Article

Blockchain-Based Patient-Driven Inter-OperableModel for Healthcare 5.0 System

Kaushal Shah [1,*], Lalit Garg [2,*], Divam Kachoria [3], Vaidehi Shah [4], Shristi Darbar [5], Andrea Visconti [6], Chintan Bhatt [7] and Sudeep Tanwar [8]

[1] School of Technology, Pandit Deendayal Energy University; shah.kaushal.a@gmail.com
[2] Faculty of Information & Communication Technology University of Malta; lalit.garg@um.edu.mt
[3] School of Technology, Pandit Deendayal Energy University; divamkachoria@gmail.com
[4] School of Technology, Pandit Deendayal Energy University; vaidehigmn1502@gmail.com
[5] School of Technology, Pandit Deendayal Energy University; shristidarbar0503@gmail.com
[6] Department of Computer Science, University of Milan; andrea.visconti@unimi.it
[7] School of Technology, Pandit Deendayal Energy University; chintan.bhatt@sot.pdpu.ac.in
[8] Faculty of Technology, Nirma University; sudeep.tanwar@nirmauni.ac.in
* Correspondence: shah.kaushal.a@gmail.com, lalit.garg@um.edu.mt

Abstract: With the rise of powerful computational technologies, healthcare systems are going through a paradigm shift to the era of healthcare 5.0, also known as" smart healthcare". This new-age healthcare system not only enhances the life of patients but also aims to reduce healthcare costs significantly. People's health data is too sensitive to be regulated by particular organizations owing to the increasing threat to privacy and security. The sheer size of data makes it difficult for centralized bodies to regulate, due to which 3rd party involvement is introduced, which again poses threats to the privacy of data holders. Motivated by the abovementioned gaps, we propose a decentralized approach using Ethereum blockchain technology and Oasis protocol. The patient-driven solution approach effectively solves the privacy problem by providing full control of data to the owner. Along with this, byproducts such as fine-grained access control and on-chain data processing capabilities are also obtained.

Keywords: blockchain technology; trusted execution environment; attribute-based encryption; patient-driven inter- operability; Ethereum

1. Introduction

Everyone is well aware of the famous proverb- "health is wealth". Nowadays, it is no more just a saying as health care data of individuals are sold to the highest bidder by centralized authorities. Health records have been increasingly digitized, but the dissemination of this information between hospitals and providers has lagged behind Electronic Health Record (EHR) adoption for various reasons, including technical and privacy concerns [1-3]. To manage this precious entity of life, proper management of data in health becomes the most crucial factor. On top of this, with the outbreak of Corona Virus in the year 2019, the need for a system to manage data, subject to the fact that it is easily accessible and attainable when required, i.e., in cases of emergencies, surged indefinitely [4]. As a result, the pressure on doctors and scientists increased immensely as the number of laboratories and wards was incapable of administering a pandemic crowd [5, 6]. Hence, one of the top-most priorities of data scientists and blockchain developers these days is to encapsulate the immense amount of data related to people in a decentralized, immutable system such that privacy and security are not an issue [7-11]. People are becoming increasingly health conscious in today's era. Therefore, there has been a spike in the quantity and quality of health check-ups. For a comparative analysis of their health, people want all their data to be stored such that it is easily attainable but, at the same time, also secure. Here, blockchain technology can play a vital role [12]. We have used Ethereum as it is one

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 February 2023 doi:10.20944/preprints202302.0178.v1

of the most flexible and efficient blockchain technologies, but any other equivalent blockchain can be used [13]. Our model provides patient-driven interoperability so that patients play an integral role in the entire system and have the power to control it [14, 15].

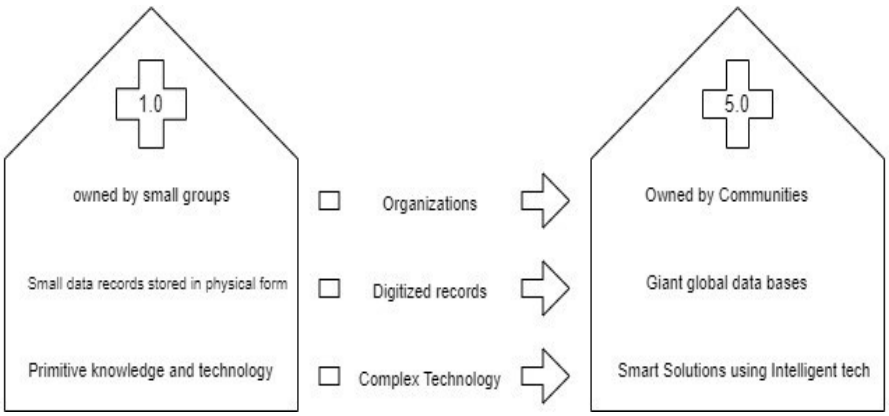

Figure 1. Health care 1.0 to 5.0.

Data handling, analysis and storage are becoming increasingly important in this era. More importantly, when it comes along with security and privacy concerns [16]. As the decentralization of data is one of the latest and most efficient approaches, more and more domains are shifting to using blockchain technology for data storage and handling. With this in mind, we analyzed various techniques and papers written for the same and created a model to minimize the existing solutions' issues while maintaining the pros. Therefore, this paper provides a novel blockchain-based framework to provide a secured and privacy-preserved healthcare data management system. Figure 1 shows the transition from Healthcare 1.0 to 5.0.

1.1. Our Contributions

We design a blockchain-based framework to minimize the cons and maintain the existing solutions' pros. The following are the significant contributions of this paper:

- By integrating the Oasis protocol in a patient-centric health system, we discuss achieving end-to-end confidentiality while ensuring smooth data flow in the pipeline.
- With attribute-based encryption, fine-grained and robust access control management in a system where multiple data producers and consumers are discussed.

1.2. Organization of the Paper

The paper is organized into six sections. Section 2 pro- vides a comprehensive review of the existing state-of-the-art solutions for using blockchain technology in healthcare. The section also identifies the current research and implementation gaps and suggests ways to overcome these gaps. Section 3 provides a detailed description of various components of our blockchain-based system and briefs about their integration. Section 4 details our contribution to the solution of this problem by thoroughly explaining the proposed system and underlying concept with the help of real-world examples. The following section is divided into four subsections describing the model's working in 4 phases. This section includes all minor technical details behind the concept of the solution proposed in this paper. Section 6 discusses our research results in a quick comparison with some existing solutions and briefs about the pros and cons of our solution. The final section provides a concluding summary of the paper. It also includes potential drawbacks and shortcomings of the proposed solution, thus opening the way for future research. Moreover, it also gives insights into possible future use cases.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 February 2023 doi:10.20944/preprints202302.0178.v1

2. State of Art and Improvements

In Table 1, readers can find a summary of various existing solutions for decentralizing healthcare data and its management.

Table 1. A Summary of Existing Models Available for Data-operability in the Healthcare Sector [17] [18].

Year	Technique Used	Observations
2020	Two-level blockchain mechanism [19]	- Privacy preservation is an intrinsic property of the mechanism - Provides transparency in audit trials - Distributed storage helps to tackle one point failure problem
2020	Permissioned Blockchain: Hyperledger Fabric [20]	- Can use more CFT and BFT consensus protocols that don't require costly mining - Smart contracts authored in general-purpose languages - Privacy and confidentiality enabled through channel architecture and private datafeatures - Two parts: – World state: distributed database- current state data – Blockchain: blockchain transaction log- history of changes
2021	Peer-to-Peer information sharing [21]	- Data Immutability with the right to forget - Use of smart contract to authorize the usage of data - Privacy is assured as blockchain stores only hash value corresponding to eachemployee
2017	DLT application pandemic [22]	- Global health supply chain management - Accurate real-time data storage - Data aggregation and trend prediction by retaining the integrity of data
2020	Middleware Ledger System [20]	- Peer-to-peer permissioned blockchain system - Privacy and confidentiality are provided using HLF. It employs channel architectureand private date features - Speedy Data Liquidity using a distributed database called CouchDB
2018	Oasis Protocol on Ethereum [23]	- Managing data privacy and confidentiality using TEE(trusted execution environment) and oasis protocol. - Selective access modifiers give the owner control over variables and functions toencrypt, saving time and resources. - Backward compatible
2019	Blockchain-based PHR [24] [25]	- A personal health record system is a bridge between existing EHR and blockchaintechnology - EHR authorized from the healthcare centre will be injected into the blockchain via the patient,and it will be patient controlled
2016	Healthcare Data Gateway (HDG) [26]	- Patient-centric Electronic health record storage using blockchain. - Use of Unified data schema and secure multiparty computing methods. - Each node has its own data gateway, which manages the data at the end of the nodes and collectively, this layer becomes the data management layer
2021	Smart contracts for consistent permissions [27]	- Simple smart-contract-based logic, so the patient can grant read/write privileges to any user through the master key provided to the patient. Information about the involvement of the third party for key generation is not provided. Furthermore, secure retrieval of data is also not planned well.
2019	Multisig solution [28]	- Ethereum-based smart contract to authorise data by providing a signature of both patient and hospital, thus accepting multiple digital signatures.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 February 2023 doi:10.20944/preprints202302.0178.v1

		Low-level access control is achieved, but anonymous data retrieval for research purposes and secure processing is still missing.
2021	Payer-Provider Patient framework [29]	• Focuses more on payment processing with blockchain in healthcare. • Basis encrypted decentralised record-keeping lacks advanced features such as access controls and secure on-chain processing. For verifiable audits, manual 3rd party intervention will be needed compromising data security.
2020	EHR blockchain [16] [30]	- Features like immutability, cryptographic function for secure communication,interoperability, accessibility, system monitoring - Issues: property trained staff requirements, privacy and security issues, confidentiality and accountability requirements
2021	Medshare system using Attribute-based Encryption [31]	- Fine-grained access control - Searchable Encryption - Search tokens generated by users will trigger the search algorithm on a smart contractwhere encrypted indexes are deployed - Works on a consortium blockchain
2020	Model Chain [32]	- A privacy-preserving predictive model based on a permissionless blockchain - It only disseminates predictive models but not health records, and transparency is not acritical issue - Machine learning takes a considerable amount of time, so transaction speed becomes negligible infront of it
2016	MedRec [33] [34]	• MedRec manages authentication, confidentiality, accountability and data sharing addresses the four major issues highlighted above: fragmented, slow access to medical data; system interoperability; patient agency; improved data quality and quantity for medical research

We will discuss a few prominent models in detail by drawing out their features and drawbacks. Moreover, we will also try to provide certain fixes for the drawbacks of these systems. The central idea of EHR blockchain solutions such as [16] [30] [35] was to make a holistic database for healthcare centres. The paper's authors focused on the features like immutability, privacy, interoperability, accessibility and system monitoring. But one of the major differences between our model and theirs is the feature of patient-driven interoperability. We chose to go with patient-driven interoperability because this system will give control and authorization of individual personal data in the hands of the actual owner (i.e., patient) rather than a healthcare institute or a research centre. Another difference that we come across is access controls. We offer fine-grained access control, while the EHR model does not provide any access control. These models use trivial cryptographic functions, and since they are resource-heavy, they consume more time. Ours, on the other hand, is a fast and efficient model. Medshare system using ABE (attribute-based encryption) [31] rather than patient-driven interoperability. This model offers institution-driven interoperability. In this case, the institution will be able to send data of a particular individual; or even manipulate it internally without informing the patient of the same. Since the authorization access is directly given to the institution, the patient will have to go through a long process to get access to his own health data personally. The principal objective of this model is data retrieval and storage, whereas we propose a model capable of processing data. One of the future use cases of our model also includes on-chain processing. This model, unlike ours, works on a consortium blockchain. We are using Ethereum for our model as Ethereum is more flexible, widely used and compatible with most of the new protocols and technologies. Middleware-Ledger system solutions such as [20] This is a peer-to-peer permissioned blockchain system. This makes it a very complex and complicated blockchain system. Ours gets on in the public blockchain, reducing our model's complexity. They have used hyperledger while we have used Ethereum. We decided to use Ethereum because it is more in use, and most ongoing systems are more compatible with Ethereum rather than hyperledger. Our model offers speedy data liquidity

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 February 2023 doi:10.20944/preprints202302.0178.v1

and significantly solves privacy and confidentiality issues. Works such as Model Chain [32] are based on permissionless blockchain, also used in our design, though there are a few significant differences. While Model-Chain is generally used for storing processed health records, our model stores and processes data. This means that in our model, the patient can directly view raw data too. Since the on-chain processing of ML models takes a lot of time, the speed becomes a significant issue in model- chain based approach. Our model offers speedy data liquidity along with fine-grained access control, while Model-Chain does not describe any information about access control. Several works, such as [33, 34], use previously existing databases of the organization as a part of the solution instead of a decentralized data store. The health centres' databases are used and then converted to decentralized data. But since the institutions still have access to these health records, the patient's privacy is not guaranteed. We have used a decentralized cloud database to preserve patient health data's privacy and confidentiality. While we provide both fine-grained access control and on-chain processing, none of this has been discussed here [33].

3. System Model

The actors of our model are: the data owner, blockchain, peers, Trusted Execution Environment (TEE), and end users. Let us briefly describe them.

3.1. Data Owner

This system gives you versatility in terms of feeding data. Any original data owner can push valid data into the blockchain. Patients' wearables are linked via a cloud, and data generated is fetched time-to-time so that the data stored remains updated. Moreover, patients can use a web portal to directly feed in health reports, lab results, blood tests and any kind of health record in any standard format (image, pdf, XML, HTML, video, and doc) with authentic sources. In an alternate approach, patients can directly ask healthcare centres to push their data into the blockchain- various lab reports and differential diagnostics by medical experts will be directly shared in the blockchain using the healthcare's web portal.

3.2. Blockchain

The system is implemented using underlying concepts of decentralization and distributed ledger, which can provide verifiable computing [36]. In this system, we take Ethereum as a basic blockchain architecture. Various APIs and protocols are used which are compatible with Ethereum. Data owners can define various access policies using smart contracts and other rules (ex: access for a certain time can also be defined). Lightweight consensus," proof of stake", is used in this system.

3.3. Blockchain Peer Nodes

Peers in public blockchains are all users who use the system for data requests. These peer nodes help run the blockchain's internal mechanism, tasks such as validating transactions, maintaining ledgers, and establishing consensus. However, these nodes can be considered as one of the main adversaries of the system as they can try to know the content of transactions; or may try to disrupt the blockchain by creating fake transactions.

3.4. Trusted Execution Environment

The basic building block of the system, the Oasis protocol [23], runs inside the Trusted Execution Environment (TEE). TEE is often hardware-based, and all major CPU vendors already have their TEEs, such as arm-trust zone, intel-SGX, and AMD-SEV. This ensures that even the node operator cannot access transaction data and state. Outside parties can't see the data inside TEE; only the final processed computational results are returned.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 February 2023 doi:10.20944/preprints202302.0178.v1

3.5. End Users

All the data-requester in the system are termed as End Users. In this system, we have divided End-Users into two main categories based on their data demand/request:

1. Users requesting raw data

2. Users requesting processed data

As shown in Figure 2. Patients, doctors, nurses- all these users can be termed as raw data consumers as they require to work with part or whole raw data of its owner. This can be further classified to provide different access types. This will be done so that patients will get full access to their data; doctors can only view limited data for a limited time, and a nurse will be able to view only current treatment and medicines required. On the other hand, research institutes and supply chain management will consume processed data which will apply some function to raw data and then give a final answer. Thus any type of confidential data is not accessible to them.

4. Proposed Work

While researching existing solutions for decentralized data sharing and interoperability among healthcare institutions, we decided that our solution should provide hassle-free interoperability and high-level confidentiality with added security. Our solution focuses mainly on patient-driven interoperability, fine-grained access control and encryption mechanism to hide crucial data from other nodes in the blockchain. Furthermore, in the context of blockchain architecture, we propose this solution using Ethereum architecture (due to the flexibility of the same).

Interoperability becomes a necessity when we talk about data-sharing between various organizations.

4.1. Toy Example

Patient" X" has a previous record which states that he took three treatments at three different healthcare centres." X" wants to retake this treatment at another institute", M", for the same disease. Institute" M" will require all of" X" 's medical history from all previous healthcare institutes. In the traditional system, all or one of the following delay-causing problems will arise:

- Collecting various records from various institutes is a very hectic task, and it will require skimming through a whole pile of records of other patients.
- All institutes might have different formats and conventions in which they save all patients' data. It will take a while to get it all straight.
- The obtained data may not be accepted by institute" M" due to various medical and other professional reasons.
- The authorities will have to re-check and verify all of these records to find any anomaly that might exist. The records might get misplaced or exchanged with another patient.

The simplest solution to avoid all these problems is to make this system patient-centric. The patients authorize which institutes or doctors can read and write data into their profiles. Patient hence has full control over individual data - from its original source to authorizing it for analysis purposes.

Our solution consists of a web-based portal where patients can directly register and manage all their data in the blockchain. This means the patient can manually enter authentic lab reports and other diagnoses to his public address or authorize a healthcare institution to do the same. Thus, our solution provides flexibility in adding data to the cloud. Further, due to the use of blockchain, this data becomes immutable; hence nobody can

 doi:10.20944/preprints202302.0178.v1

change it. Furthermore, this web portal can be transformed into a mobile app for convenience. Consequently, the patients will be notified if their data in the blockchain cloud is being accessed. The patients will also be able to easily provide their data to analysts, researchers, or other health institutes with the help of their public ID.

When we talk about storing data with the help of a decentralized public blockchain, one of the major concerns is privacy and confidentiality. Bitcoin's implementation of blockchain gives pseudo-anonymity to an extent. This is done by using addresses instead of accounts. However, it doesn't guarantee data privacy. An attacker or any malicious node can still see all the transaction data. If thoroughly analyzed, the attacker might determine the particular address by viewing its transactions, thus violating privacy. In the case of Ethereum, accounts are used; in a public setting, it becomes more prone to such security threats. We propose a system wherein the data will be encrypted before being sent to the blockchain. All blockchain operations will be performed using secure multi-computing techniques [22] or inside secure hardware [23]. This ensures that the data will not be decrypted by the node that mines the transactions.

There can be many different users of a shared data systemin the healthcare domain, with different data requests as per their job in the healthcare domain. Thus, the question of access control arises. Our solution includes fine-grained accesscontrol among different users while the data owner manages the access given to any system user. To understand this, we take a simple scenario based on a person named "A"." A" has some disease, and the doctor orders certain lab tests. In this case," A" will have to give almost full data access to the doctor treating him for his patient history- his ongoing medication, his body's reactions to various chemicals, drugs and treatments and so on. On the other hand, the nurse taking care of" A" will be required to know only what kind of disease has been diagnosed and the current medication and treatment techniques for the same. Further, if any research institute is interested in knowing about this disease," A" will share only a specific part with the institute. In addition, our system can directly carry out most of the processing of raw data and can answer research-related queries. Suppose a research institute requires to find the number of people with lung disease in a particular area. In that case, our system can process data and directly return the count while not exposing the patients' private and intricate details. As discussed earlier, on-chain processing will also be done securely so that only the final answer will be transacted to the requester. This may open a way for on-chain secure machine learning in future.

To integrate the above techniques use of the Ethereum blockchain gives us the required flexibility. The use of a private blockchain cloud to store data is proposed. Smart contract-based, Access policy for transactions can be defined such that access for certain data can be given for a limited time frame. Oasis [23] allows us to use lightweight consensus mechanisms based on proof-of-stake, which further reduces transaction time and computation power. With the use of Ethereum, we can easily incentivize our system, if and when needed, for other future applications.

5. The Model's Working

Our model's main components (see Figure 2) are web portal, blockchain, ABE, and data retrieval. In this section, we describe them in detail.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 February 2023 doi:10.20944/preprints202302.0178.v1

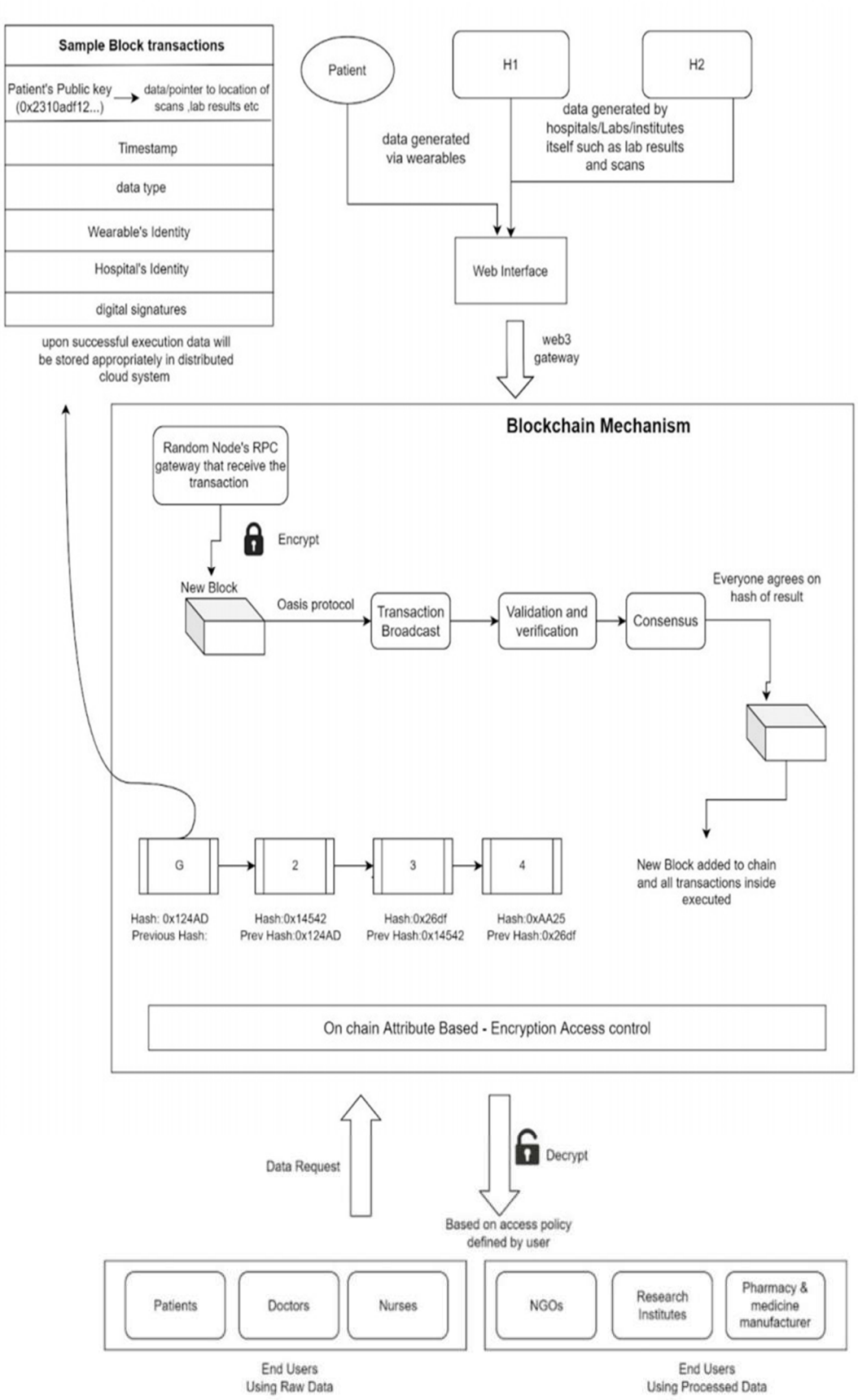

Figure 2. Flow diagram of our proposed model.

 doi:10.20944/preprints202302.0178.v1

5.1. Web Portal

The system contains a web interface that becomes a medium of interaction between blockchain and data owners. The basic functionality of this web interface is to give data owners a comprehensive view of all the data stored in their names. Data holders will get their public id corresponding to their name and unique id (private key). This id will be the data owner's sole address, and every transaction will be performed using it. The system allows more than one account per person, but as the data gets scattered into accounts, whenever there is a need for a brief overview, this may create problems.

Figure 2 shows a sample transaction with specific data fields. Internally data is stored in particular frames with fixed fields such as the public Id of the patient, timestamp, wearable id, hospital id, digital signatures, data type, and index to where the data will be stored in a distributed cloud. This provides an advantage over trivial schema-based databases, such as data holders can upload medical records in any standard electronic format (pdf, HTML, mp4, etc.). In each frame, the data type is filled, corresponding to the data index in that frame. This helps us to track which data stored in the cloud is in which format, and their retrieval becomes speedy also. This format makes it easier to make internal search tokens so that when some keyword is searched, the corresponding search token is searched, and all the frames classified under that particular search token are returned.

Data holders can select what kind of access to give for what particular data; they can select that certain lab reports can be accessed by a senior diagnostic expert only. In this way, they can define various kinds of access policies.

5.2. Inside the blockchain

Figure 2 shows each step inside the blockchain in a brief view. After a transaction is pushed to the blockchain, any data holder pushes data via the web portal. The JSON remote procedure call is made so that remote nodes in the Ethereum network can interact with the incoming transaction. JSON RPC is vulnerable, so the data holder must use an HTTPS connection for secure transactions. Inside the network, a random node will get this transaction; the oasis protocol gives a secure remote procedure call gateway (wrapped on JSON RPC) inside the TEE of every node. Thus, a transaction comes inside the blockchain via RPC, which directly lands in some node's TEE, gets encrypted suitably, and is processed. This encryption takes place inside TEE so that nobody can see the data. The data holder still has to trust the RPC gateway. Another way of doing this is manually encrypting data before injecting it into the blockchain. However, this will hinder web3 compatibility, and all the libraries and APIs must be rewritten. The RPC node then broadcasts it with the help of oasis protocol, ensuring that it is properly encrypted for each node TEE. After that, each node in the network receives the transaction, decrypts it inside TEE, and performs further computation for the hash. Each TEE receives a secret key from the rest to process confidential information. TEE receives its private key from the key manager and derives its state encryption key using that private key. All other nodes use private keys to encrypt data directly into the system, thus achieving end-to-end confidentiality. Oasis protocol helps maintain secure encrypted communication between TEEs of various nodes and provides a decentralized mechanism for all TEEs to attest themselves and broadcast encrypted transactions. The Oasis runtime environment (which runs on all oasis nodes) also provides key management capabilities to facilitate secure key exchange between all TEEs. Backward compatibility with the Ethereum network is maintained by selective encryption of state variables and preserving non-sensitive transaction headers. More efficient, lightweight consensus proof of stake is used. Validators stake their tokens to get a chance to mine/validate certain transactions. If they validate it correctly on selection, they will get the decided rewards with their original stake. Otherwise, on unfair validation, a penalty will be charged. Thus a fair and simple consensus is established. All nodes inside their TEE will verify this hash. Thus, the computation cannot be seen by any node, yet they all can update their ledgers with the same result, achieving consistency. Execution of transaction indicates state or value change, which must be recorded in some form. Ethereum main net records these state changes in unencrypted form in the database,

 doi:10.20944/preprints202302.0178.v1

which can lead to many confidentiality issues. One easy solution can be directly encrypting the data inside TEE. It is the easiest solution, and encrypted data can be stored in a database with indexes known by TEE. This method has a huge downside regarding the Ethereum implementation and efficiency of the system. Whenever a smart contract is in pure view and no function needs execution, all functions are for reading the existing values rather than processing resource-heavy tasks. With the help of the oasis protocol, our system can easily solve this problem as it allows us to mark specific data as secret. This will always be stored in encrypted form. Hence, only the node's TEE can read and execute new transactions against it. Any node can directly perform other pure view functions without encryption-decryption taking place. This method saves a lot of computation, thus significantly increasing systems performance.

5.3. Attribute-based Encryption

Attribute-based Encryption (ABE) is a well-known approach to achieving fine-grained access control in systems. Access control is a significant step in maintaining confidentiality and privacy, as people who are not related to certain parts of data should not be allowed to view that data at all. It may be possible that some nurse becomes malicious user, and if they get doctors' access, they may mistreat the patient or harm him knowingly for personal benefit. So the issue is how to achieve such access control for multiple users on the blockchain. To this end, we resort to ABE technology, which is suitable for multiple users' data access control design. However, it is tricky to apply ABE to blockchain-based platforms. The reason is that existing ABE schemes suffer from severe efficiency drawbacks due to huge ciphertext storage and large computation overhead. We know that blockchain has limited storage, and a certain level of computational power is also fixed for on-chain computation. Thus to minimize gas overhead, we take the help of a novel idea implemented in one of the existing solutions to this problem; medshare [31]. This solution provides a novel approach for ABE through constant-size ciphertext resulting in constant computation cost.

5.4. Data Retrieval

When a data request is made, the system divides the requester into two categories: users requesting raw data and users requesting processed data. Users such as the patient himself, while managing their data on the blockchain, may need access to the data or doctors treating them. Node's TEE accepts all these user's requests and then passes through ABE. According to the access policy of the data defined by its owner, smart contracts deployed will execute inside TEE and provide corresponding results to the requester. TEE can find the data stored in the database through the indexes it maintains with the help of oasis protocol and can execute a smart contract on rules on that data. After that, it returns the result safely to the requester via web3 gateway using a secure HTTPS connection and oasis RPC gateway, the same way data is injected into the system.

Let us understand with the help of a simple scenario. Patient 'A' has a previous treatment history of a certain disease from the health care centre 'H1'. 'A' uses a blockchain system and makes an account using a webapp. After 6 months' A' needs a second treatment for his disease from' H2' as he is not satisfied with the treatment from 'H1'.' H2' instructs 'A' to have all previous diagnostics and treatment records ready in the blockchain system under his public key and to get some additional lab tests from lab 'L1'. 'A' uploads all his previous treatment records into the blockchain with a specific access policy suggested by 'H2' and authorizes 'L1' to submit his lab tests into the blockchain under his account. 'H2' now can easily access all the medical records of 'A' in one place securely and speedily. Doctors of 'H2' initially made data request for records. The nurses of 'H2' will get to know only the current treatment and medicines recommended by the doctor. Similarly, others in 'H2' will be able to access data per the access policy defined in the smart contract via patients. Whenever a patient requests data from a web portal, the whole data is available to him as a data owner. They get the right to change access policy accordingly.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 February 2023 doi:10.20944/preprints202302.0178.v1

Our system is designed to use the full capabilities of resources available with the power of blockchain. To perform secure on-chain processing, the oasis protocol used in the model has a very novel way of managing computation securely. Smart-contract developers need to add confidential modifiers in their Solidity contract source code. All the fields marked with this modifier will become secret and will not be revealed to any human without access. This will help maintain fine-grained access control and increase the system's efficiency by inherently stopping the system from encrypting pure-view functions and elements. Whenever a function is executed on encrypted data via smart contract, confidential data needed will be decrypted and processed. Then the result of such functions can be returned to users in the pure-view function. Thus, while re-calling, no resources would be spent. To understand this, we take a simple case where a patient 'A' already has his data on the blockchain. All his data is marked confidential by default (can be changed by the patient from the web app individually). 'A' agrees not to make his current treatment secret. Many fields are kept public, while no one can access confidential fields without permission like DoB, age and name. If any research institute that wants to get a total number of patients suffering from a particular type of cancer belonging to a particular geographical area will access the blockchain to find suitable candidates. In this case, patients' addresses are confidential information. Thus inside TEE smart contract function will check the geographical areas and increase the count for disease if found. Thus, end-to-end confidentiality is maintained, and the institute will get the processed result directly.

6. Results and Discussion

After studying all the existing systems, we have drawn out a few benefits and shortcomings of our proposed solution in Table II. Compared to existing solutions, our system solves most of the underlying problems for data interoperability in the healthcare sector with an amalgamation of novel algorithms and a suitable architecture.

Some of the shortcomings of our solution listed in table II are solved by existing systems such as [21]. This paper gives a brief overview of a healthcare data management system which uses blockchain to manage indexes of data stored on local databases of the healthcare centre. Using this convenience as a benefit, they proposed a method of right to forget by directly deleting data from the local databases and then though indices will remain on blockchain. Still, it won't be of any use, and the system can forget that patient. Compared to our Ethereum-based system, this system [20] uses hyperledger fabric-based blockchain, CFT, and BFT algorithms resulting in very low gas-requiring transactions.

Table 2. Outcome of Our Proposed System.

Pros	Cons
Patient-centric system for data interoperability.	The patient decides which data to be kept public. This data required forresearch may face hindrances
Once recorded on the blockchain, the transaction becomes immutable.Thus providing effective and quick decisions on Medi-claims, insurance, etc.	Even if the patient wants to be completely forgotten from the system,data records are immutable and will remain forever.
Ethereum platform provides flexibility in terms of compatibility as most protocols and systems are compatible with Ethereum.	Using Ethereum as a platform to serve our system has its cons, such as high gas fees for computationally intensive data encryption algorithms.
The proposed system provides a way for the on-chain computation of certain data so that only the result gets public.	Scalability regarding on-chain computing, such as applying ML algorithms on private data, is still difficult.

 doi:10.20944/preprints202302.0178.v1

7. Conclusion & Future Scope

Record-keeping and interoperability are significant concerns with the increase in medical records generated through wearables and new technologies. We have created a solution here, keeping privacy and confidentiality concerns in mind.

Our solution focuses on the interoperability of shared raw data and chain processing of data for research purposes. We have theoretically proven how most data processing can be done securely on-chain. This concept can be extended so that machine learning can be performed on this data securely, thus only revealing the final answer of ML algorithms once executed on the data. Applying the ML model in our system will decrease systems efficiency, and the there-by system will take more time to fulfil users' requests.

The system assumes that patients are willing to make some data public which certain research institutions can only access. Still, for all these claims, there is an assumption. Some incentive-based mechanisms should be introduced to convert these assumptions into certainty, which is very easy to implement in our system as it supports native Ethereum currencies.

Supplementary Materials: Reference to all the supplementary material is provided in the manuscript.

Author Contributions: All authors have contributed equally.

Funding: This research was partially funded by the University of Malta's Research Excellence Fund, grant number CISRP02-20, "Novel Intelligent Computing mEthods for healthcare requirements forecasting, allocation and management (NICE-Healthcare)".

Institutional Review Board Statement: Not applicable.

Data Availability Statement: There is no data available to carry out this research.

Acknowledgments: The authors acknowledge the reviewers' valuable comments and suggestions to improve the manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. J. Marchibroda, "Interoperability," Health Affairs Health Policy Brief, 2014.
2. A.-M. J. Holmgren AJ, Patel V, "Progress in interoperability: Measuring us hospitals' engagement in sharing patient data," Health affairs, vol. 36, pp. 1820–1827, 2017.
3. L. Rosenbaum, "Transitional chaos or enduring harm? the EHR and the disruption of medicine," The New England Journal of Medicine, vol. 373, pp. 1585–1588, 2015.
4. H. W. Qing Ye, Jin Zhou, "Using information technology to manage the covid-19 pandemic: Development of a technical framework based on practical experience in china," JMIR Med Inform, vol. 8, p. e19515, Jun 2020.
5. C. Reichel, "Hospital administration and the covid-19 pandemic (part ii)," 2020.
6. J. D. Birkmeyer, A. Barnato, N. Birkmeyer, R. Bessler, and J. Skinner, "The impact of the covid-19 pandemic on hospital admissions in the united states," Health Affairs, vol. 39, no. 11, pp. 1856–1860, 2020.
7. C. Lepore, M. Ceria, A. Visconti, U. P. Rao, K. A. Shah, and L. Zanolini, "A survey on blockchain consensus with a performance comparison of pow, pos and pure pos," Mathematics, vol. 8, no. 10, p. 1782, 2020.
8. K. A. Shah and D. C. Jinwala, "Privacy preserving, verifiable and re- silient data aggregation in grid-based networks," The Computer Journal, vol. 61, no. 4, pp. 614–628, 2018.
9. K. A. Shah and D. C. Jinwala, "Novel approach for pre-distributing keys in wsns for linear infrastructure," Wireless Personal Communications, vol. 95, no. 4, pp. 3905–3921, 2017.
10. K. Shah and D. Jinwala, "Privacy preserving secure expansive aggregation with malicious node identification in linear wireless sensor networks," Frontiers of Computer Science, vol. 15, no. 6, pp. 1–9, 2021.
11. R. K. Gupta, K. K. Almuzaini, R. Pateriya, K. Shah, P. K. Shukla, and R. Akwafo, "An improved secure key generation using enhanced identity-based encryption for cloud computing in large-scale 5g," Wireless Communications and Mobile Computing, vol. 2022, p. 7291250, 2022.
12. "The bitcoin project," 2009. Accessed: 2021-05-15. [13] "Ethereum," 2013. Accessed: 2021-05-11.
13. W. J. Gordon and C. Catalini, "Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability," Computational and Structural Biotechnology Journal, vol. 16, pp. 224–230, 2018.
14. Y. Zhuang, L. R. Sheets, Y.-W. Chen, Z.-Y. Shae, J. J. Tsai, and C.-
15. R. Shyu, "A patient-centric health information exchange framework using blockchain technology," IEEE Journal of Biomedical and Health Informatics, vol. 24, no. 8, pp. 2169–2176, 2020.

16. R. Jabbar, N. Fetais, M. Krichen, and K. Barkaoui, "Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity," pp. 310–317, 2020.
17. W. L. S. Suveen Angraal, Harlan M Krumholz, "Blockchain technology: Applications in health care," National Library of Medicine, vol. 10, no. 9, p. e003800, 2017.
18. V. M. Harshini, S. Danai, H. R. Usha, and M. R. Kounte, "Health record management through blockchain technology," in 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), pp. 1411– 1415, 2019.
19. G. Tripathi, M. A. Ahad, and S. Paiva, "S2hs- a blockchain based approach for smart healthcare system," healthcare, vol. 8, no. 1, p. 100391, 2020.
20. T. Guimara˜es, A. Moreira, H. Peixoto, and M. Santos, "Icu data management - a permissioned blockchain approach," Procedia Computer Science, vol. 177, pp. 546–551, 2020.
21. E. Balistri, F. Casellato, C. Giannelli, and C. Stefanelli, "Blockhealth: Blockchain-based secure and peer-to-peer health information sharing with data protection and right to be forgotten," ICT Express, vol. 7, no. 3, pp. 308–315, 2021.
22. F. D. S. S. M. Alam, S.; Ahmad Reegu, "Blockchain-based electronic health record system for efficient covid-19 pandemic management," 2021.
23. "oasis protocol," 2016. Accessed: 115-06-2021.
24. A. Roehrs, C. A. da Costa, R. da Rosa Righi, V. F. da Silva, J. R. Goldim, and D. C. Schmidt, "Analyzing the performance of a blockchain- based personal health record implementation," Journal of Biomedical Informatics, vol. 92, p. 103140, 2019.
25. D. Ivan, "Moving toward a blockchain-based method for the secure storage of patient records," 2016. Accessed: 12-05-2021.
26. X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control," Journal of medical systems, vol. 40, p. 218, 2016.
27. R. J. Y. A.-H. Ibrar Yaqoob1, Khaled Salah1, "Blockchain for healthcare data management: opportunities, challenges, and future recommendations," Neural Comput Applic, p. 11475–11490, 2021.
28. K. A. C. D. S. C. Hannah S Chen, † Juliet T Jarrell and X. Huang, "Blockchain in healthcare: A patient-centered model," Biomed J Sci Tech Res, vol. 20, no. 3, pp. 15017–15022, 2019.
29. D. M. Vikram Dhillon and M. Hooper, "Blockchain enabled applications," pp. 201–220, 2021.
30. A. Shahnaz, U. Qamar, and A. Khalid, "Using blockchain for electronic health records," IEEE Access, vol. 7, pp. 147782–147795, 2019.
31. M. Wang, Y. Guo, C. Zhang, C. Wang, H. Huang, and X. Jia, "Medshare: A privacy-preserving medical data sharing system by using blockchain," IEEE Transactions on Services Computing, pp. 1–1, 2021.
32. L. O.-M. Tsung-Ting Kuo, Hyeon-Eui Kim, "Blockchain distributed ledger technologies for biomedical and health care applications," National Library of Medicine, vol. 24, pp. 1211–1220, 09 2017.
33. A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in 2016 2nd International Conference on Open and Big Data (OBD), pp. 25–30, 2016.
34. A. Ekblaw and A. Azaria, "Medrec: Medical data management on the blockchain," Viral Communications, 2016. https://viral.media.mit.edu/pub/medrec.
35. E. Chukwu and L. Garg. "A systematic review of blockchain in healthcare: frameworks, prototypes, and implementations." IEEE Access, vol. 8, pp. 21196-21214, 2020.
36. L. Garg, E. Chukwu, N. Nidal, C. Chakraborty and G. Garg, “Anonymity preserving IoT-based COVID-19 and other infectious disease contact tracing model,” IEEE Access, vol. 8, pp. 159402-159414, 2020.