Patient Full Control over Secured Medical Records Transfer Framework Based on Blockchain

Meryem Abouali
Department of Electrical Engineering
City University of New York, City College
New York, USA
maboual000@citymail.cuny.edu

Kartikeya Sharma
Department of Electrical Engineering
City University of New York, City College
New York, USA
kartikeyasharma04@gmail.com

Tarek Saadawi
Department of Electrical Engineering
City University of New York, City College
New York, USA
saadawi@ccny.cuny.edu

2022 International Conference on Electrical Engineering and Informatics (ICELTICs) | 978-1-6654-8766-5/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICELTICs56128.2022.9932113

***Abstract*— Covid-19 outbreak represents an exceptional test of the flexibility and the efficiency of patient medical records transfer among healthcare providers which ended up in boundless interruption to the healthcare industry. This public crisis has pushed for an urgent innovation of the patient medical records transference (PMRT) system to meet the needs and provide appropriate patient care. Moreover, the drawback effects of Covid-19 changed the healthcare system forever, more patients are requesting more control, secure, and smoother experience when they want access to their health records. However, the problems stem from the lack of interoperability among the healthcare system and providers and the added burden of cyber-attacks on an already stressed system call for an immediate solution. In this work, we present a secured blockchain framework that ensures patients full ownership over their medical data which can be stored in their private IPFS and later can be shared with an authorized provider. The analysis of the proposed security and privacy aspects shows promising results in providing time savings and resulted in enhanced confidentiality and less disruption in patient-provider interactions.**

Keywords*— Covid-19, Cyber Security, interoperability, patient medical records transfer, blockchain, private IPFS, security, privacy.

I. INTRODUCTION

The Covid-19 outbreak has advanced health IT adoption and has rose the issue of the importance of interoperability and forced the providers and healthcare system to make advance moves toward adopting new norms that would normally take years [1]. Moreover, the pandemic unveils the inadequacy across healthcare administration, medical workflows, and uncoordinated efforts that affect the quality of care and the response to the public health crisis. Healthcare professionals revealed the growing need for interoperability to conduct all the patient healthcare data into a single platform for a better diagnosis of patients' health conditions [2].

Expanding data interoperability will greatly cut down the time it takes to diagnose patients and will eventually help improve patients' health and positively impact the healthcare systems. Moreover, with real-time access to patient medical records, healthcare organizations and providers will be able to leverage advanced analytics to enhance real-time decision-making. As we are slowly getting ahead of the Covid-19 outbreak, it is very essential to guarantee that accessing the right information at the right time becomes vital to patients' health [3]. Hence, the Healthcare system must go through profound changes and loosening of restrictions on health data exchange among providers. If patient medical records transfer were interoperable, during this intimidating time of the pandemic, providers would not have to struggle to make the right diagnosis due to incomplete patient medical records. The Healthcare system is the most vulnerable system due to the massive health data collected daily that makes cyber criminals eager to have hold of it because it is a major source of money which makes confidentiality, security, and privacy of patient's sensitive health data of great concern. A cyber-attack added weight to already worn-out healthcare systems to control the Covid-19 pandemic [4]. The sophisticated attacks impacted the maintenance of day-to-day running health activities. Thus, cyber-attacks can cause major disruption and take advantage of the overwhelmed healthcare systems. Moreover, malware and ransomware continue to exploit the vulnerabilities in the healthcare systems with threats coming from every direction [5].

The remainder of our paper is organized as the following: In section 2, provides the background knowledge of outstanding technologies and approaches. In section 3, contains the motivation behind this work. In section 4, presents the related work. In section 5 describes and discusses the system implementation. In section 6, includes the performance evaluation regarding the developed system. Finally, a conclusion and future work are in section 7.

II. BACKGROUND

This section contains a brief technical background that explains the most outstanding technology concepts used in the proposed framework.

A. Ethereum Blockchain

Blockchain is a technology that is a decentralized and uses distributed ledgers system of record blocks that are linked together. The blockchain serves the need to track transactions [6]. The data on the blockchain is unable to be modified which makes it more appropriate for cybersecurity and healthcare. When a transaction is made between two users in the blockchain, the transaction is recorded and added to a block. Ethereum blockchain has its own currency called Ether, which is used to perform transactions on the Ethereum blockchain [7]. Ethereum also has its own programming language named solidity, which provides the ability to develop smart contracts for the blockchain.

B. Private Interplanetary File System (PIPFS)

It is a decentralized distributed file network that enables secure storage, sharing, and data replication protocol. A private IPFS operates similarly to the public IPFS and can only be accessed by the nodes that have been given access [8]. It provides a content-addressed block storage model to uniquely identify files in a global file system and allows

IPFS to only connect to other peers who have a shared secret key. With private IPFS, each node specifies to which other nodes it will connect. Also, nodes in that network do not respond to communications from nodes outside that network which results in providing complete protection from public monitoring [9].

C. NuCypher

NuCypher is an Ethereum-based network that involved a decentralized applications secret key management system, encryption, and dynamic access control service. Also, it provides a security and privacy layer for decentralized applications built on the public Ethereum blockchain. It is intended to store, share, and manage classified data and focuses on adding an interoperable security layer to various blockchains where developers can grant permission to sensitive information [10].

D. Ethereum Smart Contracts

Smart contracts are programs stored on a blockchain that is self-executed and run-in response to meeting certain predetermined terms of the agreement without the involvement of an intermediary using it to make the transactions traceable, transparent, and irreversible [11]. A smart contract leverages the decentralized blockchain's power to all but eliminates third-party enforcement of legal contracts.

E. Proxy re-encryption (PRE)

A proxy re-encryption scheme is a cryptosystem and a public key cryptographic primitive where a data sender can grant the right to decrypt data to other data receivers and perform its transaction without revealing information about the user. The objective of proxy re-encryption is to delegate decryption rights by removing the reliance on central service. It allows the data to be only visible to the owner [12]. It allows a proxy to convert a ciphertext encrypted under one key into an encryption of the same message under another key.

III. MOTIVATION

In this paper, we focus on a secured patient medical records transference system since it can be improved and scaled to serve the needs of the patients and the providers. The current system suffers from the lack of transparency on patient data, privacy, and security risks associated with transferring data to a centralized medium.

In this paper, we address these issues and propose a realistic solution to overcome these challenges and limitations by developing an interconnected patient health records transfer system. To ensure our readiness to respond to future crisis, there is desperate need to enhance transparency and have a clear definition of who has access to the data, for what purpose, and under what type of authorization and permissions.

Our developed framework breaks down barriers and enhances access to patient medical records easily by integrating systems and deploying them to one comprehensive system to enable the flexibility of transferring data between healthcare entities and simplifying the patient care journey [13]. Moreover, the cyber defense must play an important part in protecting valuable patient data from cyber-attacks. Also, this work presents a framework that would mitigate the stress between the patient and the provider and call for exceptional innovation to impact the care delivery of the patient data and its cost even beyond the Covid-19 pandemic [14].

The developed solution system can serve as a guideline to solve the challenges that face medical records transfer and improve the patient-provider experience [15]. Our developed framework will ensure that patient's medical records obtained from multiple healthcare entities such as providers, health specialists, hospitals, pharmacies, and labs are stored in the patient's private IPFS and shared by the patient among different providers securely by combining three distributed components: Ethereum blockchain, private IPFS, and NuCypher; where providers can receive patient medical records in real-time and make a better and faster diagnosis by having access to complete and accurate health data. In this paper, we took into consideration the protection of patient privacy when designing this interoperable healthcare system by applying strict privacy and security measures and keeping patient health data out of reach of unauthorized users and allowing patients to self-manage their health data and engage in the process of transferring the data.

IV. RELATED WORK

Recently, the healthcare sector has widely embraced the functionality of electronic health records. However, few concerns arise when using a digital system to exchange highly sensitive patients' data. Security and privacy are major concerns because when you make the data available to various healthcare organizations, this data also becomes accessible and targeted by attackers and hackers. Securing the transfer of this data within the healthcare sector becomes more essential. Blockchain is a distinct solution for secure data transfer and provides significant opportunities for the healthcare sector specifically for patient health data but there are still other issues related to Blockchain that require to be solved. In this sector, we will examine number of the approaches that applied Blockchain.

The authors in [16] propose a solution that uses cloud services and access management of EHR. The proposed scheme provides a secure architecture that can be scaled to allow patients and providers to have access anywhere to health data. The use of intercloud to store data supports end-to-end privacy for cloud application and facilitate the transfer of data between patients and providers. Furthermore, the access control process relies on authentication and examination of user rights. However, there is no guarantee that the patient's privacy is preserved because data can still be accessed by an unauthorized user.

The authors in [17] propose a framework that runs on Hyperledger fabric blockchain to provide strong authentication and authorization. The framework takes advantage of the use of the logic in the smart contracts to store the state variables regarding access control to PHR. HIPAA-compliant cloud storage is used to ensure the integrity, confidentiality, and availability of the stored data. With the use of the key management system, the patient would only have to upload the data once and share the records with more

than one provider. However, no evaluation or testing of the performance of the framework was done.

The authors in [18] propose a blockchain architecture for an electronic medical system that improves interoperability, security, and privacy, and provides immediate access to the data. The providers contribute by validating medical data by participating in the mining process. This architecture takes advantage of the smart contract to revoke access and implements a proxy re-encryption service to transfer the encrypted medical data between providers. However, there is no scalability evaluation of the architecture, patients are bound to a specific provider, and they are not given full ownership of their medical data.

The authors in [19] propose a framework based on the Hyperledger blockchain to manage a patient 's medical data. The framework includes access control management, cloud storage, and user interface. The data is encrypted and stored on the cloud while the generated hash is stored on the blockchain. However, this framework does not suggest a solution to the interoperability issue.

The authors in [20] propose a Hyperledger fabric blockchain based on electronic health records sharing system among patients and providers. The users of the network are registered in the system. Performance evaluation of the metrics is conducted. However, the system does not diverge from the centralized approach as the administrator has full control over the system functionality. Also, the latency is not evaluated when the number of users increases.

Our developed framework is unique from the previous approaches because it ensures data security with further steps. Although the existing solutions have used blockchain technology to share patient medical records, our approach offers extra novel steps. Our solution adds extra verification and authentication step for the provider to ensure no unauthorized provider has access to the patient medical records.

The developed framework stores patient data in the patient private IPFS and the data is accessible through managed access control policy mechanism. Therefore, preserving the privacy, integrity, and security of the patient's sensitive data. To obtain accurate patient data, the provider must request access to it. If the provider fails to provide the matching information access is revoked.

V. PROPOSED MODEL AND ITS IMPLEMENTATION

System Architecture This section describes all the aspects and details regarding the implementation of the developed system. The section focuses on highlighting the essential elements of system architecture and design.

The system model has the following entities:

- Healthcare entities- are responsible for sending, encrypting, and uploading the patient medical records to his private IPFS.
- The patient- is the data owner. The patient node contains identifiers such as Ethereum account address, providers list, and mapping of which providers are allowed to have access to the patient medical data. The patient has the responsibility to initiate the transaction to verify the provider and create an access policy on NuCypher to grant access to the provider.
- Provider- is the data receiver. The provider node contains identifiers such as Ethereum address, specialization, and board Certificate ID number. After the provider is added to the patient's access list and awarded access to the patient medical records, he will have the power to download and view the patient medical records. Figure 1 illustrates the complete architecture for the proposed framework.
- Ursula is the proxy in PRE. They are the nodes on the NuCypher network that stand ready to re-encrypt data, and they enforce the access policy created by the patient.

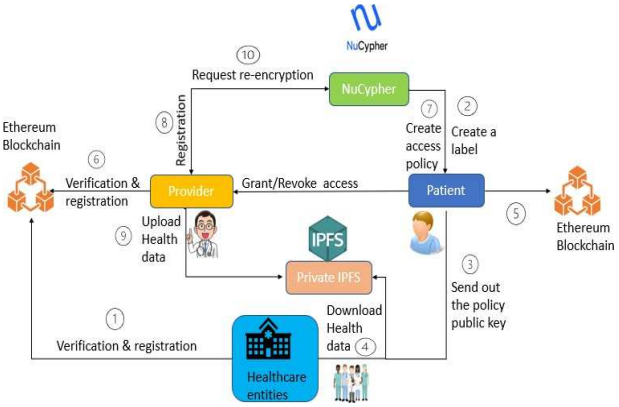

Fig. 1. The developed framework Architecture

The privacy and security of the patient sensitive data are crucial which pushed us to come out with a novel approach where every patient is entitled to store his medical records on his private IPFS and can get hold of all his prior medical records such as blood test results, doctor reports, imagery, can now prepare the medical records, encrypt the data using the symmetric key, and upload the encrypted data with the encrypted symmetric key to the patient's private IPFS, the corresponding hash value of the record is generated and stored on the blockchain. Then the patient will be able to transfer his medical record directly to the intended provider without the need for any intermediaries. Our framework enables patients to have complete control and engagement between patient-provider. Thus, it allows patients to participate, take an active engagement in their own care, let patient-provider work on delivering effective patient care, smooth out the communication channels, and improve overall patient satisfaction. Thus, the patient health data can be stored in his private IPFS and can travel with the patient anywhere he moves and change his care system or transfer to a nursing home. When the provider wants to view and access the data, the patient must create an access policy on NuCypher to grant access to the provider. Then, the provider inputs the hash of the record and downloads the encrypted data.

Now, the provider can decrypt the data with the same key generated during the encryption phase after requesting the re-encryption from the NuCypher Ursula and using his private key. This process allows health data to be accessed quickly by the authorized providers and revoked for those who are unauthorized. Moreover, it ensures that patient data is kept accurate and minimizes the amount of time spent looking for

the appropriate paperwork during patient appointments and creates better health care outcomes.

Finally, our framework is designed to coordinate care among providers, improve patients' experience to receive a high quality of care, and lower healthcare costs for patients and healthcare organizations. The developed framework aims to enforce the patient's ownership of their health data and allow them to have complete control over it.

The distributed nature of the framework components guarantees the security, integrity, and privacy of the patient health data. The access control management system reassures the patients that their data is secured. The framework system can be broken down into four main layers they are NuCypher layer, the Blockchain layer, the Smart contract layer, and the data layer. These layers will be explained in terms of their role in the system according to figure 2.

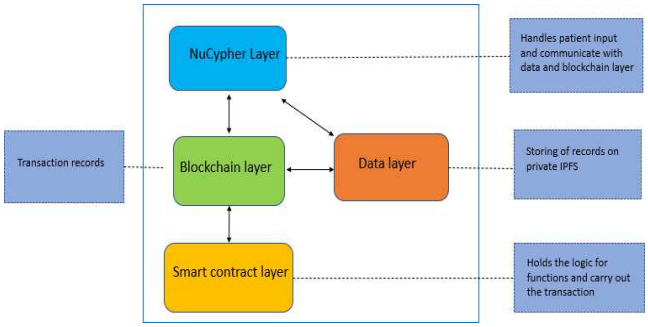

Fig. 2. System Design

Our developed framework consists of four layers:

A. *Smart contract layer*

The Smart contract is initiated by the patient and deployed onto the blockchain as part of the smart contract layer. The main functionality is to conduct transactions between the patient, the healthcare entities, and the provider on the blockchain for the verification and authentication process. The logic behind the smart contracts is made to define the fine access control of the users and make sure no unauthorized access occurs.

Each patient has the power to grant or revoke a provider's access to create an account on the blockchain which depends on a verification smart contract. By giving access, the provider can retrieve hashes of a patient's data. The store and get hash functions to serve the purpose of retrieving data from off-chain private storage IPFS in the data layer.

B. *Blockchain layer*

The blockchain layer holds the deployed smart contract to verify and authenticate the users. Each transaction performed between the users is recorded in the blockchain layer. Furthermore, it uses to store the hash value of the data that is on private IPFS.

C. *Data layer*

The private Interplanetary File System (PIPFS) is used as off-chain storage. When encrypted patient data is uploaded to the patient private IPFS, the cryptographic hash is calculated of the uploaded file, sent as a transaction, and stored in the blockchain. The provider can use this hash to retrieve the health data.

D. *NuCypher layer*

The NuCypher is built on top of the blockchain. The purpose of it is to add more security to the framework. It has two main services: dynamic access control by conditionally granting or revoking access to the sensitive data by the provider, and secrets management which manages the secret encryption and decryption keys [21].

Lastly, the NuCypher layer manages the communication between the Data layer and the encryption and decryption process of the health data uploading and downloading from private IPFS. Below is the flow diagram to provide a sequence diagram. Figure 3 shows the flow of the process of transferring patient health data to a new provider after having it encrypted and uploaded to the patient private IPFS.

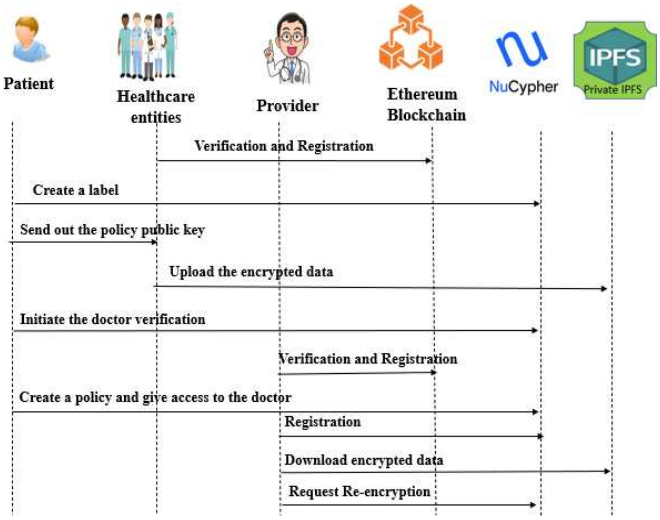

Fig. 3. Flow diagram of the proposed framework

VI. DISCUSSION

This section aims to provide an evaluation of different security aspects of the developed system and its functionality. Then, it describes the possible challenges and limitations the developed design faces.

A. *Analysis of the security and privacy aspects*

The developed framework enables patients to transfer securely their medical records to their providers. This is because all the components of our approach are decentralized technologies. In addition, the use of the identity authentication mechanism to keep the parties from acting maliciously and the use of proxy re-encryption to ensure no unauthorized provider permits access to the patient's sensitive data. The developed framework is based on the use of NuCypher which serves as secret keys management with a strict proxy re-encryption algorithm that ensures the confidentiality of the involving parties. Moreover, it serves as a dynamic access control where the patient must create an access policy for the designated provider. Furthermore, medical records are stored in a distributed and decentralized private IPFS which removes the need to trust any centralized third party to store the data and ensures security against cyber-attacks like a DDOS attack. Using Ethereum blockchain for

our developed framework makes transactions traceable and allows for storing the hash value that is generated from storing the encrypted data in the private IPFS. the Ethereum smart contract gives the ability to verify and authenticate the parties. Our approach ensures that one Ethereum account for each party which eliminates the case of Sybil attacks or impersonation attacks.

Our developed framework is protected from insider or outsider attackers. We integrated multiple levels of protection to ensure the security of transferring the medical records [23]. Therefore, it prevents the system from downtime attacks. Furthermore, we assessed the smart contracts against vulnerabilities and fixed them to prevent attacks that aim at stealing or tampering with the assets. The developed framework preserves the privacy of all parties and the anonymity of their identities. No physical identity or personal information of the parties is revealed during the

B. Data security

Data security includes the confidentiality, integrity, and availability of transferred data. The patient medical records are encrypted using an efficient algorithm and uploaded to the private IPFS which will ensure the confidentiality of the transferred data. The integrity is guaranteed.

C. Data Privacy

The data privacy of the patient medical records is safeguarded. In a data transfer system, privacy includes the content of the medical records which will not be leaked because only the authorized provider whose attribute set satisfies the access policy can gain access to the medical records. The identity of the patient and the provider will not be exposed to intruders. The access control permission specifies who has access to what type of medical records.

D. Data Integrity

The patient medical records are encrypted and stored in a decentralized private IPFS storage. The generated corresponding hash value is kept in the blockchain where the blocks constitute an immutable distributed ledger. It is difficult to alter the ledger because any modification will result in changing the hash value. In addition, data is stored in the private IPFS after performing a specific cryptographic encryption technique.

E. Patient-Centric and Fine -Grained Access

In our system, the patient deploys the smart contract to verify and authenticate the provider, creates a label and access policy to grant access to the provider using NuCypher Software. He uses a proxy re-encryption mechanism to re-encrypt his private key and the provider public key, hands the public policy key to the healthcare entities to encrypt his medical records and can revoke the permission of the provider to access his records. the patient is entitled to deny access to an unauthorized provider at any time

F. System Comparison

Our developed system, patients' full control over secured medical records transfer based on blockchain differs from our previous work [22], [23] in the concept and the choice of storage of patient data. The developed system in this paper makes use of a private decentralized database file storage system called private IPFS. The advantage of this over our previous work is that the patient will have full control and be in charge managing of his medical records. The patient medical records will be uploaded to his private IPFS immediately after each medical doctor visit. The patient will be able to store his medical records in his private IPFS and in the future will be able to transfer them to any new provider upon request.

Despite the above-mentioned features, our developed framework is limited by performance constraints such as latency. The Ethereum blockchain uses proof of work that required a massive amount of computational power and electricity and generates electronic waste as well. By shifting to proof of stake and replacing miners with validators we can lower transaction costs and supply, improve congestion, less computing power, and make the system faster and more user-friendly [24].

VII. CONCLUSION

We developed a blockchain framework that can guarantee a smooth transfer of the patient medical records and preserve the privacy, integrity, and security of the medical records.

TABLE I. COMPARISON OF OUR SYSTEM WITH OTHER WORKS

Feature	[16]	[17]	[18]	[19]	[22]	Our System
Flexibility	Y	Y	N	N	Y	Y
Availability	N	Y	Y	Y	Y	Y
Decentralize Access	N	Y	Y	Y	Y	Y
Integrity	N	Y	N	N	Y	Y
Data Privacy	N	N	N	Y	Y	Y
Private Decentralise Stroge	N	N	N	N	N	Y
Identity Management and Access Policy	Y	N	Y	Y	Y	Y
Patient-Centric	N	N	N	N	N	Y

The framework is fully developed and patient-powered and the system allowed the authorized provider to access the patient medical records conveniently. Using smart contracts and NuCypher software, patients can grant or revoke access to their medical records at any time. The patient has full ownership over his private IPFS where his encrypted medical records are stored. There is a need to shift the data ownership and its access control to the patient over his medical records by deciding on how it will be used and who will have access to it. In the future, the plan is to deploy the Ethereum blockchain that uses proof of stake to decrease the latency and evaluate out the blockchain scalability and efficiency i n t he r eal world. Also, assessed performance metrics and their effectiveness

ACKNOWLEDGMENT

NSF Grant supports this work, INRC Testbed: COSMOS Interconnecting Continents, and NSF Grant; Japan USA Networking Opportunities JUNO2.

REFERENCES

[1] Aaron Warnick" Public health vulnerable to cyberattacks during COVID-19 outbreak: US alert issued" by The Nation's Health October 2021. https://www.thenationshealth.org/content/51/8/1.2

[2] JBraquehais, M. D., Vargas-Ca´ceres, S., Go´mez-Dura´n, E., Nieva, G., Valero, S., Casas, M., Bruguera, E. (2020). The impact of the COVID-19 pandemic on the mental health of healthcare professionals. QJM: An International Journal of Medicine. doi:10.1093/qjmed/hcaa207

[3] Blumenthal, D., Fowler, E. J., Abrams, M., Collins, S. R. (2020). Covid-19 — Implications for the Health Care System. New England Journal of Medicine, 383(15), 1483–1488. doi:10.1056/nejmsb2021088

[4] Muthuppalaniappan M, Stevenson K. Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health. Int J Qual Health Care. 2021 Feb 20;33(1):mzaa117. doi: 10.1093/intqhc/mzaa117. PMID: 33351134; PMCID: PMC7543534.

[5] Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers Security, 105, 102248. doi:10.1016/j.cose.2021.102248

[6] Umair Khan, Zhang Yong and Azhar Khan, "A Blockchain Ethereum Technology -Enabled Digital Content: Development of Trading and Sharing Data," IEEE Access, 2020.

[7] W. Li and M. He, "Comparative Analysis of Bitcoin, Ethereum, and Libra," 2020 IEEE 11th International Conference on Software Engineering and Service Science (ICSESS), 2020, pp. 545-550, doi: 10.1109/ICSESS49938.2020.9237710.

[8] Sander van Laar "Deploy a private IPFS network in 5 steps" Jan 11, 2019. https://medium.com/@svanlaar/deploy-a-private-ipfs-network-on-ubuntu-in-5-steps-5aad95f7261b

[9] Kang P, Yang W, Zheng J. Blockchain Private File Storage-Sharing Method Based on IPFS. Sensors (Basel). 2022 Jul 7;22(14):5100. doi: 10.3390/s22145100. PMID: 35890780; PMCID: PMC9323017.

[10] Egorov, M., Wilkison, M., and Nunez, D., "NuCypher KMS: Decentralized key management system," URL http://arxiv.org/abs/1707.06140

[11] Techbrij, "Hello World Smart Contract inSolidity," 2019, [online] Available: https://techbrij.com/hello-world-smart-contract-solidityethereum-dapp.

[12] Ateniese, Giuseppe, et al. "Improved proxy re-encryption schemes with applications to secure distributed storage." ACM Transactions on Information and System Security (TISSEC) 9.1 (2006): 1-30.

[13] Kumar, Randhir, and Rakesh Tripathi. "A Secure and Distributed Framework for sharing COVID-19 patient Reports using Consortium Blockchain and IPFS." 2020 Sixth International Conference on Parallel, Distributed and Grid Computing (PDGC). IEEE, 2020.

[14] I. Ezine and L. Benhlima, "Technology against COVID-19 A Blockchain-based framework for Data Quality," 2020 6th IEEE Congress on Information Science and Technology (CiSt), 2020, pp. 84-89, doi: 10.1109/CiSt49399.2021.9357200.

[15] O. Ajayi, M. Abouali and T. Saadawi, "Secure Architecture for InterHealthcare Electronic Health Records Exchange," 2020 IEEE International IoT, Electronics, and Mechatronics Conference (IEMTRONICS), 2020, pp. 1-6, doi: 10.1109/IEMTRONICS51293.2020.9216336.

[16] Matos, David Pardal, Miguel Ada˜o, Pedro Silva, Anto´nio Correia, Miguel. (2018). Securing Electronic Health Records in the Cloud. 1-6. 10.1145/3195258.3195259.

[17] Dubovitskaya A, Baig F, Xu Z, Shukla R, Zambani PS, Swaminathan A, Jahangir MM, Chowdhry K, Lachhani R, Idnani N, Schumacher M, Aberer K, Stoller SD, Ryu S, Wang F ACTION-EHR: Patient-Centric Blockchain-Based Electronic Health Record Data Management for Cancer Care. J Med Internet Res 2020;22(8):e13598.doi: 10.2196/13598

[18] Daraghmi et al., 2019.E. Daraghmi, Y. Daraghmi, S. Yuan.Medchain: a design of a blockchain-based system for medical records access and permissions management.IEEE Access, 7 (2019), pp. 164595-164613

[19] Rouhani et al., 2019.Rouhani, S., Butterworth, L., Simmons, A.D., Humphery, D.G., Deters, R., 2019. Medichaintm: a secure decentralized medical data asset management system. CoRR abs/1901.10645. http://arxiv.org/abs/1901.10645, arXiv:1901.10645.

[20] Tanwar et al., 2020.S. Tanwar, K. Parekh, R. Evans.Blockchain-based electronic healthcare record system for healthcare 4.0 applications.J. Inf. Secure. Appl., 50 (2020).

[21] O. Ajayi and T. Saadawi, "Blockchain-Based Architecture for Secured Cyber-Attack Feature Exchange," 2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), New York, NY, USA, 2020, pp. 100-107, DOI: 10.1109/CSCloudEdgeCom49738.2020.00025.

[22] Meryem Abouali, Kartikeya Sharma, Oluwaseyi Ajayi, Tarek Saadawi, "Blockchain Framework for Secured On-Demand Patient Health Records Sharing" 2021 IEEE 12th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON 2021) December 1-4, 2021, New York, USA.

[23] Abouali, Meryem, et al. "Performance Evaluation of Secured Blockchain-Based Patient Health Records Sharing Framework." 2022 IEEE International IoT, Electronics and Mechatronics Conference (IEMTRONICS). IEEE, 2022.

[24] Miranda Marquit "Proof of Work vs. Proof of Stake: Ethereum's Recent Price Surge Shows Why the Difference Matters" July 29, 2022.URL https://time.com/nextadvisor/investing/cryptocurrency/proof-of-work-vs- proof-of-stake/