Applying Blockchain to the Voting System

1. Overview

Voting is one significant occasion happening once in a while, yet its result remains for a long period of time. These days, paper-based system is the most common method. In the 21st century, when the technology is increasingly developing, is it time to upgrade voting system to the next level? For example, online voting. The concept is nothing new. There are already some voting occasions that utilize electronic devices such as laptops and smart phones. The process of online voting is much easier for the voters to perform than paper-based system and they are able to vote where ever they are, just with their electronic devices. The issues arise when it comes to the result. How is the result calculated? Does the vote intact when it arrives? Where does the data go? Is it secured? This report aims to clarify the issues of online voting and proposes exploiting the possibility of blockchain technology to address those.

2. Current Online Voting

The usual technology applied to the online voting is centralize network. This means all the data which people send is stored in the database on a server. Therefore, only those who have the authority are able to access to the data. This is called third-party problem. The data is under control of

another party other than the users. As a result, the users have to completely trust the system they are using.

The trusted intermediary works as a server to collect data and implement it owns function which known by the users, in voting case is calculating the result. The process of casting a vote is pretty simple to the voters. Firstly, they use their ID card or account to login to the system provided by the one who organizes the voting event. After they cast the vote, it is delivered to the system. Finally, the system displays the result when the voting is closed.

One problem of this kind of network is the user have trust the server would keep their data secured. At the end of the process, only the server has the authority to read the data. The users have no idea about how their data are handled. This makes fraud easier to comprehend. The server has full control of the data, or more significantly, the result of the vote. It could regulate the result as their own wish by altering the decision in the ballot of the voter. Additionally, clone vote could be added to adjust the number of the votes, or else, the number of the votes could be miscounted to meet their expectations. Another problem is anonymity. The voters might not know who are in the vote, but the server does. Or better, they have a full list of them. What if these data are exploited for personal uses? This may be related to privacy of the user. Last but not least, the one and only database.

Since all the data is delivered to the database on the server, it makes the server vulnerable to attackers. They could undertake the server, steal the data including, the detail of the voting occasion and the voters and then take control of the result. Moreover, crash database could be an issue. This cause lost data, which leads to the result is impossible to calculate.

3. Blockchain technology

Blockchain technology is first applied for cryptocurrency. It is known as a distributed database where the transactions are recorded within a block. All the blocks are shared with those who are in the network. That means everyone who joins the system has a copy of the ledger (database). All the copied ledger has to be up-to-date whenever there is new data. Since there is a change in database including adding new block or someone tries to alter the existing data, the whole network notices to verify the date before it can be added to the chain. That makes it impossible to hack or change the data in the ledger. However, the potential of blockchain is much more than cryptocurrency. Blockchain is a secured and robust system that could be suitable for the online voting system. The issues of voting could be addressed using the technology of blockchain for E-voting system.

Firstly, trust is ensured. Since the blockchain is an immutable and shared database, the votes in database are unable to be altered without voter knowledge. Besides, all voters are able to verify each other votes, yet

know their identification and the detail of the votes due to the encryption mechanism of blockchain. Moreover, only legitimate ballots are counted to make the result reliable. Secondly, is robustness. Anyone who joins the network have a copy of the database so it can be recovered. This helps prevent the possibility of losing data, unlike the centralize network database is under control of one unity.

4. Centralized network in comparison with decentralized network

The strength of the current online voting centralized network is confidentiality, which is a crucial characteristic of the event, and high performance. The data from the client send directly to the server. The server task is to verify and handle the received data. After that, the result is delivered back to the client. The verification and handle data implements on one single server, that makes the whole process perform more quickly.

On the other hand, the weakness of this kind of network are trust and robustness. That makes the blockchain possible dealing with issues of the centralized network. Having said that the limitation of blockchain technology is also on the table. Since the consensus protocol required the whole network to confirm and update its database, the performance of the proposed technology is lower. In addition, everyone has a copy of a database makes the voting become open to the public. In fact, the votes are shown to everyone. Although they are not able to observe the detail of the

ballot, they might have an idea of something is about to happen. For example, they could acknowledge the number of voters taking part in the voting event by counting the number of account. As a result, this can lead to loss the confidentiality of the occasion.

5. E-voting Blockchain process

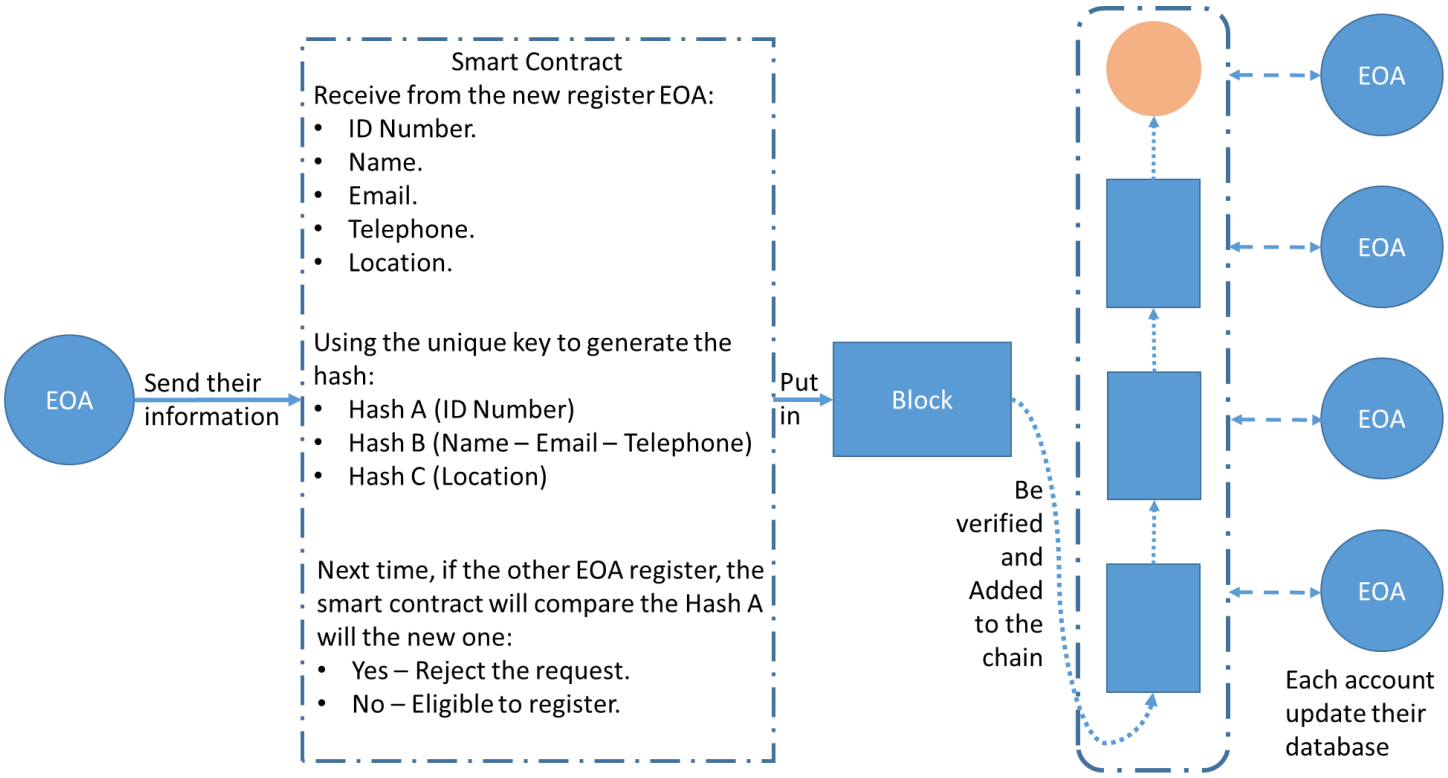
We aim to use Ethereum Blockchain technology to create the voting system for internal Bosch associates. First, you need to know a little bit about Ethereum blockchain then read our concept process of "e-Voting using Ethereum blockchain technology".

Ethereum Process:

- There are 2 types of accounts (nodes) in Ethereum:
    - Externally owned account (EOA): this is an account which can exchange and store eth (ETH is a cryptocurrency in Ethereum, like Bitcoin).
    - Contract: this is an account which can send and store eth but it also can store and execute code (like function, program), known as Smart Contract.
- Hash function: This is one-way method that each input can only go with one output (X -> F(X) = Y), can't be reversed. (Example: https://anders.com/blockchain/hash.html)

- A blockchain is known as a public shared database, which is stored in the EVM (Ethereum Virtual Machine) and each account will have a copy of that database.
- All the transactions will be put in a block, then be verified by the network before adding it into the chain (shared database). The EOAs in this network will update their database base on it.
- The shared data is immutable, can't be changed after saved.
- EOAs just verify there is a transaction with the information is save into the specific block, don't prove that the information is truth or legal. So, basically, the input is essential to be observe before send it into the blockchain network.

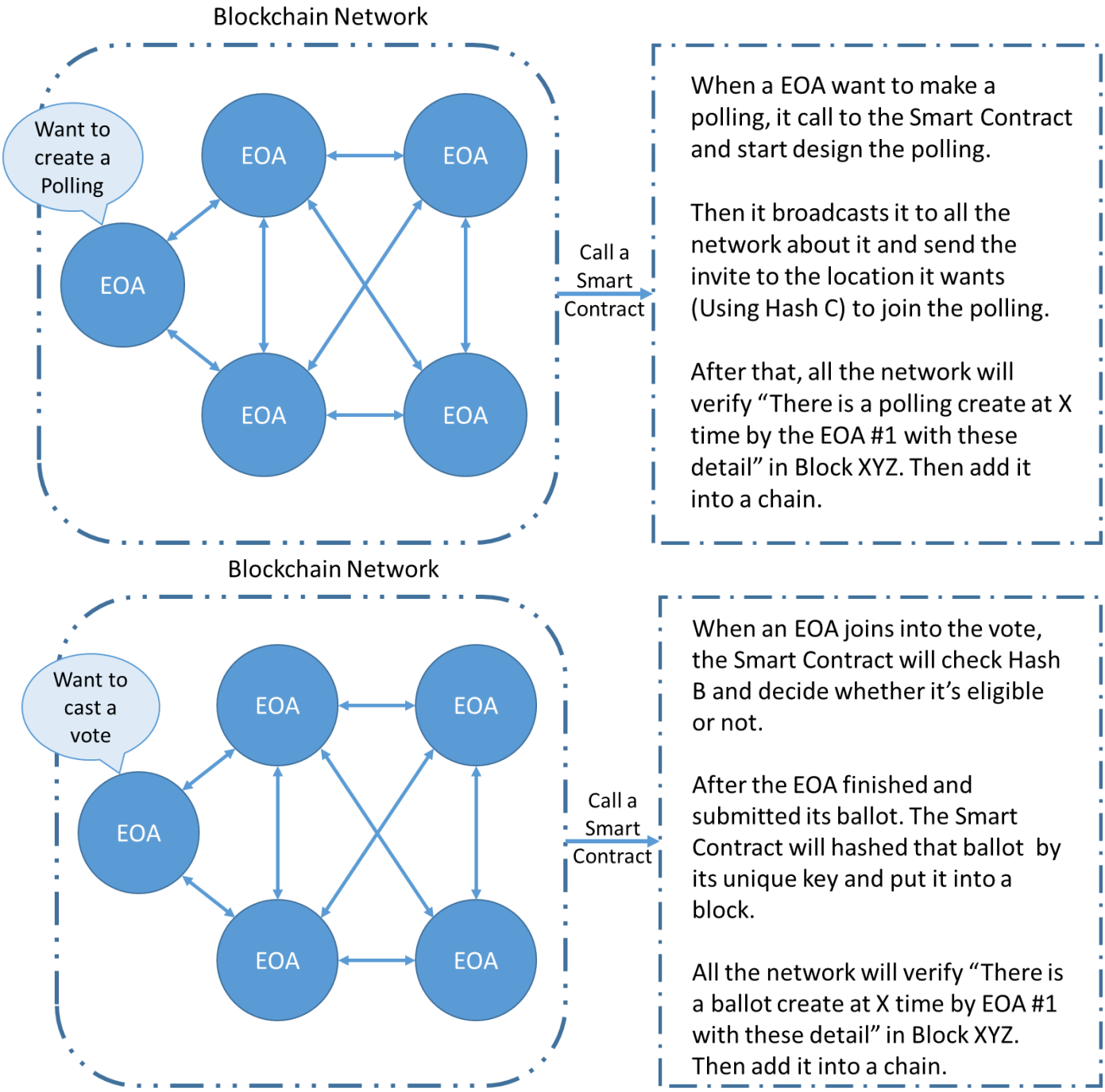
Register and Join in the blockchain network



1. The new account has to send their information to the Smart Contract.
2. The Smart Contract will generate the hash A – B –C by its unique key.
3. Then it put these hash into a block like a transaction.
4. All the network verifies that "There is the transaction X with detail Y is created at Z time and add to the block W at T time".

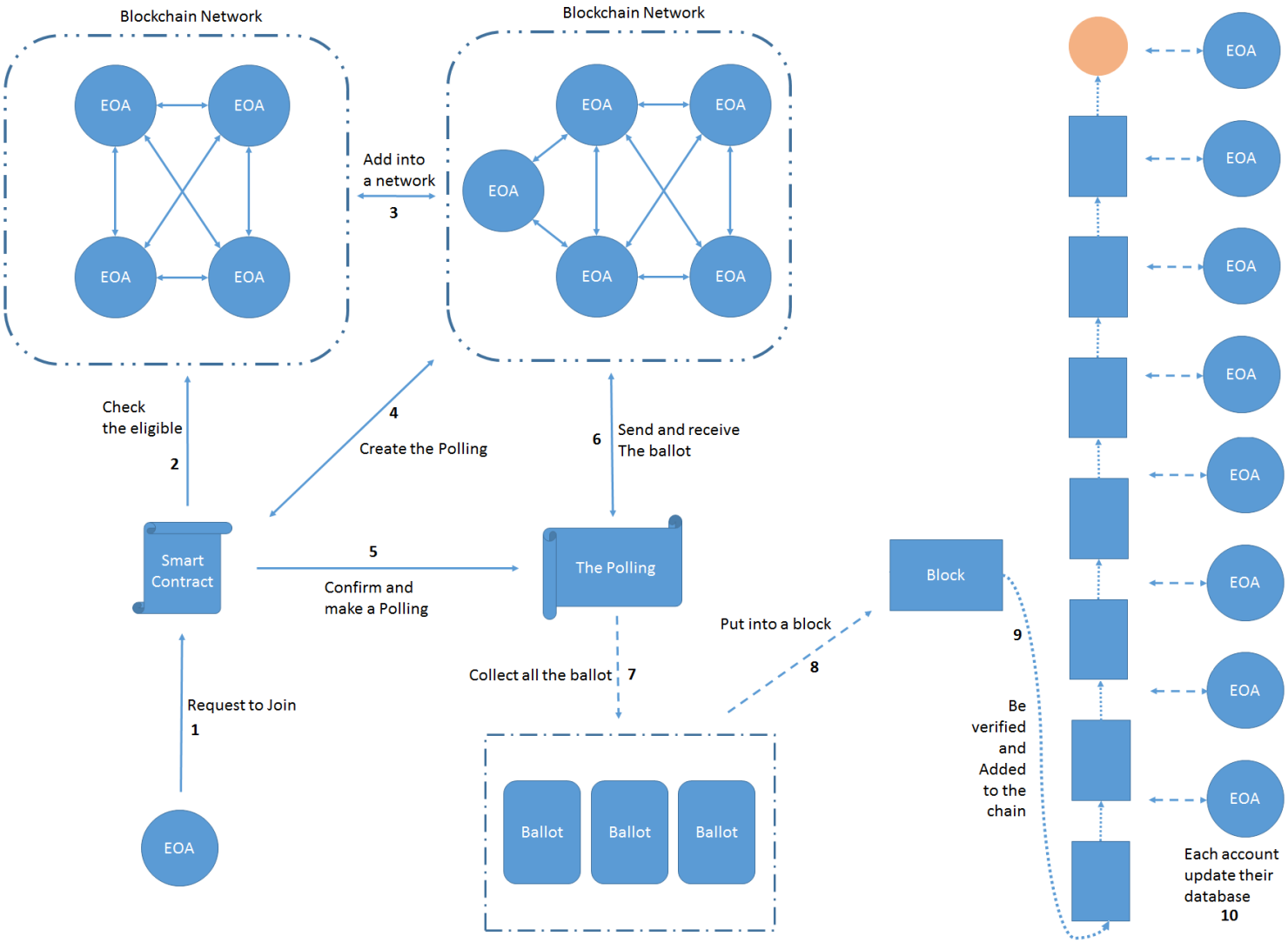
** Next time, the other new account register, the Smart Contract will compare the new hash A with the old hash A in the database, if the result is Match then reject to create an account, otherwise create an account.

Create the polling and join to cast the ballot



* We have mention about if the user randomly input the ID number to create account, we could detect it in this phase. The way we can do it consensus. A node who create a polling know how many voters in their polling (this is internal system), so when there is more Vote in the polling, we can easily detect it. After the vote is finish, the smart contract B will provide the list of user (the hashed address) choose Yes, No or None. All the network can see the result and check whether their votes are counted or not.

Overview


Blockchain Network
EOA
EOA
EOA
EOA
Add into
a network
3
Blockchain Network
EOA
EOA
EOA
EOA
EOA
Check
the eligible
2
4
Create the Polling
6
Send and receive
The ballot
Smart
Contract
5
Confirm and
make a Polling
The Polling
Request to Join
1
EOA
Collect all the ballot
7
Ballot
Ballot
Ballot
Put into a block
8
Block
9
Be
verified
and
Added
to the
chain
EOA
EOA
EOA
EOA
EOA
EOA
EOA
EOA
Each account
update their
database
10