Informed Consent as Patient Driven Policy for Clinical Diagnosis and Treatment: A Smart Contract Based Approach

Md Al Amin[a], Amani Altarawneh[b] and Indrajit Ray[c]
Computer Science Department, Colorado State University, Fort Collins, Colorado, U.S.A.

Keywords: Informed Consent, Patient, Provider, Clinical Treatment, Disease Diagnosis, Blockchain, Smart Contract.

Abstract: Digitized healthcare systems improve services, make it easier for healthcare providers to work together, improve the accuracy of diagnoses, and get the most out of each treatment. They provide healthcare services that are better, faster, more reliable, and less expensive. With the help of information technology, computing resources, and digitized health records, medical researchers are trying to solve critical health problems like COVID-19. However, electronic healthcare systems significantly risk patients' data privacy and security. Anyone with credentials can access patients' healthcare data. Patients grant consent to share or access data. But they need a way to ensure informed consent is done right and on time. Due to the centralized authority in present healthcare systems, healthcare-covered entities perform all operations. As a result, many unwanted events and security incidents happen in healthcare systems. Patients must know how their data is accessed, by whom, and when. Therefore, a blockchain and smart contract-based patient-informed consent management system is proposed. Where patients provide informed consent to share or access their health records, as well as methods to ensure that informed consent is properly completed. The immutability and auto-triggering properties of blockchain and smart contracts ensure the integrity and accountability of the given informed consent.

1 INTRODUCTION

Compared to paper-based systems, electronic health record (EHR) systems make it easier for doctors to work together, make diagnoses more accurate, speed up treatment, and give doctors ready access to patient medical records. As healthcare data become more digitized, distributed, and interactive, the healthcare ecosystem is increasingly becoming more concerned about the security of EHR information and systems. Several factors contribute to the increased vulnerability of EHR systems. Health workers are often under-trained and under-experienced in handling and securely maintaining information systems. Software bugs, security flaws, and human errors allow unauthorized users to enter these databases. Insider adversaries can also get their hands on protected medical information, which can cause sensitive patient information to be lost, misused, or shared. Consequently, healthcare providers' responsibility to protect patient privacy and health records confidentiality has increased significantly due to these factors in electronic health data processing (Sulmasy et al., 2017).

While better security and privacy technology are needed to better protect patient data from these types of breaches, there is ample evidence that shows that improper policy adoption, implementation, and enforcement cause a significant amount of unauthorized access – without a "need to know" – to EHR data (Staff, 2016; Seh et al., 2020; Marchand-Melsom and Nguyen Mai, 2020). Intentionally or unintentionally, access privileges are assigned to users when they should not be. Policies are not followed correctly, and access control rules are not checked or implemented promptly. In some cases, it has been observed that the same roles and privileges are assigned to all employees. Often, individual patient-level policies are not enforced to the word. Gaps in auditing and monitoring have also been found; they are not done unless there are serious complaints or a legal requirement to do so. Informed consent policies, in particular, are one group of policies that suffer considerably because of such gaps in policy specification and enforcement.

Informed consent (Parvin, 2022; Lorenzini et al., 2022) is a legal and ethical concept in healthcare that refers to the process in which a patient voluntarily

[a] https://orcid.org/0000-0003-1700-7201
[b] https://orcid.org/0000-0002-4885-350X
[c] https://orcid.org/0000-0002-3612-7738

Al Amin, M., Altarawneh, A. and Ray, I.
Informed Consent as Patient Driven Policy for Clinical Diagnosis and Treatment: A Smart Contract Based Approach.
DOI: 10.5220/0012090600003555
In *Proceedings of the 20th International Conference on Security and Cryptography (SECRYPT 2023)*, pages 159-170
ISBN: 978-989-758-666-8; ISSN: 2184-7711

agrees to a medical intervention, procedure, or treatment after being fully informed of the risks, benefits, and alternatives or agree to share personal health data to participate in clinical trials or research experiments (Falagas et al., 2009). Informed consent empowers patients to make decisions about their health and well-being that are in their best interests. The purpose of informed consent is to protect the autonomy and dignity of the patient by giving them control over their health and treatment decisions. It helps to build trust between the patient and the healthcare provider. Informed consent is typically governed by laws and regulations such as the General Data Protection Regulation (GDPR) in Europe or the California Consumer Privacy Act (CCPA) in the United States to avoid future legal issues and conflicts (Gopal et al., 2023).

While informed consent plays a critical role in the patient's healthcare, it is quite challenging to manage informed consent properly, preserving the privacy and security of patient health data. Patients often consent to users like treatment team members, physicians, nurses, support staff, lab technicians, insurance companies, family member(s), and other providers. When patients need more advanced care or counseling from doctors, like specialists, they must go to a different hospital. Due to work transfers and family movements, patients must move to other regions, like new states or countries. It is sometimes unavoidable to change health plans or insurance company coverage. Patients must revoke access rights granted in the past but no longer needed or valuable. Patients also give emergency access permissions where there might be an emergency, like an accident or life-and-death situation, and patients cannot approve access permission instantly. In this case, assigned emergency treatment team members must access admitted patients' data without their consent (de Oliveira et al., 2023).

We believe the following problems must be addressed to protect healthcare data from unauthorized access and preserve patients' autonomy over their consent and healthcare resources.

- Individual patient-level policies are not enforced properly, otherwise known as informed consent.
- Centralized hospital system acts as a single point failure and source of truth of access audit trails.
- Lack of consent provenance information or unaltered source of given consent execution.
- Patients are not assured that the intended users execute given consents. Other requests are denied.
- No guarantee that consents are executed only when included conditions are satisfied; otherwise, denied.
- Patients lack control over their consent to control their health record access.

In this paper, we propose a decentralized distributed ledger (DLT) (Altarawneh et al., 2020) powered with smart contracts (Buterin et al., 2014) to address the above-mentioned challenges and requirements. We propose a blockchain and smart contract-based informed consent management and enforcement framework, which runs on top of a public blockchain such as Ethereum (Buterin et al., 2014). This smart contract-based approach provides an automated system and guarantees the integrity and accountability of the given informed consent. However, this proposed approach does not address patients' protected healthcare data. For this reason, we do not focus on healthcare data security and privacy issues.

DLTs such as blockchain provide proofs that submitted acts are immutable; it keeps the audit trail's integrity and can detect any changes that shouldn't have been made. Blockchain security properties, such as nonrepudiation, are also guaranteed, where no participants can deny submitting changes. Smart contracts ensure the proper execution of informed consent and prevent random access. Also, smart contracts emit event information if there are any operations. To the best of our knowledge, this work is the first to capture patients' informed consent for disease diagnosis and clinical treatment. Our contributions include the following:

- A novel way of implementing Informed Consent for medical diagnosis and treatment. Also, storing in decentralized and distributed networks to overcome a single point of truth sources and failure.
- Enforcing mechanism to authorization module ensuring informed consent is evaluated and enforced while making authorization to access patient health records.
- Some consent services are proposed with sample graphical representations to provide patients with concise and informative reflections on informed consent.
- Certain fundamental consent management considerations and operations to support patients' treatment flow and avoid unwanted health data access.

The remainder of the paper is organized as follows. We discuss some related works in Section 2. Section 3 explains the proposed system with required components. Sections 4 and 5 discuss consent services and management. Section 6 contains the experimental evaluation of the proposed model. In Section 7, we wrap up the paper with what to do next.

2 RELATED WORK

Several suggestions exist for adopting blockchain technology in healthcare and e-health systems. So far, this research has been on how blockchain can protect medical information and store and share medical data, analytics, and informed consent systems for clinical or research experiments. Research on informed consent for clinical diagnosis and treatment is focused to some extent (Ploug and Holm, 2012). To our knowledge, ours is the first work on employing blockchain and smart contracts for clinical treatment informed consent management and enforcement.

Authors in (Cunningham et al., 2022) propose Non-Fungible Tokens (NFTs) as the mechanism for recording and transmitting records of patients' consent for medical data use. The proposed model enables subjects to record signed documents of consent that permit Data Consumers to request medical data from Data Providers in line with the consent given by the subjects to whom that data pertains. However, how NFTs can be used for provenance with regulatory policies such as HIPAA/GDPR remains to be seen.

In (Azaria et al., 2016), authors propose MedRec, a blockchain-based healthcare data access and permission management system to handle electronic medical records. The model addressed four significant issues: fragmented, slow access to medical data; system interoperability; patient agency; and improved data quality and quantity for medical research. MedRec gives patients a complete, unchangeable log of their medical information and makes it easy to get it from their providers and treatment sites. References to different kinds of medical data are put together and encoded on a blockchain ledger to create an accessible trail for medical history.

Xia et al. (Xia et al., 2017) propose a blockchain-based data-sharing framework that addresses the access control challenges associated with sensitive data stored in the cloud using the blockchain's immutability and built-in autonomy properties. Yue et al. (Yue et al., 2016) propose a blockchain-based app, Healthcare Data Gateway, where patients securely own, control, and share their data. Untrusted entities can handle healthcare data using secure multi-factor computing to protect patient privacy. In (Fan et al., 2018), the authors propose a blockchain-based information management system, MedBlock, that allows efficient EMR access and retrieval. It protects users' privacy with custom access control protocols and encryption technology while sharing data. Zyskind et al., (Zyskind et al., 2015) propose blockchain for access control management and secure data storage. Encrypted data is kept on servers that can be trusted.

A blockchain-based dynamic consent management architecture, ConsentChain, is offered by (Albalwy et al., 2021) in facilitating the exchange of clinical genomic data. ConsentChain is built on the Ethereum platform, and smart contracts are used to model the actions of patients (who can give or take back permission to share their data), data creators (who collect and store patient data), and data requesters (who need to query and access the patient data). However, this work mainly focuses on patient genome data sharing with clinicians, researchers, and bioinformaticians. Clinical treatment imposes different requirements for consent management than genome data sharing. Many users perform various operations in treatment processes, such as reading, writing, modifying, and others, and access privileges are assigned based on the role of the users. We propose a consent management framework to address complex permission assignment requirements for treatment team members, insurance agents, external doctors, pharmacists, etc.

The researchers,(Tith et al., 2020), propose an e-consent management model that uses Hyperledger Fabric blockchain and a purpose-based access control scheme. All patient records, consents, and metadata about data access are written on the blockchain and are shared among the organizations taking part. A Chaincode performs business logic for managing patient consent. Patients can create, update, and withdraw their consent in the blockchain. The proposed model can be used for data donation for biobank research purposes besides sharing patient data. However, the Hyperledger blockchain is a permissioned blockchain network where participants are limited to the organizations. It doesn't provide the public eye to provide trust. We adopt the public Ethereum blockchain network where participants with stakes can join and maintain the ledger to provide immutable information to untrusted network participants. Most important, Ethereum's public consensus mechanism adds more transparency than a permissioned network. In addition, Ethereum smart contracts are the most used, and there are many projects of development and refinements.

3 PROPOSED APPROACH

The main idea is to integrate components of informed consent into the patient-provider agreement. Then create and deploy smart contracts for informed consent components in the blockchain network. The authorization module calls the corresponding smart contract for an access request to enforce informed

consent. The request specifies which subject wants to perform which operation on what objects under what constraints or conditions. Once the smart contract is called and the authorization module decides, the corresponding event information is recorded as logs in the blockchain network. Smart contracts auto triggering feature automatically emits event or activity data without missing any specified and required components. Event or activity data is stored on the blockchain network. The blockchain network provides a distributed, immutable, and decentralized storage platform. This ensures that deployed smart contracts provide original consent made with the agreement of the patient and provider. It also ensures that event logs are the same as created and stored without any modification. Figure 1 shows the proposed approach. With the necessary parameters, the following discusses the patient-provider agreement, informed consent components, consent smart contract generation, consent enforcement, and patient interaction with the blockchain network services.

3.1 Patient-Provider Agreement (PPA)

The patient-provider agreement aims to determine who is responsible for what in treatment. The goal is to improve outcomes, lower risks, and educate patients better. A multi-center study (Pergolizzi et al., 2017) evaluated the utility of the PPA, how readily patients understood it, its ability to educate patients in an unbiased way about treatment, and the feasibility of incorporating a PPA in clinical practice. Both patients and doctors believe this PPA helped them decide on a course of treatment and was fair in laying out the treatment's risks and benefits. Most patients reported the PPA to be "somewhat helpful" or "very helpful" in deciding on a course of treatment and "easy to understand." A PPA, also known as a contract, differs from organization to organization. Healthcare organizations adjust what they need from patients and what they expect from them to match those needs, treatments, and responsibilities. This is done based on the nature and needs of treatment and services. Also, the components and representation of the PPA depend on the hospital or clinic. Examples include general hospitals, emergency rooms, urgent care or walk-in clinics, dental care, cancer treatment, physiotherapy, etc.

The patient-provider agreement is depicted in Figure 1 with necessary components. The Patient-Provider Agreement formally is composed of four tuples:

$$PPA = (PC, PrC, ROC, ICC)$$

satisfying the following requirements:

(i) *PC* is a finite set of patient components containing patient's *personal information, contact information, mailing information, pharmacy information, billing and insurance information, emergency contact*, and *others*. The patient is responsible for providing and maintaining valid information for these components.

(i) *PrC* is a finite set of provider components, including the treatment team, anonymous data sharing for research, prescription, and others. Treatment team members for a patient include *doctors, nurses, support staff, lab technicians, and billing officers*. As the treatment period for a patient, everything from treatment to insurance coverage and billing is considered.

(iii) *ROC* is a finite set of regulatory and other components. It has applicable security and privacy policy to comply with the local government, regulatory agencies (HIPAA, GDPR), federal government, and foreign government requirements if necessary.

(iv) *ICC* is a finite set of informed consent components. It indicates the permission given by the patient to access healthcare data.

This work mainly focuses on *ICC* and does not consider and discuss *PC*, *PrC*, and *ROC*. They are the future scope of this paper. Algorithm 1 shows the step-by-step instructions for creating a PPA with *PC*, *PrC*, *ROC*, and *ICC*. A patient-provider agreement is formed when a patient visits a hospital. The terms and conditions of the contract make it invalid after a certain period. There may be several contracts for a single patient. Several patient-provider agreements must be created and properly documented to deliver healthcare services. Managing many contracts involves various things, such as contract creation, development, testing, updating, etc. If the requests contain contracts, the authorization module must consider those with other required policies when making access decisions. From Figure 1, it is seen that the proposed model stores the integrity of a PPA to the blockchain network to ensure the detection of any modification, intentionally or unintentionally.

3.2 Informed Consent Components

Before giving consent, patients need to know everything about the particular consent. Figure 2 shows the informed consent conceptual framework structure. The Informed Consent formally is composed of four tuples:

$$IC = (U, O, OP, CON)$$

satisfying the following requirements:

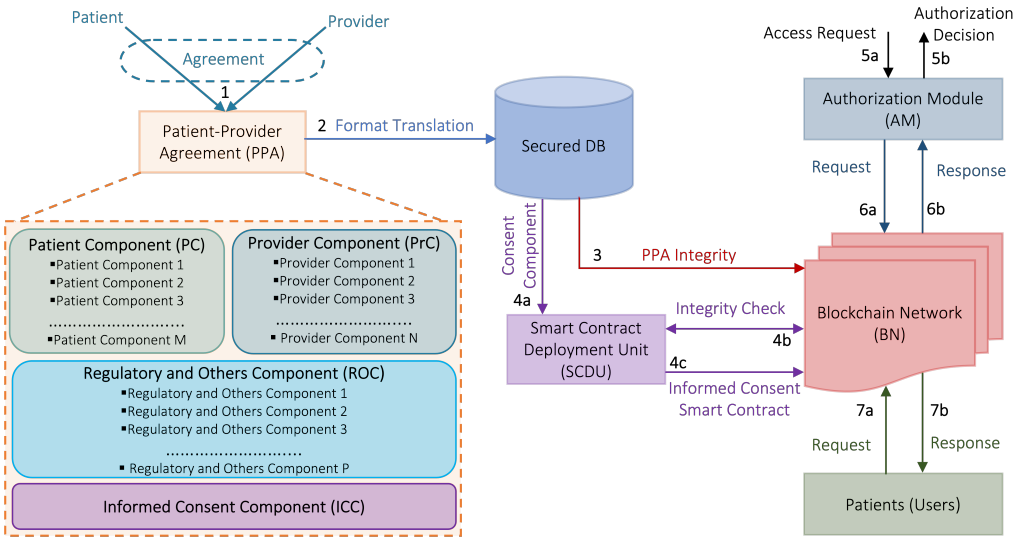

Figure 1: Proposed Smart Contract-Based Informed Consent Management Framework.

Algorithm 1: Patient-Provider Agreement (PPA).

Input : Patient Components (PC), Provider Components (PrC), Regulatory and Other Components (ROC), and Informed Consent Components (ICC).
Output: An formal agreement between patient and provider (PPA).

Input Parameters Initialization *Patient-Provider Agreement*
$PPA_i := \{PC_i, PrC_i, ROC_i, ICC_i\}$ where i indicates patient identity; $PC := \{PC_1, PC_2, PC_3, ...PC_M\}$
$PrC := \{PrC_1, PrC_2, PrC_3, ...PrC_N\}$
$ROC := \{ROC_1, ROC_2, ROC_3, ...ROC_P\}$
$ICC := \{ICC_1, ICC_2, ICC_3, ...ICC_R\}$
Agreement Parameters Hash Calculation /* $Hash(input)$ is a function to calculate hash of $input$ */
$Hash_{PC} \leftarrow Hash(PC_1, PC_2, PC_3, ...PC_M)$
$Hash_{PrC} \leftarrow Hash(PrC_1, PrC_2, PrC_3, ...PrC_N)$
$Hash_{ROC} \leftarrow Hash(ROC_1, ROC_2, ROC_3, ...ROC_P)$
$Hash_{ICC} \leftarrow Hash(ICC_1, ICC_2, ICC_3, ...ICC_R)$
$Hash_{PPA_i} \leftarrow Hash(Hash_{PC}, Hash_{PrC}, Hash_{ROC}, Hash_{ICC})$
Patient-Provider Agreement Finalization
if PPA_i *is complete* **then**
    /* complete means presence of PC, PrC, ROC, and ICC */
    add PPA_i to patient-provider agreement repository and return ID_{PPA_i};
    add ID_{PPA_i} and $Hash_{PPA_i}$ to blockchain network;
else
    Error: PPA_i can not be created
    /* incomplete patient-provider agreement */
end if

(i) U is a finite set of authorized users denoted as $\{u_1, u_2, u_3, ...\}$. The user can perform certain operations on healthcare resources when certain conditions are satisfied.

(i) O is a finite set of protected objects otherwise known as protected healthcare resources. A finite set of protected objects (O) denoted as $\{o_1, o_2, o_3, ...\}$.

(iii) OP is a finite set of operations denoted by $\{op_1, op_2, op_3, ...\}$. Operations represent the system actions that authorized users can perform on the objects. Examples of operations are read, write, and update.

(iv) CON is a finite set of conditions. It indicates the conditions that must be satisfied by the user to perform operations on the protected objects. A finite set of conditions, CON, can be denoted as $\{con_1, con_2, con_3, ...\}$.

There are many users in the healthcare system. Each user plays a different role and responsibility in performing their job. Treatment team members for a patient include doctors, nurses, support staff, lab technicians, billing officers, the patient's emergency contact person, and other hospital employees assigned by the authority. Some outsider members are insurance agents, pharmacists or pharmacy technicians, doctors or lab technicians from another hospital. As the treatment period for a patient, everything from treatment to insurance coverage and billing is considered. Informed consent users can be anyone from five groups of people: *(i) treatment team member, (ii) emergency contract, (iii) external users, (iv) insurance company agent,* and *(v) pharmacy*. External users are from different hospitals when a patient is transferred for better treatment if the situation demands it. Usually, external users have temporary access to admitted patients' health records.

The term object refers to an electronic version of a patient's medical history kept on file by the healthcare provider over time. It may include all the administra-

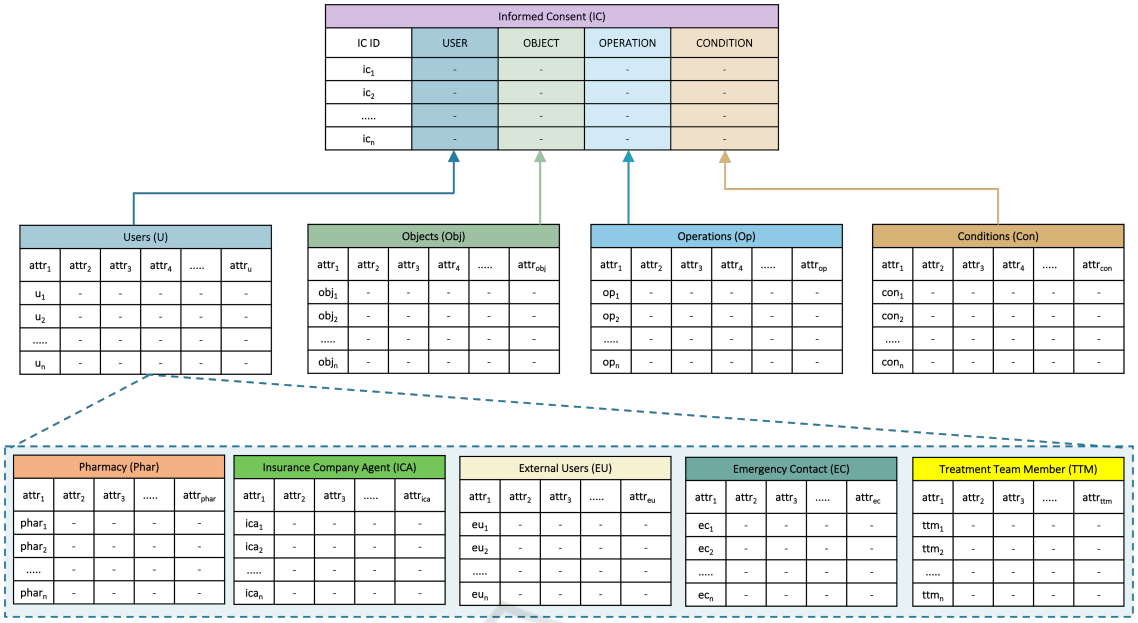

Figure 2: Informed Consent Components.

tive and clinical information pertinent to the patient's care under a specific provider, such as demographics, progress notes, issues, medications, vital signs, previous medical history, immunizations, laboratory information, and radiology reports. These objects must be protected from unauthorized users. The main purpose of informed consent permitting by patients to users to perform certain operations.

Many operations are executed by the authorized in the healthcare industry to perform required operations. Some common operations are *view/read*, *add/write*, *update/modify*, *delete*, etc. In the *view* operation, users can only view or read healthcare records or resources if the request is valid and complies with all applicable policies. The state of the data is not changed in this operation, ensuring data integrity. But it can compromise confidentiality and privacy if the access requested is granted without appropriate credentials. On the other hand, the *write* operation changes the state of the records or healthcare data. If proper policy enforcement is not ensured, it breaks the integrity of the data.

There might be various constraints or conditions under which certain consent can be enforced, rejected, revoked, and others. The conditions can be but are not limited to:

(i) ***Time Constraints.*** In time constraints, any user can access a patient's healthcare data within a certain time. For example, the time condition for consent is regular office hours: 8 am-5 pm. In this case, the request is rejected if any subject wants to access the patient's record beyond this time. The attempt is recorded as an audit trail event.

(ii) ***Date Constraints.*** The date constraints limit the calendar date. No access request is granted beyond the intended date.

(iii) ***Day Constraints.*** Day conditions can include work days (Monday-Friday), weekends (Saturday-Sunday, holidays, etc. Based on the day, the subject can access data. Suppose a regular doctor has a duty on workdays. On weekends no access is given to that doctor.

(iv) ***Location-Based Constraints.*** The location-based condition allows users to access information from a certain location, like a hospital building, inside an emergency room for treating emergency patients, and others.

(v) ***IP-Based Constraints.*** IP-based condition limits healthcare users from accessing resources from certain IPs. Devices IPs must be from the known list; otherwise, no access is granted.

(vi) ***Access Frequency Dependent.*** A user can operate for a certain number in access frequency-dependent conditions. Suppose an external doctor is given five times view permission. Once the doctor reads the patient's specified records five times, the given consent is expired, and access is denied. There is no access without getting new consent.

The above mentions list is not fixed for the conditions, but we consider them for this study. There might be other conditions depending on the treatment

nature, patient characteristics, provider business policy, nature, etc. With sophisticated technology, malicious attackers can spoof the conditions to fool the system into accessing healthcare data and other compromised credentials. Proper layered defense mechanisms must be deployed to ensure that conditions' credentials are accurate, not fabricated or manipulated.

3.3 Consent Smart Contract Generation

Once a patient-provider agreement or PPA is created and stored in the repository, all informed consent components are deployed as smart contracts. The patient owns all the deployed contracts. The authorization module needs to access these smart contracts to make decisions with other components such as subject attributes, object attributes, operations attributes, environmental attributes, organizational policies, regulatory and other policies, and others required. Algorithm 2 shows the steps to develop and deploy smart contracts for informed consent components. The smart contract deployment unit, SCDU, collects all consent components from PPA and checks integrity to confirm that collected consents are not modified deliberately or inadvertently. In step 3 in Figure 1, PPA integrity as the hash from Algorithm 1 ($Hash_{PPA_i}$) is stored in the blockchain network along with PPA id.

To verify PPA integrity, SCDU calls the corresponding smart contract function to retrieve the PPA hash value stored in the network. Any modification of consent components voids the consent. If there is no modification, then SCDU creates and deploys smart contract(s) to the blockchain network. Once the contracts are deployed, the contract addresses are added to the patient's profile and hospital systems. The contract address is an identifier for a smart contract in the blockchain network.

3.4 Consent Enforcement

Enforcing informed consent is essential to protect patient's rights and autonomy and ensure that medical treatments are performed with the patient's complete understanding and agreement. Healthcare organizations and providers must take the informed consent process seriously and provide patients with all the information they need to make informed decisions about their medical care. Consent enforcement ensures that related consents are executed while making access decisions for the requests. In the proposed model, all consents are stored on the blockchain network as smart contracts and can not be enforced until they are called. The authorization module (AM) considers a patient's consent while making an authorization decision. The user submits requests to AM for authorization to operate on an object. The user also must provide the required credentials for identification purposes. The AM needs to consider different attributes with required policies for making decisions. It also requires considering informed consent from the patient for that requested subject. The other points are subject, object, operation, and environmental attributes.

Algorithm 2: Informed Consent Smart Contract.

Input : Informed Consent Component *ICC*.
Output: Smart contract contains informed consents elements *ICC* from patient-provider agreement *PPA*.

1 **Initialization** *Informed Consent* $IC_i := \{Sub, Op, Obj, Cond\}$ where $Sub, Op, Obj, Cond$ represent one or more individual attribute(s) and i represents patient identity; *Subject Attributes* $Sub := \{SubAttr_1, SubAttr_2, ...SubAttr_M\}$ *Operation Attributes* $Op := \{OpAttr_1, OpAttr_2, ...OpAttr_N\}$ *Object Attributes* $Obj := \{ObjAttr_1, ObjAttr_2, ...ObjAttr_P\}$ *Conditions* $Cond := \{CondAttr_1, CondAttr_2, ...CondAttr_R\}$
2 **Smart Contract Generation and Deployment if** IC_i *is complete* **then**
3 `/* complete means presence of Sub, Op, Obj, and Cond with patient consent */`
4 IC_i is added to smart contract
5 **else**
6 *Denied:* smart contract for IC_i can not be created and deployed
7 `/* incomplete informed consent component */`
8 **end if**

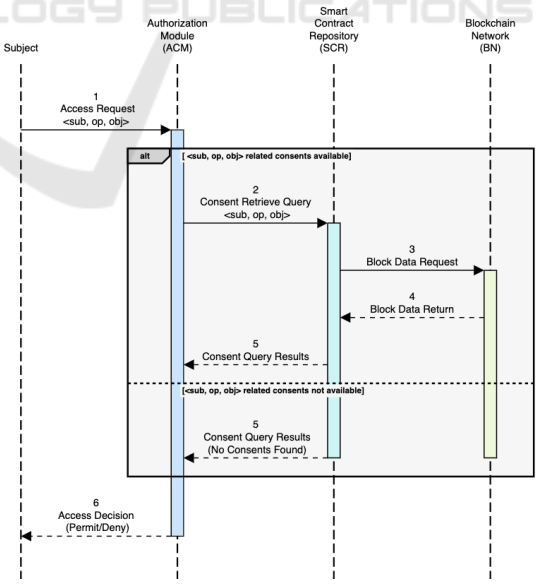

Figure 3: Informed Consent Enforcement Process.

Figure 3 shows the sequence diagram of AM and informed consent interaction. When a subject submits a request to AM. Then the AM queries the blockchain

network through the corresponding smart contract to get the informed consent information for the subject. If the subject has consent from the patient for the requested resources and other conditions, then the AM evaluates other parameters and informed consent to make final authorization. Finally, the AM generates the granted decision otherwise rejected for a legitimate request. After deciding, AM sends audit trail information to the smart contract to write in the blockchain network. For this study, it is considered that the authorization module is not compromised or tampered with. Also, the communication channel between AU and the smart contract access points or apps is secured from malicious users.

3.5 Patient Interaction

Patients must interact with the proposed system using a GUI, apps, or abstraction. Different wallets, such as Coinbase and MetaMask, interact with the blockchain network to sign the transactions and manage cryptocurrencies or tokens (He et al., 2020). Wallets store private keys and other credentials for the users. Various types of users need to use the system. Some users need specially designed software interfaces or apps to interact with the systems (Mtshali and Khubisa, 2019). These users include older adults or senior citizens with limited knowledge of information technology, physically disabled people, minors, and other notable people. However, this work focuses on designing mechanisms to record patients' informed consent for disease diagnosis and clinical treatment. Hospitals or healthcare providers can serve the unique needs of particular users for their patients. Patients do not need to understand the underlying technologies, such as blockchain, smart contracts, distributed systems, consensus mechanisms, etc. We assume that patients' devices, as well as apps, are protected from intruders. Also, communication between patients' devices/apps and blockchain network nodes is secured.

3.6 Consent Operational Costs

Some blockchain-based frameworks need transaction fees, like Gas in Ethereum. The gas consumption or transaction fee is considered for research and technical aspects, not from the patients' or users' perspective. Healthcare providers can spend on infrastructure expenses such as blockchain network nodes, apps for mobile devices to interact with hospitals, blockchain systems, and others. There are direct costs regarding storing informed consent on public blockchain networks like Ethereum. The patients, insurance companies, and others can cover these costs, like doctors' fees, medications, pathology lab tests, radiology lab tests, and other direct/indirect costs related to treatment. In blockchain networks, state change operations require spending money, while reading from the network does not need monetary expenditure. Once informed consents are deployed to the blockchain networks, relevant users can access them without spending charges.

3.7 Consent Indexing and Query

We know the importance of informed consent indexing and query mechanism to provide efficient queries for consent enforcement and patient interaction. For this work, we assume that the search operations are done by the corresponding smart contracts efficiently from the blockchain network. However, detailed indexing and search mechanisms are our future communication.

4 CONSENT SERVICES

Patients need to know they can get information about their consent given to whom, for what purpose, on what resources, and under what conditions. They can also learn how their consent is carried out, such as who does what operation and when. This section discusses user and resource-oriented consent services available for patients through the proposed framework with the required credentials. There might be other services for given and executed consents, such as operation-oriented, date-oriented, and so on (Albalwy et al., 2021). Additional services are not discussed in this paper because of space limitations. However, there should be some assurances regarding the given and executed consents. Guarantees can be served through different consent services. The main objective is to provide patients with concise and informative reflections on informed consent.

User-Oriented Services. In this service mode, a patient is aware of a specific user's consent. It displays a list of resources for which the user has obtained the patient's permission to perform certain operations. The application conditions, such as access frequency, start and end dates, and other specific requirements, are also included. The audit trails are available to the patient if a user performs any operation on any resource. So that the patient can check all of the user's consents. Figure 4 depicts all given consents for a doctor, *David*, on patient *Jordan's* health records: *Visit Notes, Prescription, Radiology Lab Report, Pathology Lab Report*, and *Immunization History* with operations and conditions. While all exe-

cuted consents are shown in Figure 5 with operations, access frequency, and access time.

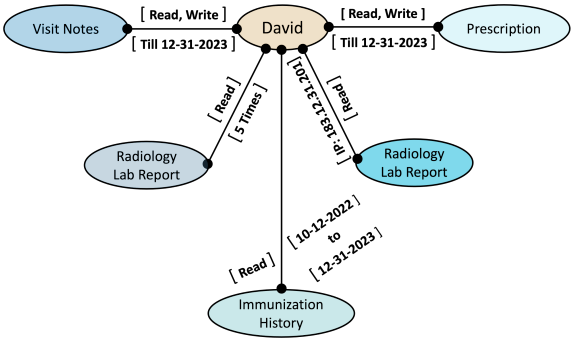

Figure 4: User-Oriented Given Consents.

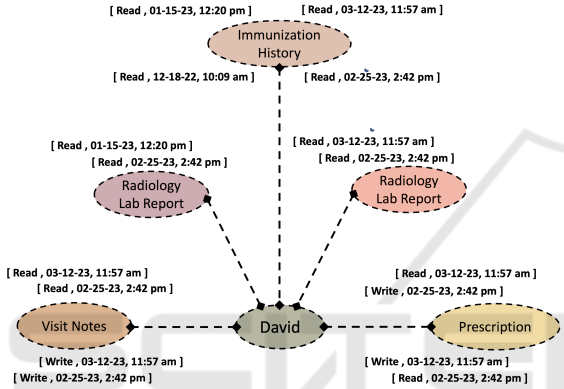

Figure 5: User-Oriented Executed Consents.

Resource-Oriented Services. Patients may need to know the given and executed consent for a particular resource or object. In an object-oriented given consent service, all permissions are listed, like who has which operation consent under what conditions. Figure 6 shows a sample presentation of an object-oriented given consent. Each user has some operations and requirements for the object. While Figure 7 depicts the executed authorizations for an object. It shows several events where each event contains which subject performs what operation when and other information.

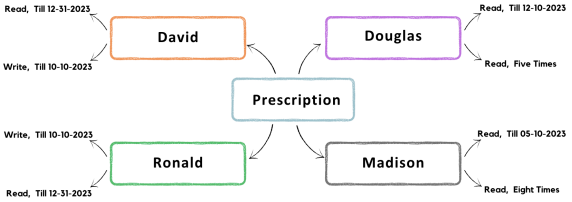

Figure 6: Object-Oriented Given Consents.

Patient consent service gives an overview of the issued and executed consents. A patient needs to know

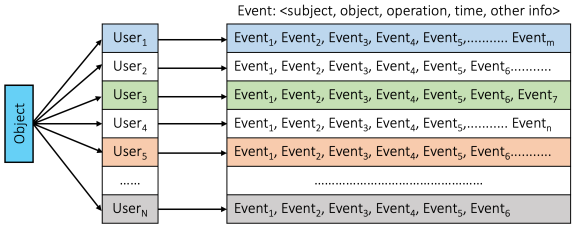

Figure 7: Object-Oriented Executed Consents.

the moment consent status. This service must be unambiguous, uninterrupted, unaltered, real-time, and easily understandable for the patients. In this work, we present some possible applications of consent services. In future directions, we want to implement consent services using graph databases. Consent-related information is collected from the blockchain network and processed as graph databases to reflect the consent status more presentable, understandable, and meaningful for the patients.

5 CONSENT MANAGEMENT

This section briefly explains consent management requirements and various operations: consent generation, modification, withdrawal, expiration, and archiving. It is essential to ensure that operations do not introduce privilege conflicts, leakages, or incomplete treatment teams. The most important point is ensuring that consent modification, withdrawal, or expiration does not interrupt the treatment process. For example, if consent for an insurance agent is revoked, that agent cannot access or process patient coverage billed by the hospital. They can refuse the treatment if the hospital is not paid promptly. Consent can include information about the people using it, the resources it will use, the activities it will be used for, certain conditions, and other relevant information. Due to page constraints, technical mechanisms or specifications for operations are not included, and they are the future scope of this work.

Management Considerations. Consent management is integral to providing healthcare services because it involves collecting, storing, and managing information about patient consent. Effective consent management requires paying close attention to several important factors, such as: *(i) legal and ethical requirements; (ii) patient autonomy; (iii) data privacy and security; (iv) interoperability; (v) user experience; (vi) continuous improvement;* and *(vii) others.* Consent management is a complicated, multi-step process that needs to be carefully thought out to work well, be efficient, and meet all relevant standards and requirements.

Consent Generation. In this process, new consent is created or generated. The detailed functionalities are given in section 3 with the necessary components and their interactions. Further consent can cause conflict with the existing consent. So, it needs to be checked before adding permission to the repository to ensure no conflict of privileges. Once the verification is done, the approval is activated for the users.

Consent Modification. Sometimes, it is necessary to update a consent for various reasons: *(i) having error(s)*, *(ii) modifying current user(s), object(s), or condition(s)*, *(iii) adding new user(s), entity(s), or condition(s)*, *(iv) dropping user(s), object(s), or condition(s)*, and others. If any modification occurs, the old consent is added to the consent archive repository and referred to as a pointer to the new permission. When giving and taking consent, the wrong people, resources, operations, or conditions can be added unintentionally. This could lead to some unwanted events, including security incidents. Once a mistake is realized, it must be fixed immediately to avoid unwanted incidents.

Consent Withdrawn. Approval withdrawal happens if patients do not want to share their data anytime. In another case, if consent is given to the wrong person or includes some extreme conditions, the given authorization can be revoked by the patient or hospital authority. When consent is withdrawn, related users or entities must be notified. It is added to the consent archive database to solve legal and regulatory problems if consent is ever taken away. If given consents are essential to the patient's treatment and are taken out before the treatment is over, there may be some consequences, like an interruption in treatment or drug supply.

Consent Expiration. A given consent can be voided if unmet conditions exist. Conditions could be a specific date, access frequency, and so on. For example, a doctor consents to view or read healthcare data for a particular patient. The approval includes a condition that access can be granted five times. The consent expires when the doctor reads or views the patient's data five times. If the doctor tries to access it for the sixth time, the system fails to authorize it since there is no consent for this access attempt. There can be multiple conditions for approval that keep the support active or valid. All conditions should be checked automatically by systems instead of manually. Manual checking can introduce delays or be overlooked by the corresponding users.

Consent Archiving. Modified, withdrawn, and expired consents are added to this read-only repository. No consent is active in this database. The main goal of this repository is to store consent metadata that can be used to answer any questions that come up because of legal or regulatory requirements. Patients can also see all the previously given consents that have been modified, withdrawn, or expired.

Implementation. We implement a smart contract, "ConsentManagement," in Ethereum using Solidity language to perform consent management operations. Consent generation is done by the proposed smart contract deployment unit in Section 3.3 using Algorithm 2. In addition, the ConsentManagement contract would perform consent modification and withdrawal invoked by the consent owner or patient. Consent expiration and archiving operations must be done automatically as default functions when the conditions are present.

6 EXPERIMENTAL EVALUATION

We implement smart contracts to interact with the Ethereum test network, *Goerli*, to store and retrieve given informed consent. We use the Python web3 framework Brownie and Ethereum solidity. We set up a multi-signature wallet to perform consent management operations. It is two members and two out of two (2 out of 2) control. Every member must sign in to store the consent in the blockchain network. The Healthcare Provider System deploys smart contracts in the *Goerli* network and transfers ownership to the corresponding patients. We use Metamask wallet to sign the transaction to interact with the *Goerli* network. *Goerli* faucet ethers are used as gas to send the transaction. We leverage Infura API to interact with the blockchain networks.

The Ethereum blockchain platform is selected for the experimental purpose. It offers Turing complete smart contract language, Solidity, and Vyper, to implement the logic for the proposed model. Since deployed codes stay in the blockchain network and can not be changed. Deploying smart contract to the main network with bugs or errors cost money and reputation. So it is essential to test smart contracts before deploying them to the Ethereum main network. Goerli and Sepolia Ethereum test networks (Sivaselvan et al., 2023) are currently available for testing smart contracts. In the following, we discuss the main resources: *(i) time, (ii) computational,* and *(iii) gas* required to deploy and evaluate the functionalities of the proposed approach. Other resources are not considered for this work.

Time. Smart contract deployment and execution stages are the basis of the time cost associated with on-chain activities. Since the time it takes to double-check and sign a transaction is entirely up to the user,

it is disregarded. The duration of a smart contract's deployment and execution is determined mainly by how long it takes for the appropriate transaction to be included in a block by miners. So, on average, the duration of either process is about the same as the time it takes for a transaction to be confirmed on the blockchain technology of ones choosing. A new block is added to the Ethereum blockchain every 12 seconds, which is ideal for our purposes. It was 15 seconds in 2019 (Pierro and Rocha, 2019). So long as there is sufficient place in new blocks, a new transaction would take, on average, no more than 12 seconds. The time it takes for a transaction to propagate is more difficult in practice. If block congestion occurs, the time it takes for a transaction to be included in a block might increase. However, blockchain users can influence this time by paying more gas for faster confirmation. Given that users may artificially extend the confirmation time of their transactions.

Computational Resource. To deploy smart contracts on the Ethereum test network, Goerli, the proposed method uses Infura blockchain API services. Infura (Panda and Satapathy, 2021) is a suite for building blockchain applications. It has tools for developers and application programming interfaces (APIs). Infura also gives developers quick and reliable access to the Ethereum network, which lets them build sophisticated next-generation software and Web3 apps that can grow to meet user demand. So, there is no need to keep a blockchain node running to use smart contracts. We assume that other resources like the CPU, HDD, and communication bandwidth on the local machine are negligible.

Gas Consumption. All the read calls of smart contracts are gas-free. Gas is needed for any activity on Ethereum that involves writing or changing data (Wood et al., 2014). Some functions are sending ether (or any other ERC20 token), minting and sending NFTs, deploying smart contracts, changing the state of the blockchain, and so on. For this work, we only need to consider smart contract deployment and function calling costs to write data on the blockchain network. The cost of smart contract deployment is proportional to the size of the code. This is a one-time cost for a single-contract deployment. How much it costs to call a function depends on how many times it is called and how much data needs to be stored or changed on the blockchain network. Code optimization is crucial to reduce gas costs. But instead of reducing gas use, we focus on the model's functions.

7 CONCLUSIONS

Consent to treatment is a crucial aspect of ethical and practical healthcare delivery. It is necessary to ensure that patients are fully informed, involved, and in control of their health and treatment decisions. Therefore, healthcare providers must take the necessary measures to ensure patients understand their treatment options and make educated decisions regarding their treatment processes. In addition, it helps build trust, empower patients, and improve the quality of care provided. Informed consent is an ongoing process; patients can change their minds and withdraw their consent anytime. Also, it is not a one-time event but a continuous process that starts before the intervention and continues throughout the patient's care.

Smart contract-based patient consent management frameworks are emerging as a promising solution to the challenges of managing health data in a secure and privacy-preserving manner. Such frameworks ensure that patients have control over their protected health information (PHI) and can provide informed consent for its use by healthcare providers, researchers, and other stakeholders. In addition, blockchain technologies can ensure that consent is managed securely and efficiently. At the same time, they can provide decentralization, transparency, and immutability that can be leveraged to improve healthcare auditability and accountability for all stakeholders involved. Such inherent characteristics make it a potential solution for healthcare data systems concerning sharing and patient privacy.

This work identifies some important consent management operations for the uninterrupted treatment process. However, there is a need for those operations to be specified and executed technically. In the future direction, the detailed technical approach will be worked on. Future research could also examine the ethical considerations of using blockchain and smart contract technology in healthcare, implementing and adopting smart contract-based systems in actual healthcare settings, and integrating smart contracts with other emerging technologies.

ACKNOWLEDGEMENTS

This work was partially supported by the U.S. National Science Foundation under Grant No. 1822118 and 2226232. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation, or other federal agencies.

REFERENCES

Albalwy, F., Brass, A., Davies, A., et al. (2021). A blockchain-based dynamic consent architecture to support clinical genomic data sharing (consentchain): Proof-of-concept study. *JMIR medical informatics*, 9(11):e27816.

Altarawneh, A., Herschberg, T., Medury, S., Kandah, F., and Skjellum, A. (2020). Buterin's scalability trilemma viewed through a state-change-based classification for common consensus algorithms. In *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, pages 0727–0736.

Azaria, A., Ekblaw, A., Vieira, T., and Lippman, A. (2016). Medrec: Using blockchain for medical data access and permission management. In *2016 2nd International Conference on Open and Big Data (OBD)*, pages 25–30. IEEE.

Buterin, V. et al. (2014). A next-generation smart contract and decentralized application platform. *white paper*, 3(37):2–1.

Cunningham, J., Davies, N., Devaney, S., Holm, S., Harding, M., Neumann, V., and Ainsworth, J. (2022). Non-fungible tokens as a mechanism for representing patient consent. *Studies in Health Technology and Informatics*, 294:382–386.

de Oliveira, M. T., Verginadis, Y., Reis, L. H., Psarra, E., Patiniotakis, I., and Olabarriaga, S. D. (2023). Ac-abac: Attribute-based access control for electronic medical records during acute care. *Expert Systems with Applications*, 213:119271.

Falagas, M. E., Korbila, I. P., Giannopoulou, K. P., Kondilis, B. K., and Peppas, G. (2009). Informed consent: how much and what do patients understand? *The American Journal of Surgery*, 198(3):420–435.

Fan, K., Wang, S., Ren, Y., Li, H., and Yang, Y. (2018). Medblock: Efficient and secure medical data sharing via blockchain. *Journal of medical systems*, 42(8):136.

Gopal, R. D., Hidaji, H., Kutlu, S. N., Patterson, R. A., and Yaraghi, N. (2023). Law, economics, and privacy: Implications of government policies on website and third-party information sharing. *Information Systems Research*.

He, D., Li, S., Li, C., Zhu, S., Chan, S., Min, W., and Guizani, N. (2020). Security analysis of cryptocurrency wallets in android-based applications. *IEEE Network*, 34(6):114–119.

Lorenzini, G., Shaw, D. M., Arbelaez Ossa, L., and Elger, B. S. (2022). Machine learning applications in healthcare and the role of informed consent: Ethical and practical considerations. *Clinical Ethics*, page 14777509221094476.

Marchand-Melsom, A. and Nguyen Mai, D. B. (2020). Automatic repair of owasp top 10 security vulnerabilities: A survey. In *Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops*, pages 23–30.

Mtshali, P. and Khubisa, F. (2019). A smart home appliance control system for physically disabled people. In *2019 Conference on Information Communications Technology and Society (ICTAS)*, pages 1–5. IEEE.

Panda, S. K. and Satapathy, S. C. (2021). An investigation into smart contract deployment on ethereum platform using web3. js and solidity using blockchain. In *Data Engineering and Intelligent Computing: Proceedings of ICICC 2020*, pages 549–561. Springer.

Parvin, A. (2022). Jurisprudential justification of informed consent in medical practice: A critical approach. *Issue 5 Int'l JL Mgmt. & Human.*, 5:956.

Pergolizzi, J. V., Curro, F. A., Col, N., Ghods, M. P., Vena, D., Taylor, R., Naftolin, F., and LeQuang, J. A. (2017). A multicentre evaluation of an opioid patient–provider agreement. *Postgraduate medical journal*, 93(1104):613–617.

Pierro, G. A. and Rocha, H. (2019). The influence factors on ethereum transaction fees. In *2019 IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB)*, pages 24–31. IEEE.

Ploug, T. and Holm, S. (2012). Pharmaceutical information systems and possible implementations of informed consent-developing an heuristic. *BMC Medical Ethics*, 13(1):1–12.

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., and Ahmad Khan, R. (2020). Healthcare data breaches: insights and implications. In *Healthcare*, volume 8, page 133. Multidisciplinary Digital Publishing Institute.

Sivaselvan, N., Bhat, V., Rajarajan, M., and Das, A. K. (2023). A new scalable and secure access control scheme using blockchain technology for iot. *IEEE Transactions on Network and Service Management*.

Staff, C. P. S. (2016). Regulatory compliance/lessons learned from hipaa enforcement. *Journal of the California Dental Association*, 44(11):703–704.

Sulmasy, L. S., López, A. M., and Horwitch, C. A. (2017). Ethical implications of the electronic health record: in the service of the patient. *Journal of general internal medicine*, 32(8):935–939.

Tith, D., Lee, J.-S., Suzuki, H., Wijesundara, W., Taira, N., Obi, T., and Ohyama, N. (2020). Patient consent management by a purpose-based consent model for electronic health record based on blockchain technology. *Healthcare Informatics Research*, 26(4):265–273.

Wood, G. et al. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151(2014):1–32.

Xia, Q., Sifah, E. B., Smahi, A., Amofa, S., and Zhang, X. (2017). Bbds: Blockchain-based data sharing for electronic medical records in cloud environments. *Information*, 8(2):44.

Yue, X., Wang, H., Jin, D., Li, M., and Jiang, W. (2016). Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. *Journal of medical systems*, 40(10):218.

Zyskind, G., Nathan, O., et al. (2015). Decentralizing privacy: Using blockchain to protect personal data. In *2015 IEEE Security and Privacy Workshops*, pages 180–184. IEEE.