Business Problems

Our project is about how to apply blockchain technology to a voting system at Bosch. After research a couple of days, there are some problems we should think about and able to solve them: Count – Clone – Progress.

In the traditional or server-client way, people have to trust the third-party that their votes will be counted. People don't know who, when and how their votes are counted, only know the result at the end. By using the blockchain technology, everyone is able to see everything from the phase register to the release result phase, everything is transparent. However, the blockchain technology aim to the Robustness and the Privacy, which leads to the problem: Clone.

No one knows the others' identities, this is good for a voting system. We only need to limit one-person-one-account. Our solution is in the register phase; any associates have to use their ID number in Bosch to sign up. The smart contract will generate the hash of that ID number (called Hash A) and store it in a database (blockchain). At Bosch, each associates have a unique ID number so we will take an advantage of it. Moreover, when someone open a vote, they will invite people by fill in the ID number, then the smart contract will generate the Hash A and send the invite to the account who own that Hash A. Everyone knows the ID number (in real life) but don't know the hash function to generate the Hash A. I believe that the privacy will be ensured and no one has a clone account.

Last but not least is the progress problem. Since every user can see everything in the blockchain network, they are able to calculate the result without waiting to the end. Take an example: "101 people join in a vote, 50 people vote Yes, 50 people vote No. The last person can see all of that information and tell everybody that who pay him more, he will vote for that person." This is a big problem, so our suggestion is hiding. We will design the smart contract in the way that it only so the progress of the vote, like 90% people has casted their vote. At the end of the vote, the smart contract will generate the list of people (Hashed ID) who vote for each option, the result of the vote.

There are some problems we find out during the research, we will keep digging and see if there are any aspects we should think more about.

EOA

Send their information →

Smart Contract
Receive from the new register node:
- ID Number.
- Name.
- Email.
- Telephone.
- Location.

Using the unique key to generate the hash:
- Hash A (ID Number)
- Hash B (Name – Email – Telephone)
- Hash C (Location)

Next time, if the other EOA register, the smart contract will compare the Hash A will the new one:
- Yes – Reject the request.
- No – Eligible to register.

Put in

Block

Be verified and Added to the chain

EOA

EOA

EOA

EOA

Each account update their database