This is the preprint version. Please see ICICT for the final official version.

PharmaSys: Towards Preventing Prescription Misuse Using A HIPAA-Compliant Blockchain Protocol

Aaron H. Nguyen[1]*, Alex Lewtschuk[2]* James Lucas Durham[3]*, Peyton Lundquist[4], and Gaby G. Dagher[5]

San Jose State University, San Jose, CA 95192, USA
Marshall University, Huntington, WV 25755 USA
Boise State University, Boise, ID 83725
aaron.nguyen03@sjsu.edu, durham35@marshall.edu,
alexanderlewtsch@u.boisestate.edu, peytonlundquist@u.boisestate.edu,
gabydagher@boisestate.edu,

Abstract. Prescription drug misuse has become a major health crisis across the United States with prescription drug abuse skyrocketing during the 21st century resulting in classification as an epidemic. The rise in prescription misuse has resulted in negative consequences including heightened instances of overdose deaths, increased crime rate, and escalated healthcare expenditures. Although illegal sales contribute to the issue, a notable portion of prescription drugs stems from licensed medical professionals who engage in over-prescribing medications. To help combat this issue we propose PharmaSys, a novel multi-party blockchain system with a quorum-based consensus protocol that aims to prevent prescription misuse. PharmaSys achieves this by introducing and establishing a checks and balances system for prescription transactions, all while maintaining compliance with HIPAA regulations. PharmaSys consists of three distinct node types: prescribers, pharmacists, and patients; each of which execute unique functions within the system. We have implemented PharmaSys to illustrate our system's scalability and security.

Keywords: Blockchain; Prescription Tracking; Healthcare; HIPAA Compliance; Consensus Protocol; Drug Abuse; Proof of Sharding;

1 INTRODUCTION

Over the last two decades, drug abuse in the United States has posed a major societal issue that has grown at an alarming rate. The increase of improper drug use has led to countless lost lives, leaving families, friends, and communities devastated. In the United States, drug overdoses accounted for over 100,000 fatalities in 2021, a figure that demonstrates the urgent need for measures to mitigate the frequency of such preventable deaths [1]. The unfortunate truth is that not all of these deaths are a result of illegal sources; a significant portion can be traced back to prescription drugs dispensed by licensed medical practitioners

[2]. Drug misuse is defined as the use of medication in a manner inconsistent with the prescriber's directions. This includes taking someone else's prescription or taking medication to feel euphoric. A closer analysis reveals that the misuse of prescription drugs has left an impact on a wide array of demographics across the United States. A 2021 survey conducted by the U.S. Department of Health and Human Services reported more than 35 million instances of prescription drug misuse among individuals ages 12 and above. Prescription drugs involved in these instances included pain relievers such as oxycodone, codeine, and opioids, stimulants like Adderall and Ritalin, and sedatives including Xanax and Valium [3]. The repercussions of prescription drug abuse extend beyond individual impact and encompass the United States as a whole. According to a report issued by the U.S. Department of Health and Human Services, illicit drug use imposes an economic burden of $193 billion every year [4]. Concurrently, healthcare systems are heavily strained due to the extensive allocation of resources for treatment and rehabilitation of drug abuse victims. Furthermore, various societal consequences such as heightened crime rates and fractured family relationships create complex issues that require concerted efforts to address and minimize their impact [5] [6].

Prescription drug misuse presents an intricate problem due to the complex challenges faced by healthcare providers in creating the most fitting prescription and dosage for each patient. The process of formulating a prescription involves careful consideration of multiple patient-specific factors. These can include the patient's present medical condition, past health history, allergies, age, physiological state, and personal preferences or requests. In addition to the challenges involved in formulating a prescription that aligns with each patient's needs, healthcare providers often face external influences including potential incentives from pharmaceutical companies [7]. This conflict of interest may lead some doctors to alter their decisions by pushing out certain medications or more medications in general. In 2015, data from Open Payments, a publicly accessible database of payments from drug companies to physicians, revealed that 48% of physicians were reported to have received a total of $2.4 billion in industry-related payments [8]. This suggests that physician prescriptions are being affected by pharmaceutical-related interests, which could be a factor in the increase of drug abuse.

Despite this, even well-intentioned doctors tend to over prescribe medications to their patients. A study done in 2016 by the National Safety Council found that 99% of the doctors surveyed were prescribing highly addictive opiates for longer than the three-day period recommended by the Centers for Disease Control and Prevention [9]. This finding reveals the widespread prevalence of overprescribing practices in the healthcare industry, and highlights the urgent need for intervening and addressing the issue.

A concerning aspect of prescription drug misuse is the lack of accountability for doctors. Their decisions are often final, allowing them to prescribe drugs without any secondary opinions. Doctors typically aim for short-term improvements in patients' health, however they may overlook long-term implications of

drug abuse and prescribe more than they knowingly should. In addition, the absence of monitoring and accountability enables "pill mill" doctors, who are doctors that accept cash in return for written prescriptions, to engage in under-the-table practices without facing instant repercussions [10]. Consequently, due to overprescription these unneeded drugs may find their way onto the streets, posing a potential danger to society. Moreover, the surplus of medications may be exploited to fulfill individuals' desires for euphoria, further contributing to the cycle of misuse.

One of the challenges encountered in our solution is establishing the validation criteria for prescription transactions within the blockchain system. Unlike traditional blockchain systems that focus on verifying sufficient funds in the sending wallet, our system must verify the accuracy of dosage and appropriateness of the drug type in each prescription transaction. This validation process posed a significant challenge and required careful consideration. Furthermore, operating within the health industry introduces additional complexities, particularly concerning the handling of sensitive protected health information (PHI). The Health Insurance Portability and Accountability Act (HIPAA) imposes strict regulations and guidelines on the privacy and security of individuals' health records. Adhering to HIPAA regulations while ensuring seamless functionality presented an obstacle that required meticulous attention.

The current landscape of prescription drug solutions primarily revolves around the development of tracking and management systems. Tracking systems have been designed to establish transparency and accountability by leveraging blockchain technology to maintain an immutable record. Thus, any suspicious transaction will be recorded on the blockchain for others to see and potentially take action upon. On the other hand, management systems offer patient-provider confidentiality and help facilitate seamless data exchange by reinforcing the design of patient-owned data. Both of these solutions contribute to the overall enhancement of prescription drug practices, but do not aim to prevent it.

1.1 Contributions

The contributions of this paper are as follows:

1) We introduce PharmaSys, a blockchain-based prescription tracking system that aims towards prevention of drug misuse by creating a checks and balances system that allows for validation and tracking in a secure and scalable way.

2) We introduce *Proof of SHarding (PoSH)*, a novel quorum based consensus protocol that requires prescribers and pharmacists to review and vote on prescription transactions. Patients actively participate in staking which allocates their computational power for transaction verification through shard assignment.

3) We design PharmaSys to be HIPAA compliant by identifying and adhering to 14 HIPAA design principles relevant to prescription tracking.

4) We implemented PharmaSys using the open-source BlueChain network as a platform [11] . Our experimental results illustrate that our system maintains robustness in the presence of malicious nodes, and is scalable in relation to network size.

Table 1: Comparative Evaluation of Related Work

Title	Consensus	Eff.	Scal.	Inter.	HIPAA	Priv.	Sec.
Optrak	PoW	✓		✓			✓
FHIRChain	PoW	✓	✓	✓			✓
MedRec	PoW			✓			✓
SecureRx	PoS	✓		✓	✓	✓	✓
VigilRx	PoS	✓	✓	✓	✓		✓
Ancile	Quorum	✓	✓	✓	✓	✓	✓
ACCORD	Quorum		✓				✓
PharmaSys	Quorum		✓	✓	✓	✓	✓

2 Related Work

There have been several research papers addressing blockchain solutions, specifically in the healthcare industry [12] [13] [14] [15] [16] [17] [18]. Many of them dive into healthcare management systems looking to utilize blockchain smart contracts to manage and organize connections between parties. Others look to blockchain for its features of security and immutability for monitoring and tracking. [12] [13] [14] [15] [16] [17] [18]

Various systems leverage smart contracts to enhance security, efficiency, and validation [12] [14] [15] [16]. While certain models utilize these for prescription tracking, others propose applications such as comprehensive networks for Electronic Health Records (EHRs) or data management systems. All work can be narrowed down to three primary goals: efficiency, security, and validation.

Optrak [12] is an Ethereum-based DApp that enhances the tracking of distributed opioids through interoperability, secure authentication, control of personal information, and the automation of record submission. In comparison to Optrak we propose a solution toward preventing all prescription misuse instead of focusing on only opiates. VigilRx proposes a patient-centric solution with a primary emphasis on interoperability, scalability, and permissioned node types[16]. Both Optrak and VigilRx utilize smart contracts on the Ethereum network.

FHIRChain [13] is a blockchain based architecture that is designed for clinical data sharing across a wide range of health IT systems. Their proposed solution includes a DApp and the structure and functionality for their blockchain network.

MedRec [14] deals with utilizing Ethereum smart contracts to create intelligent copies of existing medical records stored in network nodes. They employ three smart contract types to achieve this functionality.

The solution proposed by SecureRx [15] proposes their solution by addresses the handling of raw healthcare data, utilizing blockchain technology in supply chain and data management aspects, and incentivizing stakeholders on the application. Important solutions proposed by SecureRx to solve this issue include drug provenance, a recall management system, and cloud storage.

Ancile [17] offers a solution designed to handle EHRs in compliance with HIPAA regulations, featuring innovative approaches to enhance privacy and interoperability. They also suggest a strategy to prevent node collusion on a permissioned network, thereby reducing technical challenges within a decentralized system.

In ACCORD [18] *G. D. Bashar et al* propose a scalable consensus mechanism utilizing a group of leaders to distribute responsibilities to multiple quorum members. This new mechanism is proposed to avoid fork conflicts and each block must be asynchronously signed by a majority of network nodes before acceptance to the chain.

3 Preliminaries

3.1 HIPAA

The protection of patient health information is a constant priority in healthcare — it ensures patient privacy, builds trust with healthcare providers, and safeguards sensitive data from unauthorized access. In recognition of this crucial aspect of healthcare, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) was adopted to establish national standards for the privacy and security of sensitive PHI of patients. This act applies to all covered entities. Defined by HIPAA, covered entities are health plans, healthcare clearinghouses, and healthcare providers who electronically manage any health information [19]. HIPAA addresses everything from unauthorized access; and data breaches, to identity theft in the healthcare sector. Compliance with HIPAA regulations fosters a culture of accountability among healthcare providers, increasing patients' confidence that their health information is being handled properly.

3.2 Blockchain

The concept of blockchain in it's modern use case was introduced in 2008 with the publication of a whitepaper titled "Bitcoin: A Peer-to-Peer Electronic Cash System" by Satoshi Nakamoto [20]. The whitepaper outlined the theory of a decentralized digital currency, Bitcoin, and introduced blockchain's first practical application that would enable secure and transparent transactions without the need for intermediaries. In 2009, the implementation of the Bitcoin network was subsequently developed and launched.

3.3 Quorum-based Consensus

Quorum-based consensus has emerged as a popular mechanism for achieving concurrence among a select number of nodes in a distributed system. In this protocol, a specific number of nodes are selected, known as the quorum, to participate in the validation process of transactions. The process of quorum selection can vary significantly, quorum members can be chosen based on randomness, reputation, stake, and/or other factors.

An essential consideration in the design of any consensus protocol is fault tolerance, which refers to the system's integrity when facing malicious behavior. Often based on the principles of Byzantine fault tolerance (BFT), it is typically assumed that a quorum consensus can tolerate up to 33% faulty nodes on the network. Thus, if the amount of malicious nodes exceed this number, the system can not guarantee consistent agreement on decisions.

Quorum-based consensus also offers key features of scalability and performance. Based on the specific requirements of the system, quorum size can be adjusted, allowing for efficient scaling as participants increase. By electing only a subset of nodes for the decision-making process, the system can achieve faster consensus times and lower communication overhead, enhancing the overall performance of the system.

3.4 BlueChain

BlueChain [11], a distributed and decentralized blockchain network, operates as a research framework. Developed in Java, this network utilizes a quorum-based consensus and enables facilitating the creation of test environments with ease [11]. The system, developed at Boise State University by Peyton Lundquist, provides a solid foundation for implementation. We chose to build upon the BlueChain framework due to its ability to be rapidly modified and enable experimentation with our proposed innovations.

4 HIPAA DESIGN PRINCIPLES

HIPAA compliance is a critical aspect for any entity operating in the healthcare sector. In our endeavor to adhere to HIPAA regulations, we have conducted a comprehensive analysis of the regulation and identified a set of rules our blockchain system complies with, as shown in Table **??**. This table will later be referenced through citation blocks to indicate the exact rule/rules the design principle abides by.

5 SOLUTION: PharmaSys

5.1 Solution Overview

PharmaSys is a prescription tracking system, implementing a novel three party quorum-based consensus protocol, PoSH, that works towards preventing malicious prescriptions while conforming to HIPAA regulations. Our system utilizes role based nodes that define the actions undertaken in the system, as shown in Figure 1. Each group has differing permissions and capabilities. Prescribers and pharmacists will verify the authenticity of prescriptions and push work out to patients "staked" in the system. PharmaSys provides a solution where nodes can work cohesively while providing incentive to all parties involved.

HDP#	Rule	Description
HDP1	Privacy (Right of Access)	An individual has a right of access to inspect and obtain a copy of protected health information about the individual
HDP2	Privacy (Right of Access, Timely Action)	The covered entity must act on a request for access no later than 30 days after receipt of the request.
HDP3	Privacy (Right of Access, Manner of Access)	If an individual's request for access directs the covered entity to transmit the copy of protected health information directly to another person designated by the individual, the covered entity must provide the copy to the person designated by the individual.
HDP4	Privacy (Effect of Prior Authorizations)	A covered entity may use or disclose protected health information pursuant to an authorization or other express legal permission obtained from an individual
HDP5	Privacy (De-identification Of Protected Health Information)	Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual.
HDP6	Security (Access Authorization)	Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.
HDP7	Security (Access Control)	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those that have been granted access rights.
HDP8	Security (Audit Control)	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.
HDP9	Security (Integrity Controls)	Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.
HDP10	Security (Encryption And Decryption)	Implement a mechanism to encrypt and decrypt electronic protected health information.
HDP11	Security (Transmission)	Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.
HDP12	Security (Protection From Malicious Software)	Procedures for guarding against, detecting, and reporting malicious software.
HDP13	Security (Unique User Identification)	Assign a unique name and/or number for identifying and tracking user identity.
HDP14	Security (Data Backup Plan)	Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

Table 2: Here we propose HIPAA 14, which represents 14 HIPAA rules/standards that our system is compliant with.

5.2 PharmaSys Blockchain

As a decentralized blockchain system, our platform inherits essential properties of blockchain technology and employs other factors that compliment it. These properties encompass a wide range of benefits, including but not limited to enhanced security, improved efficiency, and increased interoperability.

Utilizing blockchain technology provides numerous security advantages. Firstly, patient prescription information on the chain will be encrypted, ensuring that unauthorized individuals cannot access them [HDP6, HDP10]. Permissioned access is required for anyone wanting to view information, addressing concerns related to data vulnerabilities. Unlike centralized systems, the decentralized nature of blockchain eliminates the reliance on a single authority for decision-making. This prevents tampering incidents, as any attempts to modify the data would be detectable due to the resulting hash being altered [HDP9]. Inconsistencies between blocks and their references to previous blocks would be easily discernible, which maintains the integrity and immutability of the information stored on the blockchain.

Our system places significant emphasis in safeguarding against malicious activities. By adopting a quorum consensus mechanism, we preserve the system's integrity by effectively mitigating the tampering attempts by individual malicious nodes. Within our system, a quorum is established, capable of withstanding up to 33% malicious nodes present on the network [HDP12]. This robustness ensures the maintenance of system integrity, fortifying the overall security measures employed.

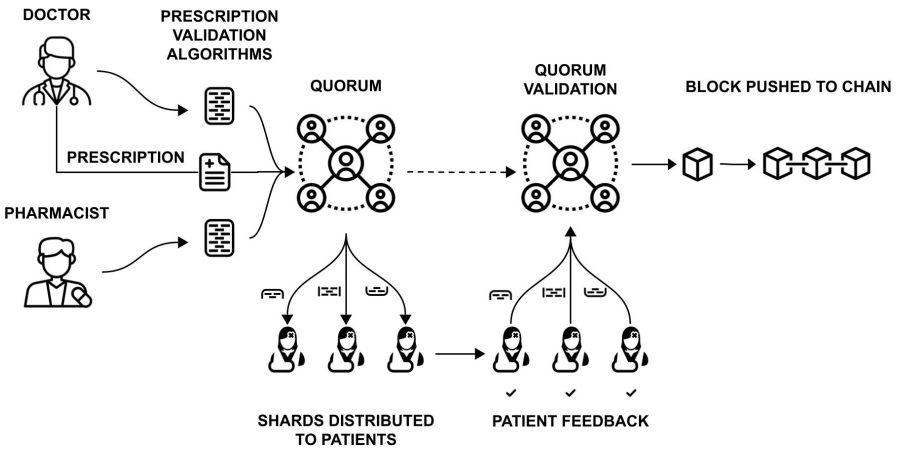

Fig. 1: An overview of the transaction validation process in PharmaSys.

Additionally, our design addresses the creation of unique identifiers to accurately identify and track user identity by generating a random hash for a user username [HDP13]. This requirement, mandatory for all covered entities, helps mitigate misidentification risks during healthcare transactions. Our system then hashes it to create a public address. Using SHA-256's preimage and collision resistance, each user identification is unique. By implementing this user identification measure, covered entities can mitigate the risk of mixing up individuals' identities and ensure the accuracy and integrity of health-related transactions.

Moreover, the decentralization of our system serves as a solution for the challenges associated with lost or inaccessible data during emergency situations [HDP14]. In our system, prescribers and pharmacists assume the role of full nodes, thereby possessing a complete copy of the entire ledger. Consequently, in the event of multiple faulty nodes we can rely on others to uphold the integrity and functionality of the chain.

In our system, a patient-centric approach is implemented wherein patients have direct ownership of their prescription data and can access it through the blockchain [HDP1]. This innovative approach eliminates the need of sending health information requests to intermediates, consequently cutting the time to receive transactions. In traditional systems, healthcare providers may take up to 30 days to fulfill information requests [HDP2], but with our system, patients can swiftly access and review their data within a matter of seconds. With the decentralized nature of blockchain, patients have full control over their data, allowing for faster and more efficient access.

With patients now assuming responsibility for their data, they possess complete control over the sharing and management of authorizations. They have

the authority to determine who can access their data and can grant permission to requesting prescribers accordingly [HDP6]. Furthermore, patients retain the ability to revoke permissions from prescribers once the visit or engagement has concluded, maintaining constant control over their PHI [HDP7]. This patient-driven approach empowers individuals by affording them autonomy in managing the authorization and access to their own healthcare information.

An additional aspect of our system pertains to a patient's power to send a copy of their PHI directly to a designated third party [HDP3]. In this process the individual must provide their digital signature to confirm that this action was made by them [HDP11]. By providing their digital signature, which can only be obtained from their secret key, patients can control permissions and share their prescription data to desired individuals [HDP6, HDP7]. This design ensures that any node lacking the requisite authorization or permission will be effectively restricted from accessing encrypted data [HDP10].

5.3 Node Types

In contrast to most blockchains, our system implements distinct node categories. The purpose behind this categorization is to grant specific permissions upon each node type, as represented in Figure 2. The arrangement of our system entails the division of nodes into three types: prescribers, pharmacists, and patients.

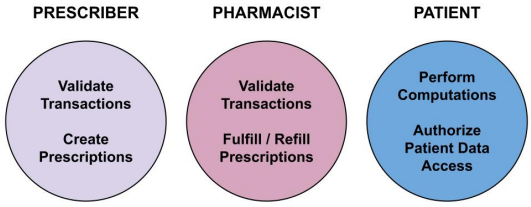

Fig. 2: The three parties within our system.

Prescribers In PharmaSys, prescribers bear the responsibility of pushing out prescription transactions, creating their algorithm, reviewing other prescribers' prescriptions, and requesting permission for patient prescription history. Prescriber nodes have the unique capability to initiate and submit prescription transactions, streamlining the essential process between prescribers and patients. It is imperative that every prescriber creates and initializes their unique algorithm to the blockchain as this will be used in the future by other nodes. Additionally, prescriber nodes are part of the selection pool for quorums that review

other prescribers' prescription transactions. In this process, their algorithm will be referenced to gather information from the blockchain to assist in devising an informed decision. Considering the decentralized nature of our blockchain, prescribers seeking access to a patient's prescription history must send a request to the patient's address and obtain their approval before gaining access [HDP4, HDP6].

Pharmacist Similar to prescriber nodes, pharmacists design their distinct algorithm and are eligible for quorum selection. However, unlike prescribers, pharmacists do not have the authority to initiate prescription transactions. Instead, their role lies in filling and refill transactions for prescriptions that have already been issued and validated. Upon verifying that a patient has picked up their prescribed medication, pharmacists will generate a filling transaction, tracking that the prescription is now in patient hands. Pharmacists also initiate refill transactions when authorized by a prescriber which, after quorum consensus, is appended to the original prescription transaction on the blockchain.

Patient A significant power patients wield is the authority to grant or refuse incoming permission requests on their prescription data, as well as the ability to manage existing permissions [HDP6, HDP7]. Every time patient information is accessed, it will be logged onto the blockchain [HDP8]. Their primary responsibility in the system lies in actively seeking and fulfilling delegated tasks distributed by quorum members, thus assisting the quorum in reaching informed decisions. Upon completing their respective computational tasks, patients return the output to the corresponding quorum member who sent out the task.

5.4 Transactions

Within PharmaSys, a diverse range of transactions are integrated. Specific to the medical industry, various interactions exist between these involved parties such as prescription creation, prescription fulfillment, and permission controls. As mentioned previously, the ability or restriction to perform these specific actions is contingent upon the node's corresponding type.

Transaction Types This network facilitates four types of transactions: prescriptions, prescription fulfillment and refills, and permissions. The transactions within our system govern the relationships between nodes, with some transactions requiring a quorum vote while others do not.

Prescription transactions involve the participation of all three parties: patients, prescribers, and pharmacists. The prescriber initiates the process by generating a prescription for the patient, which is subjected to approval from a quorum. Following the approval, the prescription is then transmitted to the pharmacists. Through this collaborative workflow, the prescriber prescribes the medication to the patient, the pharmacist receives the prescription details, and the patient can pick up their prescribed medication at the designated location.

Prescription fulfillment transactions exclusively pertain to the dispensation of medication by pharmacists to patients. These transactions are initiated by the pharmacist nodes after the patient picks up their prescribed medication.

Lastly, permission transactions occur between medical professionals to patients, where the patients possess the authority to accept or reject the permission.

Prescription Transaction Validation Upon pushing a desired prescription transaction to the mempool, a quorum comprised of prescribers and pharmacists is formed to validate the transaction. It is crucial to note that only nodes representing prescribers and pharmacists are eligible to participate in this quorum. Each medical professional possesses their own opinion that corresponds to the unique algorithm they use to determine the accuracy of the transaction. If a majority agreement of over 50% is reached within the quorum, the transaction proceeds and is appended to the blockchain as a successful transaction. Conversely, should the prescription fail to secure approval from the quorum, it will be added to the blockchain as a failed transaction, ensuring its recording on the ledger. Under such circumstances, the prescriber shall receive a notification and may proceed to modify the prescription details for re-submission.

5.5 Quorum Consensus

Employing a quorum serves the dual purpose of maintaining the integrity and optimizing the efficiency of our system. By randomly selecting a subset of prescriber and pharmacist nodes to use their unique algorithms to review transactions, a balance between system reliability and resource consumption is obtained. Based on Byzantine Fault Tolerance principles, our system reliability can be measured in accordance to its tolerate of up to 33% malicious nodes on the network [HDP12]. Furthermore, we incorporate patient nodes into part of the quorum mechanics by crowd-sourcing their computational power. To leverage this power, we shard each quorum member's algorithm and delegate the tasks to multiple patients.

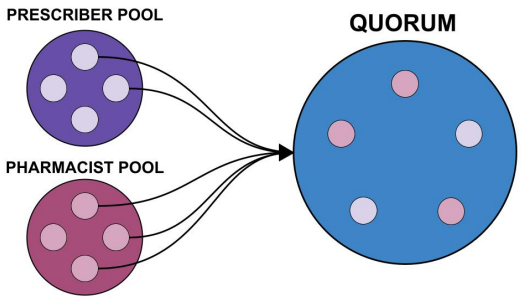

Fig. 3: Quorum Derivation.

Deriving the Quorum The formation of our quorum involves the random selection of nodes from pools of prescribers and pharmacists, as illustrated in Figure 3. Each node within the pool has an equal opportunity of being elected into the quorum, as we do not consider any additional factors such as years of experience or past quorum selection. To ensure consensus across the blockchain regarding the composition of the quorum, we utilize the hash of the most recent block as a seed for the random generator. This method guarantees agreement and consistency throughout the network regarding the nodes that compose the quorum. By incorporating an unbiased random selection process, our system promotes fairness and equal participation among prescribers and pharmacists, enhancing the integrity and credibility of the decision-making process [HDP12].

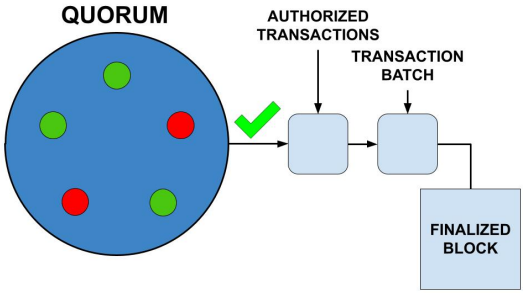

Fig. 4: Quorum Decision.

Decision Making Each medical practitioner has their own cognitive process when evaluating a prescription, which can be encapsulated through their unique algorithm. This algorithm can be a comprised of a variety of factors pertaining to the prescriber initiating the transaction such as their age, years of experience, recent prescription volume, etc. Naturally in our system, any patient-related information is de-identified, eliminating personal details and rendering it untraceable to the originating patient [HDP5]. To gather this information from the blockchain, quorum members shard their algorithm into segments and disseminate them to a mempool. Then, a patient will eventually undertake the tasks, complete them, and provide their responses. Based on the received information, the quorum member will arrive at a conclusive "yes" or "no" decision and cast their vote to the quorum, as exemplified in Figure 4.

5.6 The Sharding Algorithm

Within our system, each quorum member's algorithm is divided into shards with each shard being processed by two different patients, shown in Figure 5. Through incentives, we are able to harness the computational power of patients.

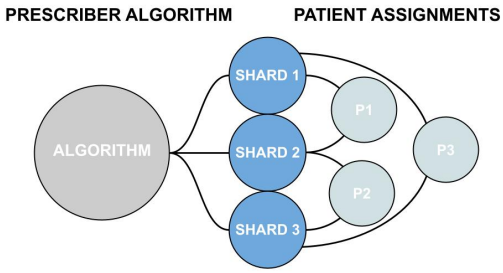

Fig. 5: Sharding process for an algorithm with three shards demonstrating how two patients are assigned to each shard.

This approach can be broken into distinct steps: algorithm distribution, answer confirmation, and returning results.

Algorithm Distribution The quorum members will transmit their respective individual algorithms to a mempool, where patients will have access to them. These algorithms may be sharded into multiple pieces to accommodate different preferences. For instance, one medical professional might consider only three factors when making a decision, while another might weigh five factors. Regardless, there will always be n patients actively engaged in solving an algorithm, where n represents the number of algorithm shards. Each patient will process two algorithm shards, and every shard will be assigned to two different patients.

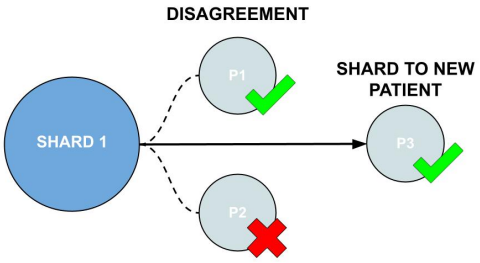

Fig. 6: Process during disagreement with original assigned patient nodes. Conflicting answers result in reassignment to a new patient node.

Answer Confirmation If these two patients produce identical results for a given computation, it is treated as correct. However, in cases where the answers do not match, the algorithm is automatically and randomly assigned to a third

patient for processing. As demonstrated in Figure 6, the correct answer is determined based on the match between the third patient's result and either of the previous two answers. However, in the event that the third patient's result does not match either of the previous answers, a redraw process ensues. This process continues until two matching answers are obtained, ensuring the identification of the correct answer through consensus among multiple patients. In instances where a patient provides an incorrect answer, appropriate measures are taken to enforce accountability. This approach effectively prevents patients from evading their responsibilities and submitting a random answer, while simultaneously minimizing the workload required to complete the assigned tasks.

Returning Results Following the completion of these tasks, the patient nodes return the computed results to the respective quorum member whose algorithms they solved. Once a quorum member receives all the computations of their algorithm from the patient nodes, they will have the necessary information to make a decision. By consolidating the returned parts of the algorithm, the medical professional gains an overview of the data, enabling them to properly analyze the information and formulate their decision.

5.7 Block Construction

Based on the quorum's decision, the transaction is added to the blockchain as either a successful or failed transaction, ensuring a record of the prescriber's actions, irrespective of the outcome. Subsequently, this information is propagated across the network to every full node.

6 Experimental Evaluation

6.1 Implementation

We implemented our proposed system for the purpose of testing efficiency and scalability. Our system focused primarily on the creation of a new use case inside the existing codebase of BlueChain gutting and optimizing the code for our system. Our implementation was written entirely in Java as well as moderate amounts of shell script for automation and Python for experiment data handling and visualization. In each simulation of a prescription transaction stakeholders perform their relevant actions as designated by their node type. Patients access algorithms and are assigned to shards, perform necessary computations, and return results to requesting quorum members. Prescribers push out prescription transactions, act as validators, and push their algorithms. Pharmacists validate transactions, and push their algorithms to the chain as well. Each stakeholder completes all actions as they are designed to in each transaction cycle after prescription transactions are pushed to the network.

6.2 Testing Environment

The system used for our experiments contained a 3.4 GHz Intel I7-6700CPU, a NVIDIA Quadro M400 GPU, 32GB of 2133 MHz DDR4 RAM, and a 512GB PCIe SSD running Windows 10. The Virtual Machine (VM) ran Ubuntu 22.04 LTS. The VM had 24GB of RAM with a 25GB VHDD, and 5 cores of CPU utilization that ran Maven V3.9.3 and Java 20 SDK dependency for execution of our system. BlueChain was designed to utilize Apache Maven as a management tool for compilation and a unified build system for all file dependencies. The client linking into the PharmaSys network was custom built for each client instance to act as one account on the network.

Setup In our research, we utilized the PharmaSys config.properties file to facilitate the setup of the system for simulations. This file enabled us to define and allocate attributes such as network size, the number of quorum members, and other essential settings that the network would have upon initialization. The PharmaSys system was executed on a local network within the testing environment using a VM. Node creation commenced from port 8000 and the defined minimum and maximum connection sizes between nodes was 4 and 7. Under this system configuration we conducted a comprehensive evaluation of the PharmaSys system in terms of scalability and robustness.

Limitations During testing we had some limitations for the network. Our limitation was mainly the VM that we were running the experiments through. This can be attributed to the computational limitations imposed by operating through a VM. The way that Virtual Box stores the guest operating system's files also affects the speed of the system, as all guest files, including PharmaSys files and dependencies are stored on a virtual hard drive. Virtual hard disks are less efficient compared to utilizing the system's hard disk, even on more powerful computers.

6.3 Scalability

Our primary objective during scalability testing was to document various stages of our transaction process. These stages consisted of quorum formation, quorum decision, block construction, and network communication. During our scalability test, we set up the network with 7 quorum members and incrementally increased the network size from 100 to 500 nodes in steps of 100 for each data recording iteration. Throughout each of these iterations, we executed 50 transactions, recorded their individual times, and calculated the average duration. In the testing design, we also measured the client's response time alongside the in-network processing time.

According to the data shown in Table 3, as our network size increases, the total network time decreases. With a mere 0.22015615-second difference observed between large and small network sizes, our transaction consensus time slightly

Table 3: This table depicts the observed outcomes at various stages of the transaction consensus from the conducted experiments.

Network Size	Quorum Formation	Quorum Decision	Block Construction	Total Network Time
100	0.00011329	4.03305100	0.00026780	4.03382640
200	0.00016470	4.08861959	0.00031734	4.08942926
300	0.00012304	3.91122543	0.00025875	3.91177063
400	0.00016594	3.87454129	0.00027795	3.87889664
500	0.00012681	3.86846344	0.00029122	3.87029214

improves. This phenomenon can be attributed to the expansion of the patient selection pool available for doctor or pharmacist nodes to appoint as sub-quorum members. The quorum decision step is the most intensive process, accounting for a majority of time in the transaction consensus. This process includes sharding to patients, patient computation and result return, and quorum agreement.

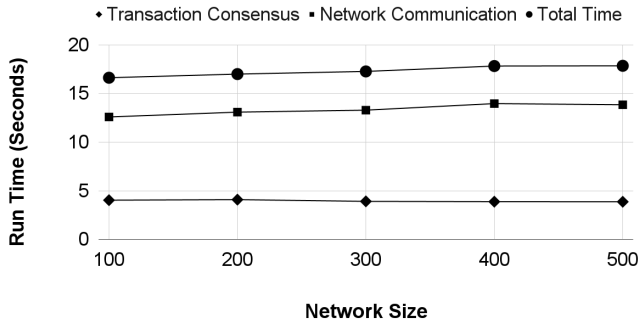

Fig. 7: A graphic comparison depicting the scalability of consensus time and network communication time.

Figure 7 demonstrates a linear rise in total transaction time as the network size expands, mainly influenced by network communication, which significantly contributes to the overall transaction time. As previously shown in Table 3, the time for transaction consensus ever so slightly decreases as the network size increases. Thus, the only contributing factor to the linear increase in total transaction time is the network communication. It is crucial to highlight that the data in both Table 3 and Figure 7 were generated simultaneously.

6.4 Robustness

Our main goal during Robustness testing was to detect malicious sub-quorums, which we defined as a sub-quorum comprised of more than 50% malicious pa-

tient nodes. Naturally, the presence of a malicious sub-quorum could result in a medical professional making a misinformed decision. To assess the accuracy of an individual quorum member's decisions, we simulated tests by purposely poisoning our network.

In this experimental study, our system was configured with 100 patient nodes and 7 quorum members. Each quorum member randomly sharded their algorithm into a range of 3 to 7 shards which were assigned to patients for data retrieval. Throughout the experiment, we progressively increased the percentage of malicious nodes from 10% to 50%, in 10% increments. During this process, we meticulously recorded the occurrences of malicious sub-quorums. With this data, we were able to determine the percentage of properly informed quorum members, which led to true-positive and true-negative responses.

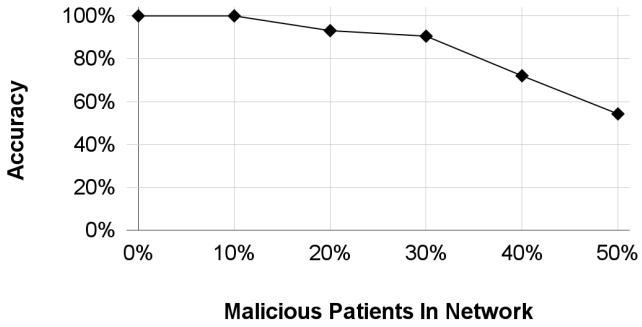

Fig. 8: A graphical representation illustrating the correlation between the accuracy of an individual quorum member's decision and the percentage of malicious patient nodes.

Figure 8 illustrates that our system maintains 90 percent accuracy with up to 30 percent malicious nodes in our network. The experimental findings can be significantly enhanced by considering the binomial probability of the quorum consensus producing inaccurate results. Presently, the graphical representation mainly focuses on the individual doctor's probabilities of true-positive or true-negative outcomes. To address this, we utilized Algorithm 1 to assess the possibility of a majority of the quorum being misinformed. However, an alternative approach could be adopted to visually represent the probability of the entire quorum generating an accurate response. Implementing this modification would greatly increase the likelihood of obtaining correct answers from the quorum as a cohesive unit.

Algorithm 1 Binomial Probability Calculation

Require: n = number of patients
Require: k = number of successes
Require: p = probability of success
Ensure: $P(X = k)$
1: Calculate binomial coefficient $C(n,k) = \frac{n!}{k!(n-k)!}$
2: Calculate binomial probability $P(X = k) = C(n,k) * (p^k) * ((1-p)^{(n-k)})$
3: **return** X

7 Conclusion & Future Work

In this paper, we sought to design a blockchain system that tracks prescriptions through the use of a novel multi-node consensus mechanism while following HIPAA guidelines for the handling of PHI. The implementation of PharmaSys system in experimentation illustrates its ability to be scalable and to remain robust and trustworthy even with large amounts of malicious nodes. Integrated large scale, PharmaSys would help alleviate data siloing, increase interoperability, improve cross-healthcare communications, and promote transparency and audibility of drug tracking on the blockchain. Each stakeholder in the system provides their unique services to other nodes and keeps the network functioning in a fluid manner. PharmaSys lays the foundation for future work on blockchains designed for prescription tracking as well as systems designed to handle the data in the chain. Utilization of the data could help provide further benefit towards ensuring accurate prescription monitoring, and combating prescription drug misuse. There is possibility that the work established in PharmaSys could be built upon by utilizing machine learning. Neural networks could be used to analyze and leverage the data in the chain and the available information used to uncover patterns and gain insights into practices, medication flow, and patient treatment adherence amongst others. Future work in this area could allow researchers to develop new methods of predicting surges in drug misuse or the flagging of prescribers acting maliciously.

ACKNOWLEDGMENT

Acknowledgment for icons used in diagrams: Blockchain by Adrien Coquet, Algorithm by Sachin Modgekar, Doctor by Iconfield, Group by Pause08, Patient by Wilson Joseph, Pharmacist by Andi Nur Abdillah, Prescription by Sergey Demushkin, Check by Numero Uno from Noun Project.

Bibliography

[1] National Institute on Drug Abuse, "Drug Overdose Death Rates," https://nida.nih.gov/research-topics/trends-statistics/overdose-death-rates, 2014.

[2] Centers for Disease Control and Prevention, "Physicians are a leading source of prescription opioids for the highest-risk users," https://www.cdc.gov/media/releases/2014/p0303-prescription-opioids.html, 2014.

[3] National Institute on Drug Abuse, "What is the scope of prescription drug misuse in the united states?" https://nida.nih.gov/publications/research-reports/misuse-prescription-drugs/what-scope-prescription-drug-misuse, Feb 2023.

[4] Office of the Surgeon General, "Addiction and substance misuse reports and publications," https://www.hhs.gov/surgeongeneral/reports-and-publications/addiction-and-substance-misuse/index.html, Mar 2023.

[5] D. C. Daley, "Family and social aspects of substance use disorders and treatment," *Journal of Food and Drug Analysis*, vol. 21, no. 4, 2013.

[6] M. Pierce, K. Hayhurst, S. M. Bird, M. Hickman, T. Seddon, G. Dunn, and T. Millar, "Insights into the link between drug use and criminality: Lifetime offending of criminally-active opiate users," *Drug and Alcohol Dependence*, vol. 179, p. 309–316, 2017.

[7] A. P. Mitchell, N. U. Trivedi, R. L. Gennarelli, S. Chimonas, S. M. Tabatabai, J. Goldberg, L. A. Diaz, and D. Korenstein, "Are financial payments from the pharmaceutical industry associated with physician prescribing?" *Annals of Internal Medicine*, vol. 174, no. 3, p. 353–361, 2021.

[8] K. R. Tringale, D. Marshall, T. K. Mackey, M. Connor, J. D. Murphy, and J. A. Hattangadi-Gluth, "Types and distribution of payments from industry to physicians in 2015," *JAMA*, vol. 317, no. 17, p. 1774, 2017.

[9] D. Teater, "Doctor-opioid-survey-national-safety-council," https://www.insurancejournal.com/research/research/national-safety-council-survey-of-doctors-prescribing-opioids/, Mar 2016.

[10] R. Hirsch, "The opioid epidemic: It's time to place blame where it belongs," *Missouri Medicine*, vol. 114, no. 2, pp. 82–83–90, Mar 2017.

[11] P. Lundquist and G. G. Dagher, "Bluechain," ISPM Research Lab, 2023. [Online]. Available: https://github.com/peytonlundquist/BlueChain

[12] P. Zhang, B. Stodghill, C. Pitt, C. Briody, D. Schmidt, J. White, A. Pitt, and K. Aldrich, *OpTrak: Tracking Opioid Prescriptions via Distributed Ledger Technology*, 01 2020, pp. 103–123.

[13] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, "Fhirchain: Applying blockchain to securely and scalably share clinical data," *Computational and Structural Biotechnology Journal*, vol. 16, pp.

267–278, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2001037018300370

[14] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," pp. 25–30, 2016.

[15] M. Alnafrani and S. Acharya, "Securerx: A blockchain-based framework for an electronic prescription system with opioids tracking," *Health Policy and Technology*, vol. 10, no. 2, p. 100510, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2211883721000332

[16] A. Taylor, A. Kugler, P. B. Marella, and G. G. Dagher, "Vigilrx: A scalable and interoperable prescription management system using blockchain," *IEEE Access*, vol. 10, pp. 25 973–25 986, 2022.

[17] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustainable Cities and Society*, vol. 39, pp. 283–297, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2210670717310685

[18] G. D. Bashar, J. Holmes, and G. G. Dagher, "Accord: A scalable multileader consensus protocol for healthcare blockchain," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 2990–3005, 2022.

[19] A. Dabrant and H. O. of Civil Rights, "Hipaa administrative simplification - hhs.gov," Mar 2013. [Online]. Available: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf

[20] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *bitcoin.org*, 2009. [Online]. Available: http://www.bitcoin.org/bitcoin.pdf