Blockchain-based Access Control Systems

Group 2
Yuan Ma, Ting-Jui Hsu,
Tianbo Lu, Zeng Tao

Apr. 18, 2023

VIRGINIA TECH™

Contents

- Introduction & related works
- Problem statement
- System design
- Network model
- Demonstration
- Security & threat model
- Conclusion

Introduction & Related Works

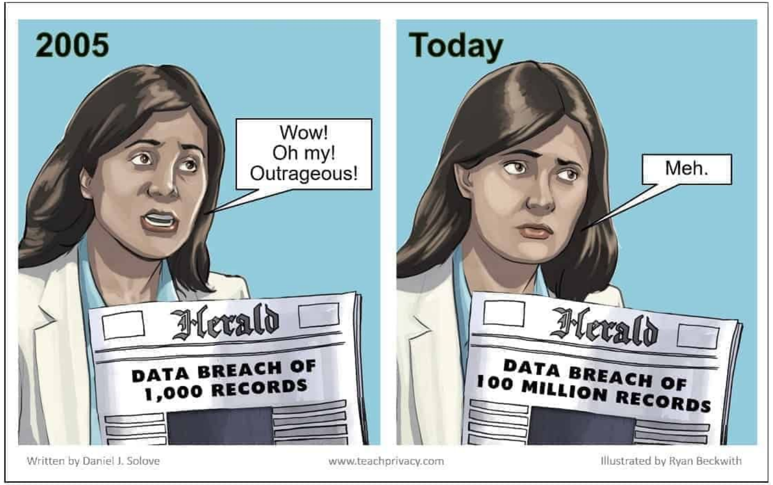
The access control systems

The risks of centralized access control systems

- Data breaches
- Vulnerable to single-point failures - low fault-tolerant

The advantages of blockchain-based access control systems

- Tamper-proof
- Fault-tolerant
- Scalable


2005
Wow! Oh my! Outrageous!
Herald
DATA BREACH OF 1,000 RECORDS
Today
Meh.
Herald
DATA BREACH OF 100 MILLION RECORDS

Written by Daniel J. Solove www.teachprivacy.com Illustrated by Ryan Beckwith

The implementation challenges in different areas

Internet of things (IoT)

- Efficiency - low computing power
- Trade a bit security for performance
- Xu Yang used modular square root and the re-implemented smart contract

Healthcare

- Privacy and data sharing
- There is no operating blockchain-based access control systems
- Junsong Fu stored electrical medical records (EMRs) on blockchains and transferred the data with encoded EMRs

Problem Statement

Problem statement

Context

- Healthcare industry
- Sharing data is complex
- Need to maintain several accounts
- It is hard for patients control the accessibility

Problem statement

Proposal

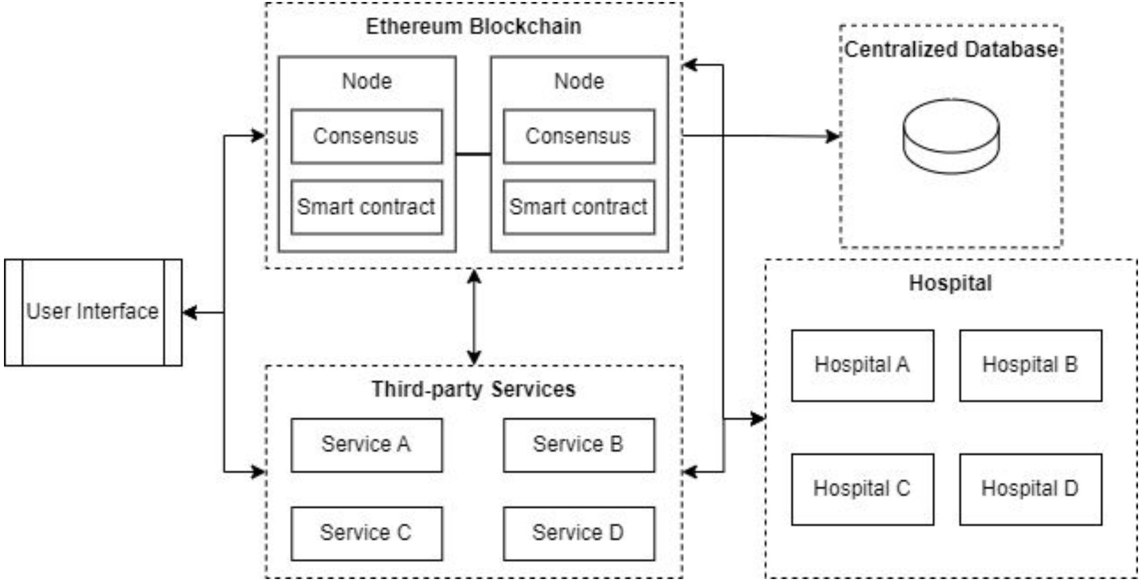
- Blockchain-based framework for secure data sharing and access control within a healthcare ecosystem
- The system can share data with hospitals and third-party healthcare providers
- Patients can permit/withdraw/reject the access requests from hospitals and healthcare providers
- Patients only need one digital identification rather than multiple accounts

System Design

Architecture

DAC & Ethereum blockchain

- Identity integration
- Secure data sharing
- Authorization



Implementation

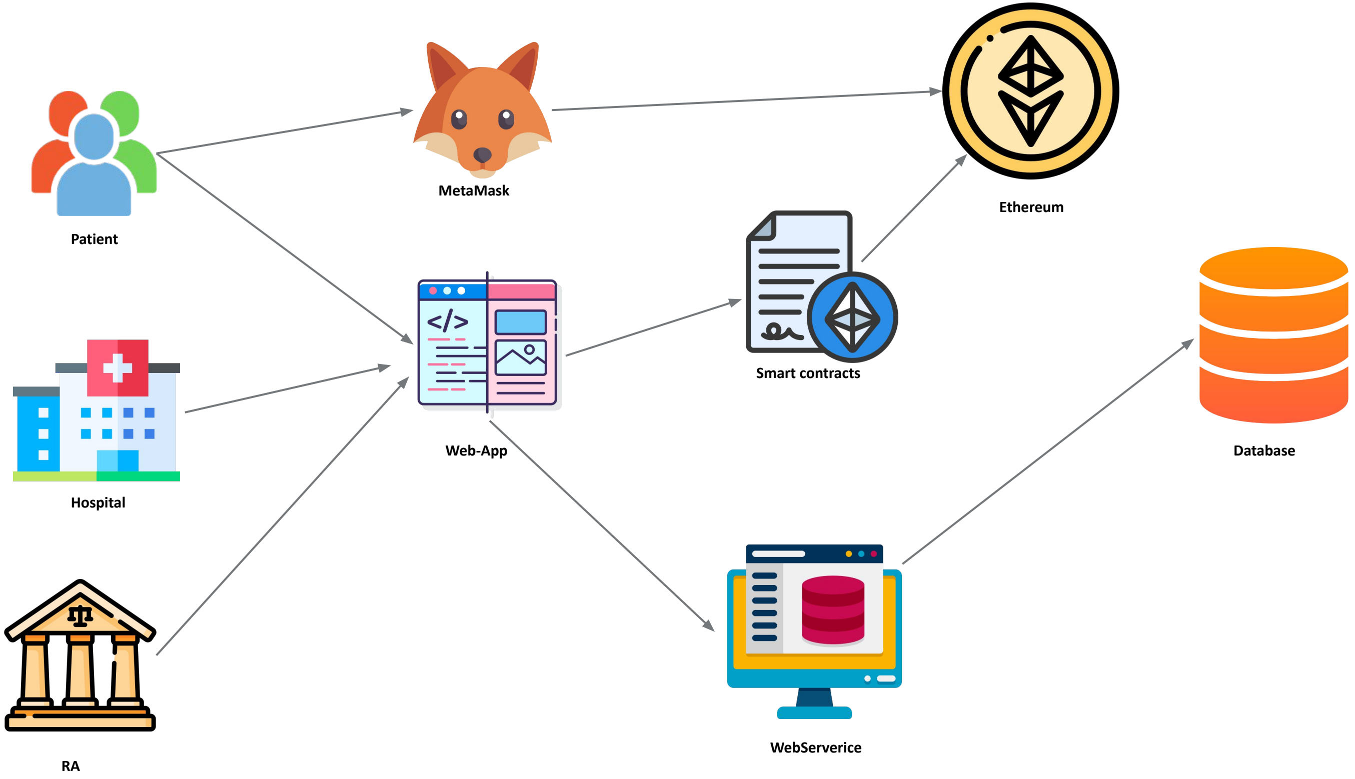
Ethereum local network

Server

Application

Network Model

System components
communications and connections



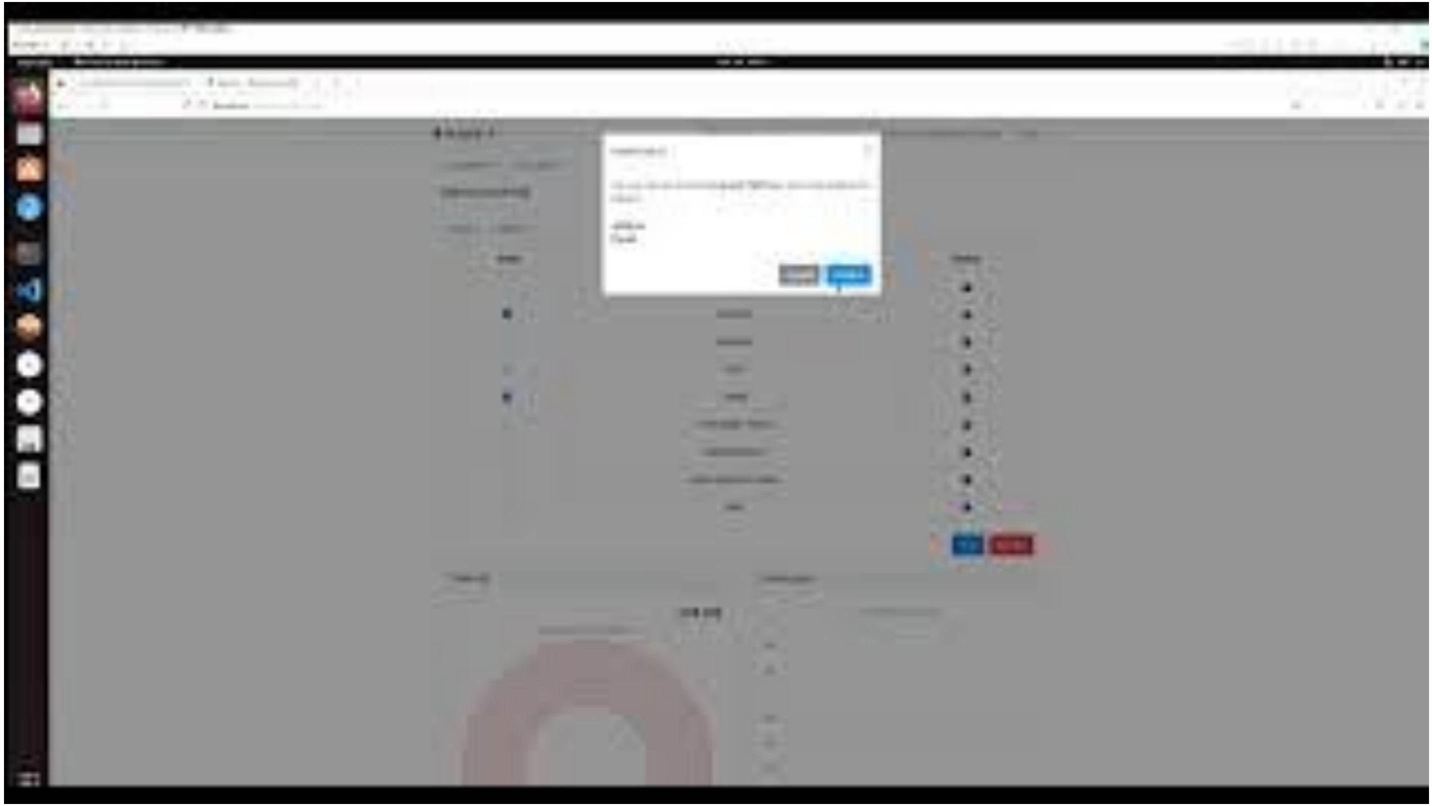
User Registration

User Authentication

User Binding

Login with Ethereum Account

User Access Manager



Functions in the process of development

- Organization Registration
- Organization Data View

Security & Threat Model

Analysis of General Attacks on Purposed System

Sybil Attacks

- ✓ PoA makes it harder for an attacker to launch a Sybil attack, as only authorized nodes can participate in the consensus process.
- △ A Sybil attack can still be carried out if an attacker creates a significant number of fake identities that mimic authorized nodes.

51% Attacks

- ✓ PoA provides better protection against a 51% attack than PoW or PoS.
- △ Even with PoA, a 51% attack is still possible if an attacker manages to gain control of a majority of the authorized nodes in the network.

This is what a sybil attack looks like..
Sybil Attacker
Gaining influence, altering decisions
Subverting systems reputation
Alt Account
Bot
Alt Account
Bot
Alt Account
Bot
Alt Account
don't let it happen to you!

Proposition & Analysis of Other Attacks

Reuse Permission Attack

When a permission token is leaked, a malicious user without valid permission might query data in the permissioned blockchain

Sol

- ○ Using JWT tokens re-authenticating the user for each request
- ○ Implement additional security measures such as secure token storage, token encryption

Create a token that's a copy of target artifact or creature.

Cipher *(Then you may exile this spell card encoded on a creature you control. Whenever that creature deals combat damage to a player, its controller may cast a copy of the encoded card without paying its mana cost.)*

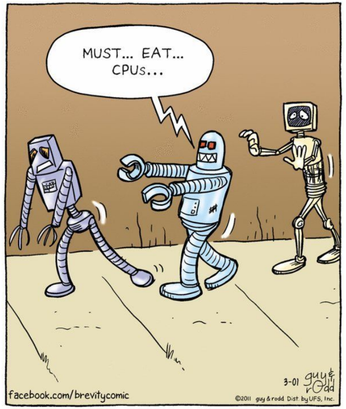
Proposition & Analysis of Other Attacks

Distributed Denial of Service (DDoS) attack

Attackers flood the network with traffic, leading to a disruption in its operation

Sol

- Implement rate-limiting and throttling mechanisms to reduce requests or traffic surges
- Optimize the system design by extending the architecture to a multi-layer or integrating distributed network infrastructure, such as Content Delivery Networks (CDNs)


MUST... EAT... CPUs...
facebook.com/brevitycomic
3-01 guy & rodd
©2011 guy & rodd Dist. by UFS, Inc.

Conclusion

✓ Milestones

- ○ Designed and implemented a blockchain-based access control system using Ethereum and POA consensus algorithm.
- ○ Completed end-to-end development and deployment of the frontend, backend, and smart contract components.

Remaining Works

- ○ Enhance security features to mitigate potential attacks, such as Sybil and insider attacks.
- ○ Conduct further experiments to validate the system's performance under different network conditions and workloads.

Q & A

Thank You