Immutable, Secure and Trustless Access Control Framework on Ethereum

Ozan ZORLU*[1], Adnan ÖZSOY*[2]
Computer Engineering Department
Hacettepe University
Ankara, Turkey
{ozanzorlu*[1], adnan.ozsoy*[2]}@hacettepe.edu.tr

Presentation Outline

- Introduction and Problem Definition
- Literature review
- Proposed Framework
- Conclusion and Future Work

Introduction-I

- Especially on the financial systems, always there is a central authority to trust,
- But, what if participants do not want to:
  - Trust any central authority,
  - Pay much fee?

Introduction-II

- Controlling restricted area's entrance is a studied problem domain,
  - Central solutions,
  - Single point of failure,
  - Management issues,
  - Security of logs and system,
  - ....

Introduction-III

- Controlling restricted area's entrance is a studied problem domain,
  - User permissions has to be managed strictly,
  - Recorded entrance logs has to be immutable,
  - Entrance grants can not be denied/revoked by any malicious party,
  - Records has to be queried/monitored by auditors,
  - Always on availability is needed,
  - Trust vs. Transparecy,

Problem Domain-I

- Technopark companies are responsible for;
  - Reporting the research process and progress,
  - Reporting the working time of their workers at technopark
- They get some benefits of deployment at technopark,
- Technopark managers are responsible for the access control, monitoring and logging.

Problem Domain-II

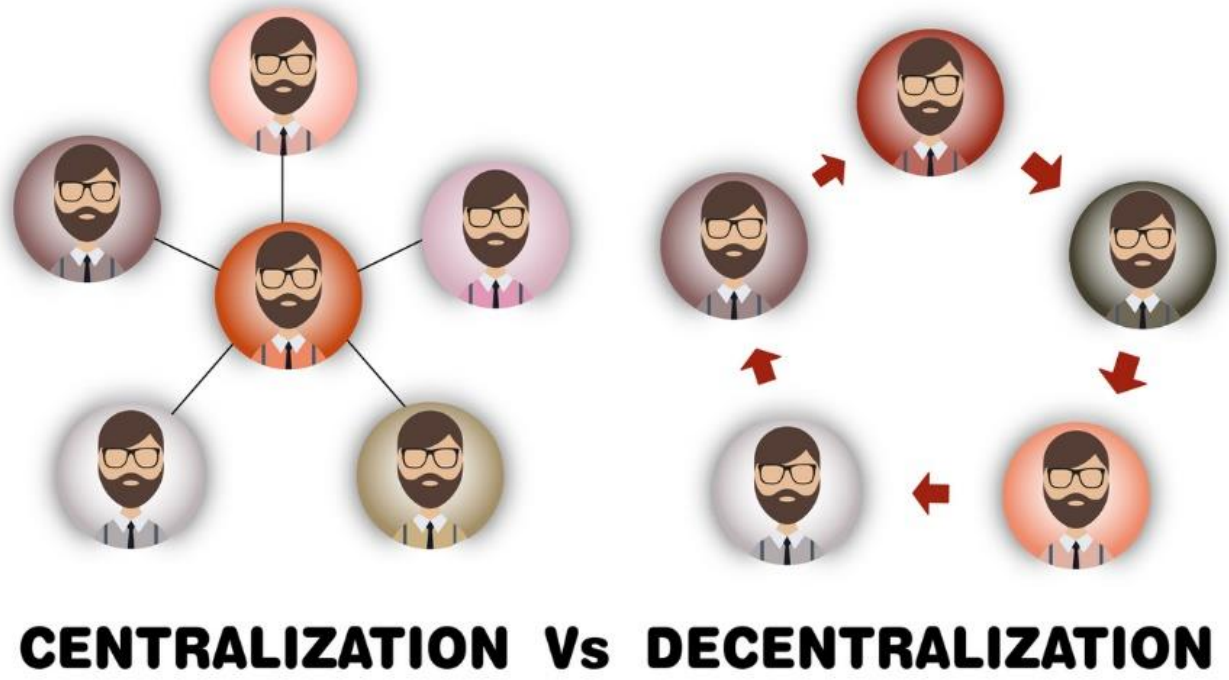
- Real life problem/scenerio,

Problem Domain-III

- Failover,
- Interruption,
- Manual log reporting,
- Trust to the managers,
- Central solutions,
- No integrated solutions

Problem Domain-IV

- The problem is recording, auditing and reporting the worked time of workers of the technopark companies to government without any interruption and fraud while controlling the access.



Problem Domain-V

- To solve the problem of centralization;
  - First thing to do is getting a consensus on the topic.
- Decentralization of the agreements are,
  - Well known and studied problem in the literature as **consensus algorithms.**

Problem Domain-VI

- Blockchain technology appeared as a solution of eliminating the need of central authority.
- Blockchain is a series of immutable record of data that can not be changed by design

- Ethereum is based on contracts that everyone agrees on the same rules
- Turing complete language,

Progress

- To solve the problem of acces control of secure buildings
  - Literature reviewed for similar studies,
  - Access control based model developed,
  - Implementation with Solidity on Ethereum network,
  - User interface implementation and contract development process is in progress,

Presentation Outline

- Introduction and Problem Definition
- Literature review
- Proposed Framework
- Conclusion and Future Work

Literature Review-I

- Used domains are;
  - Health - MedRec – Patient information share permission
  - Donation – BitGive
  - Finance – Bitcoin, Ethereum, Ripple
  - Supply Chain – IBM Blockchain
  - Social Media – Matchpool
  - Internet of Things (IoT) [6],
  - ....
- Blockchain technology proposes the trust-less, decentralized and autonomous architecture which are suitable for variable domains

Literature Review-II

- Some researchers developed an access control application which is based in :
  - Hyperledger Fabric Blockchain and,
  - HyperLedger Composer to access control of physical places .
- They used the blockchain for the reason of;
  - Non reputation and permanent records,
  - So, it provides tamper-proof database which is also decentralized.

Literature Review-III

- Authors proposed a smart contract for the access control on IoT devices [6,8,9],
- In our project also we used the access control smart contract to,
  - Manage the permissions of the actions,
  - Grants for changing the permission,
  - Reading the data.
- Transparency is important but the privacy is much important in the application of controlling the access logs of the users who are working in that facility.

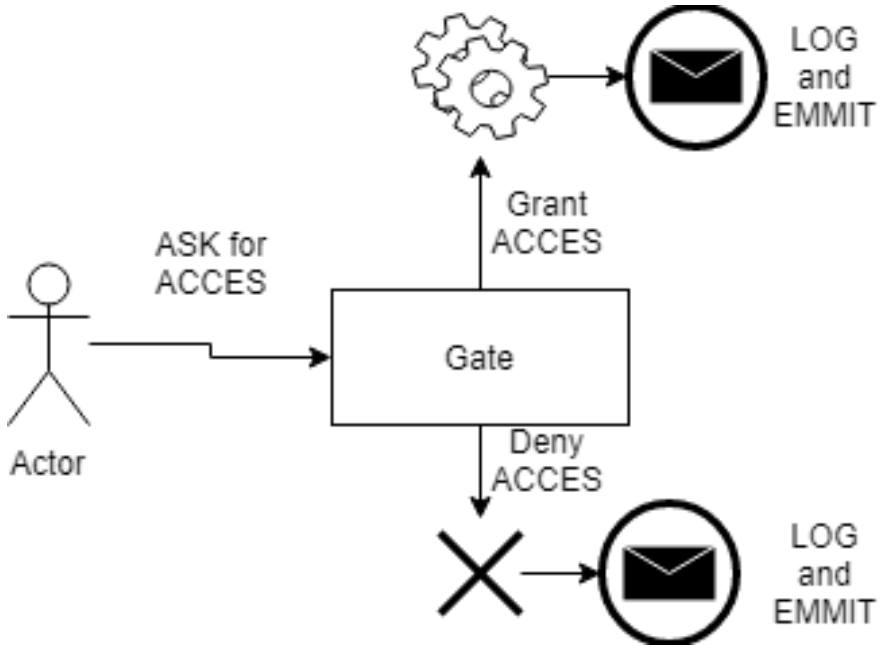
Literature Review-IV

- Securing the critical or valuable data or facility access control is used with policy based access control methodology.
- Their proposed protocol makes the policies and the rights publicly accessible and visible on the blockchain.
- This solution allows distributed audibility, preventing a party from fraudulently denying the rights granted by an enforceable policy.
- This paper much more like our contributions for controlling the access. But also logging is the other visibility and also privacy concern in our work. We try to limit the access control for reading the log transaction information of the user entrance data.

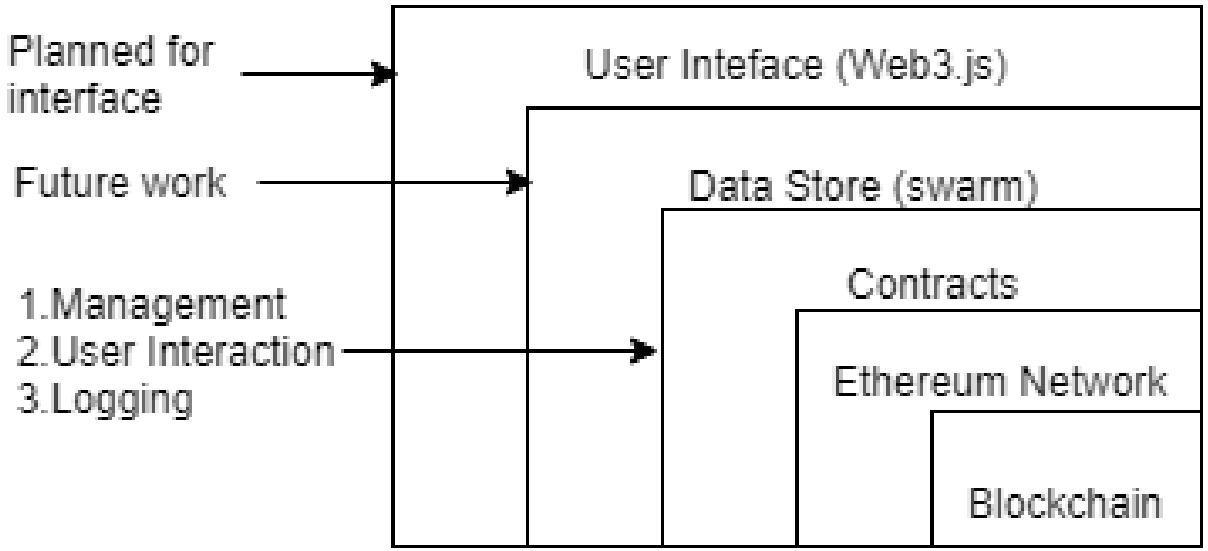
Presentation Outline

- Introduction and Problem Definition
- Literature review
- Proposed Framework
- Conclusion and Future Work

Proposed Framework-II



Proposed Framework-I

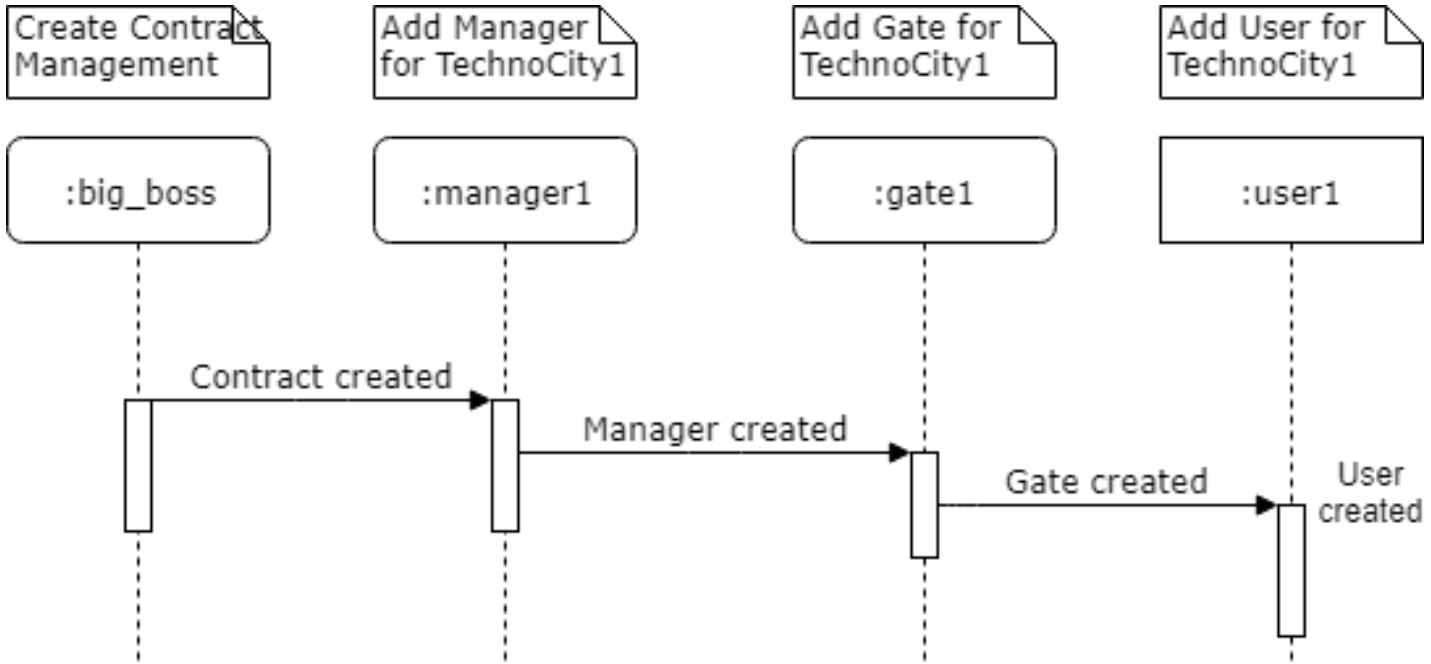


Proposed Framework-I

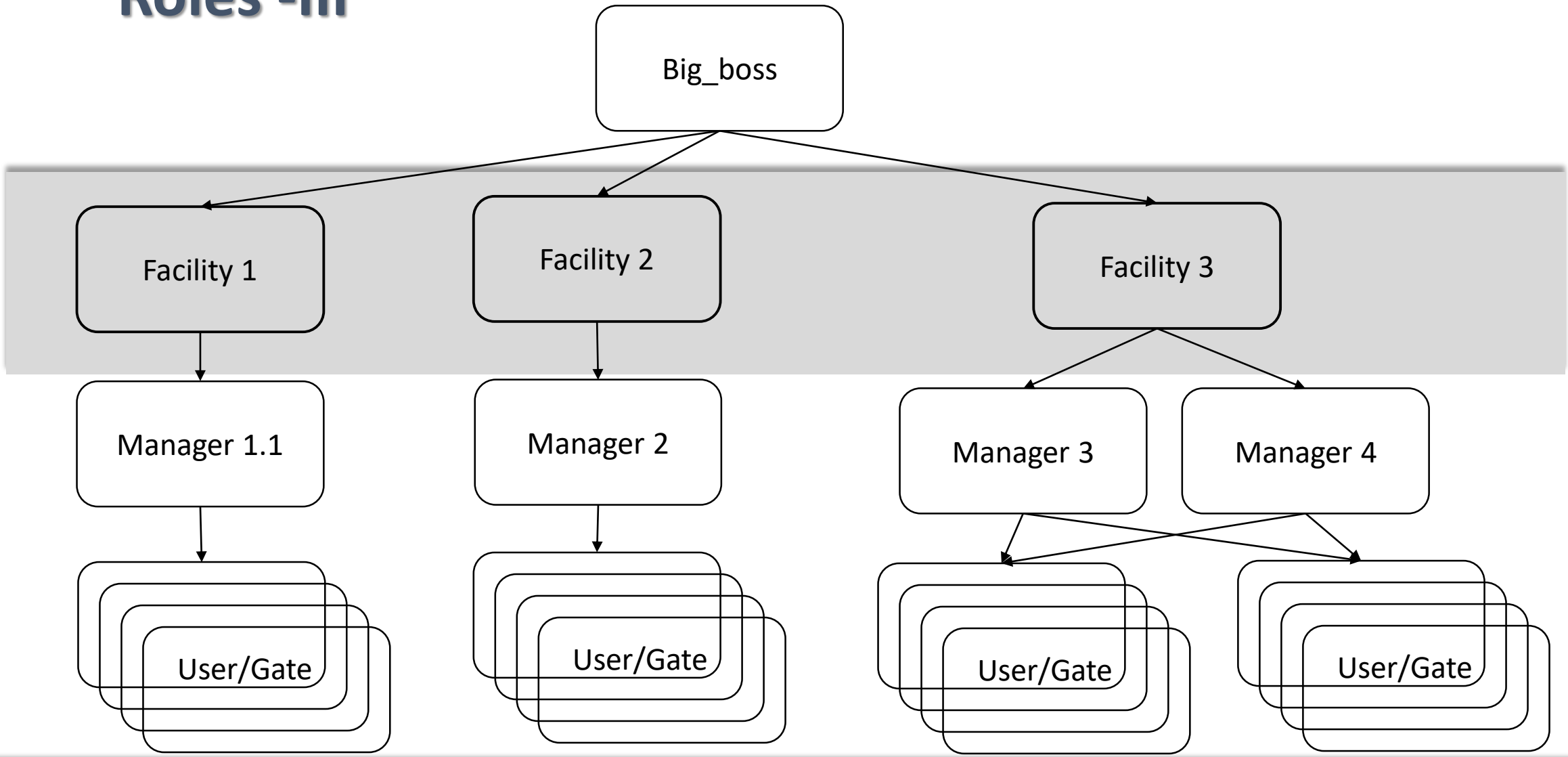
Roles -I

- Defined roles:
  - **big-boss**, which is the creator of contract ,
  - **managers**, who are responsible for the manage roles and add user,
  - **gates**, who are responsible for checking the access rights
  - **Users,** who wants to enter the facility.

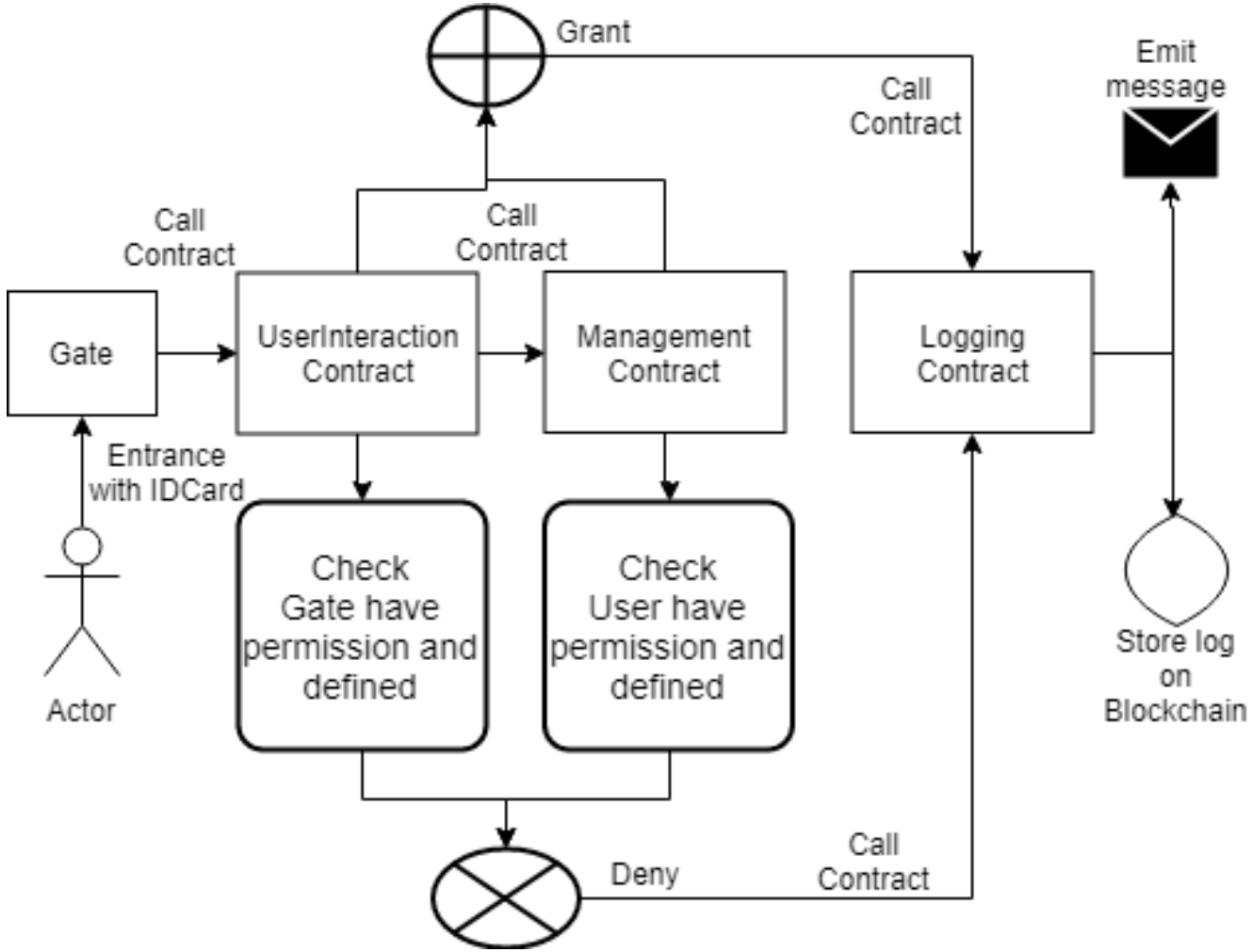
Roles -II


Create Contract Management
Add Manager for TechnoCity1
Add Gate for TechnoCity1
Add User for TechnoCity1
:big_boss
:manager1
:gate1
:user1
Contract created
Manager created
Gate created
User created

Roles -III


Big_boss
Facility 1
Facility 2
Facility 3
Manager 1.1
Manager 2
Manager 3
Manager 4
User/Gate
User/Gate
User/Gate
User/Gate

Flowchart


Grant
Call
Contract
Emit
message
Call
Contract
Call
Contract
Gate
UserInteraction
Contract
Management
Contract
Logging
Contract
Entrance
with IDCard
Actor
Check
Gate have
permission and
defined
Check
User have
permission and
defined
Store log
on
Blockchain
Deny
Call
Contract

Code Samples

```
function Add_Manager(address adres)only_big_boss() public {
require(users[user_addressToIndex[adres]].exists,"User NOT exists!");
users[user_addressToIndex[adres]].isManager=false;      emit ManagerAdded(
users[user_addressToIndex[adres]].adres,  users[user_addressToIndex[adres]].idx);        }
```

```
function getPermittedGatesList(address adres) only_gates() public returns (address[] memory){
return users[user_addressToIndex[adres]].pass_Gates;    }
```

```
 function IsManager(address adres) external view  returns(bool){
if(adres!=big_boss_address && user_addressToIndex[adres]==0){
            revert("User dos not exists!");       }
require(users[user_addressToIndex[adres]].active,"Not active");
require(users[user_addressToIndex[adres]].isManager,"Not active");
return true;    }
```

Presentation Outline

- Introduction and Problem Definition
- Literature review
- Proposed Framework
- Conclusion and Future Work

Conclusion and Future Work-I

- **Work done so far**:
  - **Defining the problem,**
  - **Reviewing the literature for similar studies,**
  - **Designing the access control model,**
  - **Implementing the contracts of access control system,**

Conclusion and Future Work-II

- **Work in progress**:
  - **Developing the user interface with js,**

Conclusion and Future Work-III

- **Future work**:
  - **Improving the proposed model for decreasing the consumed ‘gas’,**
  - **Testing the contracts for security concerns,**
  - **Applying on the real world problem (secure facility entrance).**

References

1. S. Yu, K. Lv, Z. Shao, Y. Guo, J. Zou and B. Zhang, "A High Performance Blockchain Platform for Intelligent Devices," 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), Shenzhen, 2018, pp. 260-261.
2. X. Wang, Q. Feng and J. Chai, "The Research of Consortium Blockchain Dynamic Consensus Based on Data Transaction Evaluation," 2018 11th International Symposium on Computational Intelligence and Design (ISCID), Hangzhou, China, 2018, pp. 214-217.
3. CMP619 lecture notes 1.
4. CMP619 lecture notes 2.
5. A. Ramachandran, M. Kantarcioglu,"Using Blockchain and smart contracts for secure data provenance management", journel CoRR,v. abs/1709.10000, 2017.
6. K. and A. Yurdakul, "Designing a blockchain-based IoT infrastructure with Ethereum, Swarm and LoRa",Journel CoRR, volume abs/1809.07655, 2018.
7. S. Rouhani,V. Pourheidari and R. Deters,"Physical Access Control Management System Based on Permissioned Blockchain",Journel CoRR, volume abs/1901.09873,2019.
8. Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, J. Wan,"Smart contract-based access control for the internet of things", IEEE Internet of Things Journal, 2018.
9. Maesa, Damiano and Mori, Paolo and Ricci, Laura, "Blockchain Based Access Control", pp. 206-220, 10.1007/978-3-319-59665-5-15,2017.
10. http://ethdocs.org/en/latest/introduction/what-is-ethereum.html

Questions?

Visit Blockchain Lab @ Hacettepe University

https://blockchain.cs.hacettepe.edu.tr