2020 16th International Conference on Distributed Computing in Sensor Systems (DCOSS)

Health Information Exchange with Blockchain amid Covid-19-like Pandemics

Klitos Christodoulou*, Panayiotis Christodoulou†, Zinon Zinonos†,
Elias G. Carayannis§, and Savvas A. Chatzichristofis†

*Institute For the Future (IFF), University of Nicosia, Cyprus
†Department of Computer Science, Intelligent Systems Lab, Neapolis University Pafos, Cyprus
‡George Washington University, Washington, DC, USA

***Abstract*—The COVID-19 pandemic is stress-testing existing health information exchange systems. There exists an increasing demand for sharing patient information and efficiently responding to patient medial data requests. Current health information technologies lack *data fluidity*, especially for remotely sharing medical data beyond their protected, local data storage. This paper presents a blockchain-based data-sharing framework that leverages the properties of immutability and decentralization to ensure a secure, user-centric approach for accessing and controlling access to sensitive medical data. The proposed framework builds its foundations on a peer-to-peer network fueled by the distributed InterPlanetary File System combined with on-chain tagging, and on the use of cryptographic generation techniques for enabling a secure way of sharing medical data. The flow of information is orchestrated by a smart-contract deployed on a blockchain-based protocol to ensure traceability and data integrity. The effectiveness of the framework is demonstrated with the implementation of the framework over a pilot study.**

***Index Terms*—Blockchain, Electronic Health Records, Medical Informatics**

I. Introduction

The evolution of modern societies has been driven by digital transformation, a paradigm shift that is based on the constant penetration of the Internet and the ability to generate and process large volumes of digital data from many different micro-devices. The foundations of this transformation are affected by the recent technological evolution with digitalization, the Internet of Things (IoT), Big Data, and Artificial Intelligence (AI), that are currently leading global social changes in the way humans interact and do business [1]. This ongoing digital evolution evolves artificially over the Internet layer and is build on complex interrelationships inferred from interpreting digital data; with the use of computational agents and AI. Furthermore, the technological changes over the last century enabled deterministic shifts grounded on the evolution of the third generation of Internet services (i.e., Web 3.0) amplified with new social trends from the usage of social media.

This new generation of society empowers a more human-centering mode of operation where individuals contribute to public decision-making in a way that is more decentralized, interconnected, and driven by digital data. We have already experienced pubic Democratic movements fueled by social media, alternative forms of finance (such as decentralized finance, with the use of blockchain technology [2]), and more transparent governance models. In reality, and although digital transformation has gone a long way, many organizations have faced several challenges into fully adopting a fully end-to-end digital-oriented culture and working mode.

As societies have been gradually moving into understanding the disruptive implications and challenges digital transformation is imposing on societies, human rights, and the economy, on March 11, 2020, the World Health Organization (WHO) declared that an outbreak of a virus with the code name COVID-19 has taken pandemic dimensions[1]. Due to the scale and severity of the virus WHO has been guiding governments from around the globe to take aggressive measures as a response to limit the spread of the virus [3]. As the number of infected people rises[2] governments responded by implementing a series of measures to contain COVID-19 and mitigate its impact. The measures included restrictions on social life, education, work, mobility freedom (for people, goods, and services), and border restrictions. According to the Organisation for Economic Co-operation and Development (OECD) interim report, March 2020 [4] it is with no doubt that the coronavirus outbreak will have long-term impacts on the global economy; with a reduction on the global GDP growth leading many economies into recession.

Given the circumstances with the pandemic and the upcoming economic implications, many organizations are responding to the crisis with fast-moving digital-oriented continuity plans based on the latest technological advancements. It seems that organizations look into moving towards a virtual working environment and culture. It is evident that COVID-19 is acting as a booster to digital transformation disrupting current business models.

The uncertainty brought by the pandemic to the public has also led to many incidents of disinformation concerning the

*Corresponding author: christodoulou.kl@unic.ac.cy

[1]https://www.who.int/emergencies/diseases/novel-coronavirus-2019/events-as-they-happen

[2]As of 28 Apr. 2020, the John Hopkins Coronavirus Resource Center reports more than 3 M people infected from over 185 counties/regions and more than 200 K deceased.

DOI 10.1109/DCOSS49796.2020.00071

outbreak as an attempt to undermine people's trust to the health care system and governments in general. In such a crisis it is critical to prevent misinformation and miscommunication of medical data. It is therefore essential to communicate accurate, reliable, and trustworthy medical data according to privacy and data protection standards [4]. The ongoing pandemic is adding extra pressure to existing health information exchange (HIE) systems forcing medical providers worldwide to ensure that electronic health records (EHRs) are shared effectively and securely among remote care locations.

Motivation. Current HIE systems lack a homogeneous data model for storing and exchanging medical records where access to the data remains to the control of the patient. We anticipate that the demand for user-centric HIE systems will increase. In addition, the type and scope of such systems are expected to adapt to the shifting requirements for patient care under pandemic outbreaks. Further to the above, we note that patients should be able to authorize access to partial views of the data with the use of micro-transactions on the same EHR.

Contribution. As a response to the aforementioned challenges this paper presents a blockchain-based, decentralized, privacy-preserving framework for health information exchange. At the same time, the framework provides a secure way for patients to control their medical data, authorize access to their medical records, and preserve personal autonomy.

The remainder of the paper is structured as follows. Section II reviews related work. The design and implementation details of the proposed framework are presented in Section III. The effectiveness of the approach is demonstrated in Section IV by discussing a medical journey implemented for facilitating secure information exchange of medical data. Section V concludes the paper, and discusses potential opportunities for future work.

II. Related Work

According to the European Data Protection Supervisor, medical records are considered sensitive since are referring to personal data that concern the health status of an individual [5]. Medical data are subject to intensely severe procedures for sharing and can only be handled by health specialists who are bounded by the commitment of medical confidentiality [5]. Under such regulation, research on electronic medical health systems is exploring techniques for increasing the level of compliance with data protection legislation. Recent literature is mainly concerned with the following challenges. Firstly, to explore techniques for securing medical records against unauthorized users, secondly to ensure the trustworthiness of the information being shared, and lastly to enhance the degree of patients' control over personal data.

The latest technological advancements with blockchain technology are pursued as an alternative way for safeguarding and exchanging data in a way that is secured and transparent (e.g., [6], [7]). This paper presents a blockchain-based data-sharing framework that leverages the properties of immutability and decentralization to ensure a secure, user-centric approach for accessing and controlling sensitive data from medical records. We suggest that blockchain-enabled HIE systems hold the potential for a paradigm shift for both patients and medical providers that is grounded on creating transparent audit trails of the information being shared.

Azaria et al. [8] proposes MedRec, a decentralized record management system to handle electronic medical records using blockchain technology. MedRec provides capabilities for managing authentication, confidentiality, accountability, and data sharing. The system provides easy access to patients' medical information through a blockchain network that consists of several medical stakeholders that are securing the network utilizing a Proof-of-Work consensus scheme. MedRec [8] is an early attempt on building a private blockchain network for handling medical records. This paper proposes a generic framework that is governed by a smart contract which can be deployed over any private or public blockchain protocol that runs the Ethereum Virtual Machine (EVM). Our proposed framework utilizes a distributed data storage that builds on InterPlanetary File System (IPFS) without the prerequisite of accessing any proprietary databases. In addition, the framework proposes the use of an IPFS-cluster[3] for ensuring data redundancy by pinning content over an IPFS swarm or a consortium of IPFS nodes.

Alternatively, the authors in [9] adopted the use of a permissioned blockchain for providing data sharing from the medical perspective. In contrast to MedRec, the framework presented in [9] does not require any transaction fees and utilizes a centralized cloud-based storing service to ensure the availability of data. Similarly to our work, data are hashed and signed with the secret key of the patient before sending it to the user that requests access to the medical data. In contrast to our proposal, data sharing in [9] is controlled by the cloud service (an intermediary service provider) whereas our approach empowers disintermediation by authoring patients with the capability of controlling access to their medical information. On another note, the work presented by [10] is mostly focused on enhancing security considerations when sharing sensitive data with the deployment of a discrete wavelet transform and a genetic algorithm technique [10].

Several approaches have been proposed in the literature for real-time patients' health monitoring [11] [12]. For example, authors in [12], propose LAURA system, which provides patient localization, tracking, and monitoring services within nursing institutes through a wireless sensor network. In [11], authors propose a smart hospital system that is able to collect, in real-time, both environmental conditions and patients' physiological parameters via an ultra-low-power hybrid sensing network (HSN) composed of 6LoWPAN nodes integrating UHF RFID functionalities. The majority of these approaches focuses on the data acquisition and transmission components of an IoT system. Furthermore, in [13] the authors propose cloudlet assisted IoT enabled e-Health framework which aims at facilitating real-time data access using cloudlets.

[3]https://cluster.ipfs.io/

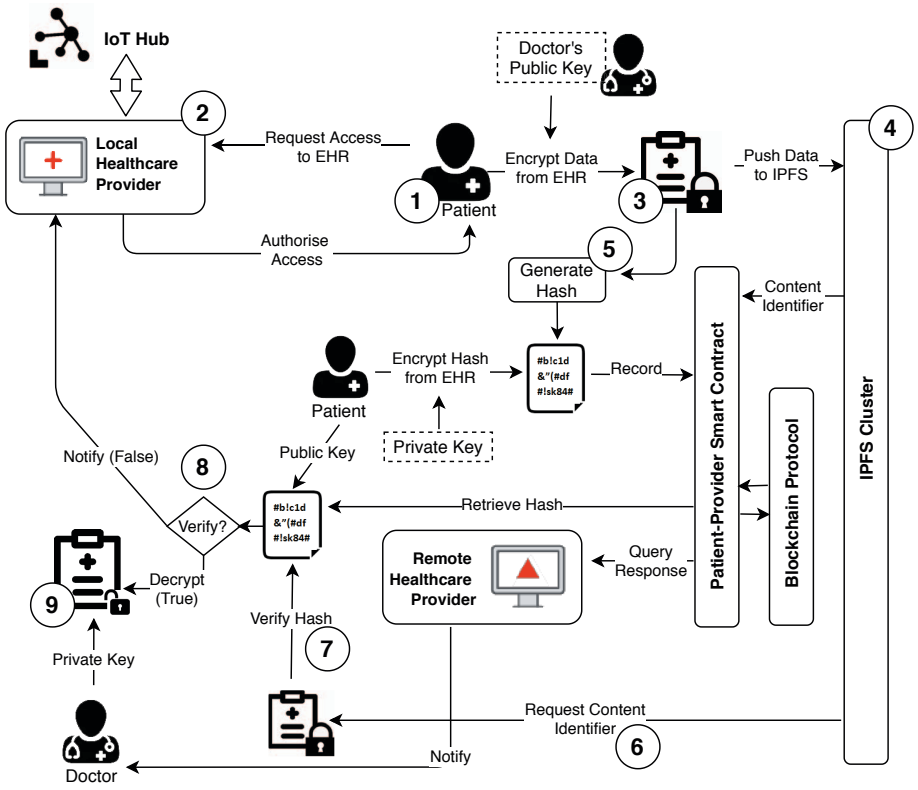

Fig. 1. System architecture of the proposed patient-driven medical data exchange framework.

Overall, our proposed framework overcomes the interoperability barrier of different hospital systems by proposing a generic framework for HIE. The framework provides immutable data exchange without the need for accessing any central storage services. Self-distribution of the information from a patient's side to a requesting party is enabled by removing any dependencies to an external healthcare provider. The generic cryptographic framework utilized i.e., PGP [14] enables communities of medial trust to be built where patients are first-class citizens, retaining full control of their medical information. Furthermore, traceability of the medical information exchanged is made possible with the implementation of a smart-contract over a blockchain protocol. Lastly, the framework ensures the handling of any type or size of EHR or medical files (e.g., radiology images).

III. System Architecture

This section describes a prototype design and implementation of the proposed framework to provide a secure way for patients to control their medical data, authorize access to their medical records, at the same time preserving personal autonomy. An abstract view of the framework is depicted in Fig. 1. The main focus of this paper is health information exchange where audit trails of the information flow are recorded with the use of a smart contract on an Ethereum blockchain [15]. We note that the implementation of the smart contract is generic in the sense that it can be deployed on any blockchain protocol that runs the EVM. The proposed framework enables the issuance of micro-transactions over a blockchain protocol for requesting partial or full access to encrypted medical information.

In more detail, the data exchange relationships between patients and healthcare providers are logged on a blockchain data structure, leveraging the state of the deployed smart contract. Thus, creating transparent and immutable audit trails of the information flow. The integrity of the exchanged data is ensured with the use of cryptographic hashes that are used to sign the encrypted medical information. The outcome of the hashing algorithm is then recorded on the blockchain with the use of a smart contract (denoted by $MedSC$, shown in Algo. 1). Medical data from EHR are securely encrypted using an open-source implementation of the PGP encryption scheme. The proposed framework uses asymmetric cryptography to encrypt medical data with the public key of the recipient. Encryption takes place at the client-side before the data re pushed for storage on a peer-to-peer (p2p) file storage maintained by an IPFS cluster.

Access to the encrypted medical data is orchestrated by a smart contract that maintains pointers to the IPFS content identifiers. Furthermore, the state of the smart contract is safe-guarding permissions to accessing the information by implementing logic for access control. The system handles

identity information for each participant with the use of public-key cryptography. To preserve privacy, identities are pseudonymous, however, the smart contract can link Ethereum public addresses with users‘ social security numbers or any other widely accepted form of identification.

Subsequent sections present design considerations and implementation details for each component of the framework.

A. Blockchain Functionality

Initially, the idea of a blockchain-based protocol was proposed as a system for facilitating the exchange of digital assets [16] wrapped as transactions that are recorded on an immutable, tamper-proof data structure (i.e., the ledger) and shared over a p2p network of participants. Following this idea, other protocols e.g., Ethereum evolved the idea to securing state machines and the execution of algorithmic logic (via Smart Contracts) over a decentralized p2p network [15]. The state of the data is preserved and agreed with the use of a consensus algorithm [17].

In this paper, we leverage the use of a smart contract that can be deployed in any blockchain-based protocol that runs the EVM, to enable tamper-evident logs of health information exchange. As shown in Section III-D the smart contract enables patient-driven medical data exchange accessed only according to the patient consent. More specifically, blockchain transactions broadcast by our framework wrap cryptographically signed metadata concerning the ownership of the data, access privileges, and data integrity. Overall, the ledger is functioning as a transparent, time-stamped trail of all medical information exchange acting as a historic log of transactions that are recorded on the blockchain‘s state. The actual medical data are not stored on the blockchain blocks but are maintained by an IPFS cluster upon the request of the user. As defined in subsequent sections the smart contract records pointers to the encrypted content identifiers of the data that are held on the IPFS cluster.

B. Key Management

To facilitate interactions with the framework, users (U) (either patients (P) or Medical Doctors (MD)) are assigned two pairs of keys:

1) an Ethereum Public/ Private Key pair $(Pub_U, Priv_U)$ generated using the secp256k1 Elliptic Curve Digital Signature Algorithm [18]. This pair is used as an authentication mechanism with the Ethereum blockchain, and for interacting with the smart contract; and
2) a PGP key pair for encrypting or decrypting the medical data $(PGPPub_U, PGPPriv_U)$ generated using the `Ed25519` standard[4] along with a strong passphrase to protect the private key,

where U is either P or MP. For the implementation of this component, two open-source JavaScript libraries are utilized. For the Ethereum key pair, the framework uses the *Web3.js*[5]

[4]http://ed25519.cr.yp.to/

[5]https://github.com/ethereum/web3.js/

Algorithm 1 Pseudocode for $MedSC$ smart contract

```
1: contract EncryptFilesdApp
2:   uint public size;
3:
4:   struct encryptFiles {
5:       address recAddr;
6:       string pgpPubKey;
7:       string ipfsURL;
8:       string hashEncFile;
9:   }
10:
11:  encryptFiles[] encrRecs;
12:
13:  function addDataIPFS(address _recAddr)
14:                  string memory _pgpPubKey,
15:                  string memory _ipfsURL,
16:                  string memory _hashEncFile)
17:
18:      size ← encrRecs.length++;
19:      encrRecs[encrRecs.length-1].recAddr ←_recAddr;
20:      encrRecs[encrRecs.length-1].pgpPubKey ←_pgpPubKey;
21:      encrRecs[encrRecs.length-1].ipfsURL ←_ipfsURL;
22:      encrRecs[encrRecs.length-1].hashEncFile ←_hashEncFile;
23:      return encryptRecs.length;
24:  end function
25:
26:  function searchFile()
27:      size ← encrRecs.length++;
28:      for (uint i = 0; i <= size; i++)
29:          if (encrRecs[i].recAddr == msg.sender) then
30:              index ← i
31:          end if
32:      end for
33:      return recAddr, pgpPubKey, ipfsURL, hashEncFile
34:  end function
35: contract end
```

library to generate externally owned accounts for each P and MD respectively. Similarly, it makes use of the *OpenPGP.js*[6] library to encrypt and decrypt the medical data exchanged between patients and medical doctors. Listing 1 shows a code snippet for generating the PGP keys for the patient, similarly for the medical doctor.

```
const openpgp = require('openpgp')
let patient = {privateKey:'', publicKey:''};

let patientConf = { userIds: [{username:'user01',
     email:'ck@mail.com'}],
 curve: "ed25519", passphrase: 'patient-secret'};
...
let patientKeys = openpgp.generateKey(patientConf)
        .then(function(key){
 patient.privateKey = key.privateKeyArmored;
 patient.publicKey = key.publicKeyArmored;
});
```

Listing 1. Generation of PGP keys for the patient.

C. Encrypt, Decrypt & Signing Scheme

Encrypt & Sign: To ensure confidentiality of the medical data exchange the framework uses asymmetric encryption to encrypt a file or any other object that includes medical data (e.g., JSON object) with the public key of the intended recipient e.g., MD. This is important to ensure that only the requestor of the information can decrypt the medical data when

[6]https://openpgpjs.org/

retrieved from IPFS. In doing so, the data are encrypted with the use of the PGP public key, $PGPPub_{MD}$, and pushed to IPFS. The content identifier that is returned by IPFS is encrypted with the recipients' public key Pub_{MD} and pushed to the smart contract. To prove that the medical data have not been tampered by an intruder, the framework hashes the encrypted medical data (using `keccak256`), and then signs the output message hash with the patient's private key (i.e., $Priv_P$). It then pushes this information to $MedSC$ that keeps track of all the metadata.

Validate & Decrypt: The intended recipient e.g., MD queries the metadata from $MedSC$. On reception, the intended recipient uses its private key (i.e., $Priv_{MD}$) to decrypt the IPFS content identifier and locally retrieve the encrypted file from IPFS. The recipient also retrieves the encrypted hash value of the file sent by the patient from the metadata and uses the Pub_P to decrypt it. The recipient then uses the same hashing algorithm to produce a message digest for that encrypted file and compare it with the one from the metadata (previously decrypted). If the two hash values are the same, then validation is successful. Only then the recipient can securely proceed with the decryption of the file, with the use of the PGP private key, $PGPPriv_{MD}$.

D. Smart Contract Layer

For each *patient-medical* doctor relationship, and to ensure that medical data is always in the control of the patient (i.e., data owner) a separate $MedSC$ smart contract is deployed on the blockchain (a snipped is shown in Algo. 1). The owner of the smart contract is the data owner which has the permission to write certain metadata on the blockchain and grant access to the medical data, thus complying with GDPR-regulations.

More specifically, the contract defines a set of data pointers and associated permissions to the medical data. At this layer access to the medical data file is represented as a reference to an IPFS content identifier. Indexing to the data is based on the public key of the intended recipient that is recorded on the blockchain. A call to the *addDataIPFS()* function performs the operation of recording the metadata on the blockchain. Similarly, a call to the *searchFile()* function retrieves the metadata that refers to a particular medical data object.

E. IoT Data Collection System

To support the collection of medical data from the patients, an IoT-based data collection system is used. The medical data collection system is composed of commercially available sensor devices able to collect information like blood pressure, airflow, pulse oximeter, heart rate, and body temperature. The data are collected by a gateway that is able to support interoperability between the different devices. The communication between the IoT devices and the back-end database is done by using both synchronous and asynchronous communication methods. Upon data are collected by the gateway, we use Web Services to simply deliver the data to interested parties.

F. Medical Data Storage

In essence, the blockchain maintains metadata for each encrypted medical data where the smart contract is safeguarding the information. In addition, the smart contract holds access rights to the data, hashes to verify digital signatures and encrypted versions of the pointers to the medical information. Storage of the actual medical data (from EHR to CT or MRI images) is maintained over an IPFS cluster that is used to pin data from multiple IPFS daemons (private or public) and provide a mechanism for data replication which is distributed among multiple peers. The implementation of the framework provides for a private implementation of IPFS storage that could be maintained by a swarm of healthcare organizations.

IV. Architecture Instantiation Example

The COVID-19 pandemic has shown that there is an increasing need for facilitating health information exchange requests and quick response for patient records, beyond the safe storage of local healthcare providers [19]. In addition, current medical systems fail to effectively streamline EHR due to the complexity of internal data structures and interoperability of EHR workflows that are too burdensome for existing health information technology infrastructure.

As a response to the above challenges, we suggest that there is a need for a more patient-centric approach to collecting medical data. An independent data structure that will enable medical doctors to start from a patient and audit trails of the patient's medical history, such as, medical data, symptoms, diagnostic tests, previous treatments etc. With the information maintained by the smart contract for each patient-doctor relationship, we suggest the creation of a digital *medical passport* that is recorded on a blockchain data structure and it is easily audible.

This section presents an example instantiation of the proposed architecture showing a medical journey that is centered around a patient. The steps of the medical journey are described below and visualized in Fig. 1, as follows:

Bootstrapping. The system can register two types of Users (U) which are either patients (P) or medical doctors MD. The registration takes at a healthcare provider. For each U a pair of keys is generated with the use of the Key Management component as shown in Section III-B. The responsibility of validating the identity of each user is outside the scope of this paper which only focuses on a secure framework for medical information exchange.

Patient Side. A patient initiates the process of information exchange due to a request from a remote medical doctor or some healthcare provider. Using the Ethereum key pair P interacts with the blockchain and deploys the $MedSC$ smart contract; one for each patient-doctor relationship using the Smart Contract Layer as in Section III-D.

Steps 1 to 2 – Access to medical data (raw data or EHR) is provided to P.

Steps 3 to 4 – Patient, P, uses $PGPPub_{MD}$ to encrypt the file, the encrypted file is pushed to IPFS storage.

Result of this step is an encrypted file with the generation of a content identifier (i.e., URL) that points to that file. The URL returned by IPFS is also encrypted using Pub_{MD} and pushed to $MedSC$ as metadata.

Step 5 – P uses `keccak256` to hash the encrypted file which is then encrypted using $Priv_P$ and pushed to $MedSC$ as metadata. This piece of information is used later as part of the digital signature validation process.

Medical Doctor's Side. A medical doctor or healthcare provider MD receives a notification and queries the $MedSC$ smart contract, shared and authorized by P.

Step 6 – The medical doctor, MD, access the metadata from the smart contact and uses $Priv_{MD}$ to decrypt the IPFS URL, and retrieve the encrypted file.

Step 7 – MD retrieves the encrypted hash h_E of the encrypted file from $MedSC$ metadata. Also, MD uses the `keccak256` hash algorithm on the encrypted file to locally produce a hash h_L of the encrypted file retrieved from IPFS.

Step 8 – MD uses the Pub_P to decrypt h_E and then compares the hash value with h_L.

Step 9 – If hashes are an exact match $(h'_E == h_L)$ then MD decrypts the file using $PGPPriv_{MD}$, otherwise notify patient and/or healthcare provider.

V. Conclusions

The recent COVID-19 pandemic exposes a lack of health data fluidity. As a response to this challenge, this paper presents a blockchain-based framework that enables user-centric access to sensitive medical data. Patients maintain full control to their data that are stored securely over a distributed p2p file storage system with the use of cryptographic techniques. The effectiveness of the proposed framework is demonstrated with an implementation of a medical user journey deployed over the Ethereum blockchain. Access to medical data is orchestrated by a smart contract that maintains pointers to IPFS content identifiers. We suggest that health information exchange should not be limited within the scope of health medical records but instead it should encompass a wider spectrum of medical data. As an example, monitoring patients' activity from wearable devices that are interconnected with the use of IoT. Especially in pandemic situations the scope of health information exchange should not be limited to a specific region but should be shared quickly and securely beyond boundaries. Further to the above, we note that patients should be able to authorize access to partial views of the data with the use of micro-transactions. For future work, we are exploring opportunities for enabling secure health information exchange over many IoT devices that are authenticated over a blockchain network.

References

[1] E. G. Carayannis, E. Grigoroudis, S. S. Rehman, and N. Samarakoon, "Ambidextrous cybersecurity: The seven pillars (7ps) of cyber resilience," *IEEE Transactions on Engineering Management*, pp. 1–12, 2019.

[2] S. Makridakis and K. Christodoulou, "Blockchain: Current challenges and future prospects/applications," *Future Internet*, vol. 11, no. 12, p. 258, 2019.

[3] E. U. A. for Fundamental Rights, *Coronavirus pandemic in the EU - Fundamental Rights*, 2020 (accessed April 13, 2020), https://fra.europa.eu/en/publication/2020/covid19-rights-impact-april-1.

[4] OECD, *OECD Economic Outlook, Interim Report March 2020*. Organisation for Economic Co-operation and Development, 2020. [Online]. Available: https://www.oecd-ilibrary.org/content/publication/7969896b-en

[5] E. D. P. S. (EDPS), *Health data in the workplace*, 2020 (accessed April 14, 2020), https://edps.europa.eu/data-protection/data-protection/reference-library/health-data-workplace_en.

[6] Z. Zinonos, P. Christodoulou, A. S. Andreou, and S. A. Chatzichristofis, "Parkchain: An iot parking service based on blockchain," in *15th Int. Conference on Distributed Computing in Sensor Systems, DCOSS 2019, Santorini, Greece, May 29-31, 2019*. IEEE, 2019, pp. 687–693.

[7] P. Christodoulou, K. Christodoulou, and A. Andreou, "A decentralized application for logistics: Using blockchain in real-world applications," *The Cyprus Review*, vol. 30, no. 2, pp. 171–183, 2018.

[8] 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)*. IEEE, 2016, pp. 25–30.

[9] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "Secure and trustable electronic medical records sharing using blockchain," in *AMIA annual symposium proceedings*, vol. 2017. American Medical Informatics Association, 2017, p. 650.

[10] A. F. Hussein, N. ArunKumar, G. Ramirez-Gonzalez, E. Abdulhay, J. M. R. Tavares, and V. H. C. de Albuquerque, "A medical records managing and securing blockchain based system supported by a genetic algorithm and discrete wavelet transform," *Cognitive Systems Research*, vol. 52, pp. 1–11, 2018.

[11] L. Catarinucci, D. de Donno, L. Mainetti, L. Palano, L. Patrono, M. L. Stefanizzi, and L. Tarricone, "An iot-aware architecture for smart healthcare systems," *IEEE Internet of Things Journal*, vol. 2, no. 6, pp. 515–526, 2015.

[12] "An integrated system based on wireless sensor networks for patient monitoring, localization and tracking," *Ad Hoc Networks*, vol. 11, no. 1, pp. 39 – 53, 2013.

[13] S. Sengupta and S. S. Bhunia, "Secure data management in cloudlet assisted iot enabled e-health framework in smart city," *IEEE Sensors Journal*, pp. 1–1, 2020.

[14] P. R. Zimmermann and P. R. Zimmermann, *The official PGP user's guide*. MIT press Cambridge, 1995, vol. 5.

[15] G. Wood *et al.*, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, no. 2014, pp. 1–32, 2014.

[16] S. Nakamoto and A. Bitcoin, "A peer-to-peer electronic cash system," *Bitcoin*, 2008, https://bitcoin.org/bitcoin.pdf.

[17] S. Bano, A. Sonnino, M. Al-Bassam, S. Azouvi, P. McCorry, S. Meiklejohn, and G. Danezis, "Sok: Consensus in the age of blockchains," in *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*, 2019, pp. 183–198.

[18] M. Qu, "Sec 2: Recommended elliptic curve domain parameters," *Certicom Res., Mississauga, ON, Canada, Tech. Rep. SEC2-Ver-0.6*, 1999.

[19] C. Jason, *COVID-19 Exposes Lack of Health Data Exchange, Interoperability*, 2020 (accessed April 29, 2020), https://ehrintelligence.com/news/covid-19-exposes-lack-of-health-data-exchange-interoperability.