolution that was introduced as the backbone of the Bitcoin cryptocurrency. It is a peer-to-peer distributed ledger technology to record transactions, agreements and sales. The benefits of the block chain technology are decentralized maintenance, data saving in the block-then-chain structure, secure transporting and accessing of data as well as anti-tamper and undeniable data security Taking advantage of these distinguishing features above in an EHRs system, block chain enables the management of authentication, confidentiality, accountability and data sharing while handing information related to privacy, medical resource saving and facilitating for the patient, and making population healthcare smarter.

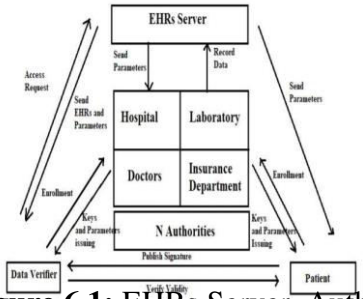

Figure 6.1: EHRs Server, Authorities, Patient and Data Verifier.

6.2 Analysis and Usability

Blockchain technology is a distributed system and should, therefore, involve many participants. To use blockchain technology in healthcare industry, the health organization and other record keeping systems would encrypt the data and send them into the public healthcare blockchain as one transaction (containing patient care data, encounter notes, prescriptions, family histories, etc.). After the documents are stored on the blockchain, the patients would use a web-based or mobile application generally call wallets to view their blockchain contents and to grant or revoke access to specific parties. this technique will facilitate the process of collecting old patient data and reduce the cost of transactions.

To ensure security and trusted access to the patient's data, the ledger component could be implemented using the Ethereum platform. Ethereum uses the proof of work consensus algorithm and its peer-to-peer protocol to secure the state-machine and transition logic from tamping and to share information with all nodes participating in the system. Ethereum is a decentralized platform that runs smart contracts. Smart contracts are programs written in solidity and stored in the blockchain ledgers and can be executed in a virtual machine. They are responsible to store a new transaction in the ledger, to receive and process requests to access, and to grant.

Its development should minimize the possibilities of exposure of sensitive data. The users must create or have an Ethereum account prior to any transaction. Our basic smart contract implementation will define the following types of methods • New Record: Used to create and store a new record containing the patient's information including his address. This address will be used to retrieve the data.

Request access: Create by the institution to request the content owned by a patient.

Granted access: Create by a patient in response to the request access.

Modify record: Create by the institution to update a patient's record. Our implemented system currently running on the test Network, allows a doctor to store new patient's information on the blockchain, allow a doctor to see or update patient's information stored on the blockchain, give or revoke access to any doctor who wishes to access patients' information. Figure 4 shows a basic interface that can be used by a patient to grant access to a doctor with an Ethereum account. and figure 6 shows a basic interface that can be used by a doctor to retrieve the patient's data. the doctor must first check if he has access before doing any further action on a patient's record

VII. RESULTS

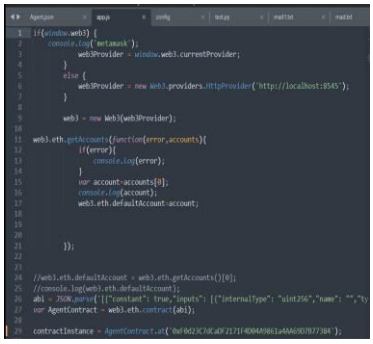

Plate 7.1: Snippet of Distributed App (Dapp) code.

```
f = open('mad.txt', 'r')
currentline = ""
for line in f:
    if line.startswith('>'):
        line = line.rstrip('\n')
        print (line)
    else:
        line = line.rstrip('\n')
        currentline = currentline + line
        print (currentline)

f.close()
f1=open('mad1.txt','w')
f1.write(currentline)
f1.close()
```

Plate 7.2: Snippet of code to initialise Blockchain & IPFS.

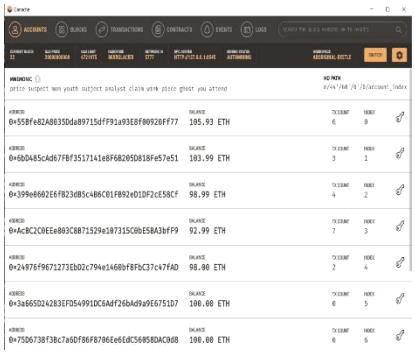

Plate 7.3: Opening Blockchain with Ganache.

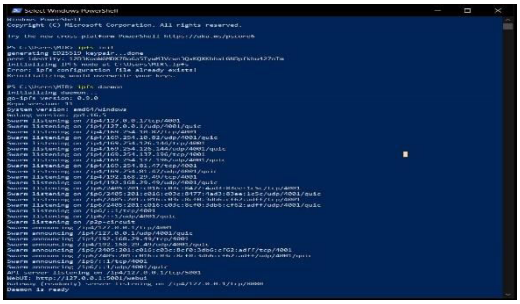

Plate 7.4: Initialising IPFS Daemon.

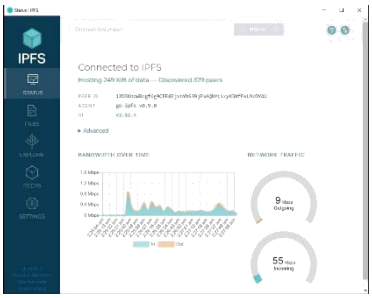

Plate 7.5: Inter Planetary File System.

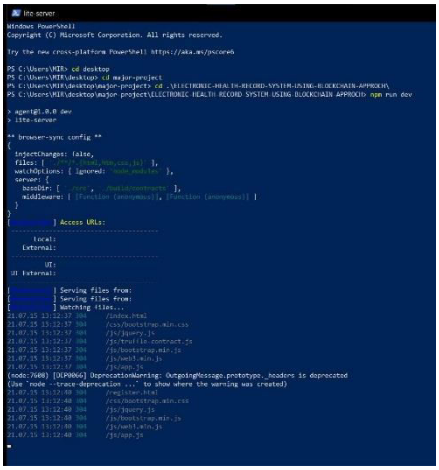

Plate 10.6: Launching Dapp from Windows Power Shell

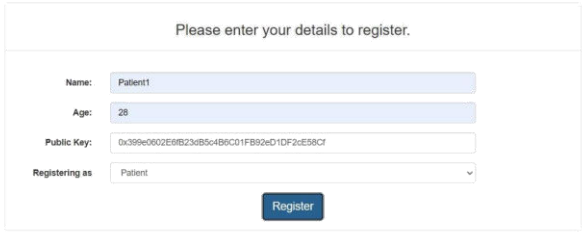

Plate 7.7: Registration of EHR in Dapp.

Plate 10.8: Recovering MetaMask with Secret Recovery Phrase

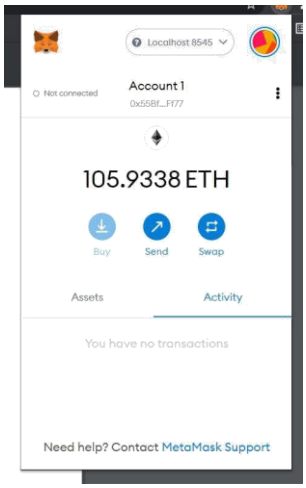

Plate 7.9: MetaMask User Interface.

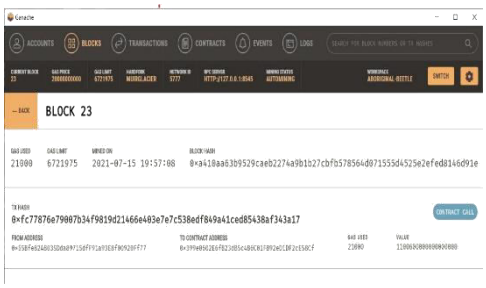

Plate 7.10: Transaction is complete and Block is appended to Blockchain

VIII. CONCLUSION

Despite the numerous opportunities offered by blockchain to improve the current EHR system management, there are also concerns about it that are still preventing its widespread adoption. Several technics and organization challenges must be addressed before it can be adopted by health care organization nationwide.

Scalability constraints: Compromises between transaction volume and available computing power. In the case of Permissioned blockchains, they can expedite the transaction processing times, but they may face computing power constraints due to reduced participation in the network. A nationwide blockchain, with many health care participants, would make the system not only more interoperable, but it would also make it more secure.

Data standardization and scope: Organizations must consider what information is stored in or out of the blockchain. For health care blockchain, the most immediate concern is the size of information stored on the blockchain. A form submission of data to the blockchain, such as doctor notes, could create unnecessarily large transaction sizes that could adversely impact the performance of the blockchain. The blockchain can be efficiently operable with a specific and confined set of data, such as demographic information, medical history, and codes for services rendered. Thus, to standardize data stored on the blockchain, organizations should align on a framework for defining what data, size, and format can be submitted. Participants can also privatize the blockchain to restrict access.

Costs of operating blockchain technology: While blockchain technology enables faster, near-real-time transactions, the cost of operating such a system are still unclear. Health institutions spend a lot of time and money to set up and manage traditional information systems and data exchanges. This requires resources to continuously troubleshoot issues, update field parameters, perform backup and recovery measures. Blockchain's open-source

technology and its distributed nature can help reduce the cost of these operations. Once the blockchain and its smart contracts are configured, the parameters become absolute and reduce the need for frequent updates and troubleshooting. Moreover, the blockchain's transparent information structure could reduce many data exchange integration points and time consuming reporting activities.

Integration with Legacy Systems: In order to make the move to a blockchainbased system, the organization must either completely overhaul their previous system or find a way to integrate their existing system with the blockchain

solution. However, it may be difficult for blockchain solutions to handle all functions needed by organizations, making it difficult to completely eradicate legacy systems. Therefore, considerable changes must be made to the existing systems in order to facilitate a smooth transition. This process may take a significant amount of time, funds and human expertise.

IX. Future Enhancements

The main aim is preserving patient privacy in an EHRs system on block chain, multiple authorities are introduced into ABS and a MA-ABS scheme is used, which meets the requirement of the structure of block chain, as well as guaranteeing the anonymity and immutability of the information. PRF seeds are needed among authorities and the patient private keys need to be constructed. The comparison analysis demonstrates the performance and the cost of this protocol increases linearly with the number of authorities and patient attributes as well. A non-monotone predicate could be used in many distributed system applications, which enriches the representation of the predicate. Supporting general non-monotone predicates in blockchain technology is the direction of future work.

We plan to further strengthen the design of the interface application with login access to allow easy and trusted user interaction, add pointer to get patient's data from the provider database, deploy on the main Ethereum and investigate on the storage capability of the blockchain. We could delegate to the blockchain the activity of data access grant, opening new frontiers to data health management.

X. REFERENCES

[1] M. Mettler, ``Blockchain technology in healthcare: The revolution starts here," in Proc. 18th IEEE Int. Conf e-Health Net., Appl. Services, Sep. 2016, pp. 1 3.

[2] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, ``Secure and trustable electronic medical records sharing using blockchain," in Proc. AMIA Annu. Symp., 2017, pp. 650 659.

[3] S. Jiang, J. Cao, H. Wu, Y. Yang, M. Ma, and J. He, ``BlocHIE: A blockchain-based platform for healthcare information exchange," in Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP), Jun. 2018, pp. 49 56.

[4] M. Meingast, T. Roosta, and S. Sastry, ``Security and privacy issues with health care information technology," in Proc. Int. Conf. IEEE Eng. Med. Biol. Soc., Aug./Sep. 2006, pp. 5453 5458.

[5] A. Ibrahim, B. Mahmood, and M. Singhal, ``A secure framework for sharing electronic health records over clouds," in Proc. IEEE Serious Games Appl. Health, May 2016, pp. 1 8.

[6] Q. I. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M.

Guizani,``MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," IEEE Access, vol. 5, pp. 14757 14767, 2017.

[7] M. Steichen, R. Norvill, B. F. Pontiveros, and W. Shbair, ``Blockchainbased, decentralized access control for IPFS," in Proc. IEEE Blockchain, Jul. 2018, pp. 1499 1506.

[8] Y. Chen, H. Li, K. Li, and J. Zhang, ``An improved P2P le system scheme based on IPFS and blockchain," in Proc. IEEE Big Data (Big Data), Dec. 2017, pp. 2652 2657.

[9] D. Spatar, O. Kok, N. Basoglu, and T. Daim, “Adoption factors of electronic health record systems,” Technol. Soc., vol. 58, no. February, p. 101144, 2019.

[10] N. Atzei, M. Bartoletti, T. Cimoli, S. Lande, and R. Zunino, “SoK: Unraveling Bitcoin Smart Contracts,” in 7th International Conference, POST 2018 Held as Part of European Joint Conferences on Theory and Practice of Software, ETAPS 2018 Thessaloniki, Greece, 2018, pp. 217–242.

[11] www.researchgate.net/publication/336393649_Using_Blockchain_for_Electronic _Health_Record

[12]https://www.ijitee.org/wp-content/uploads/papers/v8i8/H6796068819.

[13]https://medium.com/crypt-bytes-tech/medicalchain-a-blockchain-for-electronichealth-recordseef181ed14c2

[14]https://medicalchain.com/en/

[15]https://www.researchgate.net/publication/324793302_Eletronic_Health_Records_ using_Blockchain

[16] https://easychair.org/publications/open/3fW3