A Blockchain Based Approach for E-Prescription System Security and Traceability

Rayene Bounab[1], Karim Zarour[1], Bouchra Guelib[1] and Amina Bouazza[1]

[1]*LIRE Labotory, Faculty of NTIC, University of Constantine2-Abdelhamid Mehri, Ali Mendjeli Campus, 25000 Constantine, Algeria*

Abstract

Electronic medical records (EMRs) have become the standard technique for hospitals to store patient information since the advent of electronic information technology. They enable patient information and drug data exchange between doctors, patients, and pharmacies. The information is stored in different hospital databases, even for the same patient. Due to security and privacy restrictions, generating an EMR report from different hospital databases for a single patient is challenging. Current approaches for managing prescription records are suffering from transcription errors, a lack of traceability, unsecured data, access without control, increases in the percentage of fraud in E-prescription (EP), superfluous record duplication, and sluggish record transfers. In many systems, patients do not have access to their prescription information. To access or transfer their records, they must pass through an intermediary instead. Developing a standardized, interoperable, and secure prescription management system is essential for addressing these issues. When implementing such a system, it is vital to consider security, efficiency, scalability, traceability, and other barriers. This paper proposes a Blockchain-system based on the InterPlanetary File System (IPFS) and smart contracts to secure, and ensure interoperability, traceability, and efficient access to prescription records. The approach is patient-centric by assigning ownership of prescription records directly to patients and promotes transparency by providing patients with an explicit list of parties that hold permission to access their records.

Keywords

Blockchain, Electronic prescription (EP), Smart contract, transaction, InterPlanetary file system (IPFS), Healthcare

CEUR-WS.org/Vol-3616/paper1.pdf

1. Introduction

A medical prescription is a handwritten document by a physician for a patient based on the patient's symptoms or disease. Patients and pharmacists frequently misread the name of a medication on a prescription due to the doctor's illegible handwriting. Historically, this procedure involved physically transferring a piece of paper with a handwritten order to another service. For instance, it can be inconvenient for patients to seek medical care when using traditional medical information systems such as the classic Electronic Medical Records (EMRs) or the Hospital Information System (HIS), in which a large amount of medical data is stored in a centralized database at each medical institution [1]. There is a high risk of privacy violations involving patients' personal medical information during storage and transmission.

RIF'23 : The 12th Seminary of Computer Science Research at Feminine, March 09, 2023, Constantine, Algeria
rayene.bounab@univ-constantine2.dz (R. Bounab); karim.zarour@univ-constantine2.dz (K. Zarour); bouchra.guelib@univ-constantine2.dz (B. Guelib); amina.bouazza@univ-constantine2.dz (A. Bouazza)
0000-0001-9809-2617 (R. Bounab); 0000-0002-2727-2036 (K. Zarour); 0000-0001-7338-2423 (B. Guelib)
© 2023 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).
CEUR Workshop Proceedings (CEUR-WS.org)

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

Doctors cannot accurately and adequately analyze patients' illnesses in hospitals due to a lack of complete diagnosis, traceability, and treatment information [2]. As a result, the EP system was developed to address these problems. E-prescription is a way for the patient, the doctor, the pharmacist, the government, and the health insurance company to send and receive prescription information through an electronic device. By integrating information about a patient's diagnosis and prescriptions, prescription systems enable healthcare practitioners, such as physicians, to establish digital records regarding a patient's health state. Compared to paper-based prescriptions, it provides more effective communication and fewer inconsistencies [3, 4]. In most EP systems, patient participation is limited to approving the use of an EP by the doctor and the pharmacy. EP enables the parties concerned to provide a safe, effective, and high-quality service [5]. Furthermore, EP systems facilitate communication between a doctor and a pharmacist when reviewing a prescription prior to distribution[6]. Electronic prescriptions are expected to prevent drug errors resulting from paper prescriptions. Moreover, it improves the poor service quality associated with paper prescriptions by reducing the work required to sort related documentation. Importantly, giving each patient a medical history and traceability will improve patient safety during medication administration [7]. However, EPs can only avoid some pharmaceutical errors. Furthermore, there are risks associated with the prescriber's adaptation to the EP system, as they must become familiar with the software [8]. Since the COVID-19 epidemic, the importance of EP systems has increased. Isolation, limited travel, and fewer social connections are all suggested for people [9]. When prescriptions are submitted electronically to pharmacies in advance to prepare medications, fewer trips to clinics for prescription collection and shorter wait times at pharmacies will occur. Additionally, adopting EP will decrease the likelihood of catching the virus by handling prescriptions on paper. Blockchain technology is becoming increasingly popular as a decentralized database storage technique [9]. Since its beginnings in 2008, Blockchain has continued to develop as a technology that would transform the manner in which we interact, match payments, conduct research, and monitor transactions. Eliminating the requirement for a centralized authority to oversee and verify interactions and transactions between various parties can be highly cost-effective. In Blockchain, each transaction is cryptographically signed and validated by all minor nodes maintaining a copy of the whole ledger containing blocks of all transactions linked together. This generates one of the non-editable, secure, gated, and shared records [10]. In 2017, the U.S. Centers for Disease Control and Prevention began experimenting with Blockchain to exchange public health data to assist public health employees to respond more rapidly to crises [11]. Nonetheless, some pharmacies illegally offer customers medications without a doctor's prescription, leading to drug abuse. Implementing Blockchain in these applications is primarily motivated by introducing digital identification, distributed security, smart contracts, and biometrics via a distributed Blockchain ledger [12]. A smart contract is a program that can verify the execution of predefined terms and conditions [13]. Unlike verifying digital currency like Bitcoin, Blockchain mining nodes execute, validate, and store data in blocks. A smart contract is triggered by sending a transaction to its Ethereum address and executing it based on the transaction's input. The properties of smart contracts are implemented in the peer-to-peer mode without the involvement of a centralized third party, and the service is available without any central dependency. The alignment of contracts to established circumstances makes them more intelligent than paper contracts; these properties of smart contracts make them applicable to

various sectors. Ethereum is a distributed, open-source, blockchain-based platform that enables the creation of smart contracts [11]. Ether is the cryptocurrency used to pay for transactions on the Ethereum Blockchain. An Ethereum address uniquely identifies each network participant (EA). Smart contracts facilitated the creation of decentralized applications on the Ethereum platform. It gained popularity for its ability to ease the building of Blockchain applications for many use cases [14]. Due to this, Ethereum is frequently used in academic research and commercial enterprises leveraging smart contracts.
This article addresses the development of a Blockchain-based medical prescription system that might facilitate online prescription processing with safe storage, identity verification, and access permissions. The suggested solution combines the InterPlanetary File System (IPFS) and smart contracts to protect, guarantee interoperability, and expedite access to prescription information. This strategy is patient-centered by assigning control of prescription information directly to patients. Promotes transparency by giving patients an explicit list of authorized parties to access their records. This paper focuses on the following threats:

- Privacy threat: The patient's medical records contain sensitive information that should not be released to unauthorized third parties without the patient's approval.
- Illegal drug sales: Due to a lack of understanding of the prescription supply chain, illegal drug sales occur, contributing to drug overdoses.

The contributions of this paper are as follows:

1. We introduce a consortium Blockchain-based prescription management system that aims to replace existing prescription systems and prevent information blocking. It determines which actions stakeholders may perform with a specific emphasis placed on patient control.
2. The suggested system is a patient-centric design that is interoperable, scalable, and efficient, since it allows the patient to actively participate in managing their prescription data.
3. To secure users and ensure that only authorized parties may access or modify information, our system actively validates the identities of all parties.
4. Our research paper contributes a system that enables the efficient and cost-free interchange of information across stakeholders through interoperability and without the requirement for format translation. Additionally, our solution avoids data duplication across many levels and allows sharing prescription record data, and assuring total traceability.
5. We implemented the system using Ethereum smart contracts and IPFS to ensure secure large data storage.

The remainder of the paper is organized as follows: Section 2 provides related work. Section 3 presents and details the proposed system. Section 4 presents a discussion, while Section 5 provides a conclusion.

2. Related work

In recent years, researchers have proposed frameworks and systems based on Blockchain technology to secure and enable data sharing among healthcare providers, insurance companies, and other relevant parties. This section discusses works that improve secure data exchange using Blockchain technology. Electronic prescription systems work in a multistakeholder environment. Integrity and information transparency are necessary to avoid selling illegal drugs while preventing patient health problems from drug overdoses. Additionally, applying privacy technology to medical records is another requirement to prevent the misuse of sensitive prescription information. Thatcher and Acharya proposed RxBlock [15], a private Blockchain application built on Ethereum that aims to secure the electronic prescription system by leveraging the Blockchain's immutability property to ensure safe data transmissions across the network. This could be useful for regulating medication use and preventing accidental overdoses. Using a smart contract, they guarantee the functioning of role-checking. Alnafrani and Acharya [16] conducted a study in which they proposed SecureRx, an Ethereum Blockchain web application designed to store medical records and prescriptions. The database is immediately updated when the providers enter the data into the local system. The primary objective of this study is to promote the legitimacy of pharmaceuticals by strengthening accountability and credibility. The Authors in [17] developed VigilRx, a patient-centric and interoperable prescription system that ensures patient control, prevents information blocking and improves transfer efficiency by leveraging Blockchain technology for record management. The proposed method relies on Ethereum smart contracts to enable all operations required for a functional prescription system. Authors in [18] proposed a Blockchain-based information management system to manage patient data. The proposed solution effectively addresses the problem of large-scale data management and sharing within an EMR system. It also demonstrates high information security when combined with symmetric cryptography and specialized access control methods. Cao et al. [19] proposed a cloud-assisted, secure eHealth system to prevent unauthorized changes to EMRs that have been transferred to the cloud. All transactions involving outsourced electronic medical records (EMRs) are recorded in a public Blockchain and can only be executed by users who have been authenticated. To ensure the confidentiality of EMRs, the system implemented a key exchange protocol and accounted for both single and multi-doctor scenarios. Using Blockchain's immutability feature ensures the confidentiality of electronic medical records (EMRs). Authors in [20] proposed SPChain, a Blockchain-based eHealth system for sharing medical data while maintaining patient confidentiality. Using chameleon hash functions, they devised new block structures to reveal the entire medical history of a patient. Furthermore, to complete the upload of EMR from the register and label incorrect EMR, separate registration, medical, and label transactions have been designed for patients. Patient-specific micro-blocks were built so that medical records could be retrieved rapidly. They developed a trust-based consensus method to encourage hospitals to participate in the mining process and collect reputation ratings to demand patients' electronic medical information.

Table 1 provides a comparison of several previous studies and the current study based on various criteria. These criteria include the use of smart contracts, the platform used, the type of system (private, public, or consortium), the storage method (decentralized or centralized), security measures, confidentiality, and access control. Most examined research employs smart contracts

Table 1
Comparison of Previous Studies and the Current Study.

Reference	Smart contract	Platform	Type	Storage	security	Confidentiality	Access control
RXBlocks[15]	+	Ethereum	Private	Decentralized	+	+	-
VigilRx[17]	+	Ethereum	Public	centralized	-	-	-
SecureRx[16]	+	Ethereum	N/A	Decentralized	+	+	-
SPchain[20]	-	BFT-SMaRt	N/A	Centralized	+	+	+
Medblock[18]	-	-	N/A	Centralized	+	+	+
TPEHR[21]	N/A	Ethereum	public	cloud	+	+	N/A
Current study	+	Ethereum	Consortium	Decentralized	+	+	+

and the Ethereum platform, with variations in system type (public, private, or consortium-based) and storage technique (centralized or decentralized). Additionally, most studies have adopted security, confidentiality, and access control mechanisms to protect sensitive data. Notably, the current research is characterized by its use of smart contracts, consortium-based systems, and decentralized storage with complete security, privacy, and access control features. This comparison demonstrates the advantages and disadvantages of several ways to create blockchain-based systems for administering prescription records and provides significant insights for future research in this area.

3. Proposed system

This section provides an overview of the proposed blockchain-based system for EP. The proposed system is based on blockchain technology using a decentralized file system called the InterPlanetary File System (IPFS), which stores files, tracks versions over time, and guarantees security and data immutability [22]. The system's primary objective is to protect patient reports' confidentiality. Figure 1 depicts the proposed blockchain-based EP architecture.

3.1. Overall overview

To ensure privacy, we structured our framework into four parts, as shown in Figure 1: System users, Storage, blockchain, and Patient. When a patient visits a doctor, a new medical record containing diagnostic information and personal information such as name, age, and prescriptions are created. The healthcare provider uploads patient information using a Web-UI portal. The data is then encrypted using the patient's public and symmetric keys. To protect the confidentiality of a patient's diagnostic report, IPFS stores the encrypted data and generates a Content Identifier (CID) to identify the data, which is then stored in Distributed Hash Tables. After that, the transactions are sent to the smart contracts, which are validated through the mining process, signed, and added to the blockchain by miners. Information is sent to the patient, and the pharmacist can access the EP with the patient's ID number.

1. System users
   According to their functions in the prescription process and their real duties in providing healthcare, the system users were divided into the following categories:

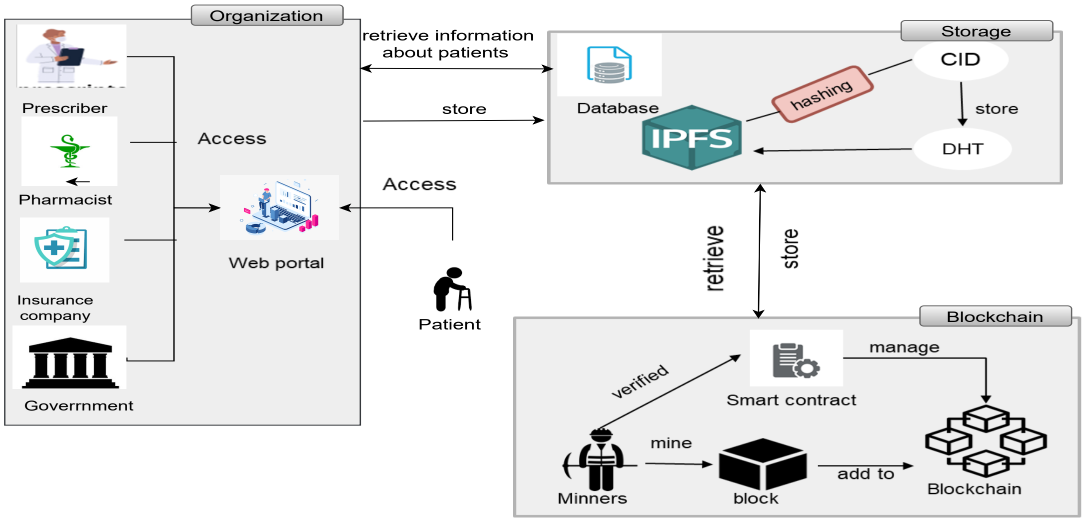

Figure 1: Proposed EP-based blockchain architecture

a) Healthcare provider: represents the physician or hospital responsible for creating or updating patient medical information and prescriptions. Medical professionals might review the patient's records in an emergency to learn more about his condition and the medications given to help with the diagnosis. Additionally, the physician has access to the patient's medication history. If a valid prescription for the same medication exists, the doctor cannot prescribe a new one. This prevents numerous physicians from prescribing the same drug to patients within the same period.

b) Pharmacist: This group of users ensures the effective and secure use of medicines. Once the prescription reaches the pharmacy, the pharmacist ensures that it is filled while considering any potential drug interactions with current treatments. To achieve this, the pharmacist consults the patient's medical history and then signs the prescription, preventing the reuse of a previously filled prescription. Its role in the system are:
   - Check the prescription ID and quantity ordered by the patient;
   - Deliver the medication once the patient's purchase order has been completed.

c) Government: The government agency is one of the participants in our architecture and has unrestricted access to patient data by requesting the patient ID from the health authority. Its role is to determine whether the patient has been treated for narcotics, is a drug dealer or is an illegal drug dealer.

d) Insurance companies: With the patient's permission, insurers can access a patient's information to verify care, collect payments, and take the appropriate actions to reimburse the patient.

2. Storage
   Consists of:
   a) Database: Health authorities electronically store patients' information in a database that retrieves all the patients' records. Health authorities and individuals have access to it at any time and can consult it. We gather patient information from this database.
   b) InterPlanetary File System (IPFS): Is divided into sub-protocols responsible for different features, such as IPLD and IPNS. The IPFS receives data from the prescriber; if it is large, it divides it into parts; each part will have a CID (content identifier), which is nothing but a hash, and then it gathers them into a single CID and stores it in the DHT (Distributed Hash Tables), as this content will be accessible through its CID. If the information is not voluminous (does not exceed 256 kb), it will not be divided but will be split as it is, and its CID will be stored similarly. Then the CID is sent to the blockchain for secure storage and sharing during transactions. The CID is unique; i.e., the slightest change in the data generates a new CID and is considered new data. Distributed Hash Tables (DHT) are hash tables that link the hash (CID) to the physical location of the data so that IPFS nodes can keep track of who has what data. Concretely, the DHT keeps the CIDs that identify each block of data, which store information about the physical location of a given content; these keys are the CIDs of the blocks. To avoid storing DHTs in a single database and getting into other problems, they are split up and distributed across numerous locations on other tables.
3. Blockchain
   Blockchain is a collection of linked data highly resistant to alteration (unchangeable) and secured by an encryption algorithm. It enables secure and immutable transactions. In this work, blockchain operates as follows: the healthcare provider sends an EP, which is considered a transaction using the private/public key of the receiver. Then, the miners participate in the mining process to solve a complex mathematical puzzle based on a cryptography hash function known as Proof of Work. Once the hash value is found, the first who finds the hash adds the transaction to a blockchain block. Ethereum smart contracts are designed to log all data requests and feedback within the Ethereum blockchain. They execute automatically once the contract terms are met. The smart contracts were built using Solidity, an object-oriented and high-level language used by Ethereum. When a prescriber requests a patient's prescription, Solidity initiates a data request stored on the Ethereum blockchain with a timestamp, and all transactions follow the same pattern. The system records all data requests and related responses on the blockchain based on the wallet address, allowing it to track and ensure the traceability of all prescription history data at any time. Smart contracts used in this system are:
   - Contract_user: This smart contract enables the user to control physicians, pharmacies, and registered patients through mapping. The prescription contract will use these mappings to validate and compare the entered addresses. Thus, we can verify

that registered physicians fill prescriptions at locations belonging to legitimate patients and that only certified pharmacies sell medications.

- Contract_prescription: this smart contract contains the following functions:
  - New_prescription(): After the doctor enters the system, he can create a new prescription for the concerned patient and add his information.
  - Authentification(): This function allows the users to access the system and verify the validity of the doctor, patient, and pharmacy addresses.
  - Verify_prescription(): This function allows the system users to verify the validity of the prescribed prescription.
  - Close_transaction(): this function closes the transaction and certifies the medicine's sale to the patient. Only the pharmacist can close the transaction when the patient confirms the purchase.
  - Prescription_details(): It provides the prescription details, such as: quantity_left, max_claim, expiration_day, status.

4. Patient
   Each patient in our system has a key to decrypt data, allowing them to be viewed through a Web-UI portal after the patient identifies himself by entering his details. The patient can also freely consult with other medical professionals and modify or add information anytime. When a physician prescribes a patient's medication, they can submit a purchase order to the pharmacy to buy it.

4. Discussion

The research paper presents a blockchain-based Electronic Prescription system that addresses data preservation and sharing challenges while ensuring patient privacy. The system employs a secure and scalable consent management approach, promoting transparency and enabling stakeholders within the healthcare industry to access prescription records. Our research provides a secure and confidential approach for storing patient prescription data by encrypting the data and storing it on both the blockchain and IPFS. This allows patients to decrypt their prescription information while purchasing medications from a pharmacy, protecting their privacy. Our methodology further enhances the process of Prescription Drug Monitoring Programs (PDMPs) by automatically updating patient files whenever healthcare providers upload new data to their internal systems, hence assuring data traceability. While counterfeit pharmaceuticals can be ineffective or dangerous for patients and the pharmaceutical sector as a whole, stakeholder involvement is critical for our EP system to regulate medicine abuse. The participation of healthcare professionals, pharmacies, insurance companies, and the government permits patients to have control over their data and prevent and reduce medication abuse. However, neither [23] nor [24] addressed this issue. Another point considered in this work is the large size of the data. Whereas [24], [17], [2], and [25] proposed storing data on the blockchain network, it is not suitable for storing large amounts of data. To address this limitation, we propose integrating the blockchain network with the InterPlanetary File System (IPFS), allowing us to store large amounts of data on IPFS and integrate immutable, permanent IPFS addresses within blockchain transactions. In contrast, some studies recommend using private. Several studies, such as RxBlocks [15], EHR [21], and PAGR [26], have proposed using private blockchain solutions due to their ability to regulate who may join the network. Nevertheless, private blockchains may be vulnerable to data breaches and other security problems, particularly if a consensus mechanism is implemented, which typically requires a limited number of validators to agree on transactions and data. Others, such as VigilRx[17], have adopted public blockchain; however, there are significant limitations, such as the lack of complete privacy and anonymity, as public blockchains allow anybody to examine transaction amounts and addresses. If the address owners are identified, the anonymity of the user is compromised. Public blockchains also attract participants with unethical intentions. We propose employing a consortium blockchain, which combines the advantages of the two preceding models. It allows system participants to join the restricted network following an appropriate identity verification procedure. Some offer special permissions to perform specific network tasks. This allows users to consult, access, and enter patient information onto the blockchain. It brings together a number of typically inaccessible actors. Certain nodes may be made public while others remain private, enabling and securing their use.

5. Conclusion

The research paper introduced a novel patient-centric prescription system that uses blockchain technology, IPFS, and smart contracts to promote secure and efficient information exchanges. The system includes a network of physicians, pharmacists, insurance companies, the government, and patients, each possessing a unique role in the network, validated by smart contracts. Integrating a consortium blockchain network and IPFS enables the storage of large amounts of data, hence providing data transparency, tracing, and preventing medication abuse. The proposed architecture for data governance provides a solid platform for future multi-stakeholder applications dealing with sensitive and confidential digital data. Considering future study and development in this sector, there are a number of potential avenues to investigate. First, the suggested system has the potential to be extended to additional healthcare domains, such as clinical trial data management and medical records administration. Second, user studies and feedback mechanisms could be implemented to improve the usability and user experience of the system. Finally, advanced cryptographic techniques, such as zero-knowledge proofs and homomorphic encryption, could be applied to enhance the security and privacy of the system. Addressing these research directions could further improve the proposed system's effectiveness, efficiency, and security and lead to greater adoption of blockchain-based solutions in the healthcare industry.

Acknowledgments

The PRFU project partially supports this research under the number C00L07UN250220200002.

References

[1] K. Zarour, O. A. Bounab, Y. Marir, I. Boumezbeur, Blockchain-based architecture centred patient for decentralised storage and secure sharing health data, International Journal of Electronic Healthcare 12 (2022) 170–190.

[2] T. Zhou, X. Li, H. Zhao, Med-ppphis: blockchain-based personal healthcare information system for national physique monitoring and scientific exercise guiding, Journal of medical systems 43 (2019) 1–23.

[3] R. Dutra Garcia, G. Sankar Ramachandran, R. Jurdak, J. Ueyama, A blockchain-based data governance framework with privacy protection and provenance for e-prescription, arXiv e-prints (2021) arXiv–2112.

[4] B. A. Stewart, S. Fernandes, E. Rodriguez-Huertas, M. Landzberg, A preliminary look at duplicate testing associated with lack of electronic health record interoperability for transferred patients, Journal of the American Medical Informatics Association 17 (2010) 341–344.

[5] K. Zarour, M. O. Fetni, S. Belagrouz, Towards electronic prescription system in a developing country, Applied Medical Informatics 43 (2021) 56–67.

[6] M. Samadbeik, M. Ahmadi, F. Sadoughi, A. Garavand, A copmarative review of electronic prescription systems: Lessons learned from developed countries, Journal of research in pharmacy practice 6 (2017) 3.

[7] B. Aldughayfiq, S. Sampalli, A system to lower the risk of dispensing medication errors at pharmacies using nfc, in: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE, 2018, pp. 196–202.

[8] J. Timonen, S. Kangas, H. Kauppinen, R. Ahonen, Electronic prescription anomalies: a study of frequencies, clarification and effects in finnish community pharmacies, Journal of Pharmaceutical Health Services Research 9 (2018) 183–189.

[9] B. Aldughayfiq, S. Sampalli, Digital health in physicians' and pharmacists' office: a comparative study of e-prescription systems' architecture and digital security in eight countries, Omics: a journal of integrative biology 25 (2021) 102–122.

[10] Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, An overview of blockchain technology: Architecture, consensus, and future trends, in: 2017 IEEE international congress on big data (BigData congress), Ieee, 2017, pp. 557–564.

[11] K. Salah, M. H. U. Rehman, N. Nizamuddin, A. Al-Fuqaha, Blockchain for ai: Review and open research challenges, IEEE Access 7 (2019) 10127–10149.

[12] I. Yaqoob, K. Salah, R. Jayaraman, Y. Al-Hammadi, Blockchain for healthcare data management: opportunities, challenges, and future recommendations, Neural Computing and Applications (2021) 1–16.

[13] T. Bocek, B. B. Rodrigues, T. Strasser, B. Stiller, Blockchains everywhere-a use-case of blockchains in the pharma supply-chain, in: 2017 IFIP/IEEE symposium on integrated network and service management (IM), IEEE, 2017, pp. 772–777.

[14] M. N. M. Bhutta, A. A. Khwaja, A. Nadeem, H. F. Ahmad, M. K. Khan, M. A. Hanif, H. Song, M. Alshamari, Y. Cao, A survey on blockchain technology: Evolution, architecture and

security, Ieee Access 9 (2021) 61048–61073.
[15] C. Thatcher, S. Acharya, Rxblock: Towards the design of a distributed immutable electronic prescription system, Network Modeling Analysis in Health Informatics and Bioinformatics 9 (2020) 1–11.
[16] M. Alnafrani, S. Acharya, Securerx: A blockchain-based framework for an electronic prescription system with opioids tracking, Health Policy and Technology 10 (2021) 100510.
[17] A. Taylor, A. Kugler, P. B. Marella, G. G. Dagher, Vigilrx: A scalable and interoperable prescription management system using blockchain, IEEE Access 10 (2022) 25973–25986.
[18] K. Fan, S. Wang, Y. Ren, H. Li, Y. Yang, Medblock: Efficient and secure medical data sharing via blockchain, Journal of medical systems 42 (2018) 1–11.
[19] S. Cao, G. Zhang, P. Liu, X. Zhang, F. Neri, Cloud-assisted secure ehealth systems for tamper-proofing ehr via blockchain, Information Sciences 485 (2019) 427–440.
[20] R. Zou, X. Lv, J. Zhao, Spchain: Blockchain-based medical data sharing and privacy-preserving ehealth system, Information Processing & Management 58 (2021) 102604.
[21] J. Mahatpure, M. Motwani, P. K. Shukla, An electronic prescription system powered by speech recognition, natural language processing and blockchain technology, International Journal of Scientific & Technology Research 8 (2019) 1454–1462.
[22] R. Kumar, N. Marchang, R. Tripathi, Distributed off-chain storage of patient diagnostic reports in healthcare system using ipfs and blockchain, in: 2020 International conference on communication systems & networks (COMSNETS), IEEE, 2020, pp. 1–5.
[23] R. D. Garcia, G. Ramachandran, J. Ueyama, Exploiting smart contracts in pbft-based blockchains: A case study in medical prescription system, Computer Networks 211 (2022) 109003.
[24] J. W. Kim, A. R. Lee, M. G. Kim, I. K. Kim, E. J. Lee, Patient-centric medication history recording system using blockchain, in: 2019 IEEE International Conference on Bioinformatics and Biomedicine (BIBM), IEEE, 2019, pp. 1513–1517.
[25] J. Li, A new blockchain-based electronic medical record transferring system with data privacy, in: 2020 5th International Conference on Information Science, Computer Technology and Transportation (ISCTT), IEEE, 2020, pp. 141–147.
[26] R. W. Seaberg, T. R. Seaberg, D. C. Seaberg, Use of blockchain technology for electronic prescriptions, Blockchain in Healthcare Today (2021).