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

Information and Communication Technology (ICICT), 2024


Aaron Nguyen


Luke Durham


Alex Lewtschuk


Peyton Lundquist


Gaby Dagher

February 21-22, 2024

BOISE STATE UNIVERSITY

MARSHALL

BOISE STATE UNIVERSITY

Table of Contents

INTRODUCTION

Motivation

- Over the last two decades, drug abuse in the United States has posed a major societal issue that has grown at an alarming rate.
- In 2021, the United States suffered over 100,000 fatalities due to drug overdoses. [6]
- 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. [7]

Challenges

- Defining an “accurate” prescription
- HIPAA Compliance
- Implementation into BlueChain

The Problem We Address

The healthcare system needs a platform that:

- Empowers individuals through patient-owned data
- Keeps an immutable record of prescription data
- Works towards preventing mis-prescription by doctors

Contributions

- The PharmaSys system
- A HIPPA-Compliant prescription tracking blockchain
- Proof of SHaring (PoSH)
- Implementation and experimental tests on scalability and robustness

RELATED WORK

Medical Blockchain Solutions

- Ancile [5]
  - Handle EHRs maintaining HIPPA-compliance
- ACCORD [3]
  - consensus mechanism utilizing a group of leaders to distribute responsibilities
- SecureRx [1]
  - Drug provenance, recall management system, and cloud storage

Prescription Tracking Blockchain Solutions

- VigilRx [8]
  - Patient-centric solution with focus on interoperability between parties
- Optrak [9]
  - DApp enhances opioid tracking distribution
- FHIRChain [10]
  - Architecture of prescription tracking network
- MedRec [2]
  - Introduce SC deployment for 3 stakeholders
  - Record system for medical records

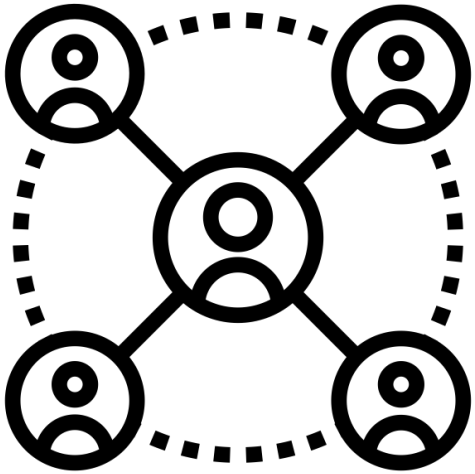
BACKGROUND

HIPAA

Security & Privacy

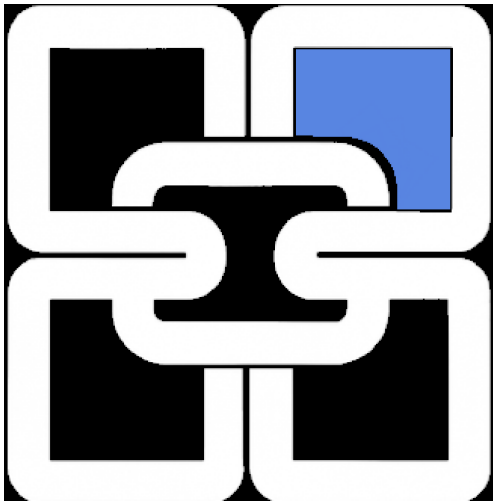
- Federal regulations for Private Health Information (PHI)
- Covered entities are health plans, healthcare clearinghouses, and healthcare providers who electronically manage any health information [4]

Quorum-based Consensus



- Select nodes participate in block validation
- Can be chosen based on a variety of factors
- Can tolerate up to 33% faulty nodes in the network

BlueChain



- Research framework developed in Java at Boise State University by Peyton Lundquist
- Utilizes quorum consensus and can facilitate faster development times
- Utilized as the code base for PharmaSys

SOLUTION

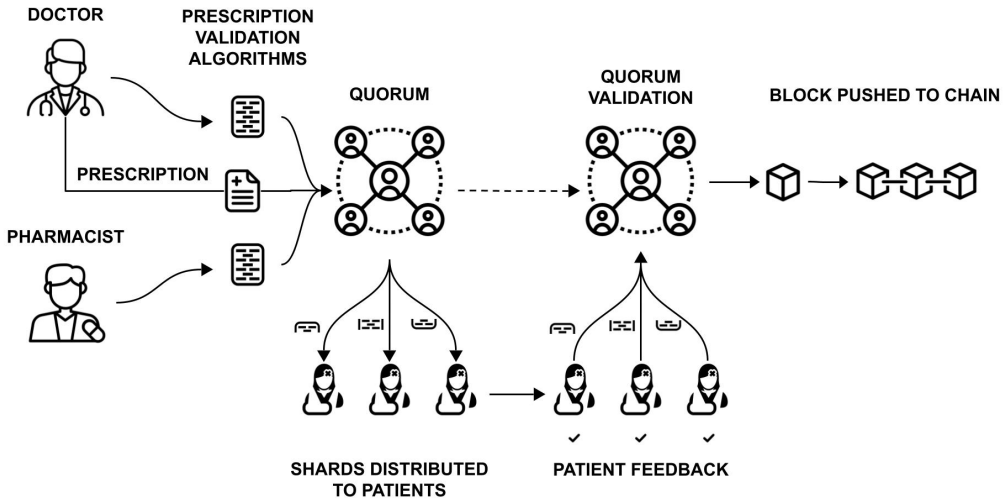
Overview

- HIPAA Design Principles
- 3 Node System
- Proof Of SHarding (PoSH)

HIPAA Design Principles

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.

System Overview



- Authorized parties push algorithms on chain
- Authorized parties push transactions to chain
- Quorum is formed and shards work to patients
- Patients return required data and quorum makes decision

System Overview

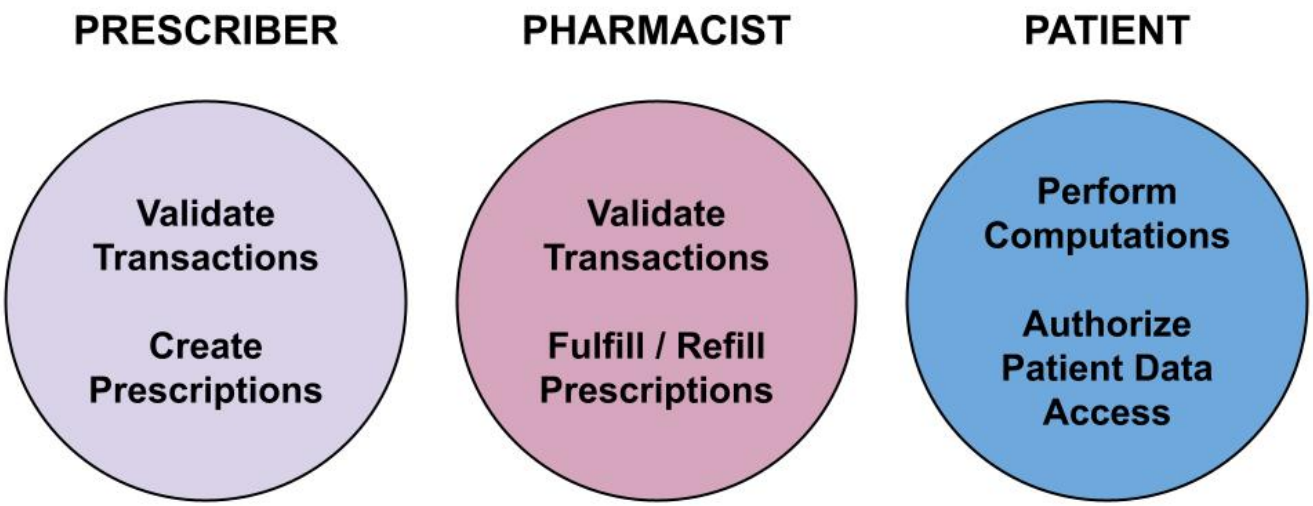


Figure: Three node types in PharmaSys and their responsibilities.

System Overview

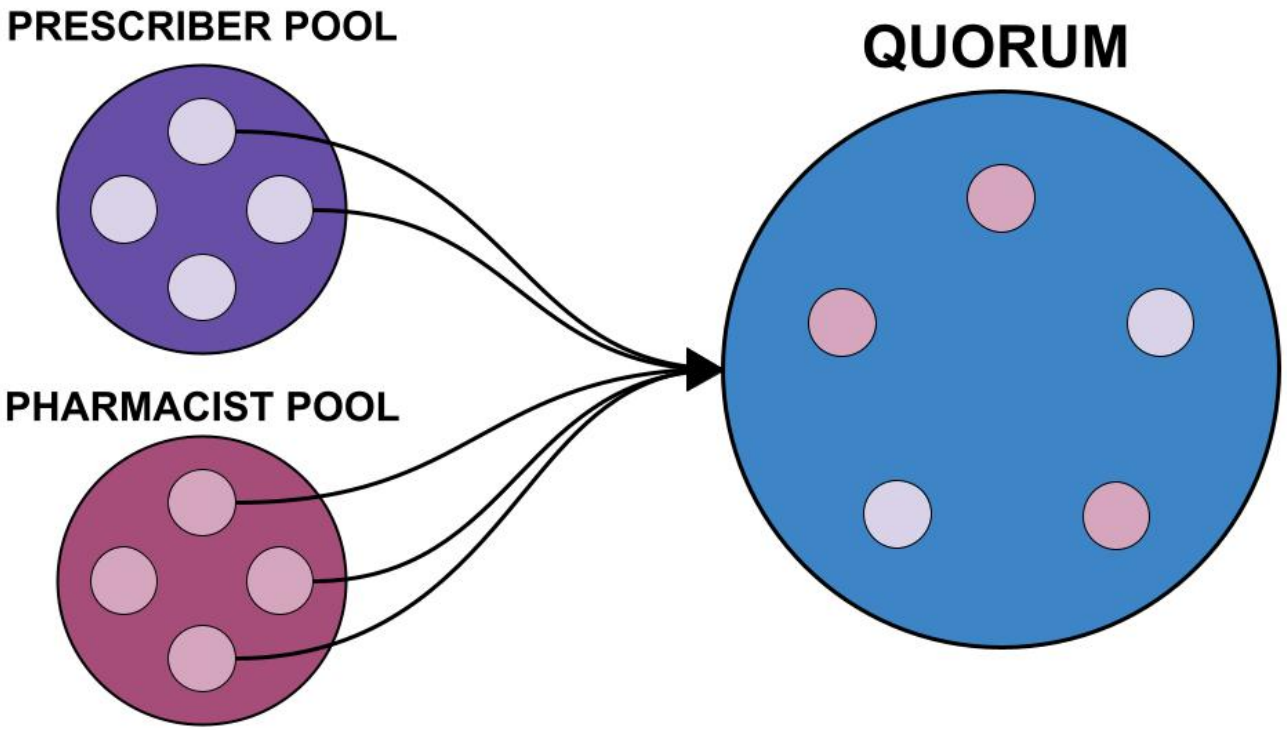


Figure: Prescribers and Pharmacists are randomly selected from their respective pools using the hash of the last block and join the quorum.

Proof of SHarding (PoSH)

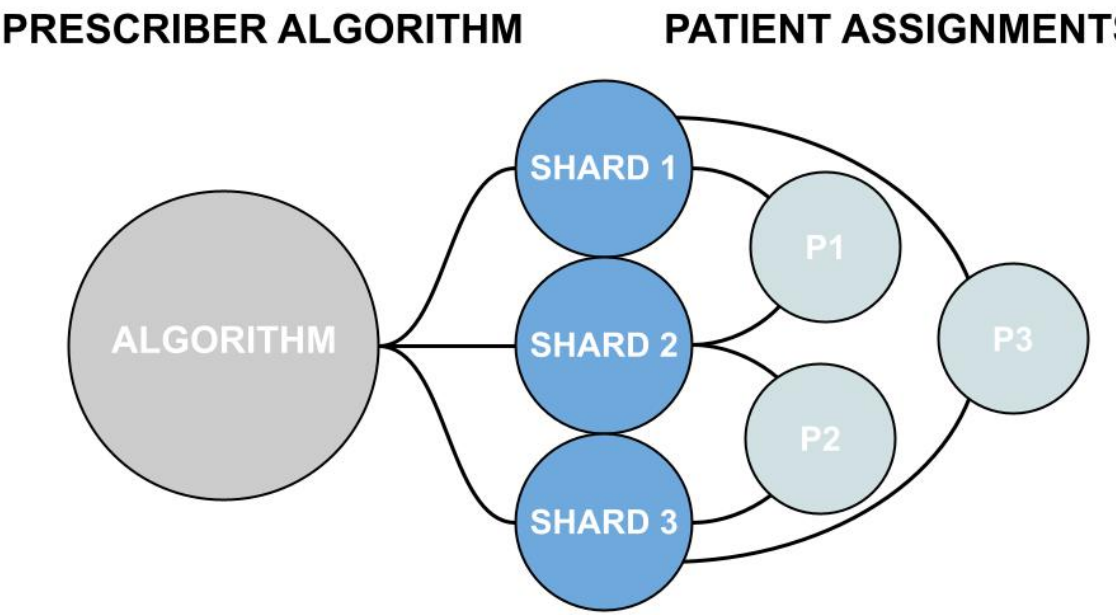


Figure: Visualization of an individual quorum member's algorithm being sharded

Proof of SHarding (PoSH)

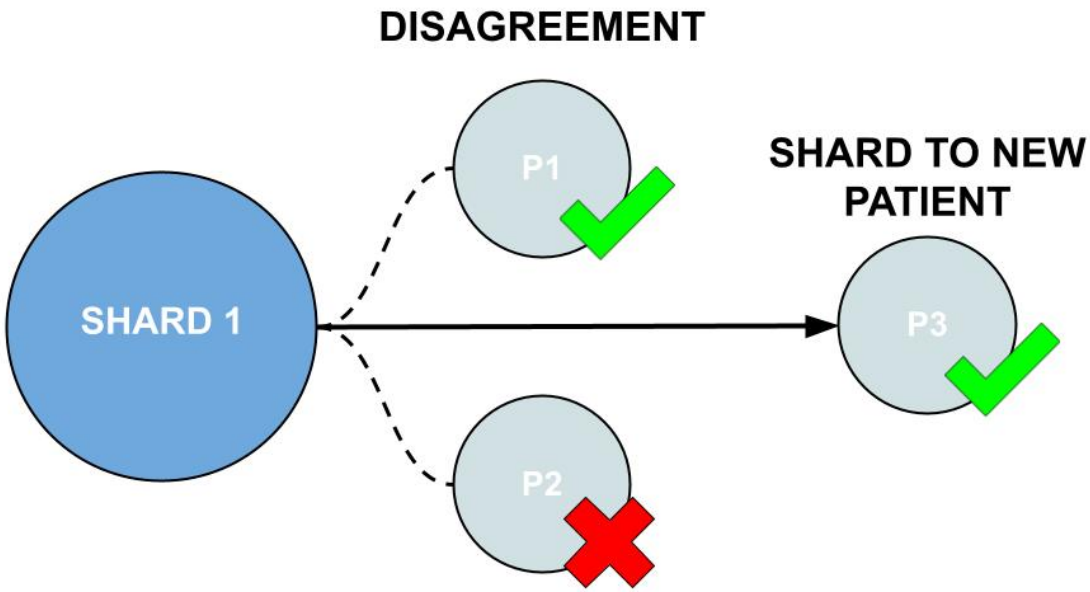


Figure: Demonstration of instance where two worker nodes have disagreement

EXPERIMENTAL EVALUATION

Setup & Testing Environment

- Setup
  - Executed on a local network within a Virtual Machine
  - MIN_CONNECTIONS = 4 and MAX_CONNECTIONS = 7
- Testing Environment
  - 3.4 GHz Intel I7-6700CPU, NVIDIA Quadro M400 GPU, 32GB of 2133 MHz DDR4 RAM, 512GB PCIe SSD running Windows 10
  - Ubuntu 22.04 LTS (24GB of RAM, 25GB VHDD, 5 cores of CPU utilization that ran Maven V3.9.3 and Java 20 SDK dependency

Scalability

- We experimented on various stages of our transaction process which consisted of quorum formation, quorum decision, block construction, and network communication.
- 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.
- Each iteration we executed 50 transactions and calculated the average duration.
- We also measured the client's response time alongside the in-network processing time.

Scalability Result 1

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

Figure: In-network time of various processes

Scalability Result 2

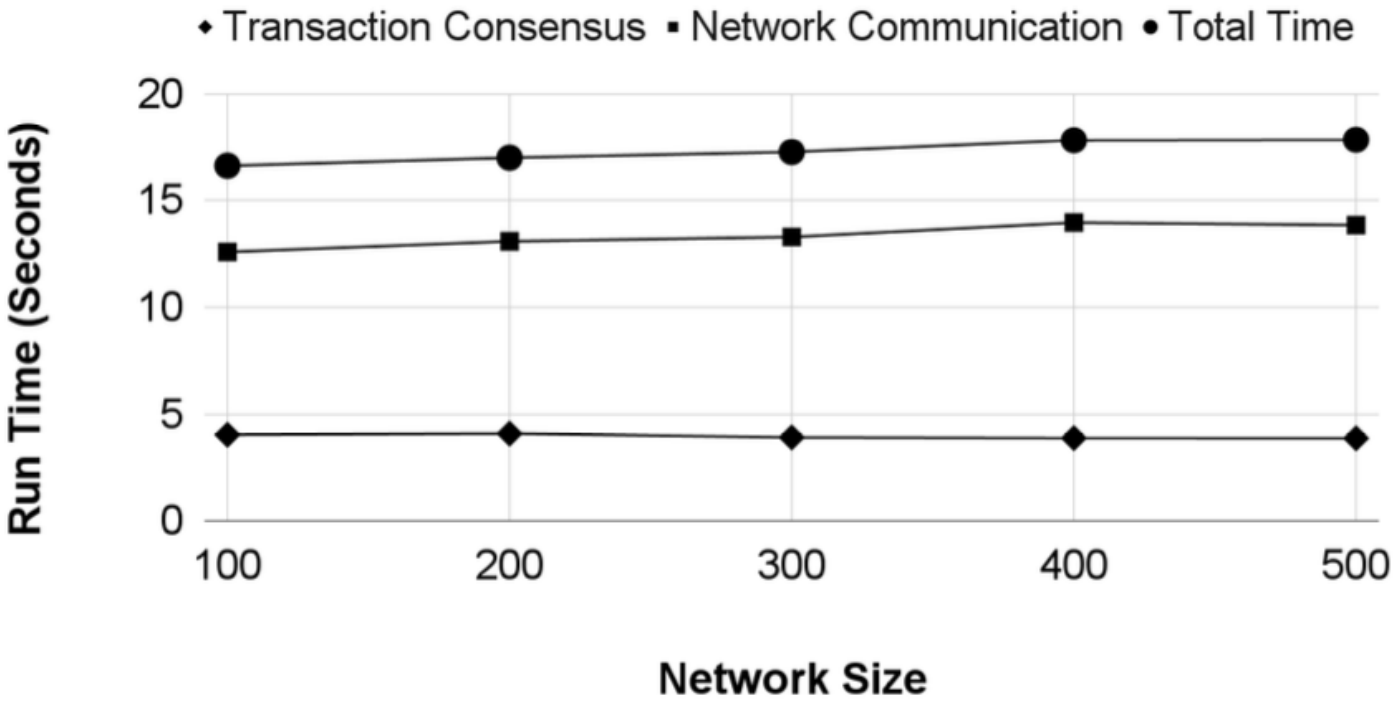


Figure: Graph of Run Time in relation to Network Size of various processes

Robustness

- A non-accurate transaction occurs when majority of the sub-quorum of patients is malicious
- Malicious Activity in Scientific Research
  - *Ran experiments from 10% to 50%* malicious patient nodes in the system
  - increased by 10% each iteration
- Measured the occurrences of a malicious sub-quorum

Robustness Result 1

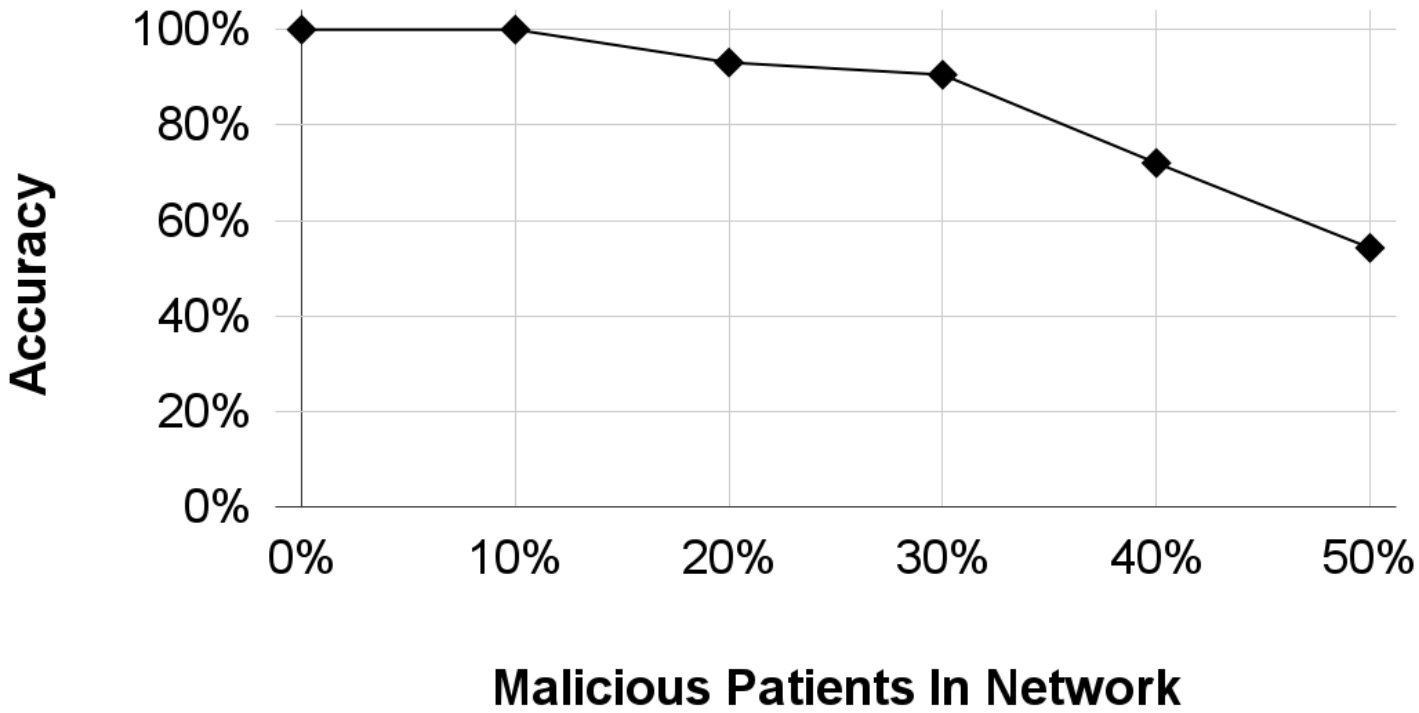


Figure: Accuracy of quorum member decision with n percent of malicious patients in network.

CONCLUSION

Summary

- We propose PoSH a novel quorum consensus protocol for prescription validation to flag malicious actors and work towards prevention of prescription misuse
- We propose a HIPPA-compliant design enabling security for patient data
- We implemented a full system of our use-case
- Experimentation proves our system's scalability and robustness

Future Work

- 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 through machine learning applications.
- Increase ease of access for parties involved to integrate them into the network. We need to try and make Web3.0 technology as close to Web2.0 ease of use as possible.

Questions?

[1] May Alnafrani and Subrata Acharya. Securerx: A blockchain-based framework for an electronic prescription system with opioids tracking. *Health Policy and Technology*, 10(2):100510, 2021.

[2] Asaph Azaria, Ariel Ekblaw, Thiago Vieira, and Andrew Lippman. Medrec: Using blockchain for medical data access and permission management. pages 25–30, 2016.

[3] Golam Dastoger Bashar, Joshua Holmes, and Gaby G. Dagher. Accord: A scalable multileader consensus protocol for healthcare blockchain. *IEEE Transactions on Information Forensics and Security*, 17:2990–3005, 2022.

[4] A Dabrant and HHS Office of Civil Rights. Hipaa administrative simplification - hhs.gov, Mar 2013.

[5] Gaby G. Dagher, Jordan Mohler, Matea Milojkovic, and Praneeth Babu Marella. Ancile: Privacy-preserving

framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable Cities and Society*, 39:283–297, 2018.

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

[7] 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.

[8] Alixandra Taylor, Austin Kugler, Praneeth Babu Marella, and Gaby G. Dagher. Vigilrx: A scalable and interoperable

prescription management system using blockchain. *IEEE Access*, 10:25973–25986, 2022.

[9] Peng Zhang, Breck Stodghill, Cory Pitt, Cavin Briody, Douglas Schmidt, Jules White, Alan Pitt, and Kelly Aldrich. *OpTrak: Tracking Opioid Prescriptions via Distributed Ledger Technology*, pages 103–123. 01 2020.

[10] Peng Zhang, Jules White, Douglas C. Schmidt, Gunther Lenz, and S. Trent Rosenbloom. Fhirchain: Applying blockchain to securely and scalably share clinical data. *Computational and Structural Biotechnology Journal*, 16:267–278, 2018.