Health Policy and Technology 10 (2021) 100510

Contents lists available at ScienceDirect

Health Policy and Technology

journal homepage: www.elsevier.com/locate/hlpt

Original Article/Research

SecureRx: A blockchain-based framework for an electronic prescription system with opioids tracking

May Alnafrani *, Subrata Acharya

Towson University, Department of Computer and Information Sciences, 7800 York Rd, Towson, MD 21204, USA

A R T I C L E I N F O

Keywords:
Blockchain
Ethereum
Healthcare
Electronic records
Opioids
Prescription drug monitoring programs

A B S T R A C T

Objectives: The proposed research aims at attaining several objectives. To start with, it assesses the limitations associated with the current electronic prescription systems. Accordingly, it proposes a proactive method for providing real-time monitoring to prevent overdose prescriptions. The proposed approach should ensure that health providers have access to a comprehensive dataset without state or geographical limitations. More importantly, the research aims to improve drug monitoring to enhance accountability and trust, which are central to promoting drug legitimacy.
Methods: A blockchain-based framework for secure, interoperable, and efficient access to prescription records. The proposed solution, SecureRx, is a web-based application developed on the Ethereum blockchain and RxCheck hub.
Results: Based on the evaluation results, SecureRx is functional as it allows health providers to verify patient history and make informed decisions regarding whether to prescribe opioids. The proposed solution exhibits adequate scalability and handles transactions quickly when the number of nodes is reduced. It is also robust and secure, supports HIPAA compliance, and requires minimal operational expenses.
Conclusions: The safe utilization of medications, especially opioids, continues to be a major problem in the United States and around the world. Part of the reason for this is the inability of health providers to access health databases for patients. Current drug prescription systems are limited in terms of tracking the usage of prescription drugs.
The SecureRx framework has highlighted the potential of the record-keeping technology to nurture effective and efficient sharing of information about prescriptions while ensuring the safety and privacy of the original sources of the data.

Summary

I wrote a paper describing a framework for prescribing medications electronically and track opioid use referred to as SecureRx. The framework is based on blockchain technology, which ensures that records are updated as soon as the health provider enters data in their local systems. On top of adopting a patient-centered approach, the framework enhances provider accountability as it allows authorities to evaluate transactions. The main strength of SecureRx, besides the ability to update records across platforms and eliminate duplications, is that it is secure and robust. Furthermore, it is compliant with relevant regulations, fast, and requires minimal operational expenses. I feel that the adoption of this framework would ease the process of tracking prescriptions, improve transparency, and help patients with opioid dependency problems.

Introduction

Over the recent past, the world has witnessed the continued adoption of electronic health records (EHR) in health care settings. The role of these EHRs is to store patient data electronically, ease information retrieval, enable data sharing, and support clinical decision-making. At the same time, the risk of cyberattacks targeting EHRs has increased primarily due to the sensitive nature of data stored in these systems. It is for this reason that the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and other security standards and laws were implemented. Despite the enactment of laws and regulations, sharing medical data remains challenging due to the security concerns involved.

* Corresponding author.
E-mail addresses: may.alnafrani@gmail.com (M. Alnafrani), sacharya@towson.edu (S. Acharya).

https://doi.org/10.1016/j.hlpt.2021.100510
Received 11 November 2020; Received in revised form 25 March 2021; Accepted 12 April 2021
Available online 29 April 2021
2211-8837/

As Ekblaw et al. [1] explain, Electronic Health Records (EHRs), were not designed to provide lifelong access to different institutions. The inability to share medical data securely impedes many activities, chief among them being prescription drug monitoring. Stakeholders within the health care industry recognize that opioid misuse and abuse can be reduced if health care workers are able to share data efficiently and effectively.

One potential solution that could address this problem is blockchain technology, which is an append-only data structure that can act as a distributed ledger. It does so by replicating data across all nodes in the blockchain hence guaranteeing redundancy. In addition to lacking a single point of failure, blockchains can be verified easily. Nodes in the system mine blocks or create additions to the structure to create blockchains. As a result, blockchains are immutable. Although data retention and mining require additional storage space and computational power, they are essential to guarantee an immutable and decentralized system. Smart contracts refer to functions written to blockchains and executed by nodes. Ethereum manages smart contracts by requiring people to pay for gas using Ether if they want to run a contract. Ethereum also allows the creation of private blockchains that can be managed by a few users for applications that require additional security and in situations where the cost of “gas” can be altered.

Background

Opioid overdose and misuse

Incidents of prescription pain relievers overdose have increased dramatically in recent years [2]. An example of a commonly abused prescription is opioid, which used to treat chronic and acute pain. Although this is an important drug to those who rightfully need it, prescription misuse, overdose, and opioid use disorder pose a national threat. Since the quantity of opioids prescribed started rising, fatalities are reports of overdoses also soared. In the years 1999 to 2018, an excess of 232,000 lives have been lost in the U.S. due to overdoses from opioids [3]. Besides, a report released in 2018 revealed that 128 individuals in the U.S. lose their lives daily after overdosing on opioids [3]. Moreover, the total economic impact of prescription opioid misuse in the nation is estimated to be $78.5 billion annually, including healthcare costs, criminal justice process, decreased productivity, and treating addicts [3].

Many opioids addicts were initially prescribed to receive the medication. Unfortunately, the extremely addictive nature of the drug makes the users heavily dependent on the medication. Upon completing their treatment, patients are forced to endure the pain that comes with the withdrawal symptoms of opioids or seek alternative, illegal ways of obtaining the drug.

Current prescription systems contribute to this pandemic as they have failed to track and supervise the dispensation and consumption of opioid adequately. There is a lack of a centralized source and distribution chain of opioids, making it readily available to anyone.

Prescription Drug Monitoring Programs (PDMPs)

PDMP refers to an electronic database that tracks controlled substance prescriptions within different states [4]. The systems help health officials to detect patients that are, or risk misusing prescription opioids or other prescription drugs. This state-based data collection system helps to record medications of controlled substances.

PDMPs enables medical practitioners to confirm their patient’s prescription status on their state’s database before prescribing them with a controlled substance. The initiative is among the different state-level interventions to prevent abuse of prescribed drugs such as opioid and improve clinical practice.

RxCheck

On the other hand, RxCheck allows states to easily participate in the nationwide Prescription Drug Monitoring Program (PDMP) data sharing and integration program [5]. The RxCheck hub is a comprehensive data sharing system that enables states to efficiently and securely share prescription drug monitoring program (PDMP) data amongst themselves or with a Health Information Exchange/Electronic Health Record (HIE/EHR) system [5].

While PDMP is a noble initiative, it is characterized by several limitations that hinder its ability to prevent abuse of prescription in the United States. First, since PDMP is a state-based system, it lacks a universal workflow and effort to combat prescription abuse. The states lack a coordinated and consistent approach in both the design, characteristics, implementation, and evaluation of PDMP programs.

Besides, loopholes within the program allow patients to circumvent the policy by crossing borders to obtain more prescriptions. While most states are sharing data, the process is mainly inefficient, due to the absence of standards on state requirements and processes. Hence, it is much more difficult for physicians to check the prescription records from other states. The system’s technical inefficiencies also push most physicians only to generate reports when they suspect a particular patient might be guilty for drug abuse. Nonetheless, since the usage of PDMP is optional, most doctors are not willing to take their time to check their patient’s drug consumption records before prescriptions. As Alogailiet et al., [6] explain, without a robust and mandatory PDMP, drug abuse incidents cannot be reduced significantly.

The frequency with which pharmacies report data to PDMPs, the ability to access the necessary information, staff authorized to handle the relevant information, as well as the technical ability of the providers varies significantly. Consequently, the accuracy and timeliness of PDMP data across states is inconsistent. The same is also true regarding the consistency and frequency by the healthcare practitioners. The characteristics of a retrospective submission as compared to a real-time entry results in delays that adversely affect the process’s effectiveness.

RxCheck also has several weaknesses that limit its effectiveness. For instance, the database supposed to hold patients’ records is largely passive, and functionalities are meant to prevent the prescription from being functional. Besides, physicians are required to locate and check for previous records before giving prescriptions. However, the checking feature is not enforced.

The lack of real-time data enables people to exploit the outdated database by abusing the prescriptions. Furthermore, pharmacists, physicians, and officials from national pharmacy associations also complain of incorrect search results when locating patient’s records in the RxCheck hub. Inaccurate patient matching not only means no records for a patient, but also causes privacy concerns by returning records for the wrong person [7]. According to physicians and pharmacists, matching issues often arise due to clerical errors, patients having similar birthdates and names, patient name changes, use of multiple names by the same patient, and having duplicate PDMP records [7].

Related work

Over the recent past, scholars have developed frameworks and systems based on blockchain technology to enable data sharing among health care providers, insurers, and other key players. This section explores trends concerning the use of blockchain technology to improve secure data sharing.

Ekblaw et al. [1] conducted a study in which they presented “MedRec”, a prototype for implementing blockchain in health care. MedRec is a decentralized record management system designed to manage electronic health records (EHRs) using blockchain technology. A key component of this system is the modular design that integrates data storage solutions to facilitate interoperability and enhance adaptability and convenience. It utilizes Ethereum smart contracts to enable access to content in diverse storage locations to enable secure authentications. It also encompasses encouraging stakeholders within the health care industry to take part as miners.

Xia et al. [8] presented a system based on blockchain to enable trust-less medical data sharing between providers of cloud computing services. Specifically, they proposed a system called MeDShare that enables secure data sharing in a trust-less setting using smart contracts. It supports data provenance, control, and auditing. In addition to monitoring entities accessing data for malicious purposes, the system records data transitions and sharing in a tamper-proof way.

Dagher et al. [9] developed a model referred to as Ancile that is premised on blockchain technology to enable access to patient records by key stakeholders. According to the authors, blockchain technology presents an opportunity for enabling data sharing in a transactional and decentralized manner. Ancile employs smart contracts in a blockchain-based on Ethereum to enhance access control and data obfuscation. Another key component of the system is the integration of cryptographic methods to enhance security further.

Zhang, White, Schmidt, Lenz, and Rosenbloom [10] demonstrated the application of blockchain technology to secure clinical data while enabling scalability through a system referred to as FHIRChain. The authors note that the current ineffective data exchange is due to the siloed character of conventional clinical data. Accordingly, they present blockchain technology as a solution for enhancing information exchange while adhering to the Fast Healthcare Interoperability Resources (FHIR) standard, which is a requirement of the Office of the National Coordinator for Health Information Technology (ONC).

Xu et al. [11] developed a privacy-preserving scheme based on blockchain technology for large-scale health data. The authors note that the centralization of data storage and limited computing power limit user control over their data, increase privacy leakage, and introduce single-point bottlenecks in computing. The scheme presented, Healthchain, not only includes blockchain technology but also encompasses strong access control mechanisms and encryption to enhance data privacy.

Zhang, Stodghill, Pitt, Briody, Schmidt, White, Pitt, and Aldrich [12] created a decentralized application referred to as OpTrak that utilizes distributed ledger technology to track opioid prescriptions. The application utilizes Ethereum blockchain technology to leverage the disintermediation, network consensus, and immutability features of distributed ledgers. Therefore, OpTrack relies on blockchain technology to enable health care providers to exchange prescription data securely.

Proposed framework: SecureRx

This section provides an overview of the architecture of SecureRx, the technical components, and features.

Architecture

SecureRx is a web-based application developed on top of Ethereum blockchain, and alongside RxCheck hub, as illustrated in Fig. 1 below. SecureRx receives messages (such as a request to provide a patient's prescription records or prescription transactions) through its smart contracts from the SecureRx web application. Subsequently, SecureRx delivers data (such as prescription information about a particular patient) to be used in prescription tracking.

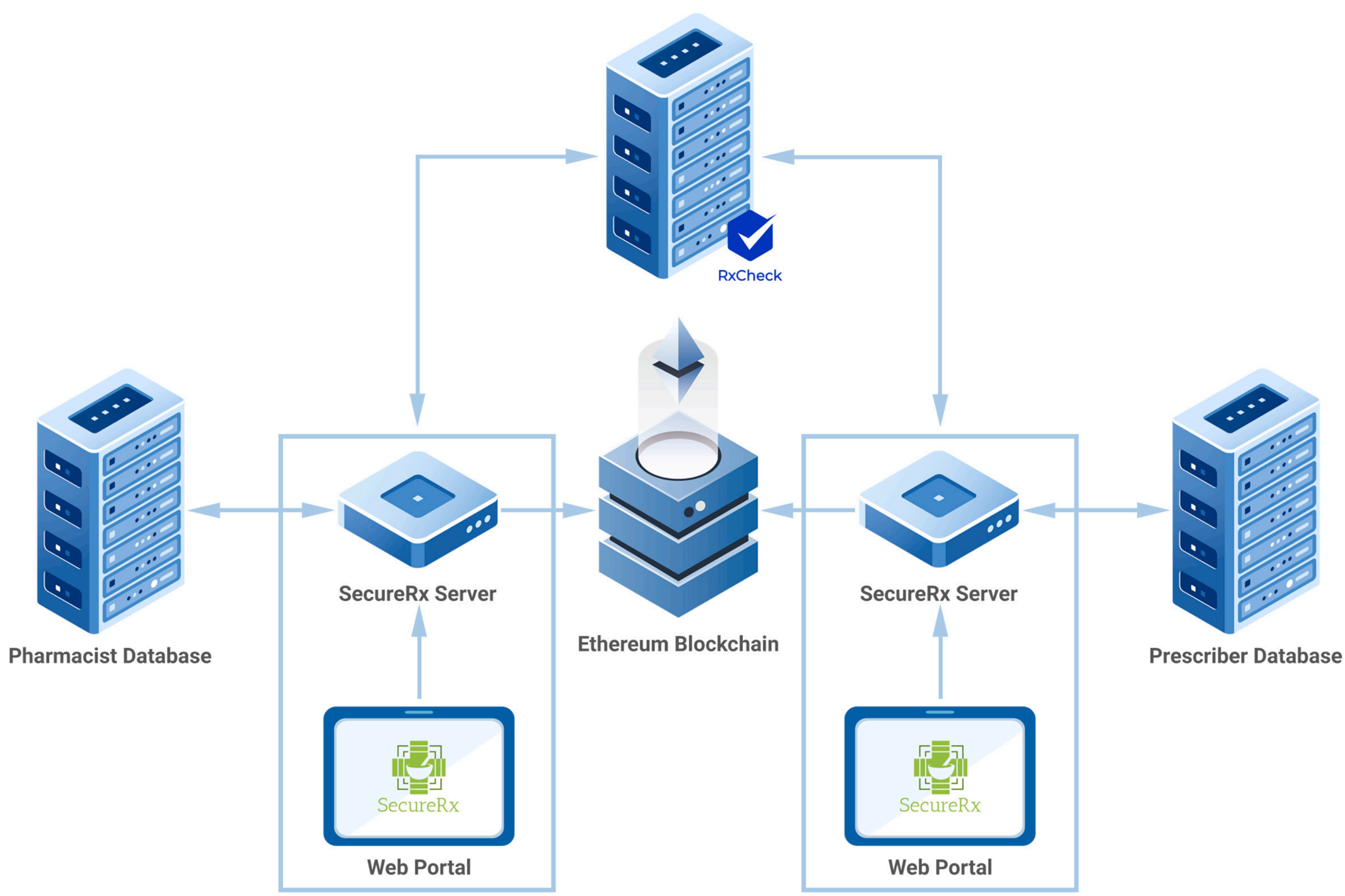

Fig. 1. SecureRx Architecture

Software components

SecureRx consists of three main software components, i.e., the Database simulator, Ethereum smart contract, and JavaScript-based web application.

Database simulator

We used a standardized Mongo DB database simulator that includes API keys to permission access to allow data exchange SecureRx and RxCheck databases. This database simulates the RxCheck database, which holds patients' prescription records for all controlled substances and opioid agonists.

Ethereum smart contract

Ethereum smart contracts were also created to facilitate logging of all data requests and feedback within the Ethereum blockchain. Solidity, an object-oriented and high-level language used by Ethereum, was used to implement the smart contracts. When a prescriber requests a patient's prescription, Solidity initiates a data request to be recorded on the Ethereum blockchain with a timestamp, and the same thing happens with all transactions. Keeping a record of all data requests and respective responses on the blockchain based on the wallet address allows SecureRx to track all prescription history data at any given time.

Smart contract functions. A key component of the SecureRx is that only authorized users should be able to add data to the blockchain to enhance security. To do so, the implementation utilizes internal and private functions that allow the administrator to push data into the blockchain. Table 1 below summarizes some of the functions utilized in smart contracts and their parameters.

JavaScript-based web application

A JavaScript Web Application based on the React Web Framework facilitates all SecureRx's services, providing users with a familiar web experience. The SecureRx Web Application is mainly composed of React Js, Web3 Js, and Node Js. Web3.js is a collection of libraries that enables users to interact with the Ethereum nodes. React JS JavaScript library supports the development of user interfaces and components, while Node.js is a JavaScript runtime environment that provides robust features for mobile and web applications.

The SecureRx web application includes a unique portal meant for drug prescription stakeholders, whose server is tasked with facilitating and encapsulating all blockchain communications. It provides users with a user-friendly portal that they can use to create accounts and login into the system, as per their roles (e.g., pharmacist, physician, prescriber, etc.). Users are required to provide valid Ethereum addresses to be used as unique system identifiers. After their requests have been approved and updated, users will be allowed to manipulate the system without any restrictions. This web service will handle all communications with the blockchain, thus avoiding burdening the users with technical tasks. The JavaScript remote procedure call facilitates the interaction between SecureRx's web application and the Ethereum smart contract. Both prescribers and pharmacists will be allowed to utilize the application to increase awareness of patients' behavior before issuing prescriptions. The system also permits prescribers to query information on a given patient using his/her unique identifier. After the web application submits the data request, the server prompts a new request object within the smart contract component and stores it on the Ethereum blockchain.

Table 1
Smart contract functions and parameters

Function	Header
Add new prescriber	*setPrescriber(string _name, string _clinicAddress, string _contactNumber, string _ePrescribeNetworkID, string _prescriberID, string _stateLicenseNumber)*
Add new patient	*setPatient(string _patientName, string _patientLocalAddress, string _patientGender, string _patientDOB, string _patientContactNumber, string _patientID, uint256 _consultedPrescriber)*
Add new pharmacy	*setPharmacy(string _pharmacyOwnerName, string _pharmacyName, string _pharmacyAddress, string _pharmacyContactNumber, string _pharmacyID, address _pharmacyAddress)*
Add new pharmacist	*setPharmacist(string _pharmacistsName, string _pharmasistAddress, string _pharmacyName, string _contactNumber, string _pharmacistID, address _pharmasistAddress)*
Add new drug	*setDrug(string _drugName, string _drugType, string _drugDescription, string _drugForm, uint256 _pharmacyID)*
Set prescription	*setPrescription(uint256 _drugID, uint256 _drugQuantity, uint256 _patientID, uint256 _pharmacistsID, uint256 _consultedDoctor)*
Fill prescription	*Function: fillPrescription(uint256 _pID, bool _pActiveRefillStatus)*

System users

The system users were classified based on their roles within the prescription process and their actual healthcare duties. Fig. 2 below shows the different groups of system users, as well as their permitted access levels. Each of these groups is assigned different levels of access based on their responsibilities. They include;

- Prescribers: Medical practitioners tasked with writing orders for medicine, as well as directing how the drugs will be used. These individuals will be required to counter-check with SecureRx before prescribing medications. Examples of these individuals include physician, physician assistant, paramedics, Emergency Medical Technician (EMT), and nurse practitioner.
- Pharmacists: Similar to real-world pharmacists, this group of users will ensure safe and effective use of medications.
- Administrators: Admins will oversee the system, ensuring all technical features function as expected. They will be in charge of ensuring other users can use the system functions and access the required data. Some of their duties involve adding prescribers, adding new drugs, checking login errors from the users, and deleting old/unused accounts.
- Other users: This category will only be permitted to view the history of a patient's medical prescriptions and use this information allowed duties such as conducting tests, diagnosis, or administering treatment. Examples of people in this group are the Prescription Drug Monitoring Program (PDMP) users. Besides, patients can also be classified under this group, as they seek to access their medical records or prescription history from different providers or reports on their health status.

Supported prescription transactions

It is impossible to delete data from a blockchain network. As such, the proposed system introduces a unique, effective approach to store all general prescription transactions used in the system as illustrated in Fig. 3. This contrasts with centralized systems, which are likely to lose the data after a server crash. The supported transactions include;

- New prescription request (NewRx): performed by inserting a new transaction with the prescription details.
- Change of new prescription (ChangeRx): performed by inserting a new transaction with the updated details and the ETH address of the original transaction.
- Cancel of prescription (CancelRx): performed by inserting a new transaction with the updated status and the ETH address of the original transaction.
- Refill/renewals request/response (Refill Request): performed by inserting a new transaction with the updated refill quantity and the ETH address of the original transaction.

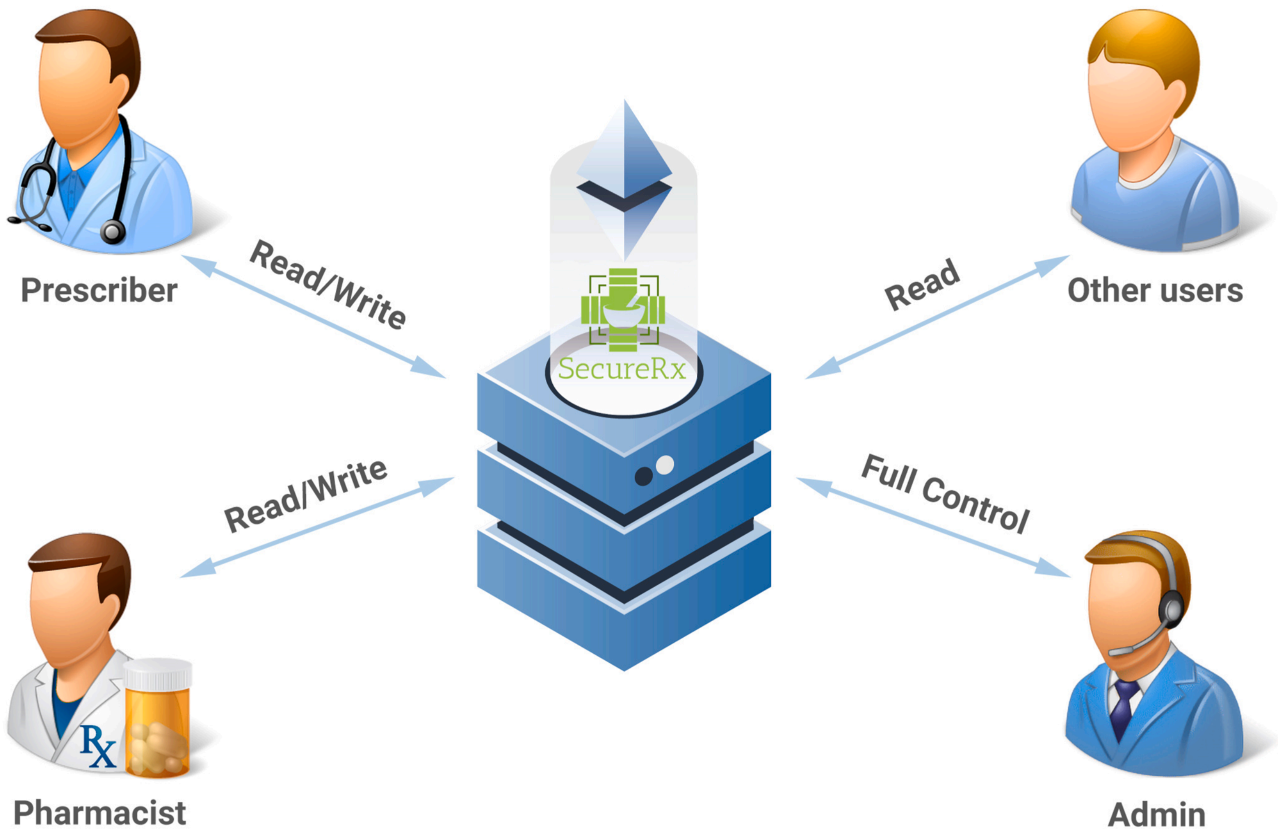

Fig. 2. SecureRx Users

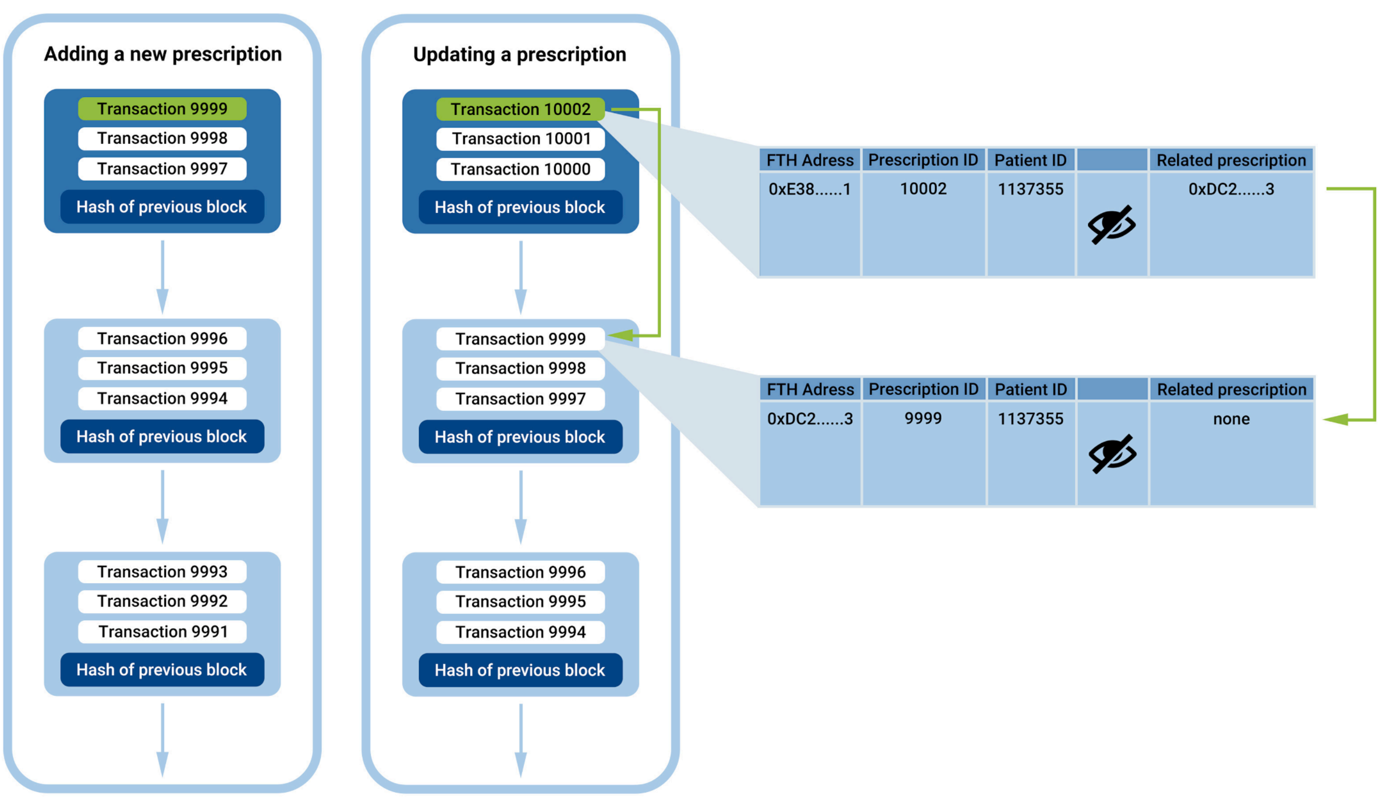

Fig. 3. SecureRx Prescription Transactions

Deployment and performance evaluation

Ropsten test-net was used to evaluate the proposed solution. Ropsten test-net is Ethereum's testing blockchain environment that allows the user to perform tests in an emulated environment. The environment performs in a similar fashion to the public Ethereum network. A key benefit of this solution is that the user does not pay since Ropsten offers a faucet to request Ethers. It also allows the user to utilize a private instance of Ethereum in a cloud-based environment. In our evaluation, we used the cloud-based environment using the Digital Ocean Cloud Platform. We selected private instances because the user can set the mining difficulty in the genesis block. This feature is essential as it allows the user to initiate the blockchain with the proof-of-work (PoW), in the difficulty, adjusted to the infrastructure to be used in maintaining the blockchain. It also enables the user to set an appropriate difficulty for evaluating the time required to produce new blocks with high throughput as compared to the main public Ethereum network.

We evaluated the different Ethereum options that can be adopted in SecureRx qualitatively. Based on our findings, both Ropsten and Private instances exhibited a mining time lower than a minute, signifying that their behaviors are similar. However, the public Ethereum network exhibited a higher mining time (more than a minute) due to the high difficulty in the public network. In such public networks, the dynamic difficulty increases over time because miners have high computing power. Nevertheless, the user must consider the infrastructure costs associated with using a distributed application (dApp) on a private instance of Ethereum. Although small applications require fewer nodes to validate blocks, larger applications must utilize a high number of nodes to ensure effective performance and resilience in executing smart contracts.

We analyzed the public Ethereum network by estimating the cost in gas for transactions. Table 2 below presents the fees required to execute different functions. Gas refers to the fee needed to execute a contract on the Ethereum blockchain platform whereas Ether is the associated unit of currency.

The functionality of SecureRx

SecureRx helps to resolve the main challenge within the current prescription system by providing relevant authorities with the ability to securely monitor and track patients' prescription records (especially opioid) across different states. As a result, this presents providers with broader access to prescription information and promotes the integrity of stakeholders involved in all prescription transactions. Besides, this significantly reduces the misuse of opioids.

Fig. 4 below illustrates a scenario whereby a prescriber tries to prescribe opioids from without reviewing RxCheck/PDMP data. Fig. 5 illustrates the functionality of SecureRx and how it resolves the challenges of the previous system in the same scenario.

Table 2
Smart Contract Functions Deployment Cost

Function	Gas Used by Transaction (Gas Limit = 2,000,000, Gas Price = 0,00000007 Ether)	Transaction Fee (Gas Price * Gas Used by Transactions) in Ether
Add new prescriber	302,834 (15.14%)	0.01211336 Ether
Add new patient	259,811 (12.99%)	0.01039244 Ether
Add new pharmacy	280,626 (14.03%)	0.01122504 Ether
Add new pharmacist	280,593 (14.03%)	0.01122372 Ether
Add new drug	236,136 (11.81%)	0.00770188 Ether
Set prescription	192,547 (9.63%)	0.00761163 Ether
Fill prescription	29,100 (1.46%)	0.00116411 Ether

Fig. 5 indicates how SecureRx allows prescribers to verify patient history via RxCheck. This method enables prescribers to make better and more informed decisions of whether to issue patients with opioid prescriptions or not, based on (near) real-time data on patients' prescription requests and fulfillment history.

Evaluation

The proposed SecureRx system aims at improving the management of prescriptions to minimize opioid abuse. In addition to being functional, the system should be robust, secure, compliant with regulations, cost-effective, and fast. Accordingly, this section presents an in-depth evaluation of the system to demonstrate its feasibility in health care settings. It does so by defining a set of significant metrics that influence the choice of such a solution. Scalability is an important consideration when developing health care systems as requirements and resources change frequently. Robustness and security are particularly essential as they illustrate the ability of the system to cope with errors and protect sensitive information. Compliance with regulations not only enhances its acceptance but also helps to secure personally identifiable information. Cost-effectiveness and the speed of operation are also key as they influence the likelihood of adoption.

Scalability

SecureRx exhibits adequate scalability. Based on the design adopted, the system only stores hashes and small records on the Ethereum blockchain. Because much less storage space is required, increases in data accumulation would not adversely affect the storage needs of the system. Additionally, only a few nodes validate transactions containing data hashes hence reducing mining costs of the blockchain. Although reducing network nodes involved in transactions compromises decentralization, it enhances the ability of the system to process transactions quickly.

The salability of SecureRx was analyzed to determine its ability to handle an increasing number of transactions within the minimal time possible. Based on the experimentation setup, the number of nodes was varied up to ten nodes and the execution times and throughputs in datasets of a hundred transactions were measured. Table 3 below presents the execution time and throughput when the network size (the number of nodes) increases when performing the insert functions and keeping the number of transactions in the dataset at 100. Fig.s 6 and 7 illustrate the graphs of execution times and throughput as the nodes are increased, respectively. As can be seen, the execution time increases slightly as the number of nodes increases whereas the throughput decreases. Therefore, selecting a network size that offers the best execution time with a good throughput is required. This explains why SecureRx is based on a reduced number of nodes.

Robustness and security

SecureRx is a robust and secure solution as it enables the sharing of data in a tamperproof and secure manner. The system is based on blockchain technology, which is particularly strong as it leverages the benefits of decentralization. SecureRx does not have a central target for content attack since both the global authorization log and the medical raw data are distributed. In an era characterized by data leaks and cyberattacks, decentralization makes it difficult for attackers to steal information as there is no single point where the whole data and authorizations are stored. Another key component of SecureRx is encryption as it furthers the level of security. The main role of encryption is to protect sensitive data from being understood and utilized by intruders or authorized parties. Therefore, the use of blockchain technology, the distributed nature of the system, and the inclusion of encryption make SecureRx robust and secure.

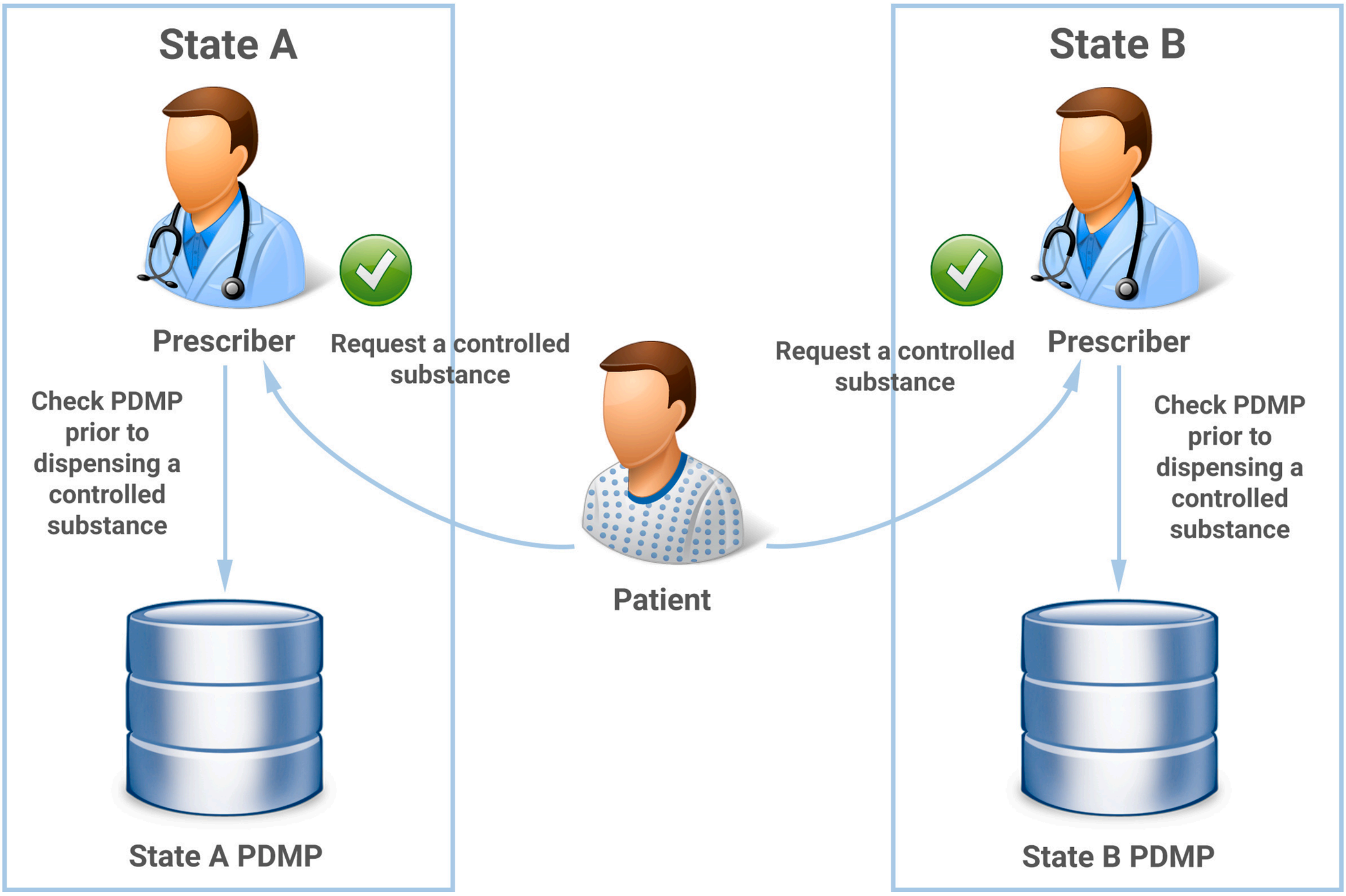

Fig. 4. Prescription workflow with the traditional prescription system

HIPAA compliance

Systems developed for use in the health care industry must adhere to the relevant laws, especially the Health Insurance Portability and Accountability Act (HIPAA). Health care plans, providers, clearing-houses, and business associates are some of the organizations that are required to comply with HIPAA. HIPAA contains a series of regulatory standards that define the lawful utilization and disclosure of sensitive patient information, including the security, privacy, breach notification, and omnibus rules [13]. The proposed SecureRx system satisfies both the security and privacy rules of HIPAA. Concerning the security rule, the system satisfies four essential technical safeguards. To start with, it ensures that only authorized persons can access protected health information (PHI) by embracing role-based access control, authentication, and identity verification.

SecureRx employs encryption to prevent unauthorized persons from comprehending PHI. Based on the design adopted, the data obtained from the RxCheck simulator is encrypted through Transport Layer Security (TLS) and then encrypted with web3.js using the private key of the user and then added to the Ethereum blockchain that supports asymmetric encryption [9]. Moreover, the security rule emphasizes system audits to identify malicious activity. SecureRx meets this requirement because it is based on blockchain technology that ensures an immutable record of transactions. The system utilizes both eth_calls and transactions to ensure data integrity and privacy. It also enables the creation of a comprehensive record of data for auditing. Finally, the security rule requires organizations to implement technical safeguards to eradicate the possibility of data being stolen or altered during transmission. Similarly, SecureRx meets this requirement by utilizing TLS to secure electronic transmissions. As a cryptographic protocol, TLS ensures that data communications over a network are secured.

Operational cost

The operational cost of a system is a key evaluation metric, and running the proposed SecureRx requires minimal expenses. Performing computations and storing data, which form the main transactions on Ethereum, cost the network CPU cycles and storage space. The account initiating the transaction is responsible for paying this cost, which is referred to as “Gas” and paid using ETH. To evaluate the operational cost of SecureRx, MetaMask, an extension for accessing Ethereum-enabled distributed applications, was utilized to send transactions and deploy contracts. MetaMask was selected as it is easy to operate and can record the amount of *Gas* automatically. Lastly, the total *Gas* amount was converted to the USD value using the exchange rate provided by the Markets Insider (“United States dollar – Ethereum”). At the time of evaluation, 1 $Gas = 4 * 10^{-8}$ ETH = 0.0000136 USD [14], and the typical transaction needs 29,100 *Gas*. Since a prescription record does not exceed 1KB that requires 29,100 of *Gas*, the equivalent USD cost is 0.395. According to Statista [15], the total number of retail prescriptions in 2020 in the United States is 4.55 billion prescriptions. As a result, the cost of implementing the proposed system is 4,550,000,000*0.395 = 179,725,000 USD, a Fig. that is way lower compared with the cost of leading EHR and cloud storage solutions today.

Speed

SecureRx is based on blockchain technology that enables an efficient approach for tracking prescriptions. The current prescription tracking systems are centralized, which means that updating records is a manual

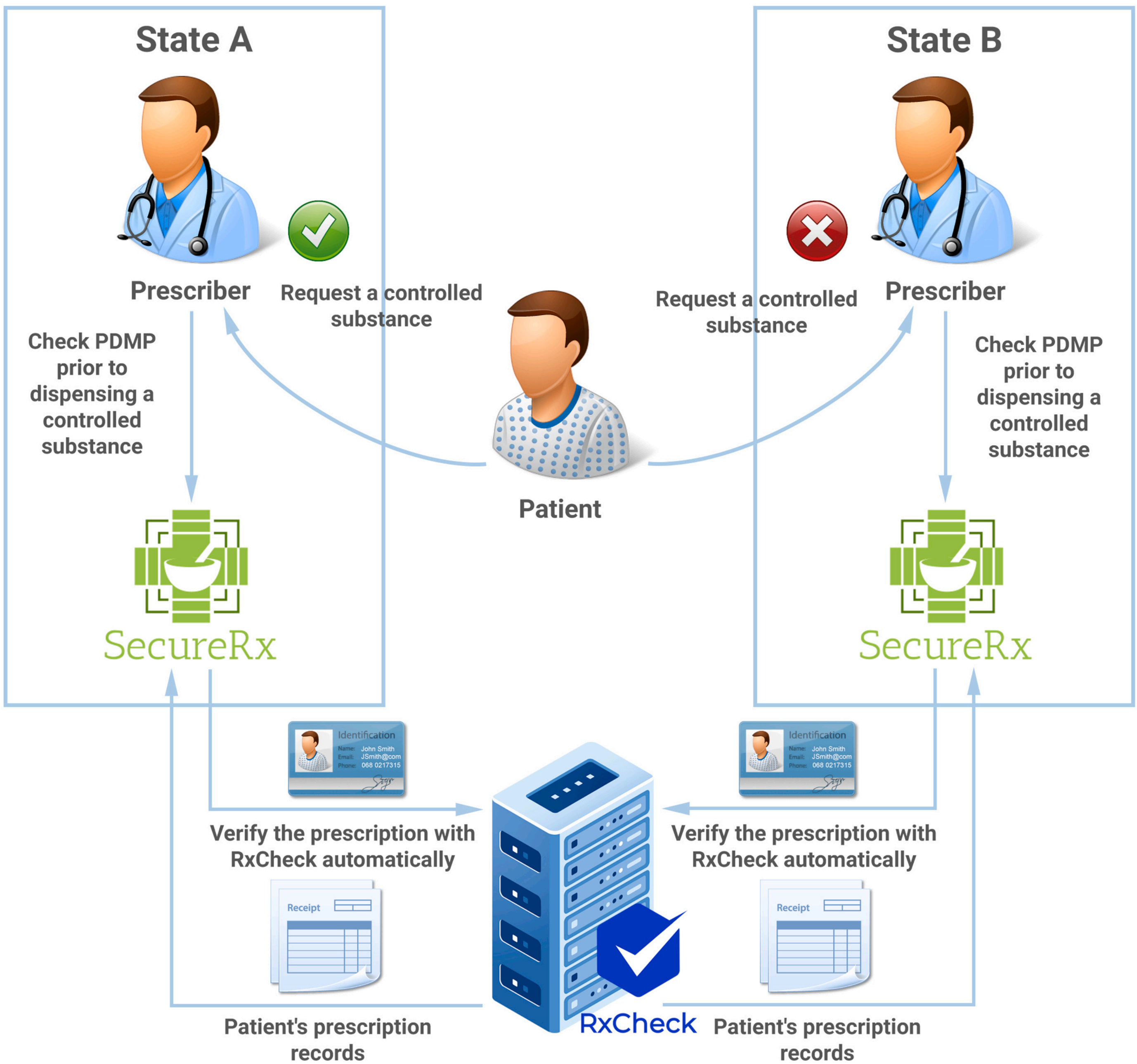

Fig. 5. SecureRx enforces checking RxCheck data before prescribing

Table 3
Execution Time and Throughput in a dataset of 100 transactions

Network size (number of nodes)	Execution time (seconds)	Throughput (transactions per second)
1	4.41	23
2	5.23	19
4	4.59	22
6	5.01	20
8	6.07	16
10	6.19	15

process. Accordingly, prescription tracking data is not often up-to-date. On the contrary, SecureRx enables near real-time updating of records across the entire chain. This approach offers a more feasible and efficient method for tracking prescriptions and preventing the misuse of opioids.

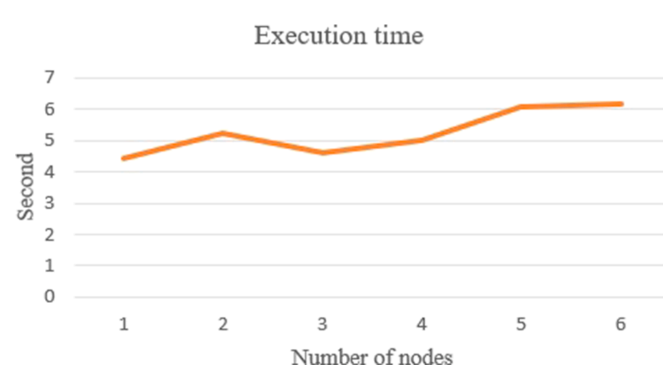

Fig. 6. Relationship between the number of nodes and execution time

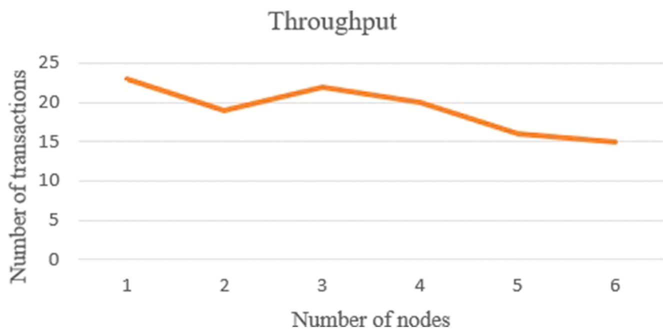

Fig. 7. Relationship between the number of nodes and throughput

Discussion

The proposed SecureRx framework focuses on addressing the limitations associated with the prescription drug monitoring program (PDMP) in the United States. It is based on blockchain technology that can allow stakeholders within the health care system to access prescription records of patients to influence policy and minimize prescription fraud. Most PDMPs today require health providers to submit data to a central agency to enable the updating of records. However, SecureRx automates this process because the records are updated as soon as the provider enters patient data in their local systems. In addition to eliminating the need for record submission, SecureRx enhances provider accountability in terms of ensuring that the transactions they sign off on are accurate. Since each transaction can be evaluated, providers are likely to be careful when prescribing opioids. Additionally, authorities can monitor each provider's rate of prescribing opioids to determine potential fraud. Furthermore, the system will provide incentives for providers to minimize prescribing opioids, which should foster safer prescription practices.

Although all the studies in the literature explored utilize blockchain technology to enable the secure sharing of medical data, only two studies focus specifically on drug prescription. Besides none of the studies adopts an active approach to the prevention of opioid and drug prevention abuse. Table 4 below compares the proposed SecureRx system to the other existing systems highlighted in the literature.

Table 4 above compares SecureRx with six other related solutions across five measures. As can be seen SecureRx is the only solution that satisfies the five measures: blockchain-based, drug prescription system, patient-centeredness, adoption of an active approach to the prevention of opioid and drug prescription, and integration with PDMP. MedRec [1], MeDShare[8], Ancile[9], FHIRChain[10], and Healthchain[11] are a blockchain-based medical solutions. However, they do not focus specifically on drug prescription, lack patient-centeredness, fail to prevent opioid and drug abuse actively, and do not integrate with PDMP. OpTrak [12] is the only solution that comes close to SecureRx as it is a drug prescription system based on blockchain, which integrates with PDMP. However, it lacks accommodations for ensuring patient-centeredness in terms of ensuring that the patient's beliefs and wants are incorporated into prescription decisions. Additionally, it fails to adopt an active approach to preventing opioid and drug prescription abuse.

While SecureRx is a promising solution for enhancing prescription drug surveillance and preventing opioid and drug abuse, it is based on technologies such as blockchain and smart contracts that are still in their early stages of development in the Ethereum community. Accordingly, the adoption of this solution depends on future advances resulting from the ongoing research. These advances will also enable acceptance of blockchain technology in legislations accompanying drug prescription and monitoring in the United States.

Future work

Future work should explore the practicality of SecureRx through case studies to establish the functionality of the solution in practical settings. The assessment of the solution ought to be performed using different performance metrics. Today, there is no clear methodology for evaluating blockchain platforms in terms of dimensions such as scalability, execution time, and latency in high workload situations. Having a standardized measurement system can introduce objectivity into the way blockchain solutions are evaluated. Future SecureRx evaluations must be thorough. To do so, workloads and nodes should be varied as the testing team observes outcomes such as throughput, scalability, execution time, and latency.

Future studies must also examine the feasibility of SecureRx as practicality determines the acceptance of the solution in practical health settings. Technological feasibility must be emphasized as the SecureRx should integrate with RxCheck and PDMP and produce or accept standardized data formats. From an administrative perspective, health care providers and administrators should find the system easy to utilize. Furthermore, incorporating monitoring and analysis capabilities, including prediction techniques, into SecureRx to identify patients who are susceptible to drug dependency proactively is an interesting research direction. The classification of patients using appropriate prediction methods should enable health providers to implement interventions to prevent opioid addiction.

Our framework demonstrates the potential of blockchain to foster effective prescription data sharing while maintaining the security of the original data sources. SecureRx can be further extended to address other healthcare interoperability issues. For example, it could be utilized to enhance coordination between health providers and insurance companies. It can also provide patients with easy and secure access to their prescription records. Moreover, there is potential for using it to offer identity management for stakeholders in the health care industry. Blockchain applications for identity management hold great promise but further research is needed.

Conclusions

Blockchain has revolutionized many sectors of the economy, with the record-keeping provision creating enormous value and disruption in the global marketplace. In the healthcare sector, blockchain has enabled elimination expensive middlemen, consequently removing outdated and unproductive cross-organizational processes. Additionally, the innovation has returned data ownership to the patients who are allowed to securely access their medical and prescription information [16].

One of the lessons from the process of designing and deploying the SecureRx framework for e-prescriptions entails the role of the decentralized and shared permission blockchain in enabling healthcare providers to access data banks without requiring approval from a

Table 4
Comparison between proposed system and other related systems

Metric	MedRec[1]	MeDShare[8]	Ancile[9]	FHIRChain[10]	Healthchain[11]	OpTrak[12]	SecureRx
Blockchain-based	Y	Y	Y	Y	Y	Y	Y
Drug Prescription System	N	N	N	N	N	Y	Y
Patient-centric prescription model	N	N	N	N	N	N	Y
Active approach to prevent opioid and drug prescription abuse	N	N	N	N	N	N	Y
Integration with PDMP	N	N	N	N	N	Y	Y

centralized administrator. The inclusion of decentralized data silo provides clinicians with some benefits that are missing in a centralized architecture [17]. For instance, the decentralized architecture avail a less costly, effective, and more secure approach for distributing drugs to patients. Additionally, stakeholders should leverage the high speed of the technology to efficiently track opioid prescriptions in real-time tracking as well as along the entire chain. This provision ensures an automatic update on each stakeholder's system in case a healthcare provider issues a prescription. This tactic offers a practical solution to tracking prescriptions to reduce cases of opioid abuse. Over-prescription of opioids is a highly likely without the real-time updates and the ability to track presented by the SecureRx framework.

The SecureRx framework has highlighted the potential of the record-keeping technology to nurture effective and efficient sharing of information about prescriptions while ensuring the safety and privacy of the original sources of the data. Patients can be assured regarding the confidentiality of their personal information while profiting from real-time tracking of their medical needs. The SecureRx framework can also be scaled and utilized in various other healthcare applications. For instance, the technology can assist in coordinating interoperability issues within the healthcare centers and link users of their services with insurance providers and other stakeholders in the industry [18]. Furthermore, the ambiguity in the information pertaining the healthcare sector is minimized through the help of the record-keeping system availed by the prototype. The application enables patients to easily and securely access their individual prescription records, reducing the time taken to attain the information. These features improve efficiency and healthcare outcomes for all stakeholders in the sector.

Funding

None.

Author contribution

None.

Declaration of Competing Interest

None.

References

[1] Ekblaw Ariel, et al. A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data. In: Proceedings of IEEE Open & Big Data Conference. 13; 2016.

[2] Wartell Julie, Vigne Nancy La. Prescription Drug Fraud and Misuse: 2nd Edition. Community Oriented Policing Services; 2013. https://popcenter.asu.edu/sites/default/files/problems/pdfs/prescription_fraud.pdf. Accessed 12 October 2020.

[3] Centers for Disease Control and Prevention, CDC. "Opioid Overdose: Overview". 2020, https://www.cdc.gov/drugoverdose/data/prescribing/overview.html. Accessed 10 October 2020.

[4] Sacco Lisa, Duff Johnathan H, Sarata Amanda K. Prescription Drug Monitoring Programs. Congressional Research Service; 2018. https://fas.org/sgp/crs/misc/R42593.pdf. Accessed 12 October 2020.

[5] The Prescription Drug Monitoring Program Training and Technical Assistance Center, PDMP TTAC. "RxCheck: A No-Cost Solution for Nationwide Prescription Drug Information Sharing". 2020, https://www.pdmpassist.org/RxCheck. Accessed 11 October 2020.

[6] Alogaili Fahd, Ghani Norjihan Abdul, Shah Nordiana Ahmad Kharman. Prescription drug monitoring programs in the U.S.: a systematic literature review on its strength and weakness. J. Infect. Public Health 2020.

[7] United States Government Accountability Office. "Prescription Drug Monitoring Programs: Views on Usefulness and Challenges of Programs". 2020, https://www.gao.gov/assets/710/709907.pdf. Accessed 11 October 2020.

[8] Xia QI, et al. MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. IEEE Access 2017;5:14757–67.

[9] Dagher Gaby G, et al. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustain. Cities Soc. 2018;39:283–97.

[10] Zhang Peng, White Jules, Schmidt Douglas C, Lenz Gunther, Trent Rosenbloom S. FHIRChain: Applying blockchain to securely and scalably share clinical data. Comput. Struct. Biotechnol. J. 2018;16:267–78.

[11] Xu Jie, et al. Healthchain: A blockchain-based privacy preserving scheme for large-scale health data. IEEE Internet of Things J. 2019;6(5):8770–81.

[12] Zhang Peng, Stodghill Breck, Pitt Cory, Briody Cavin, Schmidt Douglas C, White Jules, Pitt Alan, Aldrich Kelly. Optrak: Tracking opioid prescriptions via distributed ledger technology. Int. J. Inf. Syst. Social Change (IJISSC) 2019;10(2):45–61.

[13] Chen Jim Q, Benusa Allen. HIPAA security compliance challenges: The case for small healthcare providers. Int. J. Healthc. Manage. 2017;10(2):135–46.

[14] "United States dollar – Ethereum." Markets Insider, 21 Oct. 2020, markets.businessinsider.com/currencies/usd-eth.

[15] Total number of retail prescriptions filled annually in the United States from 2013 to 2025 (in billions). Statista 21 Oct. 2020. www.statista.com/statistics/261303/total-number-of-retail-prescriptions-filled-annually-in-the-us/.

[16] McGhin Thomas, et al. Blockchain in healthcare applications: Research challenges and opportunities. J. Netw. Comput. Appl. 2019;135:62–75.

[17] Hölbl Marko, et al. A systematic review of the use of blockchain in healthcare. Symmetry 2018;10(10):470.

[18] Bennett Brennan. Blockchain HIE overview: a framework for healthcare interoperability. Telehealth Med. Today 2018;2(3):110–25.