PolyDoc - A Blockchain-based IoT application for Improving the Auditability of Healthcare Systems

Lewis Strawbridge MSc Cyber Security[1 [*]]0000-0003-4546-2703

Newcastle University, Tyne Wear, UK, NE1 7RU c1024829@newcastle.ac.uk
https://www.ncl.ac.uk/ {outreach}@ncl.ac.uk

Acknowledgements: Thank you to M.Barati for supervising this project — masoud.barati@newcastle.ac.uk and H.Ghahramani for aiding in research of section 1.1 and Fig.3. hosna.ghahramani92@gmail.com

Abstract. Internet of Things (IoT) computing is becoming more prevalent in healthcare internationally. As the landscape changes to accommodate for more interconnected electronic devices the intrusion gap increases. Patient-provider trust and transparency are therefore key challenges in facilitating the developments to the medical landscape. The popular approach for RPM is the collected health data is forwarded via a central-ized software application to healthcare professionals to monitor. However, transparent audit trails of this data relayed to the user has become a major challenge. A scalable, blockchain based IoT system framework is presented which utilizes the traceable and immutable features of the blockchain to allow for transparent audit trails of the patient data. Additionally, the system uses IPFS in order to store data in a decentralized manner, whilst ensuring the security of data during distribution on the public chain with attribute based encryption.

Keywords: Healthcare · Blockchain · Internet of Things

Contents

1 Introduction

There are issues surrounding traditional healthcare systems. Patients personal data is either stored locally or in a centralised system with poor audit trails, resulting in a sub-par failsafe for detecting and preventing data malpractice. Additionally these healthcare systems are often breached in terms of confidentiality, integrity and availability [1]. In order to prevent misuse of data in addition to cybersecurity threats it is important to take advantage of emerging technologies which can help mitigate these issues.

1.1 IoT in healthcare: benefits

Healthcare applications serve many purposes, such as decision-making, workflows, and clinical facts, electronic health records (EHR), genomics medicine, neuroscience, biomedical, and pharmaceuticals. Data standardization and communication protocols can enable IoT technologies to deliver efficient healthcare services. Better connectivity, user interfaces, the security of patient data, and data interoperability can reduce the challenges of providing efficient healthcare services. Presently, healthcare is one of the most popular ongoing research domains; researchers strive to make more reliable healthcare applications for the community and healthcare industry. The benefits of data driven, safely handled patient data has been brought to the attention of the UK government, which has recently commissioned a proposal to reassure people their data is handled safely and ethically in combination with funnelling over 200 million GBP in data for research and development [2]

Several stakeholders, such as patients, hospitals, and pharmacies, need to maintain, share, and access health records in a secure way without any changes. The use of IoT devices in healthcare has shown an increase in recent years and this is forecasted to only keep growing [3]. Wearable real time-monitoring being a particular area of development including: Smart watches, sensors and patches [4]. These IoT devices can offer healthcare support, efficiently to those who need it, to people that have found it difficult to receive prior. For example in the case of diabetics allowing real-time monitoring of glucose levels whilst improving safety and reducing pressure on outpatient departments. The importance for these devices has only been demonstrated further by the Covid-19 pandemic where in person consultations were not always an option. During this time many were confined to their own homes (particularly the elderly population) and rapid adjustments were required to facilitate a new, more accessible, medical landscape.

Importance of Auditability As more electronic devices are introduced to the healthcare system, the intrusion gap for malicious threat actors to intercept EHRs increases. It is pivotal for informed and coherent audit trails of this personal data to ensure the data is not viewable, or tampered with by any unauthorized parties. In the worst case of a breach, this should be discovered and an emergency backup plan can be effectively implemented. Additionally, not

all threats come from outside an organization. According to the The European Union Agency for Cybersecurity, 34 percent of business environment respondents suffered from insider privilege abuse [5]. By implementing effective auditability organizations can help keep track of digital assets and records to ensure there is no misuse from inside or outside threats.

How Blockchain may help The immutability and auditability of blockchain technology has been pivotal in its rapid increase in popularity with an adoption rate similar to the internet in the 1990's [6]. These traits have led to many applications ranging from: Supply chain management in the pharmaceutical sector [7], finance (Bitcoin), decentralized communications [8] and many more. It could also be an effective method to improve auditability when integrated with healthcare systems involving Electronic Health Records. More detail on the blockchain will be supplied in the related work section.

2 Motivation

2.1 Importance of Research

The traditional processing of patient data usually follows a procedure in which the data is digitally monitored, then recorded by the medical professional who enters the data into a centralised system to store as EHR's. The centralised system leaves the data at risk from breach with a single point of failure. Once the patients data is entered into the system, it is virtually untraceable from the patients perspective and at risk of being tampered with.

The research at hand will take advantage of emerging technology by implementing a blockchain-based IoT system for improving the auditability of Healthcare records. With this increase in auditability, the aim is to prevent tampering and the unauthorized disclosure of Electronic Health Records (EHR). This is an important research field due to the benefits of transparent data auditing within the growing IoT medical landscape. By utilising the "trustless system" within blockchain, the aim is to improve trust between healthcare organizations and patients alike.

Contribution The proposed system describes a framework to create a more transparent, scalable and secure IoT healthcare model than previous designs that can reduce transaction fees to provide a more realistic option for patient monitoring. To achieve this, the public layer 2 Polygon network is used over Ethereum for smart contract interactions. This will be deployed using remix IDE [9]. A framework is proposed for an application where the user will be able to connect their web3 wallet, interact with smart contracts and submit their encrypted data to the blockchain which is received by managers in the admin view of the platform. The data can then be distributed securely to an approved data requester such as a doctor or GP. Queries can be made on this data in order to find specific records. In summary the principle contributions from this paper are as follows:

- IoT based architecture has been proposed based on blockchain technology in order to protect health records and improve auditability of healthcare systems.
- Smart contracts have been deployed to Layer 2, Proof of Stake, public blockchain Polygon which sits over Ethereum in order to improve operational functionality and cost compared to the Proof of Work model.
- Healthcare data in the proposed model is dual encrypted: The data itself in addition to the IPFS content identifier (CID), offering exceptional security.
- Performance metrics are measured in terms of mining time, transaction cost, operational effectiveness and how CID generation time varies with the amount of users. The mainnet was used where appropriate, in order to provide realistic results.

Paper Roadmap The remaining article is structured as follows: Section 3 discusses related work including further background on Blockchain, InterPlanetary File System (IPFS) and databases. This is followed by related research works presented in a table format with specific comparisons and review of the sources. Section 4 highlights the proposed system, its objectives and layers. Section 5 is deployment which will present the proposed architecture, its interactions and some specific protocols. Section 6 discusses the implementation of the system into the prototype applications including smart contracts, additional tools and access control. Section 7 is performance evaluation and finally Section 8 is the conclusion which provides a comparative analysis from other research models followed by future work.

3 Related work

3.1 Blockchain overview

Blockchain technology has become increasingly popular, particularly in the last few years. The amount of IEEE publications from books, journals and conferences including "blockchain" as a topic between 2019 and the time of writing is 10,783. Comparably, the prior 3 years between 2016-2019 this number totalled 4213 [10].

The idea of trustless systems, in which the participants involved do not need to know or trust each other or a third party for the system to function [11], strongly links to many blockchain systems such as: Bitcoin for "Smart" monetary transactions and Ethereum [12] and Polygon [13] for creation of decentralized applications and "Smart" contracts. In the trustless trust model, no single party has control over the system therefore all the trust a user needs to place is in the system itself. It is worth noting that trust still needs to be placed in the validity of the system. It does however reduce the need for placing trust in so many intermediaries/individuals as opposed to traditional systems, having

the potential to overhaul many systems currently used today. With blockchain technology trust is established when each owner transfers to the next by digitally signing a hash of the previous transaction and the public key of the next owner, then adding these to the end of the hash. A payee can verify the signatures to verify the chain of ownership [14]. The details of every transaction made are stored in the blockchain ledger. These details can be viewed publicly on the internet [15]. The fact this information is stored publicly, makes for many applications for transparent and open systems, with the chain of records and the corresponding addresses available for all to view. In this form, the use of the blockchain to transmit sensitive data (such as patient data in healthcare) can be seen as a limitation by compromising confidentiality. Section 4 and 5 of this report present a framework to resolve this.

Variations of Blockchain Decentralization. Transparency. Tamper proof. These are the fundamentals blockchain was founded on in 2011 with the creation of Bitcoin for smart monetary transactions. Since then, the use case has expanded, with this expansion, there are now different branches of blockchains for different applications. Public blockchains refer to the chain of transactions visible on the public ledger (as described above) however private blockchains such as Ethereum Private [16] and Hyperledger [17] are used by organizations to deal with data which should not be visible to the public. Ethereum Private Chain is on a completely separate chain to its Ethereum counterpart whereas Hyperledger is a private blockchain framework which is founded by the Linux foundation. Aside from the proposed benefit of limited access to these networks, they also lend to the possibility of faster transaction times.The reason for this is congestion on the networks will be lower in comparison to the public blockchain (which can range drastically even depending on time of day.)

Hybrid blockchains are a combination of public and private features. It lets organizations set up a private, permission-based system alongside a public permissionless system. Transactions are typically not made public however can be verified when needed for example through access to a smart contract. This allows participants in the network to protect their personal data and at the same time benefit from the fundamentals of blockchain technology to improve the level of trust for organizations processing their data. An example of a Hybrid blockchain is IBM food trust [18] which aims to address food sustainability issues in the supply chain.

Lastly, Consortium blockchains are similar to hybrid blockchains in the way they both reap benefits of public and private chains, however operate with multiple entities. Since there is no single centralized authority governing control, the blockchain manages to somewhat maintain its decentralized nature. It achieves this by pre-selecting a number of institutions to make changes in the best interests of the network and to implement these changes, every institution must approve the change.

Decentralized Storage and Database Layers Storing large amounts of data on the blockchain is expensive, time consuming and overall not feasible because of the

way blockchains log a chain of the data for all previous transactions. Currently, other methods of off chain storage must be considered. A popular method is IPFS (Inter Planetary File System) [19]. IPFS acts as a peer to peer, decentralized off chain file system. The protocol aims to address censorship, inefficiency and poor security by providing a resilient, trustless and scalable system. To access the files the user needs a content identifier (CID). This comes in the form of a hash, and anyone with the hash can access the file. It is therefore important to encrypt this value to ensure security of private data to only be retrievable with the correct permissions.

3.2 Table of Contributions

This section will present and discuss contributions from other works, along with their limitations. Table 1 gives a summary of research works into blockchain healthcare systems.

3.3 Literature Review

In [20], a privacy-preserving technology was implemented using a blockchain-based methodology. They propose a binary spring search (BSS) algorithm which consists of a hybrid deep neural network approach. The proposed approach effectively detects the intrusion within the IoT network. The data collected was sent to a Hyperledger Fabric network with the blockchain itself being used as a distributed database. In addition, the proposed system implements a homomorphic encryption technique and key revocation algorithm to improve security. They performed benchmark simulations based on the blockchain-based tool Hyperledger Caliper [29] and OrigionLab [30] for analysis and evaluation. They found by comparative analysis that the proposed framework provides better security and searchable mechanisms for healthcare systems.

Healthcare systems such as HealthBlock [22] use a private blockchain for consultation in their model, whereas others use a private blockchain for real time monitoring [21]. Both are similarly created with Hyperledger framework and benchmarked with Caliper. The scope of Healthblock's performance assessment was throughput, latency and resource utilization and demonstrated a reduced mining cost, latency and provided a considerable increase in overall throughput when compared to other models. The latter provided a fully comprehensive result section to their report measuring throughput, transaction time, latency in transactions by testing different congestion levels on the network. It is clear that additional users on the private network affect the transaction time significantly. A novel ability of the remote monitoring sensor was to notify the admins if the device behaved in an abnormal way via smart contract. This increases the suitability for real-world applications where IoT device management and maintenance are key.

The authors in [23] propose a novel contribution of vaccine passports considering GDPR with blockchain and IPFS. Several protocols were designed for agreement, creation, access, verify and erasure of data. The experimental results

Table 1. Table summarizing related works

Paper	Contribution	BC	Security	Storage	Tests	Limits
[20]	BC as a distributed DB.	Private, Hyperledger	Access control using homomorphic encryption	Blockchain	Hyperledger Caliper	Data is stored on the BC - Scalability issue.
[21]	Monitoring patient vital signs using smart contracts.	Private, Hyperledger	Enrollment key is in the form of users BC private key.	CouchDB	Hyperledger Caliper	Lack of authentication, only deployed on local server.
[22]	BC to improve access control & auditability.	Private, Hyperledger	MSP's authenticate the identity	IPFS/Orbit-DB	Hyperledger Caliper	Private blockchain may seem centralized.
[23]	Novel contribution of vaccine passports.	Permission, Ethereum	Hash created for each IPFS CID	IPFS/Local	Ganache/Ropsten	May have scalability issues with high gas fees on Ethereum network.
[24]	Realtime monitoring integrates IoT with BC.	Permission, Ethereum	Proxy re-encryption	IPFS	Test Networks	Private Ethereum, may still be costly.
[25]	Medical access control by means of smart contracts.	Private, Ethereum	attribute-based encryption (CPABE)	AWS	Rinkeby	Amazon Cloud services are used.
[26]	Scalable blockchain for healthcare data.	Private, Custom	(AES-128), (RSA-4096), Digital signatures	IPFS	User testing	Needs to be tested in real time.
[27]	Patient vital signs monitoring.	Private, N/A	N/A	Blockchain	N/A	Scalability issues with storing data directly in blockchain.
[28]	Patient monitoring and sharing.	Hybrid, Ethereum	API Keys/Async Ciphers	Cloud	Not stated	Specific encryption techniques not defined.

demonstrated the scalability of the proposed solution by measuring the CID generation time for IPFS and then directly comparing this to the amount of vaccinations given to the UK population at the time of writing. They found that generating CID's all vaccines would take 38 minutes. Further experimentation included the use of Ropsten [31] and Ganache [32] test networks in order to investigate the transactional costs, mining time and how these variables were affected by the number of actors. In comparison to other works, their platform provides a technical solution for checking data erasure requests,which is a significant user right in GDPR which was not touched upon in prior works. The only concern is one with scalability due transaction costs on Ethereum (Although smart contracts have been minimally designed in order to combat this.)

Similarly, another design deployed on Ethereum is [**?**] and proposes a secure PoA (Proof of Authority) healthcare system involving real time monitoring connected to a smartphone user side with a separate app for physicians that integrates IoT with Blockchain. The system is designed to support remote patient monitoring and the encrypted IPFS hash is stored on the blockchain. The report features a section on resistance to common types of cyber attack with the relevant countermeasure which provides additional real world context not seen in many other reports. In the testing, the blockchain transaction time was measured and deduced to be an improvement on PoW (Proof of Work) models. Scalability and real world application are likely once again to be bottlenecked by the mining fees on the Ethereum network.

The storage methods of encryption keys vary along with the encryption itself: [23] uses a local encryption manager to store encryption hashes in order to extract data from IPFS whereas [22] uses an off chain decentralized database OrbitDB [33]. In order to keep in line with the decentralized nature of blockchain and the benefits of moving sensitive information to the cloud. This makes storing the encryption data on a decentralized database that can interact with the blockchain an attractive option for the future, given the functionality and continued development of these databases is in place. However, in their current state, most are lacking support and still very much in the early stages of development. An alternative which will guarantee an exceptional service in this area is cloud servers. [25] Uses AWS cloud which is hosted by Amazon. Despite this improved service and operability, in order to adhere to the fundamentals of blockchain, these types of databases should be avoided. In an ideal scenario, records could be stored on the blockchain itself. [27] suggest this in the proposed solution. In practice this is not feasible. Due to the nature of blockchain to store a log of all previous transactions on the network the transaction costs will be extremely costly and time consuming resulting in an unscalable model.

In terms of encryption methods, [26] uses symmetric encryption (AES-128) for the data to be stored on IPFS Asymmetric encryption (RSA-1024) for generating the digital envelopes to pass on the symmetric key to authorized entities. The multiple layers of encryption offer security of patient data whereas other models such as [27] and [28] offers little insight into what (if any) encryption methods they propose.

4 Proposed System

4.1 System objectives

In this project the objective is to improve the scalability compared to previous blockchain healthcare systems by deploying smart contracts to the layer 2 public blockchain Polygon (which sits over layer 1 Ethereum architecture.) Comparatively to Ethereum based systems, this system operates with a Proof of Stake (PoS) instead of Proof of Work (PoW) algorithm. PoW algorithms are inefficient, therefore by making this change should show an increase in operational effectiveness and cost. For real-time monitoring situations for use with IoT devices this is of crucial importance to functionality. Transactions need to be fast and affordable in order to make the system feasible. In addition, by using a hybrid blockchain, this system aims to achieve a transparent audit trail of the data, improving patient-provider trust throughout healthcare as a whole.

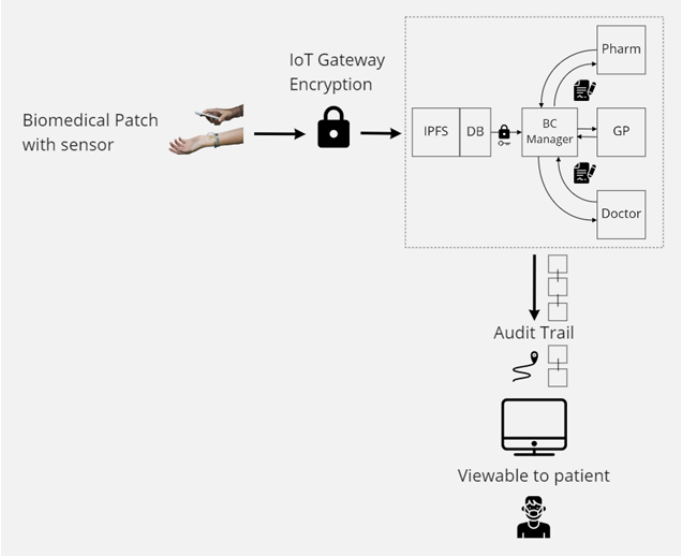

Fig. 1. Audit trail accessible to patient via blockchain app

4.2 Layers

(see Fig. 2). The first layer of the proposed system is the Physical layer. The physical layer is the device itself which extracts patient data, this may come in the form of an "on-skin" biomedical patch [34]

The second layer is the IoT gateway. This can be achieved by utilizing a raspberry pi connected to a REST server API. There will need to be device side

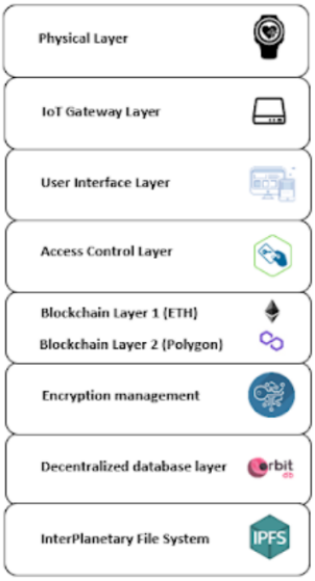

Fig. 2. Layers of Proposed PolyDoc system

encryption in order to send records to the manager on the public blockchain. There are various software security companies that create IoT gateway devices where encryption is handled internally [35].

The third layer is the user interface, this will be prototyped via a blockchain web app for the purposes of this project. This user interface is hosted on the fleek platform which allows the app to be hosted on the decentralised web IPFS.

The fourth layer is access control. In terms of admin and user portals of the platform, only certain elements will be available for respectively privileged users. Furthermore, to access the admin panel the wallet address of the connected wallet must be on a list of verified wallet addresses. In order to gain access to a specific wallet, a user must enter a 12-24 word secret phrase. This secret phrase is generated from a list of words taken from a dictionary, each word assigned a number. The number it can be converted to is used as the seed integer to a deterministic wallet that generates all the key pairs used in the wallet. This private key number is encrypted with Elliptic Curve Cryptography before being hashed with Keccak-256.

The fifth layer is the blockchain layer which will consist of smart contracts hosted on layer 2 network Polygon which sits over the Ethereum blockchain. The reason for hosting smart contracts on Polygon is in an attempt to make the system more scalable, affordable and applicable for real-time monitoring applications. Most research in this area either uses standalone Ethereum, or private Hyperledger blockchains.

The sixth layer is encryption management. This refers to the management of the encryption of the patients healthcare data. The Blockchain manager will encrypt the medical record under the agreement defined in the access policy negotiated with the patient. Once encrypted, the data can be uploaded to IPFS. Once IPFS returns the location to the manager where the medical records are stored. The manager encrypts the medical record location then imbeds the ciphertext into the transaction then broadcasts the transaction to the BC.

The seventh layer is the decentralized database layer which sits over IPFS. In order to run queries on the data and still maintain the decentralized storage aspect of the medical records, this method has been chosen above a local database in the system model. Currently these decentralized databases are in early stage development so are prone to bugs with limited functionality however the core principles of these databases make for a desirable option regardless, especially looking towards future iterations of these databases. Some options currently available are OrbitDB, BigChainDB [36], ThreadDB [37] and GunDB [38]

The eighth and final layer is InterPlanetaryFileStorage (IPFS). IPFS is used as a file system to host the encrypted medical records and the records can be accessed via the CID (Content Identifier.) Once again in the PolyDoc model this CID will be encrypted (Please see the interactions section for more details.)

5 Deployment

The proposed architecture for the PolyDoc system is demonstrated in fig. 2. IPFS stores the ciphertext of the patient's medical information encrypted by the blockchain manager and then returns the corresponding hash value to the data requester (pharmacy, doctor or GP) where the hash value is equivalent to a file address. Once the address is obtained, the authorized data requester can download the ciphertext according to the address. The BC network is the core of this paper and it executes smart contracts in a distributed manner without relying on central entities which is necessary to ensure the secure storage and sharing of electronic medical information. In order to improve system efficiency, the Polygon layer 2 network is used over the Layer 1 Ethereum blockchain to deploy smart contracts.

5.1 System Interactions

(see Fig. 3).Firstly, the patient connects their wallet to the blockchain app and follows the authentication process outlined in the protocol section (1).

Once authenticated the medical records are encrypted patient side by the IoT device connected to the user and then sent via the public blockchain to the manager (2). The manager uploads the encrypted medical records to IPFS (3). IPFS returns the location to the manager where the medical records are stored (4). Then, the manager encrypts the medical record location, imbeds the ciphertext into the transaction and broadcasts the transaction to the BC (5). When the transaction is confirmed the manager records the transaction access

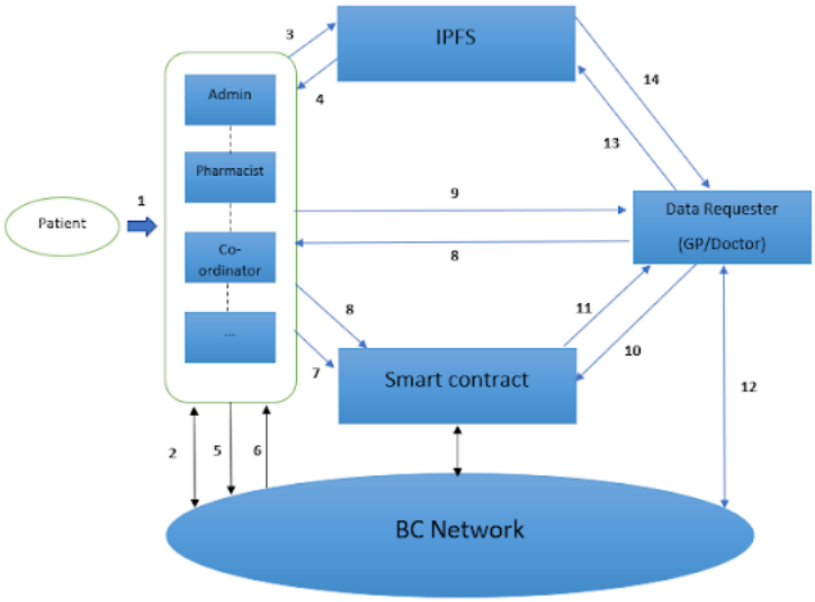

Fig. 3. System Interactions of PolyDoc

(6). The manager encrypts the key words of the medical records, generates the key words index and then stores the transaction address and keyword index into the smart contract (7). Then, the data requester sends a medical recorded access request to the manager and the manager authenticates the identity of the data requester and adds it to the authorized user of the smart contract (8). The manager distributes the appropriate attributes and his attributes key which is then returned to the data requester through a secure channel (9). The data requester creates a search token and then invokes the smart contract with the token as a parameter (10). The smart contract verifies the identity of the data requester. If an authorized user, the smart contract returns the relevant search to them (11). Then, the data requester reads the transaction information from the BC and calculates the file location (12). The data requester obtains the file location and downloads the encrypted medical record from IPFS (13). Finally, the data requester judges whether his attributes satisfy the access structure in the ciphertext and if so decrypts and obtains the medical records (14).

Protocols

Authentication Firstly, the patient connects their wallet to the platform and enters their phone number. This phone number gets sent via a public BC smart contract to the manager. The manager sends the phone a text containing the

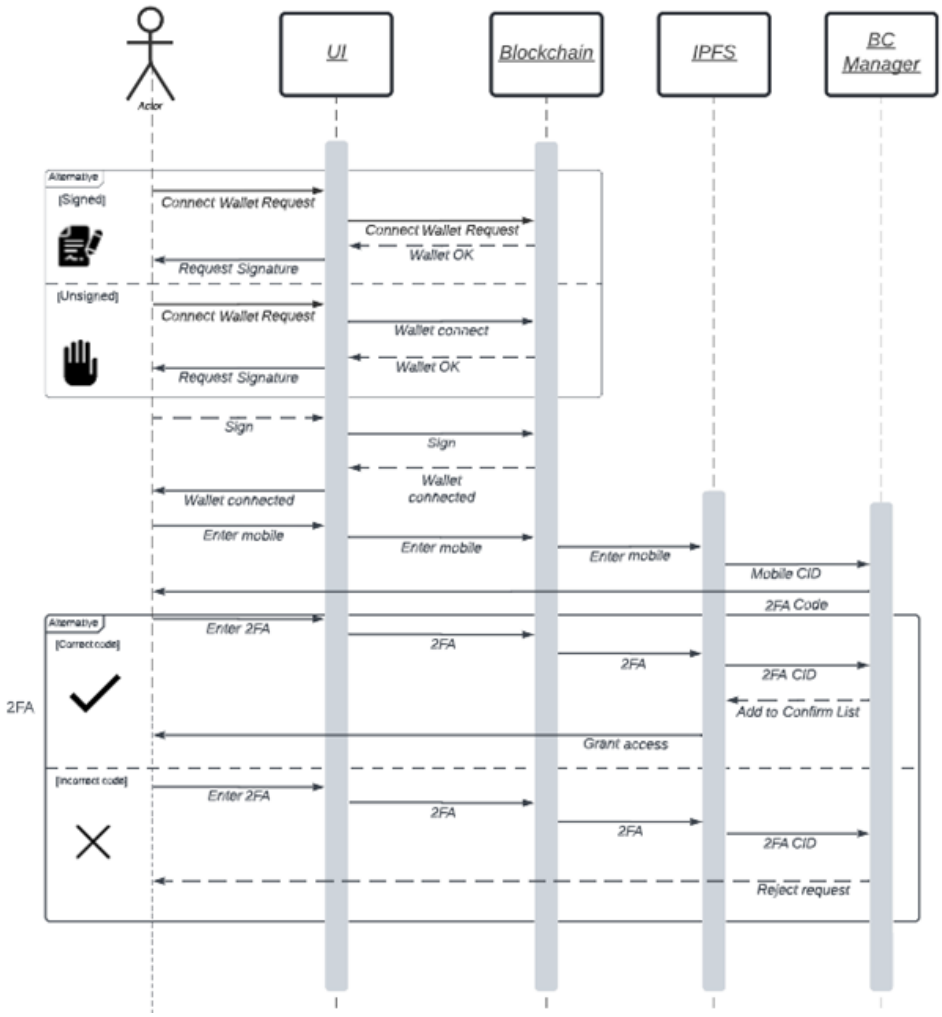

Fig. 4. Patient Authentication Protocol

2FA code. The user receives the code to their mobile phone and enters the code in the platform which is uploaded to IPFS via public BC smart contract and viewable to the manager via the CID. If the manager receives the correct code from the initial patient address in step (1) then they authenticate the user on the network. (see Fig. 4)

6 System Implementation

This section discusses the technology used to create the prototype PolyDoc system proposed in section 4. The system can be divided into the categories which were implemented.

- Smart contract design and deployment.
- Additional tools and technologies.
- API access control.

6.1 Smart Contract Design and Deployment

Remix IDE was used to create and deploy the smart contracts written in the Solidity language. The environment to deploy the contracts was set to injected web3 provider (metamask) connected to the Polygon mainnet (see Fig. 5).

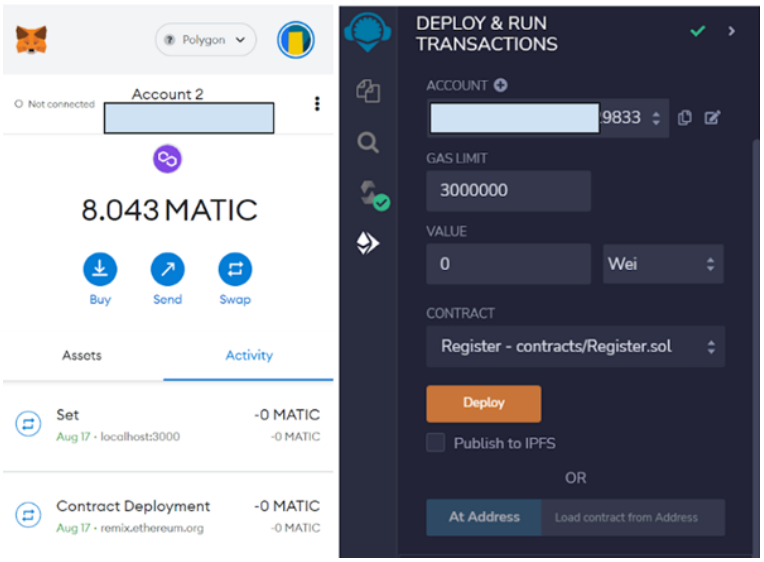

Fig. 5. Contract deployment using remix IDE

The reason for choosing the mainnet in order to deploy the application was to provide accurate results in regards to transaction times and costs which could be discussed in the evaluation section.

Because Polygon is a public layer 2 blockchain over the Ethereum Virtual Machine with its own ledger for transactions, its mainnet offers the same audit trails of data as Ethereum (see Fig. 6).

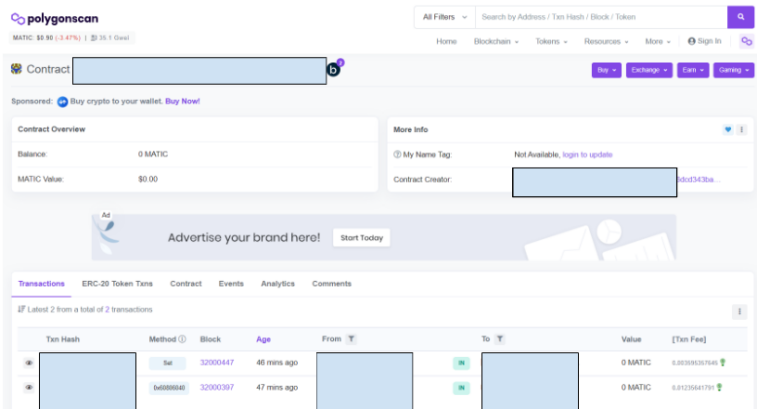

Fig. 6. Deployment of smart contract on Polygon Mainnet

Once the smart contracts were deployed they were viewable on [39] which displays all interactions with the smart contract itself, allowing for time stamped audit trails.

Additional Tools and Technologies In order to keep as much of the system public as possible without compromising security of data. The app was created with react and hosted on fleek [40] (see Fig. 7). The fleek integration allows the blockchain application to be hosted on IPFS and is automatically updated with the github repo. The live patient application frontend is viewable at: https://polydoc.on.fleek.co.

When an admins wallet connects to the site they will have the option to view the admin portal of the blockchain application, which allows them to retrieve IPFS CID hashes for user inputted data and view other admins. (see Fig. 8)

The Infura API [41] is used to manage the IPFS integration with PolyDoc. The values entered by the patient are uploaded to IPFS. The hash is then stored/retrieved in the smart contract. The IPFS hashes are visible on Infura in one place for the blockchain manager to verify.

Access control for the API Smart contracts combined with a novel 2 factor authentication method outlined in section 4 are used to authenticate the patient and grant them access to the system. Once the user has authenticated the admin can view the CID hashes on Infura, grant them permission via access control to upload to IPFS using the API and unlock the ability to connect their data to PolyDoc. (Fig. 5.)

Fig. 7. User section of the prototype application hosted on IPFS via fleek

Fig. 8. Admin section of the prototype application hosted on IPFS via fleek

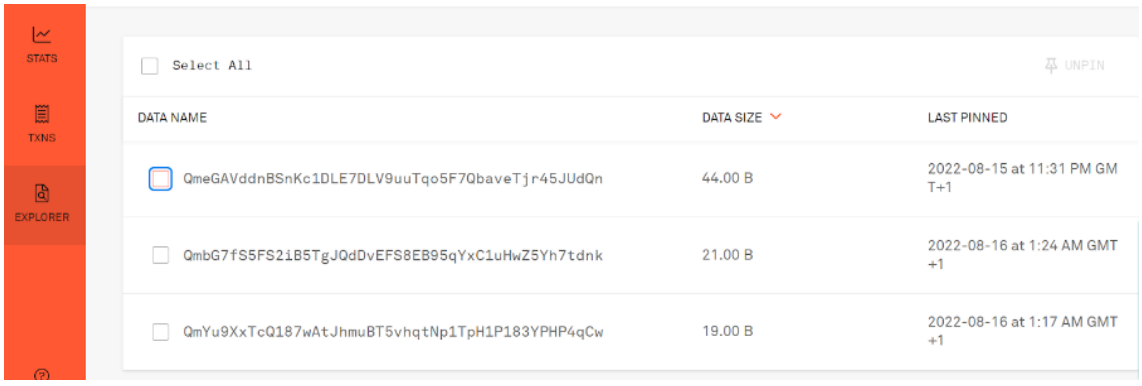

Fig. 9. Timestamped IPFS hashes on Infura

Furthermore requests per second can be rate limited along with the total daily requests as a countermeasure to prevent DDoS and front-running attacks [42] from threat actors seeking to deny patient service. (Fig.6.)

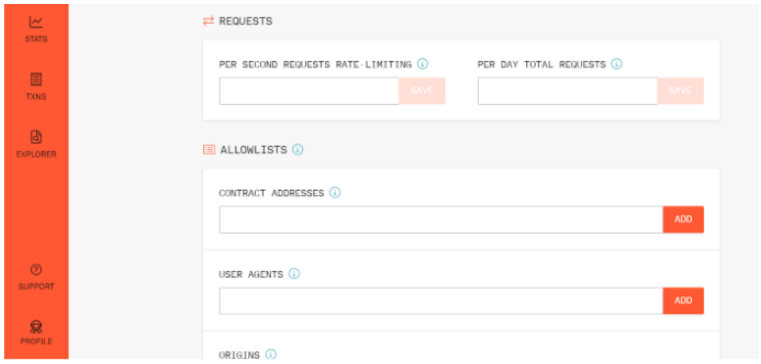

Fig. 10. Allowlists and rate-limiting in the Infura admin panel

7 Performance Evaluation

In order to evaluate the operational effectiveness of the proposed model: Key attributes such as processing time and cost were monitored for various operations and how this value fluctuated with the number of transactions. In order to accommodate variation in gas and coin prices, multiple transactions were taken across the same day for each operation in regular 1 hour intervals. Comparisons between the smart contracts hosted on the Polygon and Ethereum mainnet were made with data presented in Table 2 and Table 3

Operation	Mining time (ms)	Contract deployment time (ms)	Contract deployment cost (USD)	Mining fee (MATIC)	Mining fee (USD)
Patient Registration	300	300	0.003218	0.00359	0.003220
Patient Verify Submission	500	400	0.01073	0.001262	0.001026
Admin Retrieve CID	N/A	N/A	N/A	N/A	N/A

Table 2. Table displaying Polygon interactions

Average CID generation time was measured by using a python script on windows in combination with the console log timestamps. The number of actions were measured in increasing increments of 10 to produce the following results in4 and Fig. 11

Operation	Mining time (ms)	Contract deployment time (ms)	Contract deployment cost (USD)	Mining fee (ETH)	Mining fee (USD)
Patient Registration	400	500	10.928	0.00033	1.74
Patient Verify Submission	400	300	4.21	0.0002960	0.48
Admin Retrieve CID	N/A	N/A	N/A	N/A	N/A

Table 3. Table displaying Ethereum interactions

Users	CID Generation Time (Seconds)
10	0.147
20	0.414
30	0.417
40	0.395
50	0.427
60	1.036
70	0.634
80	1.158
90	1.131
100	1.253

Table 4. Table displaying how CID generation varies with amount of users

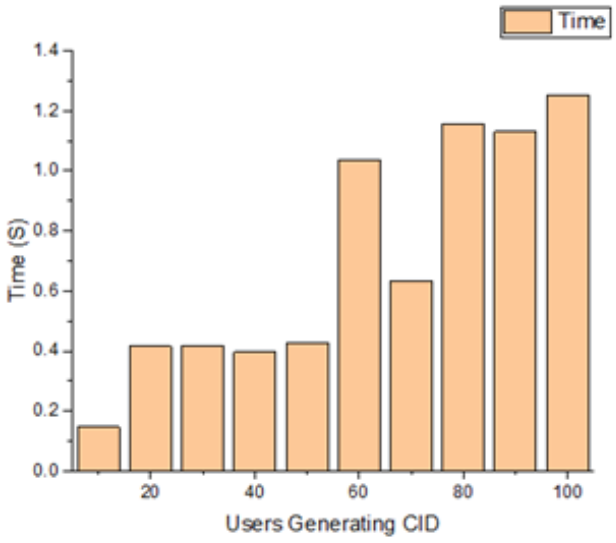

Fig. 11. IPFS CID generation time

From the results it is clear that there are many proposed benefits t o using layer 2 Polygon in IoT healthcare blockchain applications. The cost to call and execute the registration smart contract on the Polygon mainet in comparison to Ethereum was over 500 times cheaper. Furthermore smart contract deployment was over 3000 times cheaper. With this additionally comes a comparable per-formance in terms of transaction time. In real-world healthcare applicable IoT scenarios where continuous monitoring is key, this is game changing in terms of scalability.

7.1 Defence against Cyber Attacks

- *Distributed Denial of Service DDoS*: All requests to upload to IPFS are managed through Infura API admin panel. This includes IP limiting, allow-lists and rate-limiting. These features can be utilized by the blockchain manager to nullify void requests and prevent these types of attack from occurring. In terms of the fleek.io IPFS hosted web interface itself, the system continually monitors traffic patterns to detect any abnormalities, routes, filters and provides post analysis.

- *Frontrunning* attacks: [42] the term for types of attacks on the blockchain where malicious users will attempt to 'frontrun' transactions on the network. They come in the form of: *Suppression, displacement and insertion.* Once again, the Infura API controls the interaction of IPFS with smart contracts and can prevent this.

- *Man In The Middle (MITM)* attacks: the term for a type of attack where an adversary will place themselves between two parties in a bid to gather sensitive or authentication information. In the PolyDoc model, the EHR's are encrypted along with the IPFS location of the data itself.

- *Impersonation* attacks: When a malicious actor impersonates a trusted user. In order to do this they will have to either gain access to the private wallet key or break the eliptic curve discrete logarithm problem. This is very difficult. Alternatively they may attempt to impersonate an admin via API. In this model, the API secret is encrypted with AES encryption and stored in a decentralized database.

- *Message forgery* attacks: This attack is used when the threat actor is trying to fabricate a digital signature for a message without having access to the signing key. Elliptic curve cryptography is used to sign messages and is very difficult to solve.

8 Conclusion

This paper describes a blockchain based application framework for auditable healthcare systems suitable for use with IoT devices. The platform uses the

decentralized storage method IPFS in addition to smart contracts deployed on layer 2 architecture Polygon in order to store data in a transparent manner without compromising data privacy. The prototype application created presents some features of the proposed framework.

8.1 Comparative analysis

Compared to recent blockchain healthcare platform frameworks [43] [44] the PolyDoc platform improves performance in terms of data secu-rity including a 2FA method for user registration/authentication, patient side encryption within the IoT device with further levels of attribute based encryp-tion during transmission on the blockchain. The multiple stages of encryption ensure the data is secured whilst the public ledger gives patients the ability to verify where their data is headed with an immutable, decentralised audit trail. A prototype application has been implemented and the evaluation data shows CID generation time which is practical for this application. The CID generation in [23] is comparable however slightly faster than the PolyDoc model between 10-70 users becoming significant in the 80-100 range. This discrepancy is likely due to the IPFS CID generated via the Infura API in the PolyDoc platform (Which provides benefits in terms of access control itself.)

The analysis also presented a mining fee reduction by a factor of 500 and smart contract deployment fee reduction by a factor of over 3000 by using the Polygon layer. This makes the PolyDoc framework more scalable than all previous public blockchain healthcare models so far, being the first of its kind.

Future work to build on this project should be to continue to develop the UI to implement the full security measures proposed. Additionally a decentralised database layer should be added to the application which allows admins to run queries on patient data. Once this has been done rigorous user testing should take place in order to expose any unforeseen vulnerabilities in the software.

There should also be developments in the design of the physical monitoring device itself. The framework discussed in this paper suggests the use of a form of on skin wearable device such as a biomedical RFID tattoo/patch to collect patient data. The intricacies of this device lay outside the scope of research for this submission. Future work should look to incorporate the findings from this paper with biomedical IoT device research in the area of on skin IoT sensors.

References

1. M. Muthuppalaniappan and K. Stevenson, "Healthcare Cyber-Attacks and the COVID-19 Pandemic: An Urgent Threat to Global Health," *International Journal for Quality in Health Care*, p. mzaa117, Sep. 2020. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7543534/
2. "Data saves lives: reshaping health and social care with data." [Online]. Available: https://www.gov.uk/government/publications/data-saves-lives-reshaping-health-and-social-care-with-data/data-saves-lives-reshaping-health-and-social-care-with-data

3. R. a. Markets, "Global Patient Monitoring Devices Market Report 2020-2027: Availability of Services Such as Home Healthcare and Nursing Care Increasing the Demand for the Use of Patient Monitoring Devices." [Online]. Available: https://www.prnewswire.com/news-releases/global-patient-monitoring-devices-market-report-2020-2027-availability-of-services-such-as-home-healthcare-and-nursing-care-increasing-the-demand-for-the-use-of-patient-monitoring-devices-301227567.html
4. T. G. Stavropoulos, A. Papastergiou, L. Mpaltadoros, S. Nikolopoulos, and I. Kompatsiaris, "IoT Wearable Sensors and Devices in Elderly Care: A Literature Review," *Sensors*, vol. 20, no. 10, p. 2826, Jan. 2020, number: 10 Publisher: Multidisciplinary Digital Publishing Institute. [Online]. Available: https://www.mdpi.com/1424-8220/20/10/2826
5. "ENISA Threat Landscape 2021." [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021
6. "Cryptocurrencies – Too early or too late? | Wells Fargo Investment Institute." [Online]. Available: https://www.wellsfargo.com/investment-institute/cryptocurrencies-too-early-or-too-late/
7. "Pharmaceutical supply chains." [Online]. Available: https://origintrail.io/case-studies/pharmaceutical-supply-chains
8. "Helium – Introducing The People's Network." [Online]. Available: https://www.helium.com/
9. "Remix - Ethereum IDE." [Online]. Available: https://remix.ethereum.org/optimize=falseruns=200evmVersion=null
10. "IEEE Xplore." [Online]. Available: https://ieeexplore.ieee.org/Xplore/home.jsp
11. C. Taçoğlu, "Trustless." [Online]. Available: https://academy.binance.com/en/glossary/trustless
12. "Home." [Online]. Available: https://ethereum.org
13. "Bring the World to Ethereum | Polygon." [Online]. Available: https://polygon.technology/
14. "Bitcoin: A Peer-to-Peer Electronic Cash System." [Online]. Available: https://bitcoin.org/en/bitcoin-paper
15. "Blockchain.com Explorer | BTC | ETH | BCH." [Online]. Available: https://www.blockchain.com/explorer
16. "Private Ethereum for Enterprise." [Online]. Available: https://ethereum.org
17. "Hyperledger – Open Source Blockchain Technologies." [Online]. Available: https://www.hyperledger.org/
18. "IBM Food Trust - Blockchain for the world's food supply," Sep. 2021. [Online]. Available: https://www.ibm.com/uk-en/blockchain/solutions/food-trust
19. P. Labs, "IPFS is the Distributed Web." [Online]. Available: https://ipfs.io/
20. A. Ali, M. A. Almaiah, F. Hajjej, M. F. Pasha, O. H. Fang, R. Khan, J. Teo, and M. Zakarya, "An Industrial IoT-Based Blockchain-Enabled Secure Searchable Encryption Approach for Healthcare Systems Using Neural Network," *Sensors (Basel, Switzerland)*, vol. 22, no. 2, p. 572, Jan. 2022. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8779424/
21. F. Jamil, S. Ahmad, N. Iqbal, and D.-H. Kim, "Towards a Remote Monitoring of Patient Vital Signs Based on IoT-Based Blockchain Integrity Management Platforms in Smart Hospitals," *Sensors*, vol. 20, no. 8, p. 2195, Jan. 2020, number: 8 Publisher: Multidisciplinary Digital Publishing Institute. [Online]. Available: https://www.mdpi.com/1424-8220/20/8/2195

22. B. Zaabar, O. Cheikhrouhou, F. Jamil, M. Ammi, and M. Abid, "HealthBlock: A secure blockchain-based healthcare data management system," *Computer Networks*, vol. 200, Sep. 2021.
23. M. Barati, W. Buchanan, O. Lo, and O. Rana, "A Privacy-Preserving Platform for Recording COVID-19 Vaccine Passports," Dec. 2021.
24. K. Azbeg, "BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security | Elsevier Enhanced Reader." [Online]. Available: https://reader.elsevier.com/reader/sd/pii/S1110866522000160?
25. D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems," *IEEE Access*, vol. 7, pp. 66 792–66 806, 2019, conference Name: IEEE Access.
26. "Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy | Elsevier Enhanced Reader." [Online]. Available: https://reader.elsevier.com/reader/sd/pii/S0743731522000648?west-1originCreation=20220818172403
27. P. Mukherjee, R. Barik, and C. Pradhan, "A Comprehensive Proposal for Blockchain-Oriented Smart City." [Online]. Available: https://www.springerprofessional.de/en/a-comprehensive-proposal-for-blockchain-oriented-smart-city/18439358
28. D. H. Wang, "IoT based Clinical Sensor Data Management and Transfer using Blockchain Technology," *Journal of ISMAC*, vol. 2, no. 3, pp. 154–159, Jul. 2020. [Online]. Available: https://www.irojournals.com/iroismac/V2/I3/03.pdf
29. "Hyperledger Caliper – Hyperledger Foundation." [Online]. Available: https://www.hyperledger.org/use/caliper
30. "OriginLab - Origin and OriginPro - Data Analysis and Graphing Software." [Online]. Available: https://www.originlab.com/
31. etherscan.io, "TESTNET Ropsten (ETH) Blockchain Explorer." [Online]. Available: http://ropsten.etherscan.io/
32. "Ganache - Truffle Suite." [Online]. Available: https://trufflesuite.com/ganache/
33. "Home." [Online]. Available: https://orbitdb.org/
34. D. R. Varma, M. Murali, and M. V. Krishna, "Design of Wearable Microstrip Patch Antenna for Biomedical Application with a Metamaterial," in *Evolution in Signal Processing and Telecommunication Networks*, ser. Lecture Notes in Electrical Engineering, P. S. R. Chowdary, J. Anguera, S. C. Satapathy, and V. Bhateja, Eds. Singapore: Springer, 2022, pp. 421–434.
35. "IoT Encryption - Application-level Encryption." [Online]. Available: https://www.ubiqsecurity.com/solutions/iot-encryption/
36. "BigchainDB • • The blockchain database." [Online]. Available: https://www.bigchaindb.com/
37. "ThreadDB | Documentation | Textile." [Online]. Available: https://docs.textile.io/threads/
38. "GUN — the database for freedom fighters - Docs v2.0." [Online]. Available: https://gun.eco/
39. polygonscan.com, "Polygon (MATIC) Blockchain Explorer." [Online]. Available: http://polygonscan.com/
40. "Fleek: Build on the New Internet." [Online]. Available: https://fleek.co/
41. "Ethereum API | IPFS API & Gateway | ETH Nodes as a Service." [Online]. Available: https://infura.io

42. C. F. Torres and R. Camino, "Frontrunner Jones and the Raiders of the Dark Forest: An Empirical Study of Frontrunning on the Ethereum Blockchain," p. 18.
43. 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)*, Aug. 2016, pp. 25–30.
44. X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Oct. 2017, pp. 1–5, iSSN: 2166-9589.