Blockchain Technology Based E-Voting Internet of Things System

- Ass. Prof. Dr. Ali Hussain Hamad

Outline

- The Introduction
- The Blockchain Technology
- Why Choose Hyperledger Fabric Platform
- Hyperledger Fabric Network Architecture
- Hyperledger Fabric Transaction Flow
- Iraqi Elections on Oct 2021
- Problems Definition
- Propose System Design

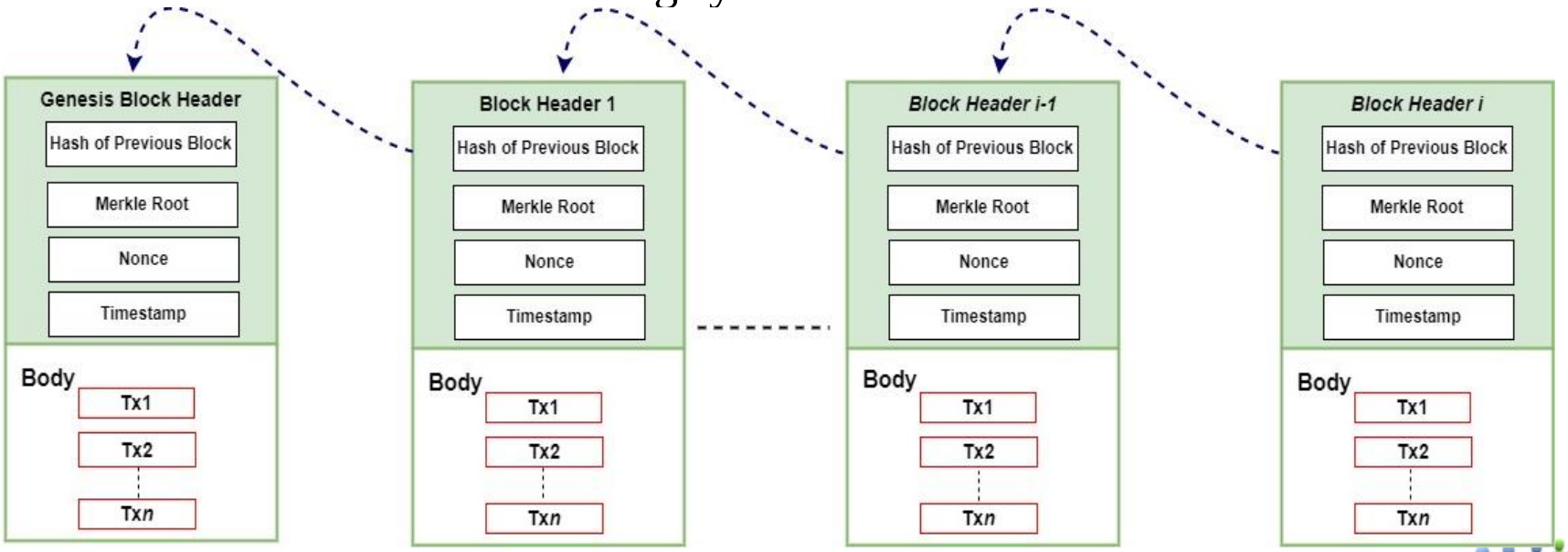
Introduction

Voting is one of the most fundamental components of a democratic society. The trust in the voting results and the privacy of each voter are always the most important concerns in designing a secure E-Voting system.

Recently, **blockchain** has hit the technology space with many promises, especially to make a **verifiable, transparent and decentralized** system.

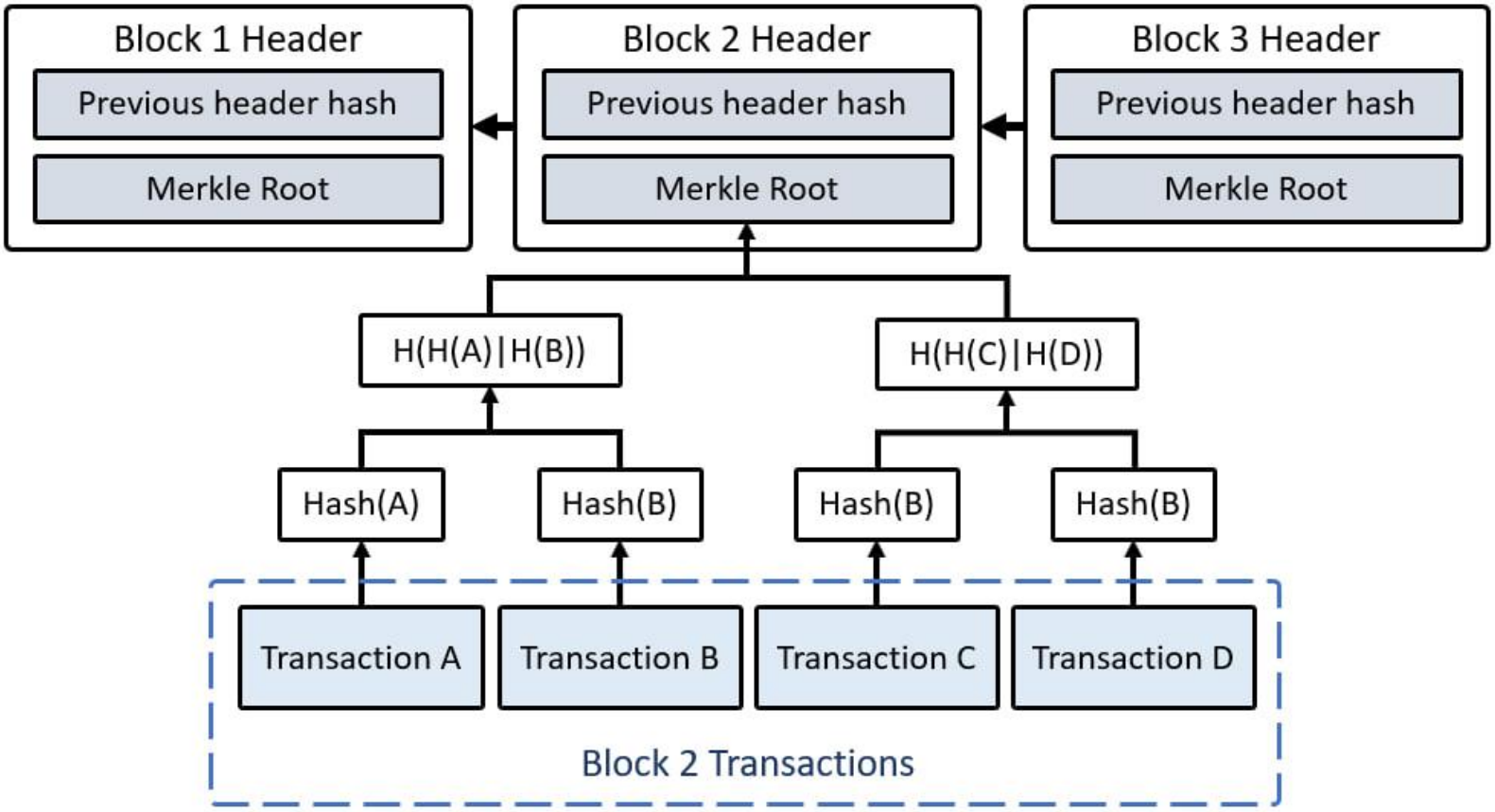
The Blockchain Technology

- A blockchain is a distributed ledger in which entries, or "blocks," are appended to and secured by cryptography as they are added. The blockchain is a decentralized, immutable, and distributed database ledger that logs transaction data in timestamped blocks connected via hashes.
- Because all blockchain transactions are kept in various locations and are available to all users, blockchain is transparent, making it a good alternative for electronic voting systems



Block Architecture

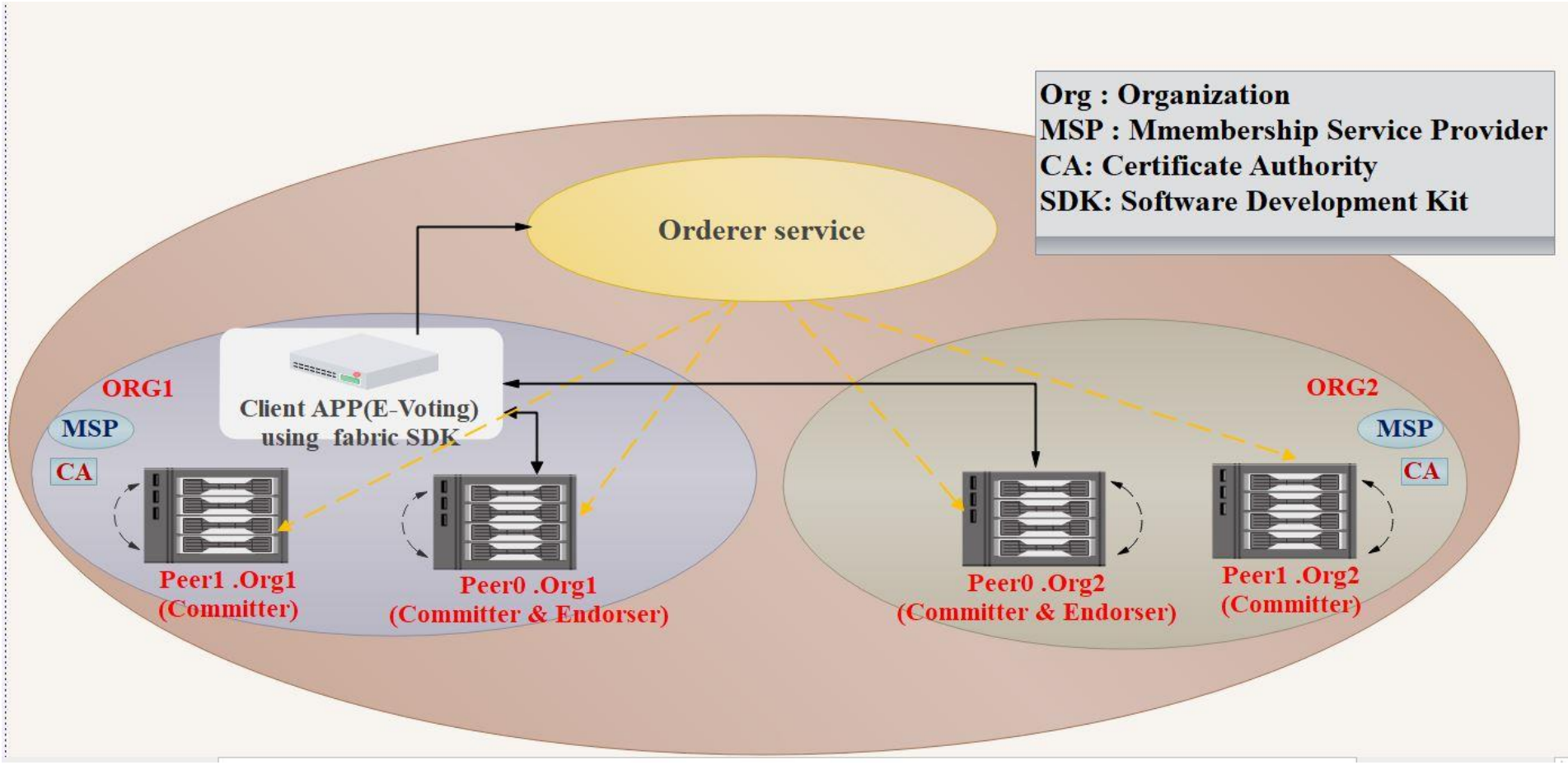
Merkle trees are fundamental part of blockchain technology. For a block, the Merkle root comes from a hashing transaction and pairing two transactions to hash and generate the upper level tree node.



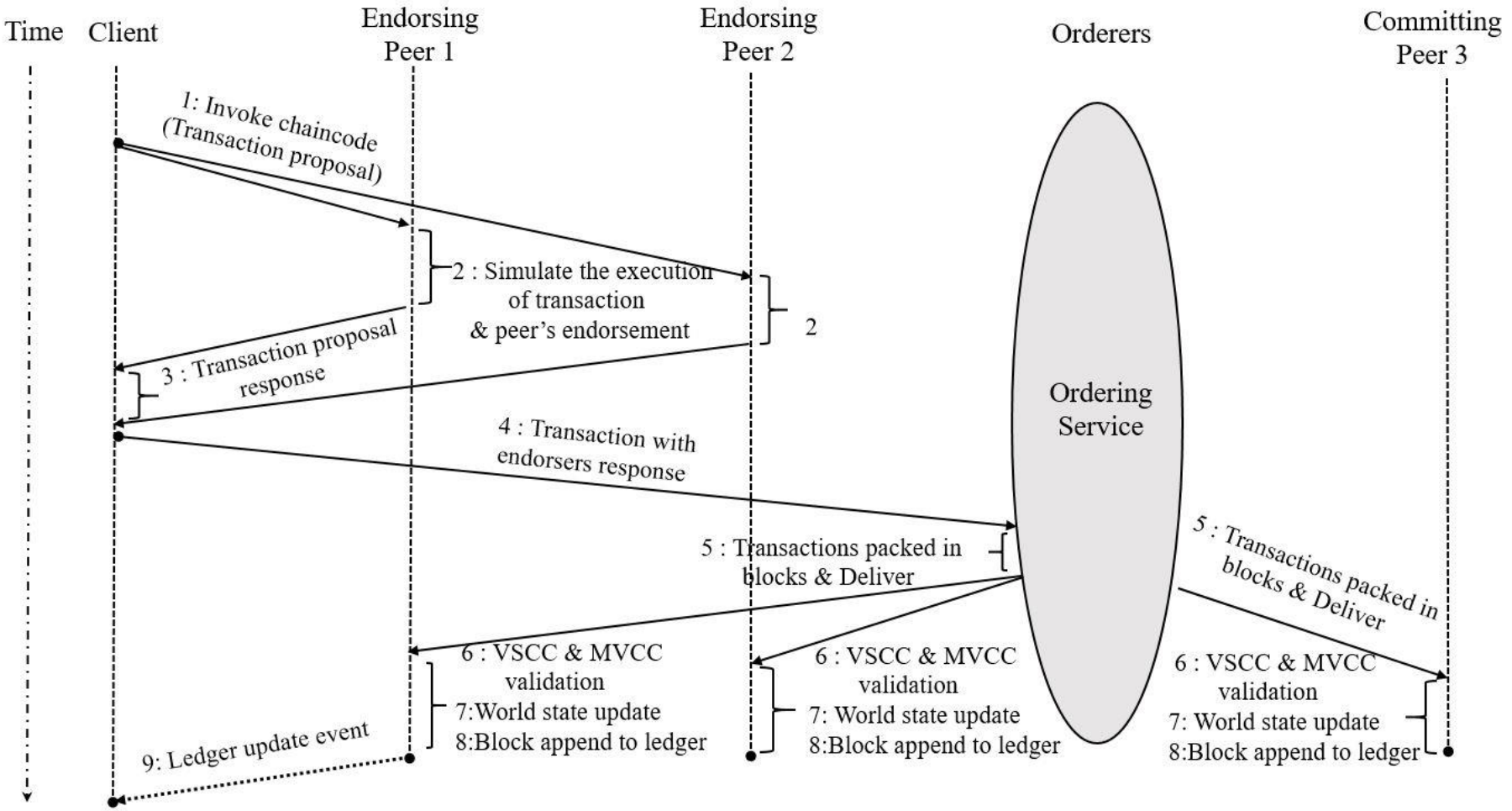
Why Choose Hyperledger Fabric Platform

- Hyperledger Fabric is launched by Linux foundation, it is an open source permissioned distributed ledger technology (DLT) platform.
- Hyperledger Fabric can run decentralized applications (Dapps) developed in languages like Go, java, or node.js.
- In this platform, access to the network is restricted to the network members only.
- Hyperledger fabric doesn't have any cryptocurrency like Bitcoin and Ethereum.
- The blockchain implemented through Fabric ensures the integrity of transactions through TLS certificates for communication between nodes and PKI-based X.509 certificates for node and user authorization.
- Like other types of blockchain technology, fabric has a ledger, rich ledger queries, uses smart contracts, and enables participants to manage transactions.

Hyperledger Fabric Network Architecture

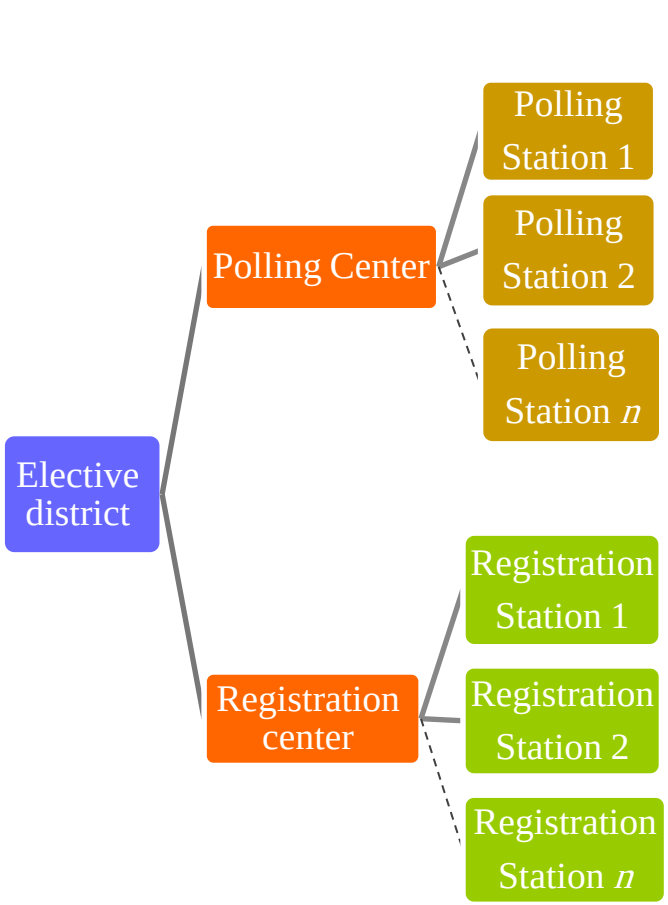


Hyperledger Fabric Transaction Flow



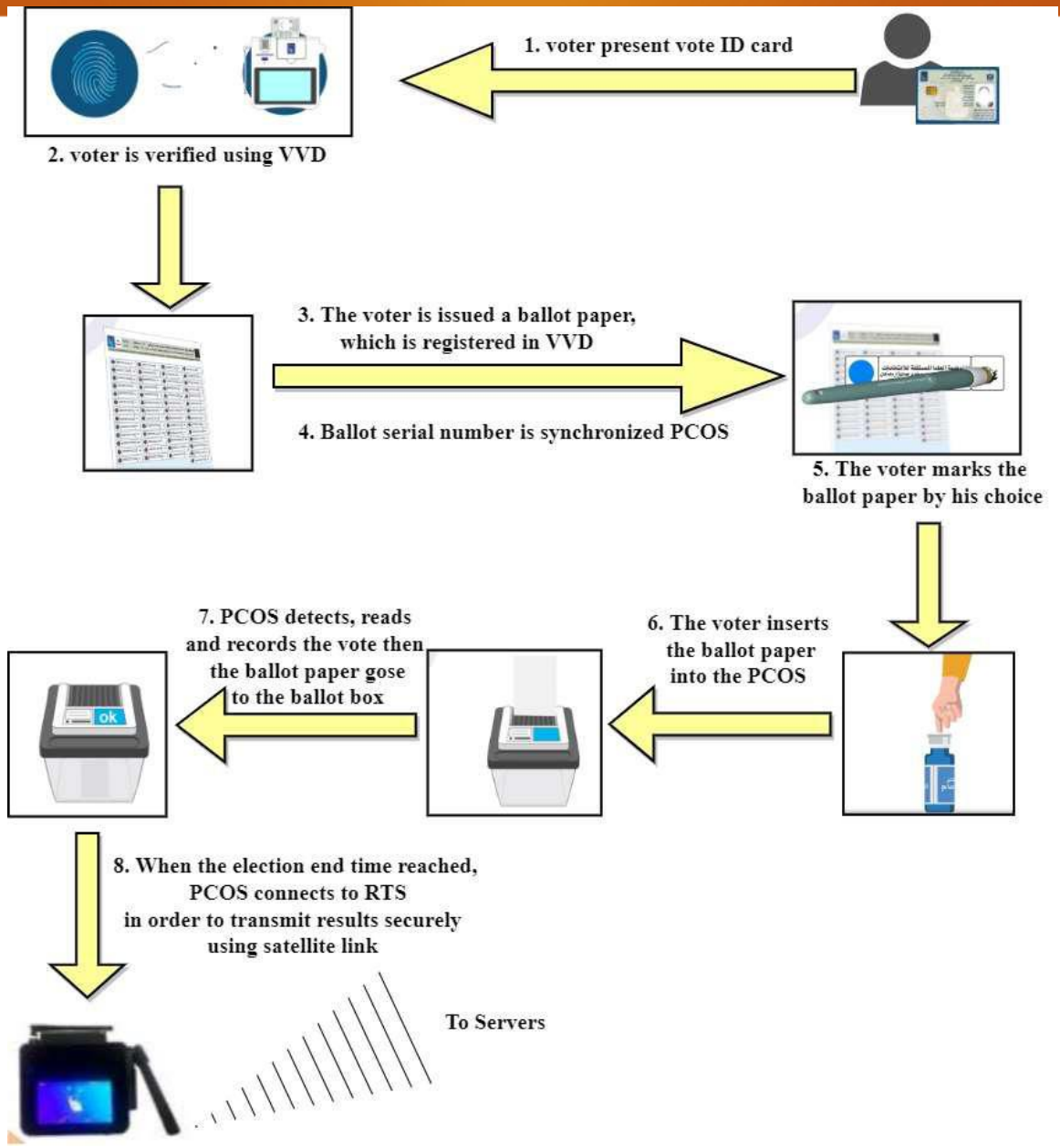
Validation System Chaincode (VSCC)
Multi Version Chaincode (MVCC) validation

Iraqi Elections on Oct 2021



Current issues in election process

- Transparency in the voting process is hampered by the fact that most procedures in electronic voting systems are centralized.
- Current electronic voting techniques pose risks of over authority and altered details, compromising fundamental voting rights to secrecy, privacy, anonymity, and openness.
- Most electronic voting systems are based on traditional databases, which are by nature mutable. In addition, they can only be accessed by a limited group of entities who have been granted permission to add and modify records.
- Manipulation and fraud by those with insider knowledge or by computer hackers.
- The traditional E-voting method is challenging to understand and use, which reduces public faith in the proposed solution and defeats the system's intended goal.
- Factors such as electrical supplies and communication technologies contribute to the rising price of electoral infrastructure.


1. voter present vote ID card
2. voter is verified using VVD
3. The voter is issued a ballot paper, which is registered in VVD
4. Ballot serial number is synchronized PCOS
5. The voter marks the ballot paper by his choice
6. The voter inserts the ballot paper into the PCOS
7. PCOS detects, reads and records the vote then the ballot paper gose to the ballot box
ok
8. When the election end time reached, PCOS connects to RTS in order to transmit results securely using satellite link
To Servers

Aim of the proposed system

1. Suggests an electronic voting system for the Iraqi council of a representative election based on blockchain technology.
2. The proposed E-Voting system based blockchain must meet the electoral law requirements currently in force with the Iraqi government.
3. The primary objective of this work is to propose and envision a permissioned blockchain-based solution for the electronic recording and transmission of votes that will bring confidence, transparency, and integrity to the process of result collation and the entire election process. With this level of openness, interested parties, including voters and political parties, may track votes from every polling location.
4. Design and implement permissioned hyperledger fabric blockchain network.
5. Developed web application for E-voting system
6. Performance evaluation of the proposed system design

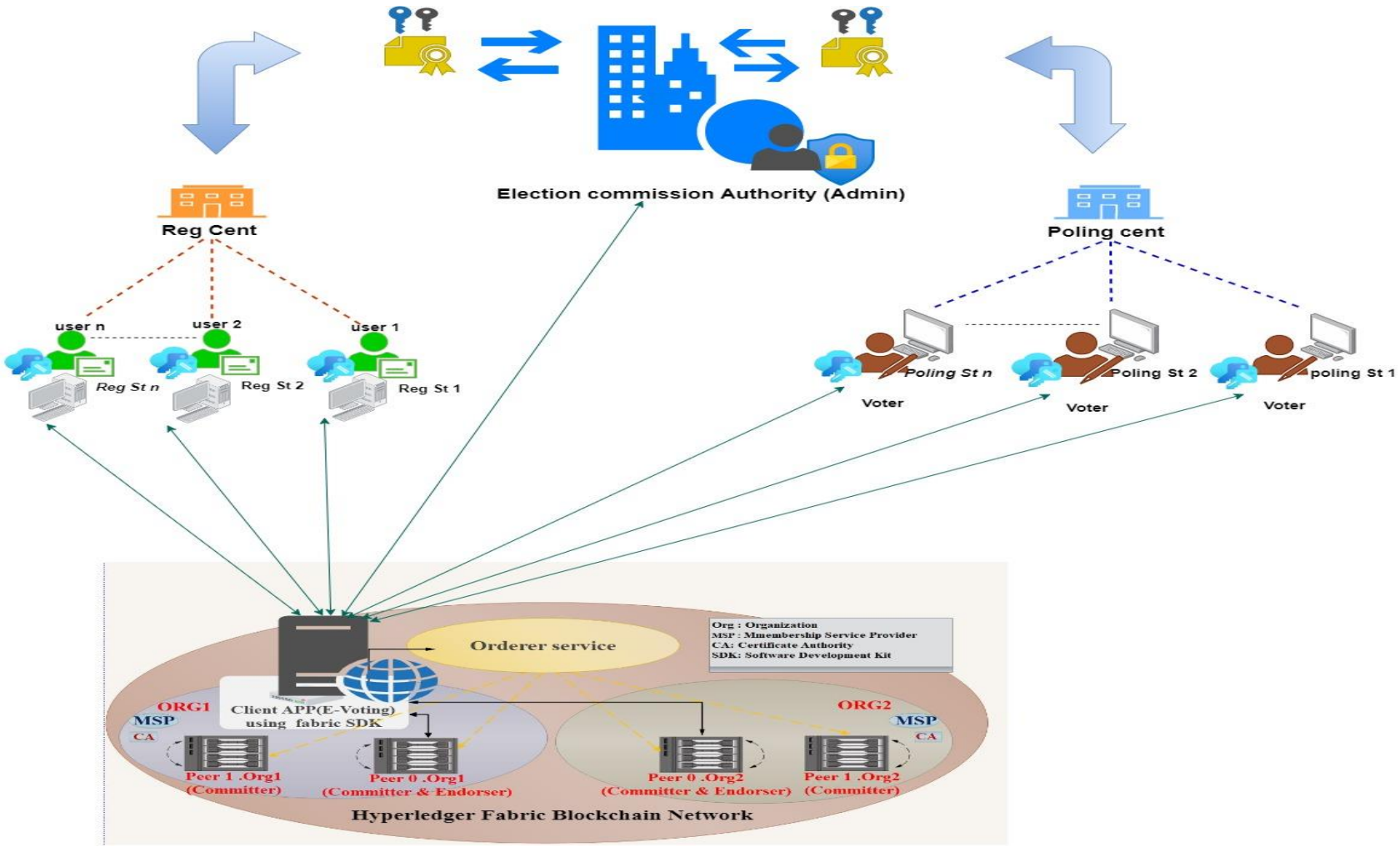
Propose System Design

Proposed Election Roles:

Election Commission Authority (Admin)

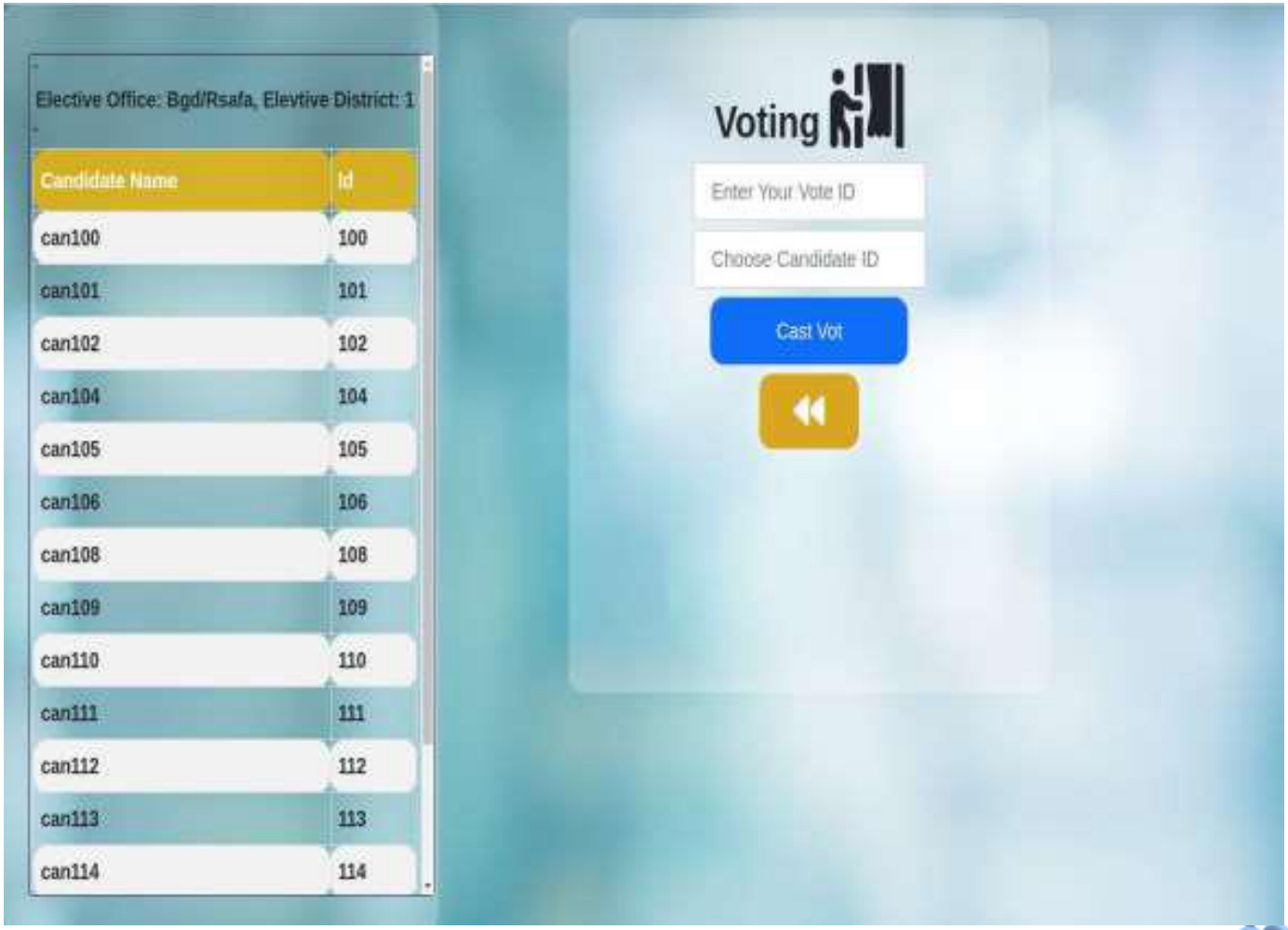
- Set the lifetime of the election
- Manage the lifecycle of an election
- Add the candidates specified to their elective district within their elective office
- Assign registration center and polling center according to their elective district within their elective office
- Create an account on the E-Voting application for the registration center users, and polling center users
- Grant and revoke users' access right to fabric network, the CA's admin register users (i.e. registration center users, polling center users, and voters) and store its credentials in the wallet

Proposed E-Voting System based Hyperledger Fabric Network

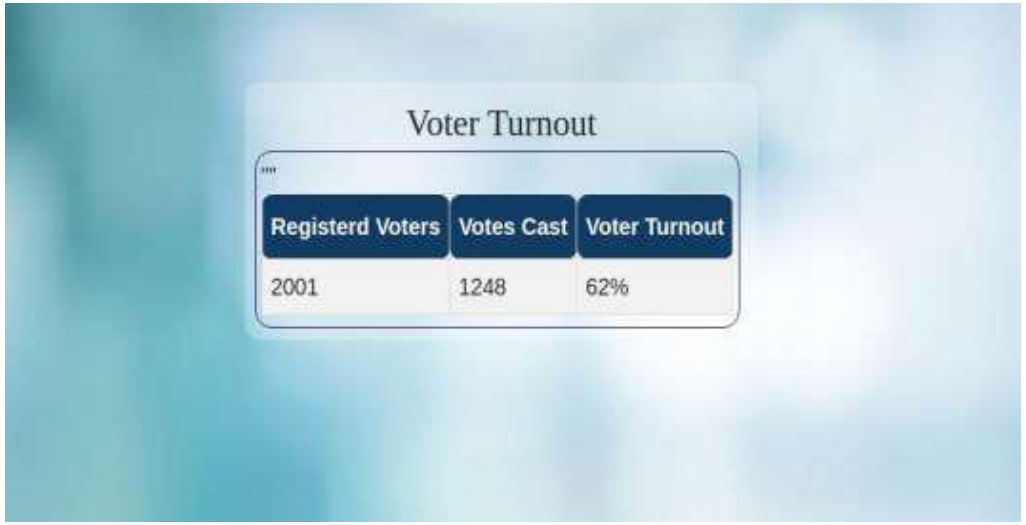


" ========== Candidate List ========== "

Candidate Name	Id	Election Office	Election district
NOTA	0	0	0
can100	100	Bgd/Rsafa	1
can101	101	Bgd/Rsafa	1
can102	102	Bgd/Rsafa	1
can104	104	Bgd/Rsafa	1
can105	105	Bgd/Rsafa	1
can106	106	Bgd/Rsafa	1
can108	108	Bgd/Rsafa	1
can109	109	Bgd/Rsafa	1


Elective Office: Bgd/Rsafa, Elevtive District: 1
Candidate Name
Id
can100
100
can101
101
can102
102
can104
104
can105
105
can106
106
can108
108
can109
109
can110
110
can111
111
can112
112
can113
113
can114
114
Voting
Enter Your Vote ID
Choose Candidate ID
Cast Vot


Result Search vote by ID
"==========="
voter Id
CandidateId
Candidate Name
Elective Office
Election district
5000
108
can108
Bgd/Rsafa
1


Voter Turnout
""
Registerd Voters
Votes Cast
Voter Turnout
2001
1248
62%

View All Casted Votes

" ========== Voter List ========== "

vote Id	hasVoted	CandidateId	Candidate Name	Elective Office	Elective district
0	true	108	can108	Bgd/Rsafa	1
1	true	103	can103	Bgd/Rsafa	1
10	true	103	can103	Bgd/Rsafa	1
100	true	104	can104	Bgd/Rsafa	1
1001	true	601	can601	Babel	1
1002	true	602	can602	Babel	1
1003	true	601	can601	Babel	1
1004	true	601	can601	Babel	1
1005	true	600	can600	Babel	1

Conclusions

1. The proposed E-voting system based hyperledger fabric blockchain network is applicable
2. It could satisfy electronic voting security requirements such as eligibility, anonymity, immutability, traceability, and Integrity.
3. The proposed system based on hyperledger fabric is scalable according to business requirements.
4. The proposed system obtained good results with high transaction send rates on large block sizes. Therefore, to maintain high throughput and low latency, the block timeouts and block size should be large.
5. The proposed E-Voting web application is easy to use by each election participant(such as election commission authority, registration center users, polling center users, and voters).
6. The proposed electoral system could be applied successfully when an advertising campaign and voter education about the system's reliability, and has other advantages, such as maintaining the confidentiality of voter data and integrity, and any voter can verify his/her vote.

The End…

Thanks for your Listening