Smart Access Control using Blockchain

Mentor: Dr. Rajendra Prasath

Team Members

Adwait Thattey (S20170010004)

Siddhant Jain (S20170010151)

Mahammad Adam Bagwan (S20170010021)

Contents

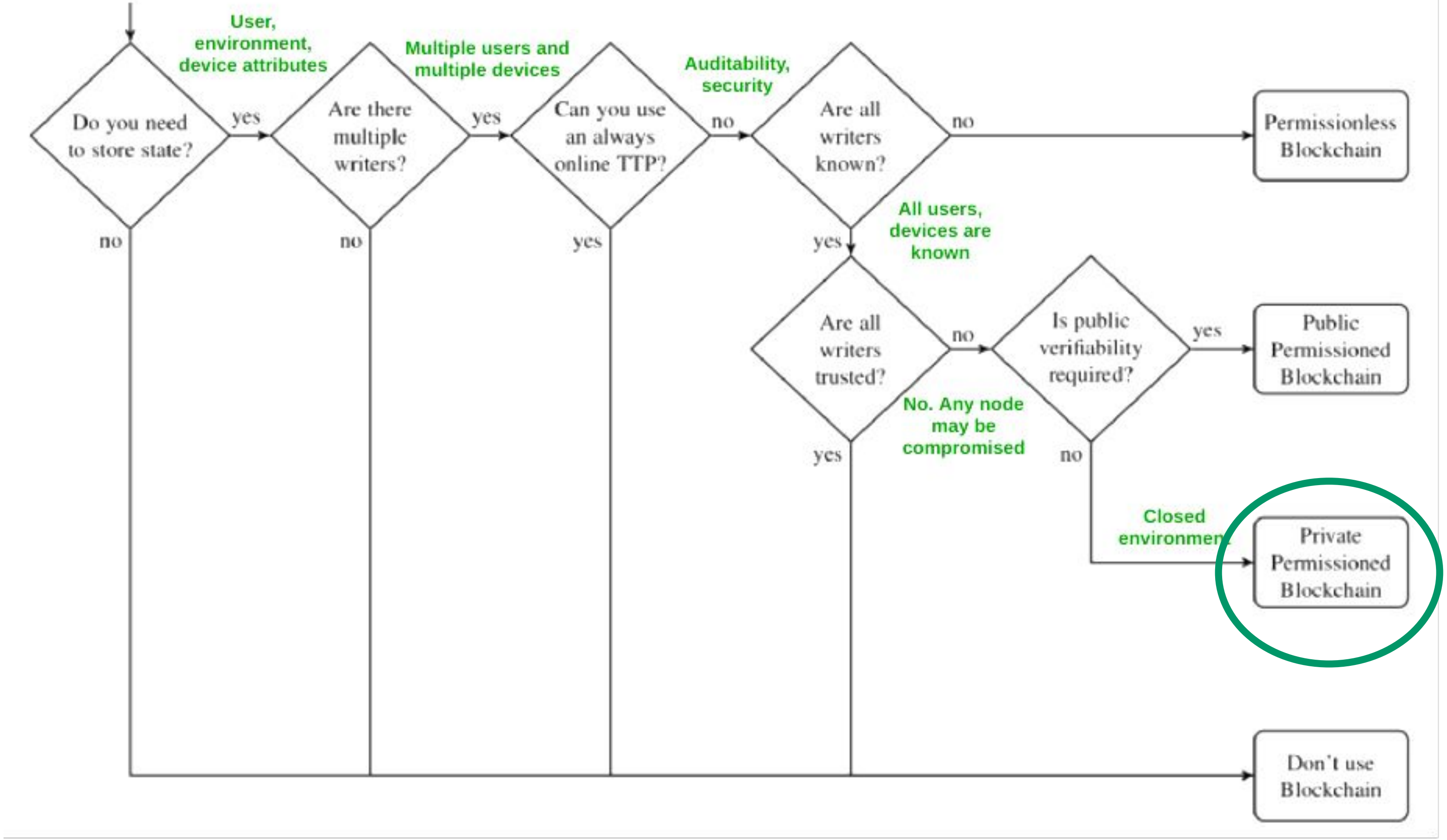
1. Project Idea
2. Justifying Blockchain for ACS
3. BTP work overview
4. Workflow of our proposed solution
5. Components
    a. Users
    b. Policy Models
    c. Contracts
6. Transactions in Hyperledger Fabric
7. References

Project Idea

Understanding the Scope of Blockchain in Access Control Systems & Building an ABAC System for IOT Data.

Key Questions

1. Is Blockchain suitable for an ABAC Access Control Systems?
2. Why IOT Data?
3. Permission-less or Permissioned Blockchain with IOT ACS?


User, environment, device attributes
Multiple users and multiple devices
Auditability, security
Do you need to store state?
yes
Are there multiple writers?
yes
Can you use an always online TTP?
no
Are all writers known?
no
Permissionless Blockchain
no
no
yes
yes
All users, devices are known
Are all writers trusted?
no
Is public verifiability required?
yes
Public Permissioned Blockchain
No. Any node may be compromised
yes
no
Closed environment
Private Permissioned Blockchain
Don't use Blockchain

Access Control Systems

Key factors to consider for any production grade ACS

1. No Single Point of failure (Hardware Crashes)
2. Throughput
3. System Security
4. Auditability
5. *Security (no single weak system)

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

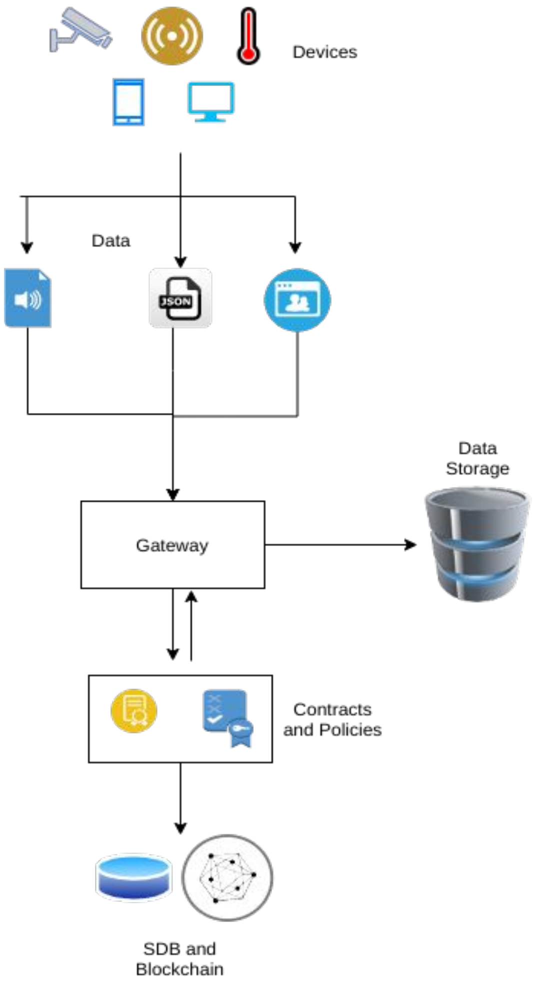
Hyperledger Fabric

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

Work already done	Work for this evaluation	Work for next semester
1. Exploring Industrial use cases of Blockchain 2. Challenges in Centrally Operated ACS 3. High Level view of Blockchain components	1. Indepth Research on ACS using Blockchain. 2. Implemented some Blockchain Components from scratch in Golang (components, POW) 3. Learning Hyperledger Fabric 4. Finalizing the workflow, models, and Smart Contract in the project 5. Coding the models in Golang	1. Coding different types of smart contracts in the chain code for the fabric 2. Scripts for enrolling admins, registering users 3. Web UI 4. Connecting with ipfs 5. Integrating all components 6. Analysis of performance with large number of Transactions using different consensus algorithms

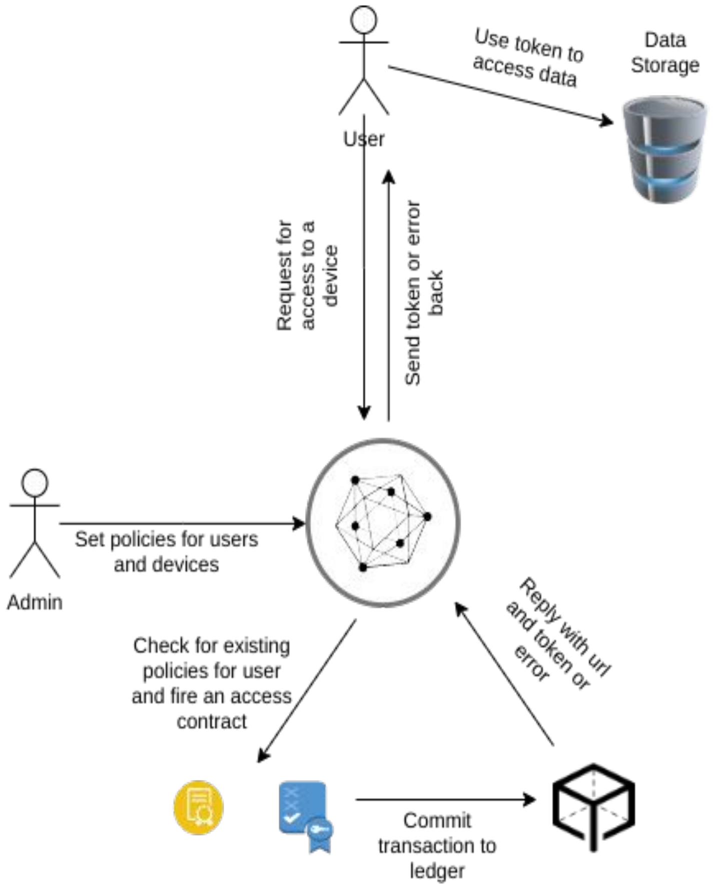
Workflow (Part 1)

- The devices capture the data in various formats
- They send the data to Gateway
- The gateway checks for existing device and policies
- If not, it fires device contracts to create url and device records
- The contract commits to the Blockchain and the SDB
- Data and the url is sent to the data storage



Workflow (Part 2)

- The admin user sets policies and contracts for device and other users
- User requests the system for access to the device data
- Policies are retrieved and access contract is fired
- If successful, token is generated and is sent back to the user
- User uses the token to access the data


User
Use token to access data
Data Storage
Request for access to a device
Send token or error back
Admin
Set policies for users and devices
Check for existing policies for user and fire an access contract
Reply with url and token or error
Commit transaction to ledger

Policy Model

This model is designed with focus on IoT systems

- **User Attributes**
  - User-id
  - Role
  - Group
- **Device Attributes**
  - Device ID
  - Mac address
- **Environment Attributes**
  - End time
  - Allowed IPs
- **Permission Attributes**
  - Permission (allow or deny)

Policy Model = **{UA, DA, EA, PA}**

Policy Contract

- **Make Policy**
  - Admin defines policy for users
  - Encrypt and sign data
  - Send the request to add policy
- **Check Policy**
  - Check if policy is valid, all attributes are present etc
  - Check for any existing policy with similar attributes
- **Add Policy**
  - Write the policy in the ledger
  - Add the policy in the state database
- **Update Policy**
  - Update a policy instead of creating a new one
- **Delete Policy**
  - Either the admin manually revokes a policy
  - Or time of policy has expired

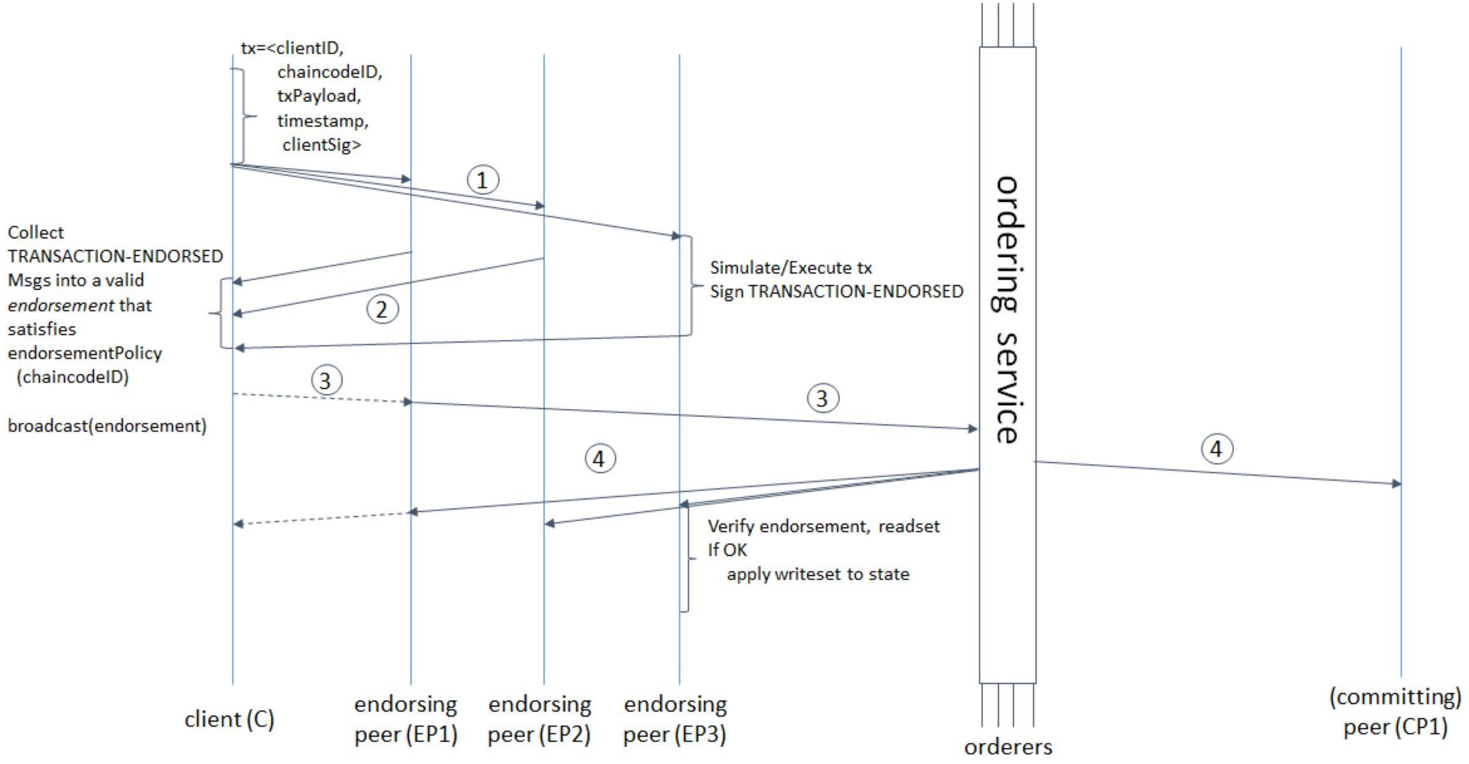
Device Contract

- **Add URL**
  - Take the device ID, Mac, IP
  - Write the URL of device into State database
- **Get URL**
  - Given a Device ID, get URL
- **Update URL**
  - If the device Mac, IP, ID changes
  - Update the signature and the url
- **Delete URL**
  - If the device is removed
  - Remove the URL from state DB

Access Contract

- **Verify User**
  - Check user’s key and verify identity
- **Fetch attributes**
  - Get all the relevant attributes for user, device, environment
- **Check Access**
  - Query the SDB for the relevant policies
  - Check if access should be granted or revoked
- **Generate Token**
  - If the request is valid, query the SDB and get URL for the device
  - Generate the token for the request.
  - Token will contain attributes like Device_ID, hash of transaction, Policy ID, expire time, etc.

Transaction Flow in Hyperledger Fabric



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.
- 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]
- Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., … Yellick, J. (2018, April 23). Hyperledger fabric. Proceedings of the Thirteenth EuroSys Conference. EuroSys ’18: Thirteenth EuroSys Conference 2018. https://doi.org/10.1145/3190508.3190538