Smart Access Control using Blockchain

Mentor: Dr. Rajendra Prasath

GroupID: RP01

Team Members

Adwait Thattey (S20170010004)

Siddhant Jain (S20170010151)

Mahammad Adam Bagwan (S20170010021)

Contents

1. Project Idea
2. Use Case Modelling
3. Project Architecture
4. Demo
5. References

Tech Stack

1. Hyperledger Fabric
2. Golang - for Smart Contracts
3. Node.Js + Fabric SDK - for application
4. Bash - Network Scripts
5. ReactJs - Application UI
6. Git - for Version Control
7. Docker - running blockchain nodes
8. CouchDB - Blockchain state Database

Project [Chaincode, application, network scripts] [Web UI Link]

Project Idea

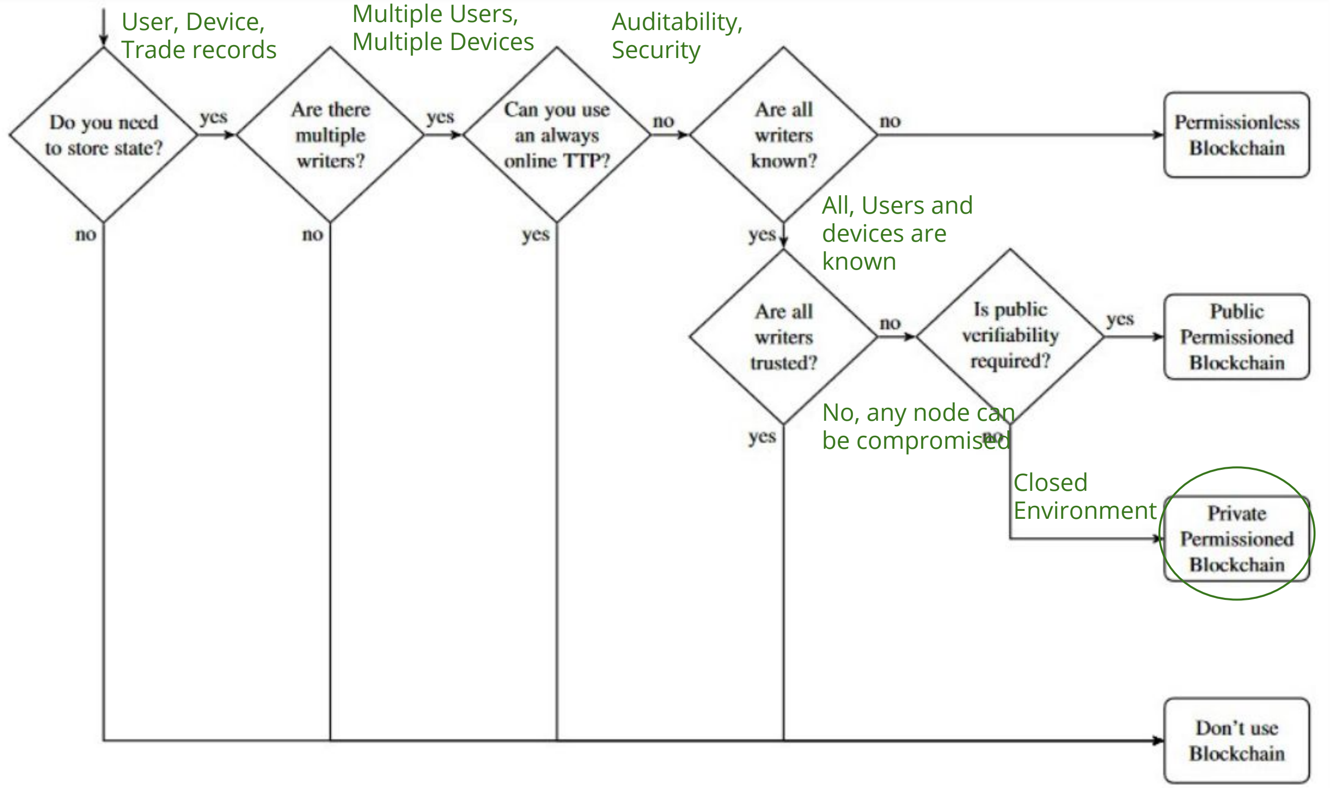
1. Building a Smart Access Control System for data governance where user has all the rights over their data

2. We have created a decentralized digital marketplace owned by users. The users are both Individuals and organizations buying and selling IOT Data. Built using Hyperledger fabric.

Deliverables

1. Network scripts for docker containers running blockchain network nodes
2. Developed Smart contracts to interact with Blockchain
    a. Creating / Updating / Deleting devices and users
    b. Adding / Reading data to/from devices
    c. Creating / Deleting Trade Agreements
    d. Creating Trade Receipts
    e. Time based Revoking Data access
3. Developed Application to interact with smart contracts
    a. Registering Users / Devices, also handling digital certificate creation
    b. APIS for device-data, creating trade flow (buyer and seller), viewing trade status,
    c. Event listener for trade receipt
4. Application UI

Karl Wüstl and Arthur Gervais Model 2017


Do you need to store state?
yes
no
Are there multiple writers?
yes
no
Can you use an always online TTP?
no
yes
Are all writers known?
no
yes
Permissionless Blockchain
Are all writers trusted?
no
yes
Is public verifiability required?
yes
no
Public Permissioned Blockchain
Private Permissioned Blockchain
Don't use Blockchain

User, Device, Trade records

Multiple Users, Multiple Devices

Auditability, Security

All, Users and devices are known

No, any node can be compromised

Closed Environment

Also evaluated with
1. J. Gardner 2018
2. A. Lewis model

Why Hyperledger Fabric

Cons of POW based Public Blockchain

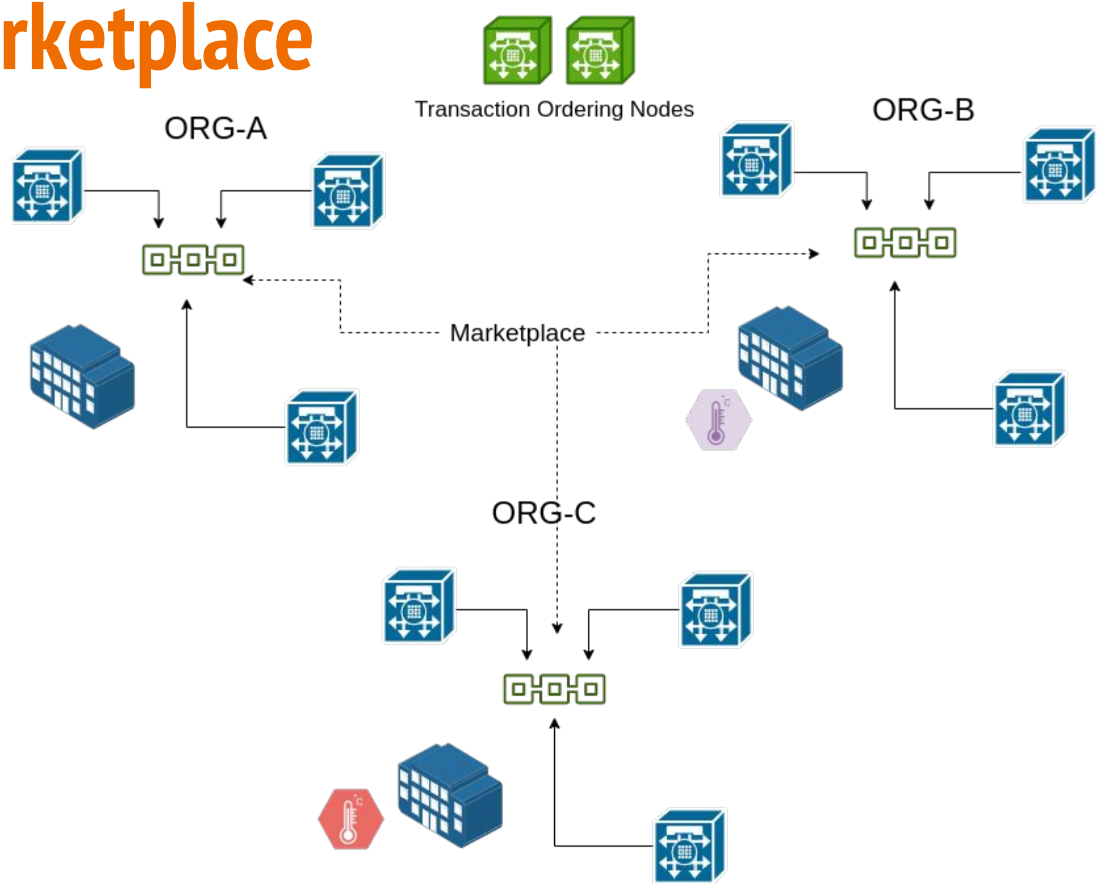
1. Longer Transaction Confirmation time
2. Waste of resources. POW consumes a lot of resources and power
3. Consistency issues. Branching of Blockchain
4. Privacy issues

Hyperledger Fabric

1. Faster consensus - less confirmation time - more throughput
2. Each member needs to be authorized to join a specific channel
3. No consistency issues (ordering service)
4. Network based on business use case

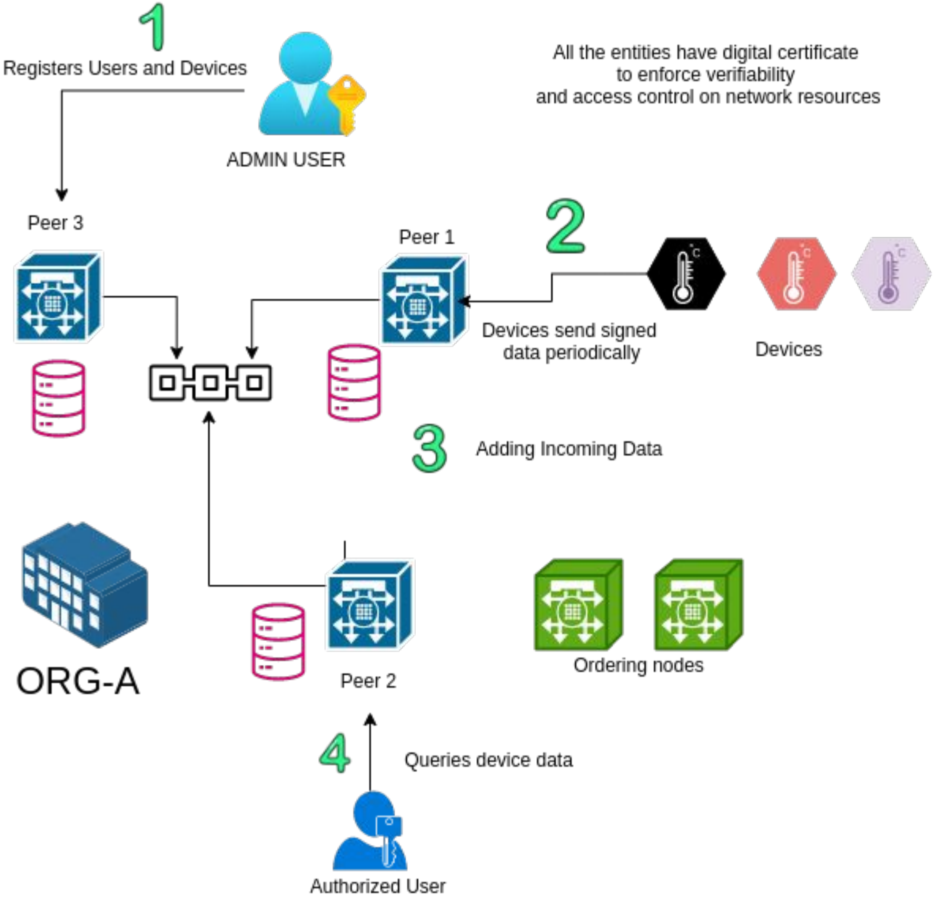
Decentralized Marketplace

1. 1 blockchain per marketplace
2. Sellers can put device data on sale
3. Buyers can query Marketplace for on-sale assets
4. For every Successful Trade, Receipt is generated and stored on Blockchain for auditing



Intra Org Flow

1. Participants = Individuals and corporations
2. Orgs can put device data on marketplace for sale
3. Every device has some secret key associated which remains with owner organization
4. Digital Identity for all users, peer nodes, devices
   a. X.509 certificate
   b. Private Key



Data Sharing

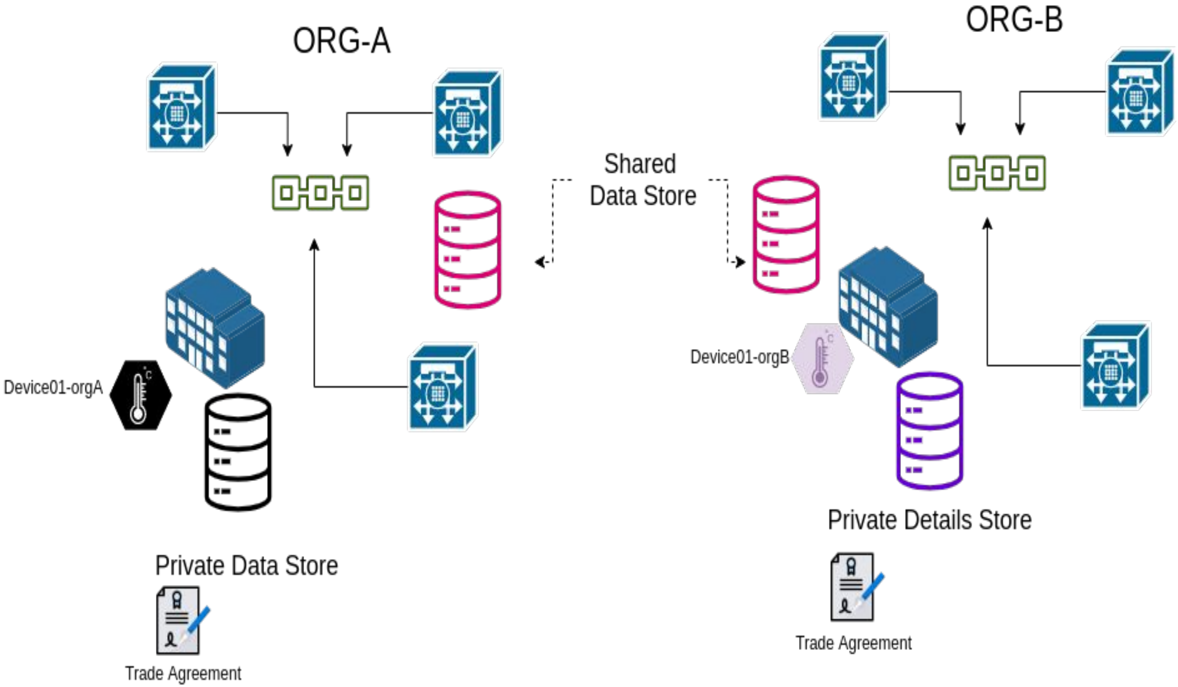
Blockchain Ledger

- Accessible by all on marketplace

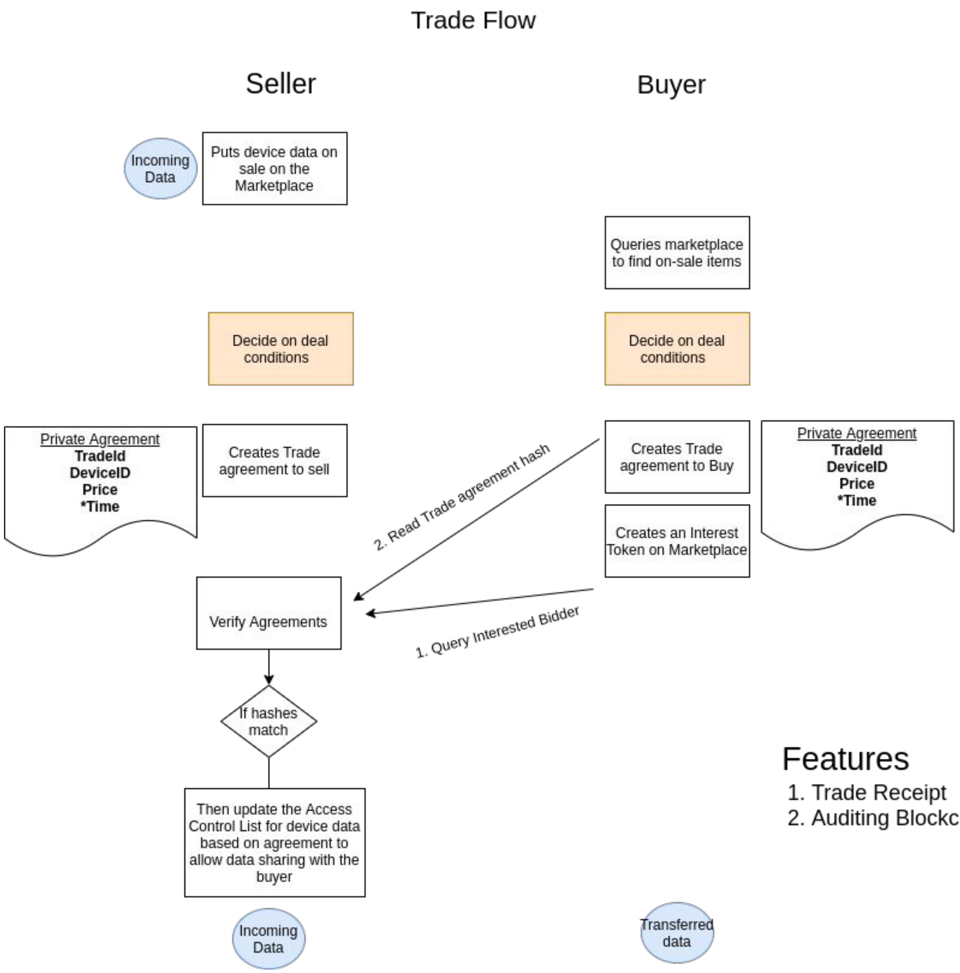
Private Data store

- Implicit (only one org)
- Explicit (Shared data store)

<u>Trade Deals</u> and <u>shared data</u> **must not** be public to others. So, they are stored in <u>private data store</u> and sent via <u>gossip protocol</u>, defined in HL Fabric



Trade Flow



Trade Flow

Seller

Buyer

Incoming Data

Puts device data on sale on the Marketplace

Queries marketplace to find on-sale items

Decide on deal conditions

Decide on deal conditions

Private Agreement
TradeId
DeviceID
Price
***Time**

Creates Trade agreement to sell

Creates Trade agreement to Buy

Private Agreement
TradeId
DeviceID
Price
***Time**

Creates an Interest Token on Marketplace

2. Read Trade agreement hash

Verify Agreements

1. Query Interested Bidder

If hashes match

Then update the Access Control List for device data based on agreement to allow data sharing with the buyer

Incoming Data

Transferred data

Features

1. Trade Receipt
2. Auditing Blockchain

How is consensus achieved among untrusted nodes

1. Raft [visualization] [Raft Protocol]
    a. Crash fault tolerant
    b. Raft follows a “leader and follower” model, where a leader node is elected (per channel) and its decisions are replicated by the followers
    c. can sustain loss of nodes including leader node, as long as majority of nodes are alive
    d. Leader election in raft -
        i. Every ordering node is in one of 3 states Leader, follower, candidate. Initially as follower
        ii. If a leader is already elected, follower receive logs from leader and replicate deterministically
        iii. If no heartbeat message is received, this means no leader has been elected so far
        iv. Nodes self-promote to candidate state and asks for votes from peers
        v. If quorum number of nodes are received, this node becomes leader
    e. Snapshots - Incase an ordering node goes down, it syncs with leader using snapshots when it is back online
2. Kafka [Apache Kafka]
    a. Similar to Raft, CFT
    b. Messages replicated from leader node to follower nodes

How does data sync across all nodes

The gossip-based data dissemination protocol performs three primary functions on a Fabric network:

1. Manages peer discovery and channel membership, by continually identifying available member peers, and eventually detecting peers that have gone offline.
2. Disseminates ledger data across all peers on a channel. Any peer with data that is out of sync with the rest of the channel identifies the missing blocks and syncs itself by copying the correct data.
3. Bring newly connected peers up to speed by allowing peer-to-peer state transfer update of ledger data.

Performance and scalability

Performance of a blockchain platform can be affected by many variables such as transaction size, block size, network size, as well as limits of the hardware, etc. The Hyperledger Fabric Performance and Scale working group currently works on a benchmarking framework called Hyperledger Caliper.

Several research papers have been published studying and testing the performance capabilities of Hyperledger Fabric. The latest scaled Fabric to 20,000 transactions per second.

Individual Contribution

Adwait Thattey	Siddhant Jain	Bagwan Mahammad Adam
1. Chaincode for devices, data and data queries 2. Application server controllers for data sharing, devices, queries, certificate managing, network management	1. Chaincode for data sharing, trade agreements, Access Control Lists, Time based Revoking 2. Application Server controllers for trade receipts, event listeners, network management	1. User Interface for data display, trade agreements, logging 2. User interface for creating new devices, interest tokens

Future Work

1. More types of complex trade agreements can be added that can be used in different business scenarios.
2. More consensus algorithms can be explored that may give better performance.
3. A richer access control system can be created that gives access only to some part of device data or past data.
4. Automated scripts can be made that ease in deployment of the project.

References

- D. Di Francesco Maesa, P. Mori, and L. Ricci, “A blockchain based approach for the definition of auditable Access Control systems,” Computers & Security, vol. 84, pp. 93–119, Jul. 2019, doi: 10.1016/j.cose.2019.03.016.
- Do you need a Blockchain? https://eprint.iacr.org/2017/375.pdf
- Raft Protocol https://raft.github.io/raft.pdf
- C. Lin, D. He, X. Huang, K.-K. R. Choo, and A. V. Vasilakos, “BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0,” Journal of Network and Computer Applications, vol. 116, pp. 42–52, Aug. 2018, doi: 10.1016/j.jnca.2018.05.005.
- Mounnan, Oussama & Abou, Anas. (2019). Efficient Distributed Access Control Using Blockchain for Big Data in Clouds.
- [S. Ding, J. Cao, C. Li, K. Fan, and H. Li, “A Novel Attribute-Based Access Control Scheme Using Blockchain for IoT,” IEEE Access, vol. 7, pp. 38431–38441, 2019, doi: 10.1109/access.2019.2905846.
- T. Sultana, A. Ghaffar, M. Azeem, Z. Abubaker, M. U. Gurmani, and N. Javaid, “Data Sharing System Integrating Access Control Based on Smart Contracts for IoT,” in Advances on P2P, Parallel, Grid, Cloud and Internet Computing, Springer International Publishing, 2019, pp. 863–874. [Link]