# **Voting Blockchain Process**

We aim to use Ethereum Blockchain technology to create the voting system for internal Bosch associates. There is something you need to know before reading the process:

* Hash is a one-way function which will generate the unique string base on an input. Just like X -> F(x) = Y. When X go through the function F(X), there is only one result Y, can’t using Y to find X.
* There are 2 types of accounts (nodes) in Ethereum:
  + Externally owned account (EOAs): an account controlled by a private key, and if you own the private key associated with the EOA you have the ability to send ether and messages from it.
  + Contract: an account that has its own code, and is controlled by code.
* All the EOAs connect together and create a blockchain network, each EOA will have a full copy of the shared data (called the ledger).
* Every action in the network is called a transaction.
* 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.
* Imaging a smart contract is like a function, it will be called and execute when it meets its conditions. EOA can read the smart contract before start using it.

## **Register and Join in the blockchain network**

* When a person wants to take part in the network, they will create an account, then call a smart contract A to be verified that they come from Bosch and don’t have any account in this network (requirement: one-person-one-account). This smart contract A will generate the hash A – B – C by using its unique key, then hash these hash A – B – C again to Hash Z and put it in the block like a transaction. From now, if the new user input the existed ID number, the smart contract can find in the shared data, decrypt the block and compare the other hash A. Furthermore, when they try to random input the ID number to create an account, the smart contract will accept that but when they use it to cast the ballot, it will be detected (mention later below). Like we said at the beginning, the input of the blockchain network is essential so basically, it will base on the honest of participants 50 and the logic of smart contract 50.

## **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**