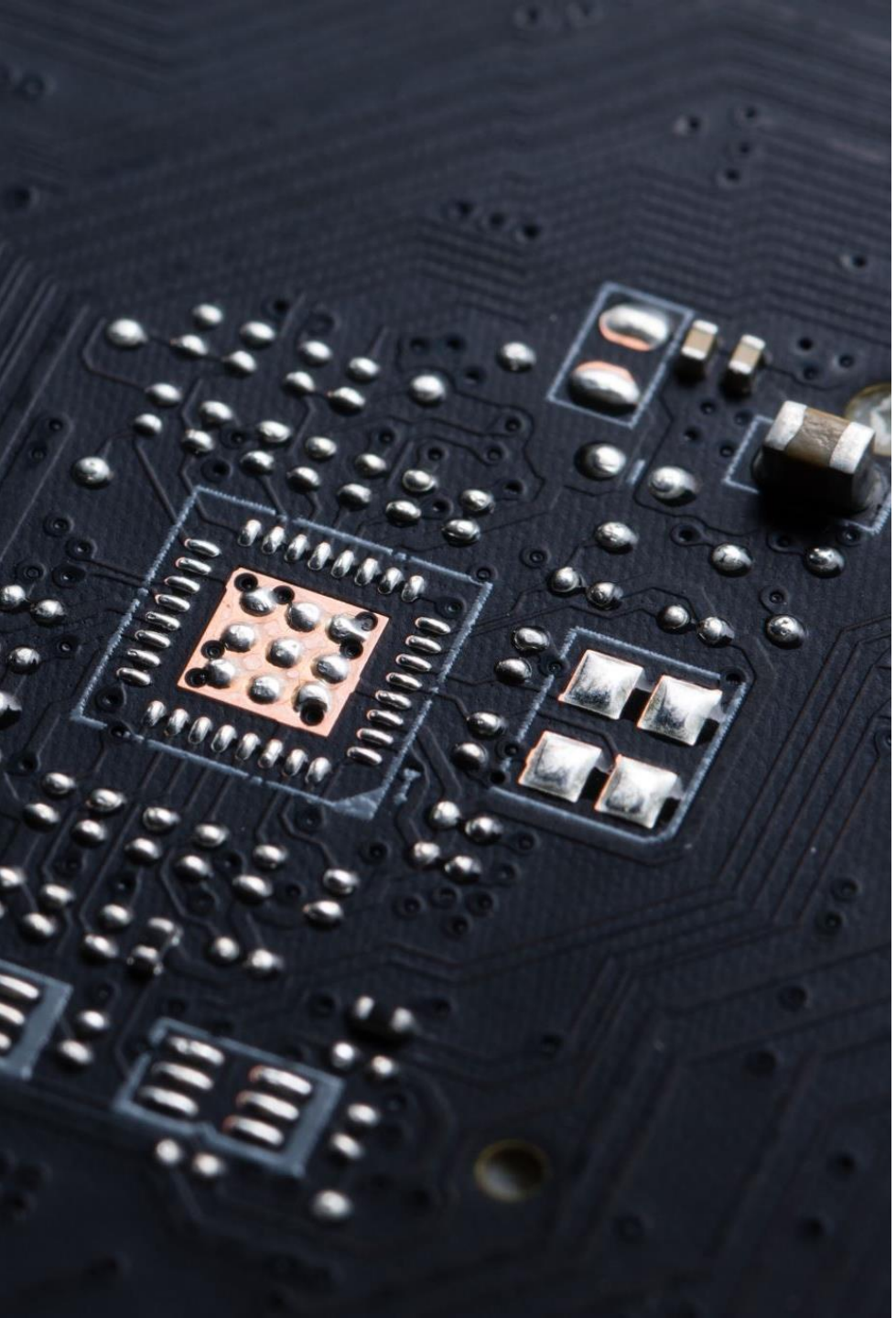
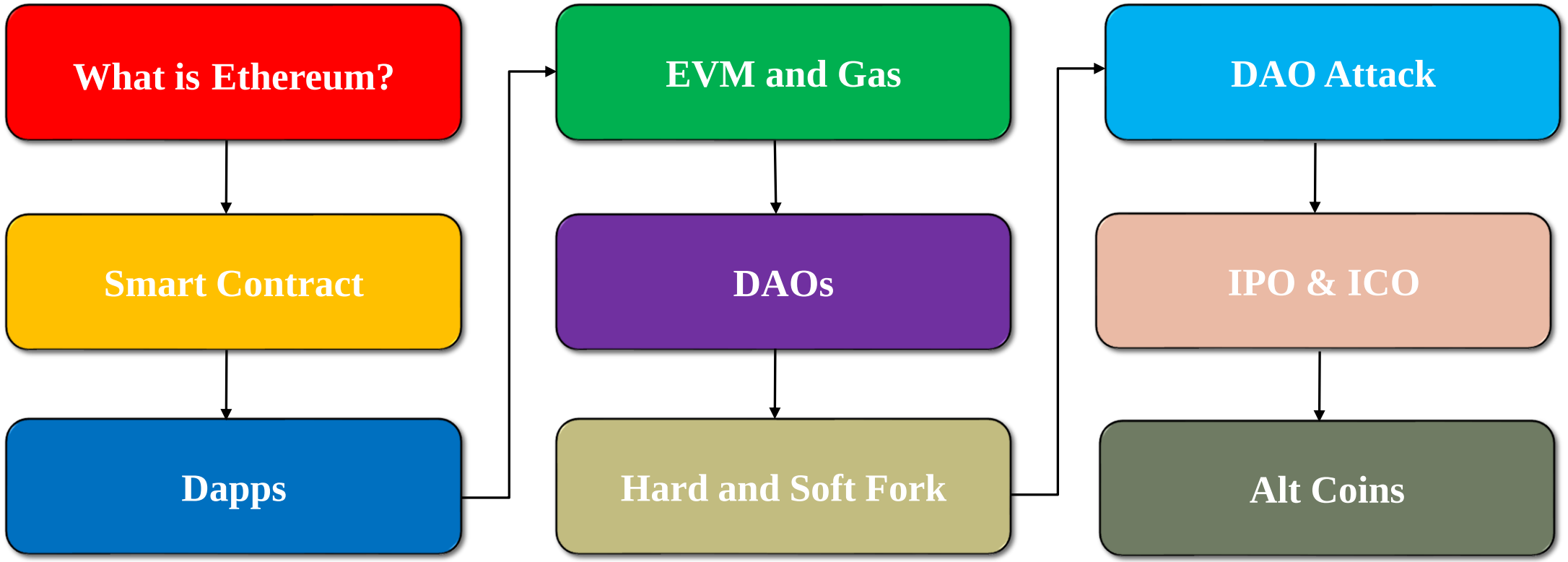
Blockchain

Dr. Bahar Ali
Assistant Professor (CS), National University Of Computer and Emerging Sciences, Peshawar.



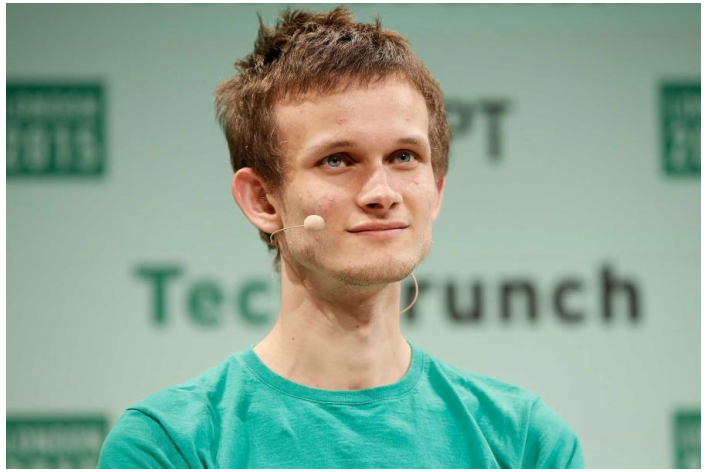
Ethereum

Contents – Module C

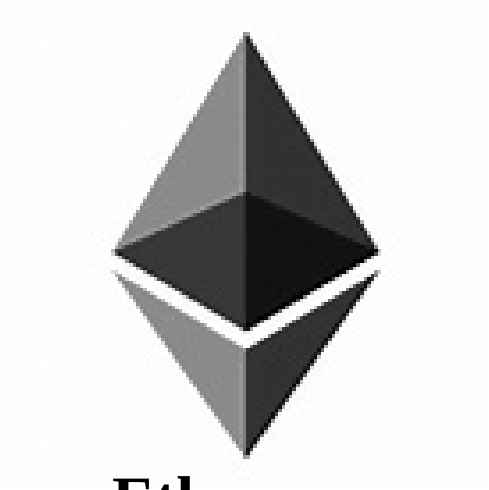


Founder of Ethereum

- Vatalik Buterin founded Ethereum in 2013 at the age of 19

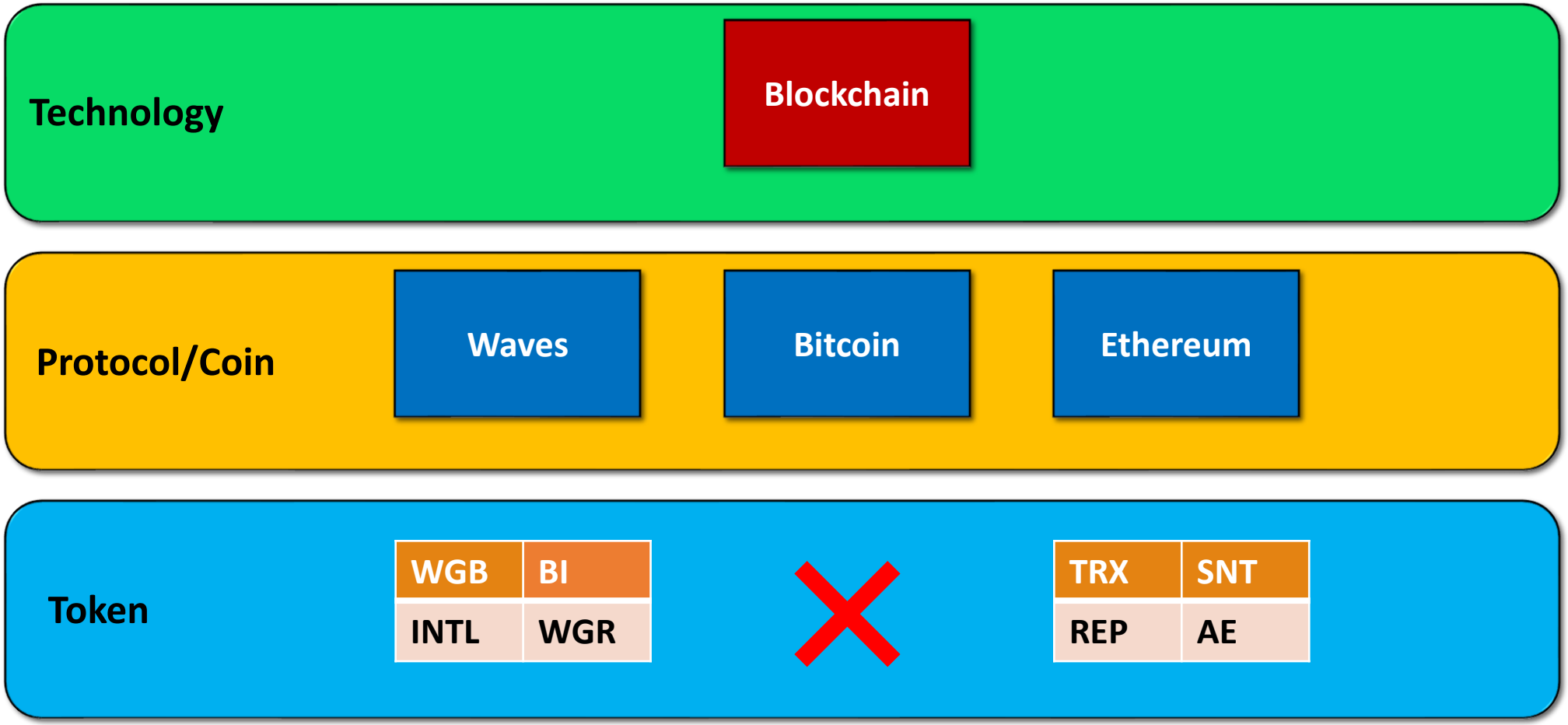


Vitalik Buterin



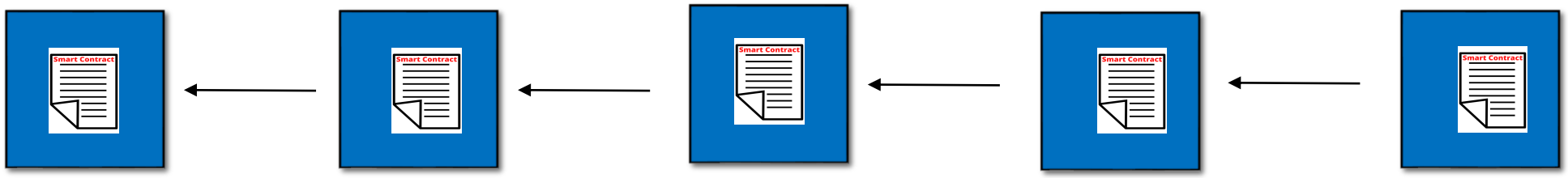
Ethereum

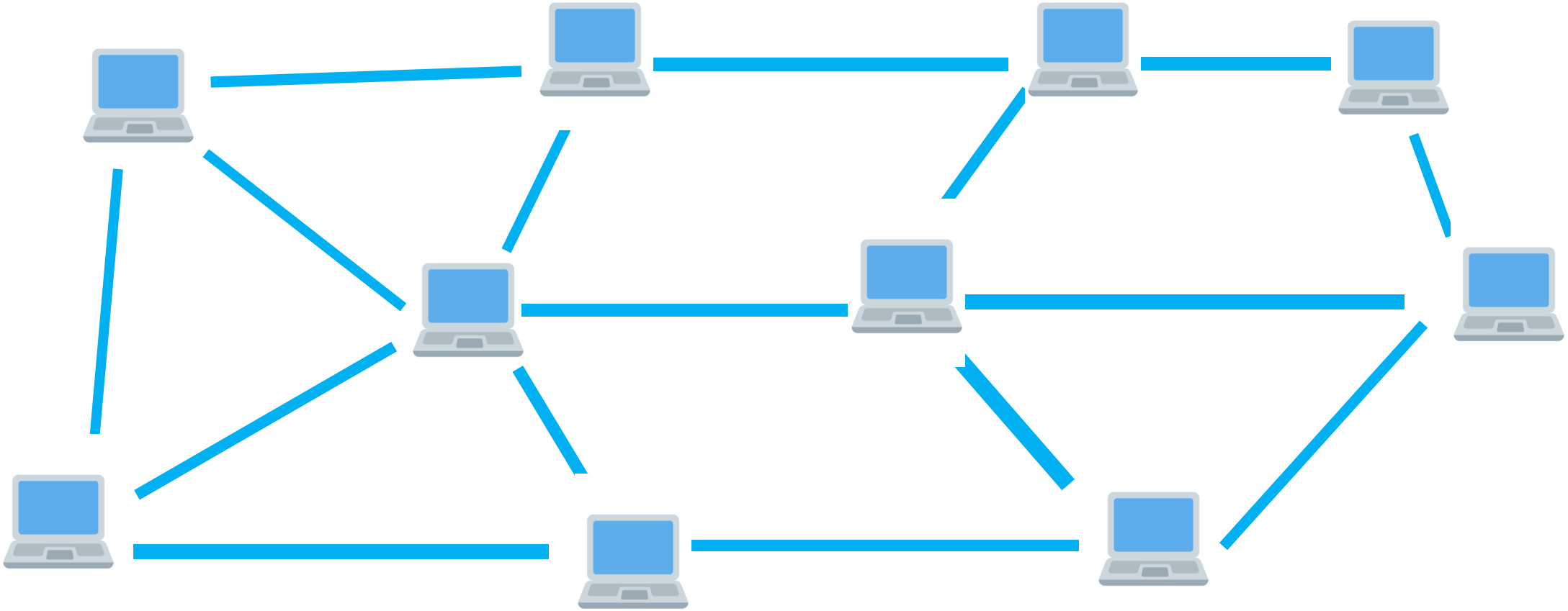
What is Ethereum?



What is Ethereum?

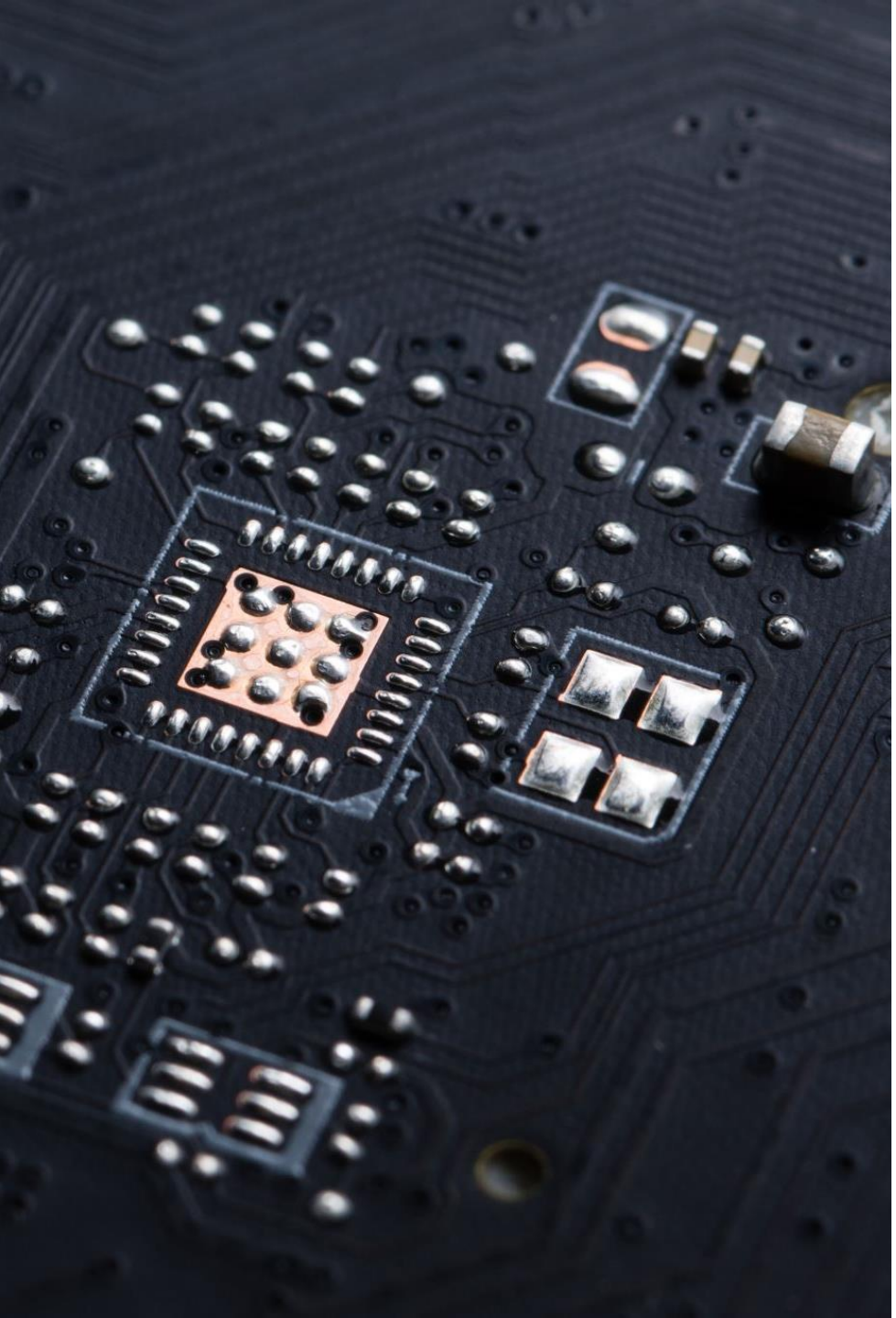
- Apart from data and transactions, Ethereum runs programs on the Blockchain
- Ethereum get popular as it provides tokens, while the Bitcoins protocol does not provide tokens
- Ethereum is an open-source blockchain-based platform


Smart Contract
Smart Contract
Smart Contract
Smart Contract
Smart Contract



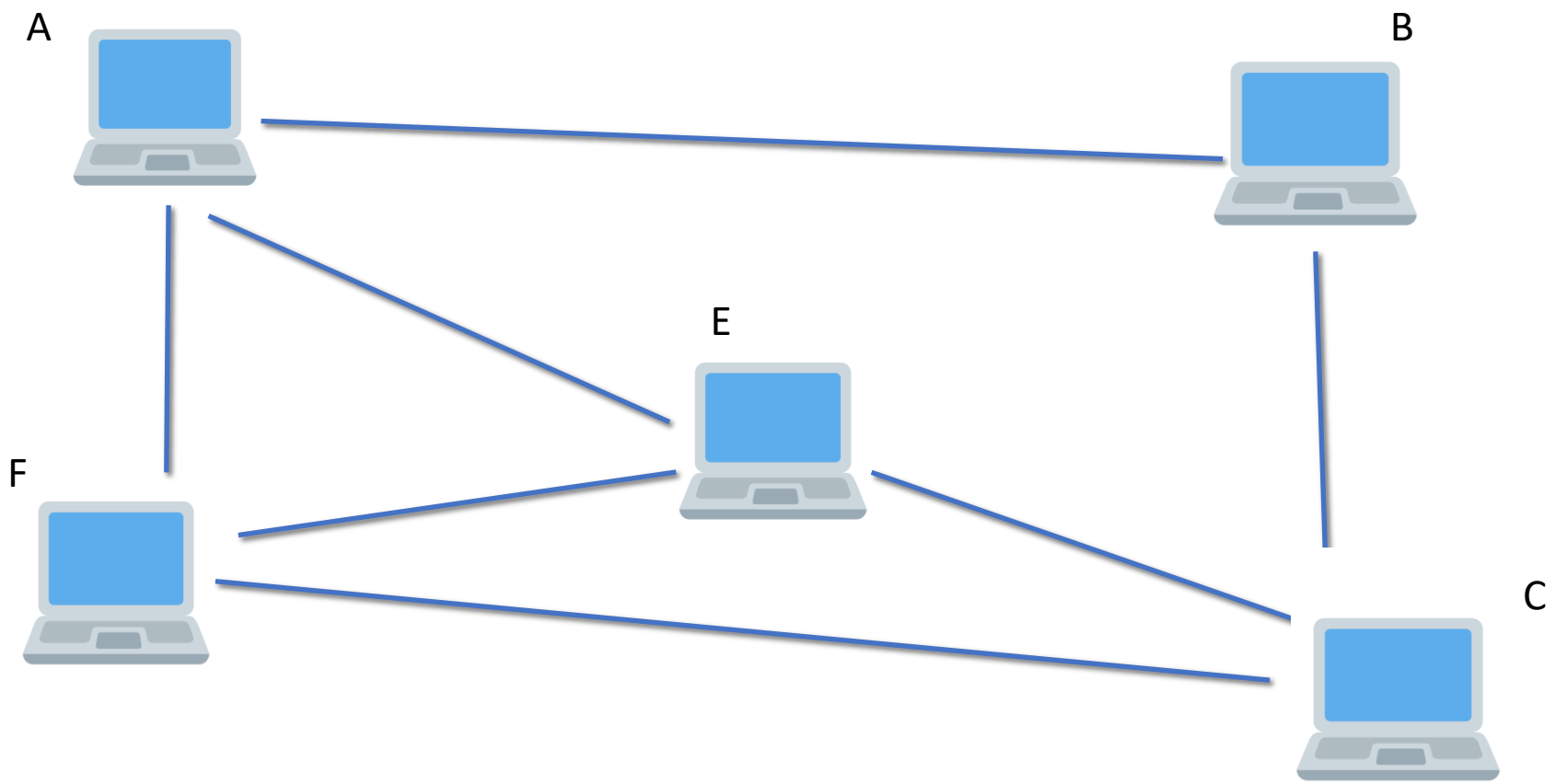
Bitcoin

Ethereum



Ethereum Nodes

Ethereum Nodes



Types of Nodes

Full Node

Light Node

Archive Node

Full Node

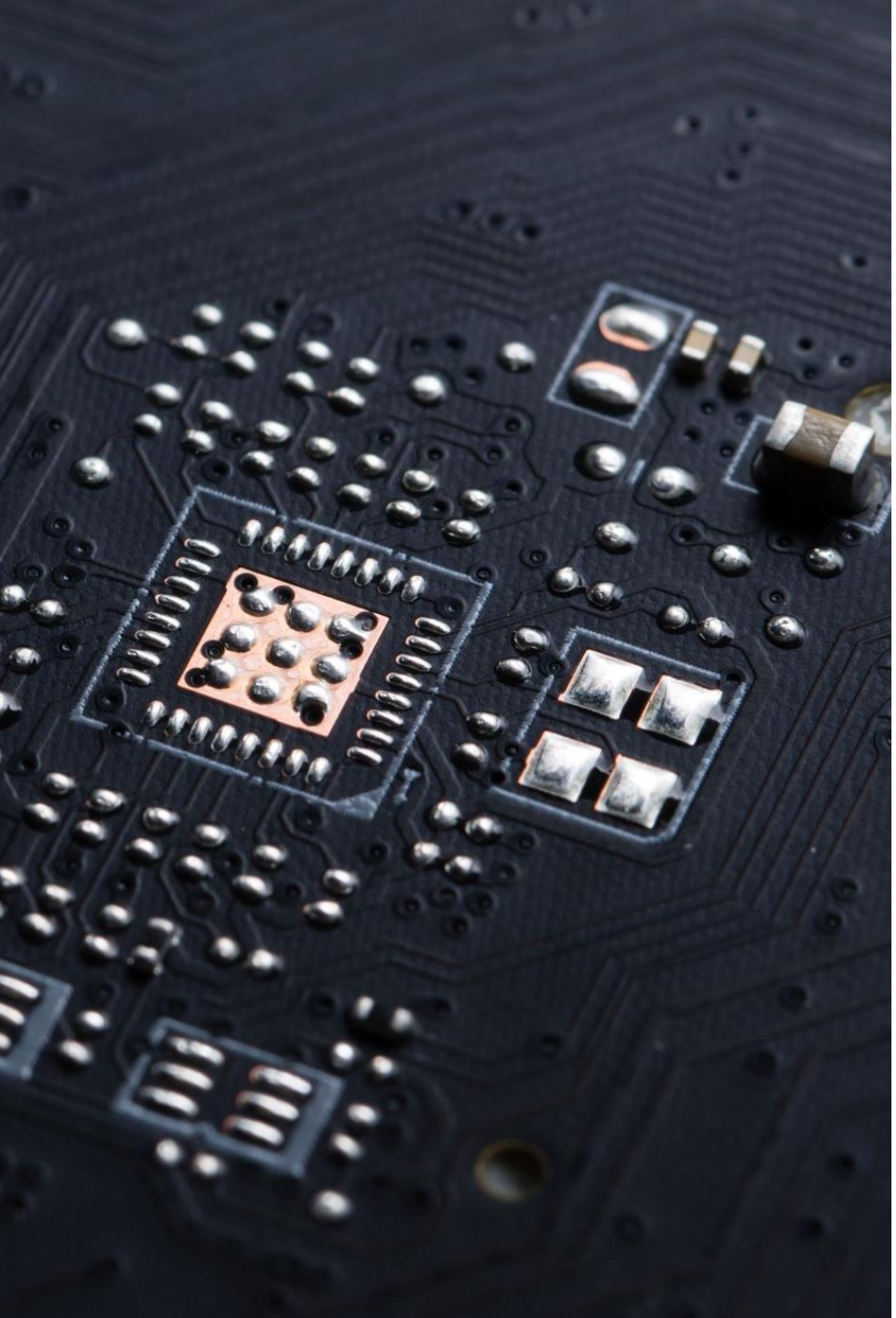
- Locally stores a copy of the entire blockchain.
- Verifies and validates all the blocks.
- Participate fully in all types of operations

Light Node

- Stores only the block headers
- Only do transactions
- Low-capacity devices which cannot afford to store the gigabytes of data
- Depends on the full node and gets data from the full node
- Full node is like a book, while light is like the index page

Archive Node

- Inherits the same capabilities as a full node and builds an archive of historical states
- Keep a record of the history of the blockchain
- Full node keeps a record of the current state, while the archive node stores all the states/ snapshots of the blockchain
- Useful when querying historical data that is not accessible on Full nodes. i.e. To get block data before the last 10 blocks
- Requires terabytes of disk space



Ethereum Accounts

Ethereum Accounts

- An Ethereum account is an entity with an ether (ETH) balance that can send or receive transactions on Ethereum.

Types of Ethereum Accounts

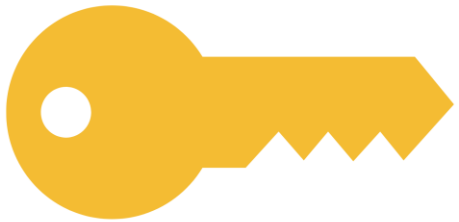
Externally Owned Account(EOA)

Contract Account(CA)

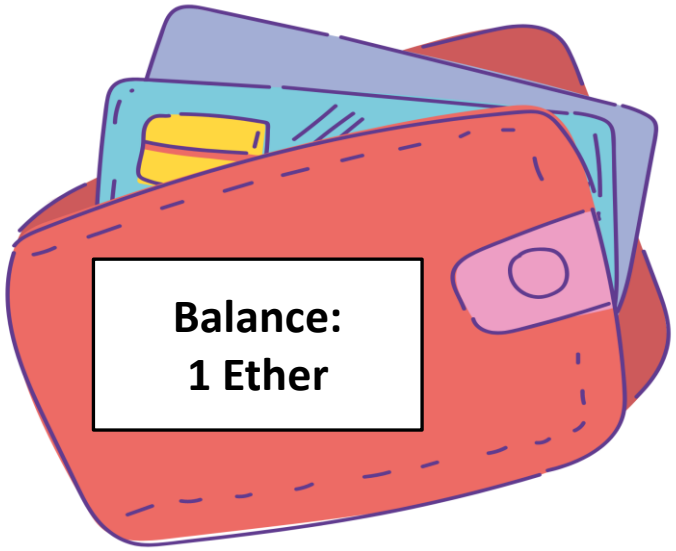
Externally Owned Account (EOA)

- It is mostly controlled or managed by a human
- For transactions, a wallet account is needed, with a wallet account the EOA is created
- An externally owned address is an account with **public** and **private key pair** holding funds
- Controlled by a private key and identified by a unique address
- It holds ether balance and has no **associated code** and thus **no cost** (Free)
- Used for holding, sending, and receiving **ether**
- Used for interacting with smart contracts (Deployment, calling function, etc.)

Externally Owned Account(EOA)



Private Key



Wallet

Send Transaction

Receive Transaction

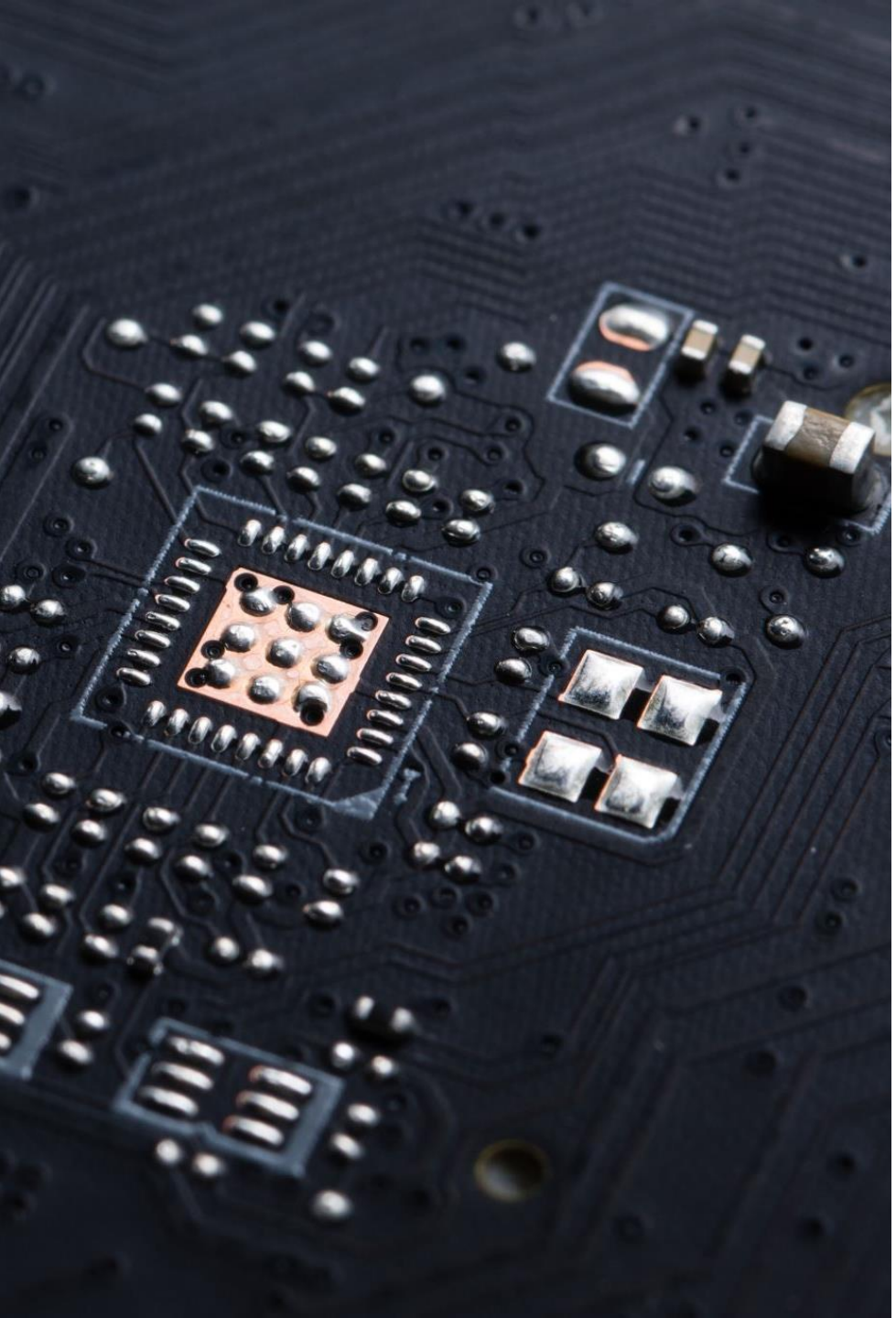
Smart Contract

Contract Account (CA)

- Controlled by contract code
- The smart contract should be deployed on the Ethereum blockchain
- For smart contracts deployment, we need an account called a **contract account (CA)**
- Thus, the CA is created when a smart contract is deployed
- CA has a unique address, and it does not have public and private keys
- CA can be used to transfer and receive ethers, and to create new contracts
- As smart contract creation needs cost, thus cost is associated with CA
- For a transaction between **A** and **B** the smart contract is accessed using **CA**

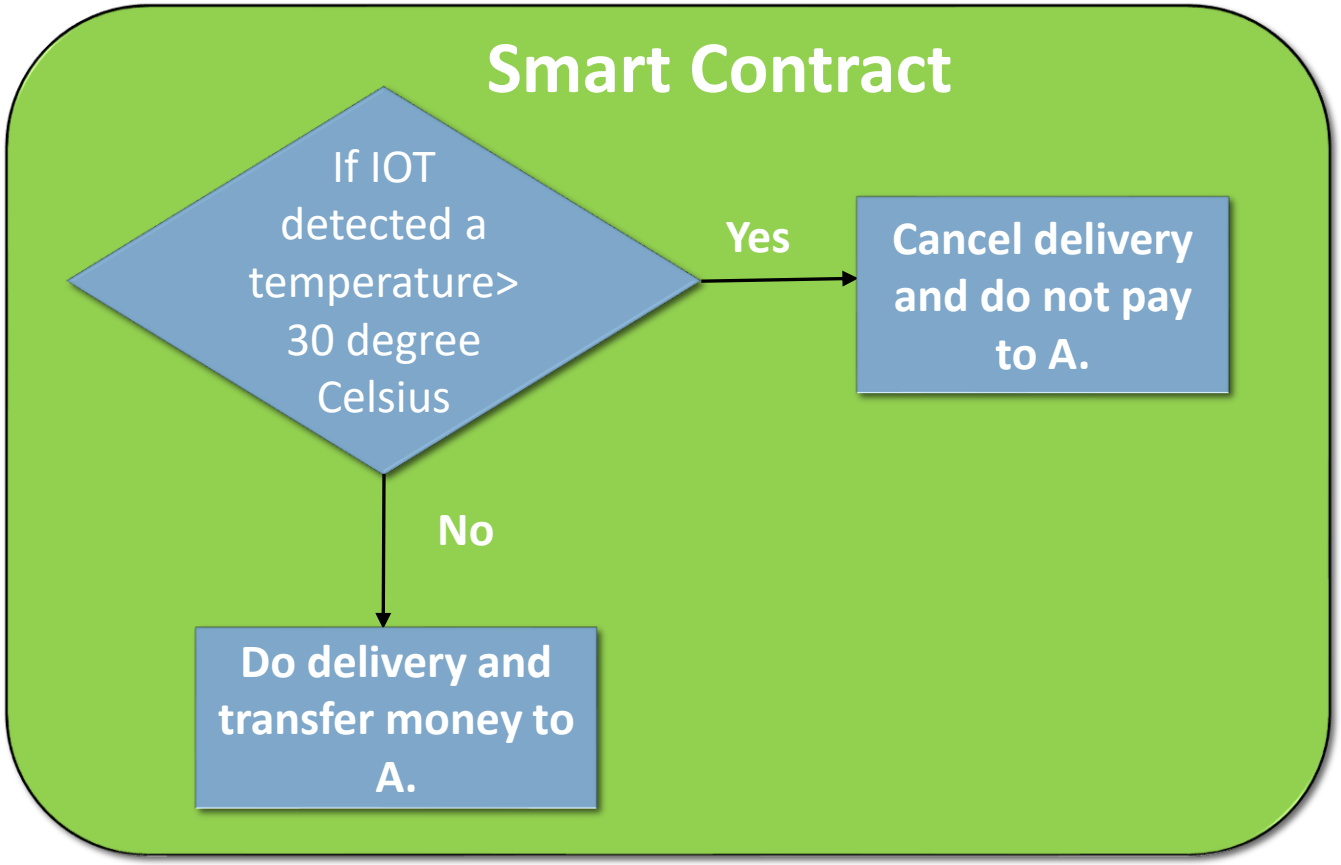
EOA vs. CA

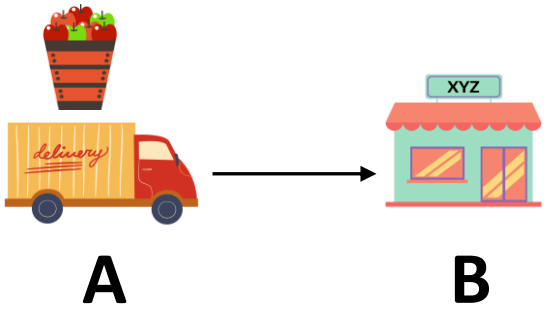
EOA	CA
Private Key is needed	No private or public key is needed.
Controlled by Human	Controlled by Contract code
No gas is associated	Gas is associated
Has a unique address	Has a unique address
Holds ETH balance	Holds ETH balance



Smart Contract

Smart Contract





Note: Assuming optimum temperature <30 degree Celsius.

Smart Contract

- A program that runs on Ethereum Blockchain

Smart Contract

Why is a smart contract not supported by a Bitcoin?

- The coding language in the bitcoin protocol is a **Bitcoin Script**
- **Bitcoins Script** is not Turing Complete and does not support loops.
- Loops are excluded from Bitcoin script so that hackers are unable to keep the network busy using indefinite loops

Smart Contract

- Ethereum uses **Solidity,** which can be run on the Ethereum blockchain
- A blockchain is distributed, thus the contract runs on all the nodes
- Solidity is **Turing Complete** and supports loops like normal languages
- To run a program on Ethereum, you pay according to your program

How is the indefinite loop problem solved by the founder?

- If a program runs for a longer time, you will pay much amount.
- Thus, if you add infinite looping, the Ether will be finished soon

Smart Contract

Bitcoin Script

Not Turing Complete

Solidity

Turing Complete

Smart Contract

Block No.-1

Nonce:

Timestamp:

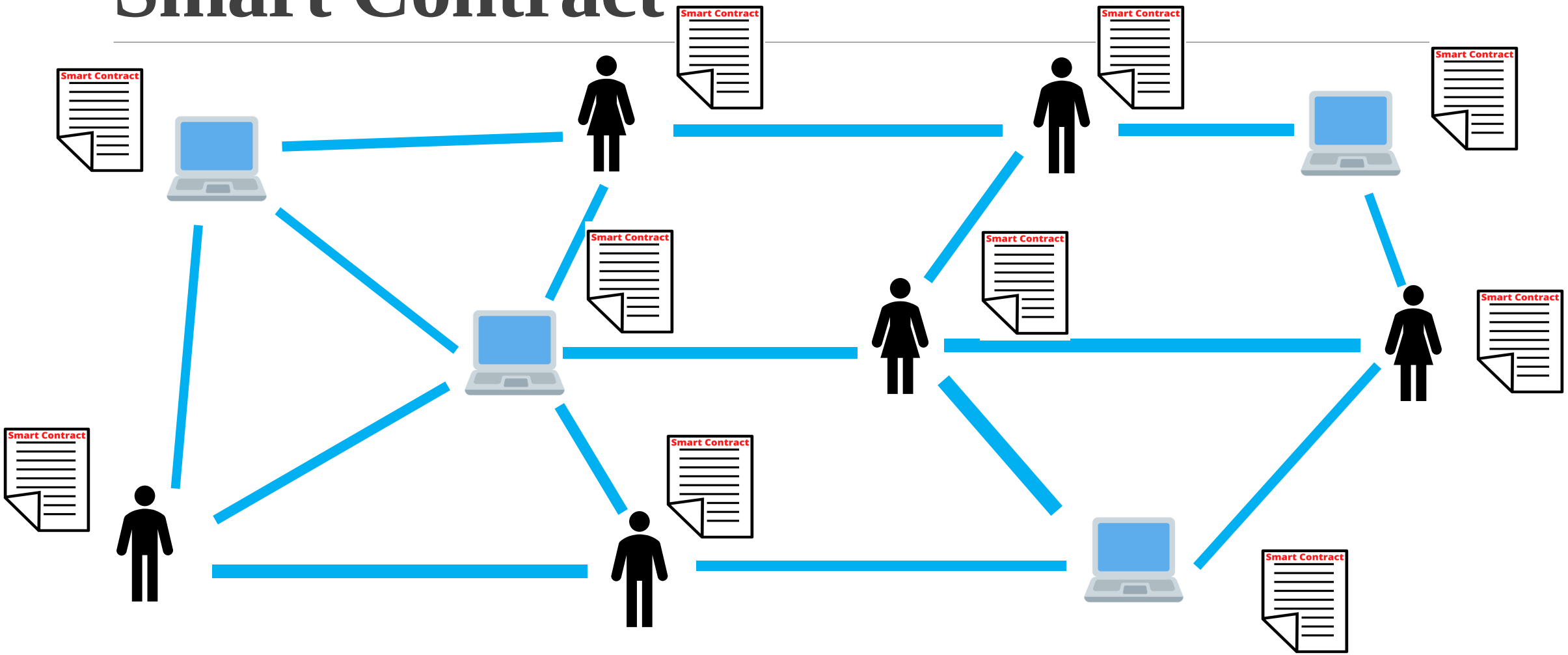
Transactions:

D67F232

Prev Hash:000000000

Hash:

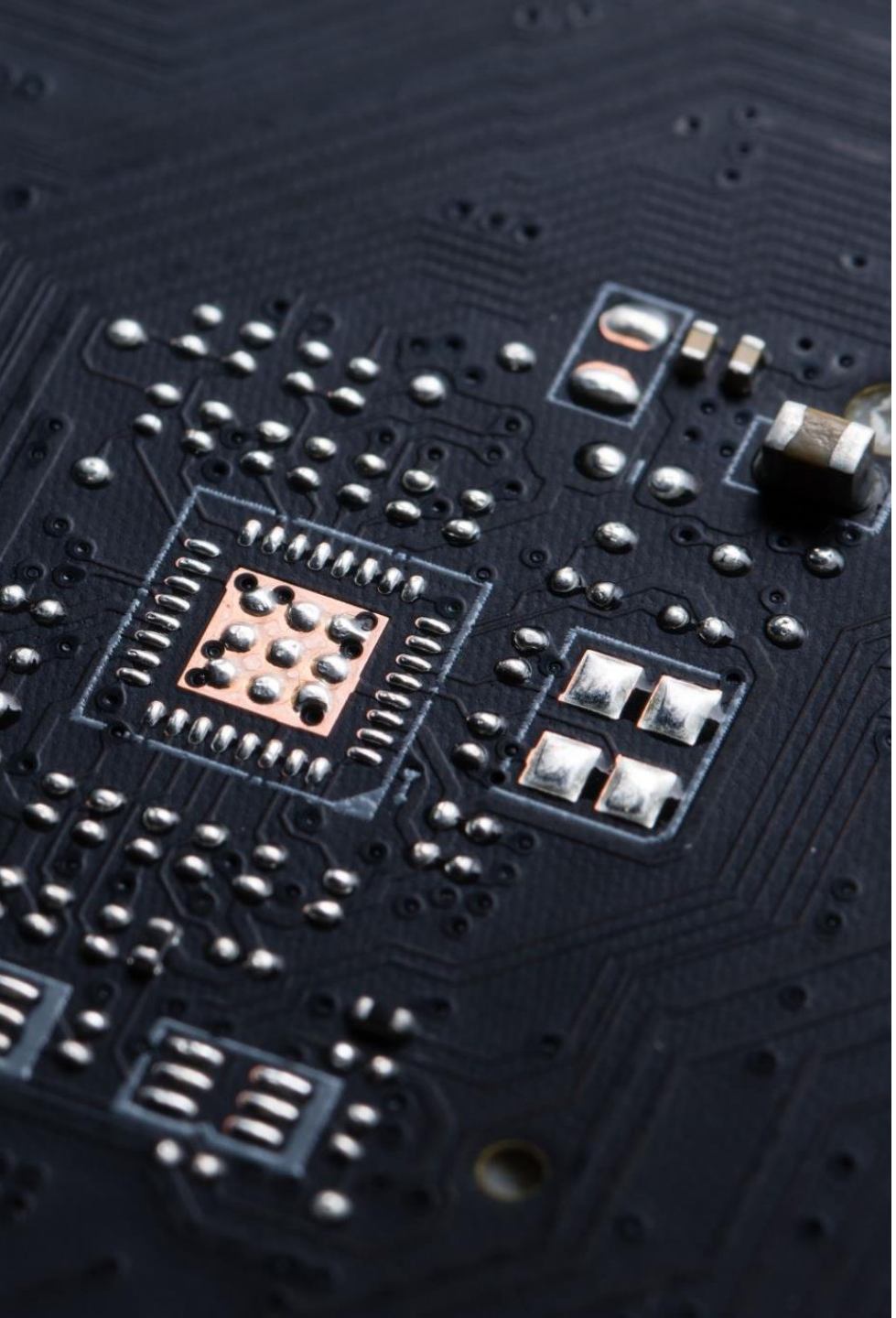
Smart Contract



Smart Contract

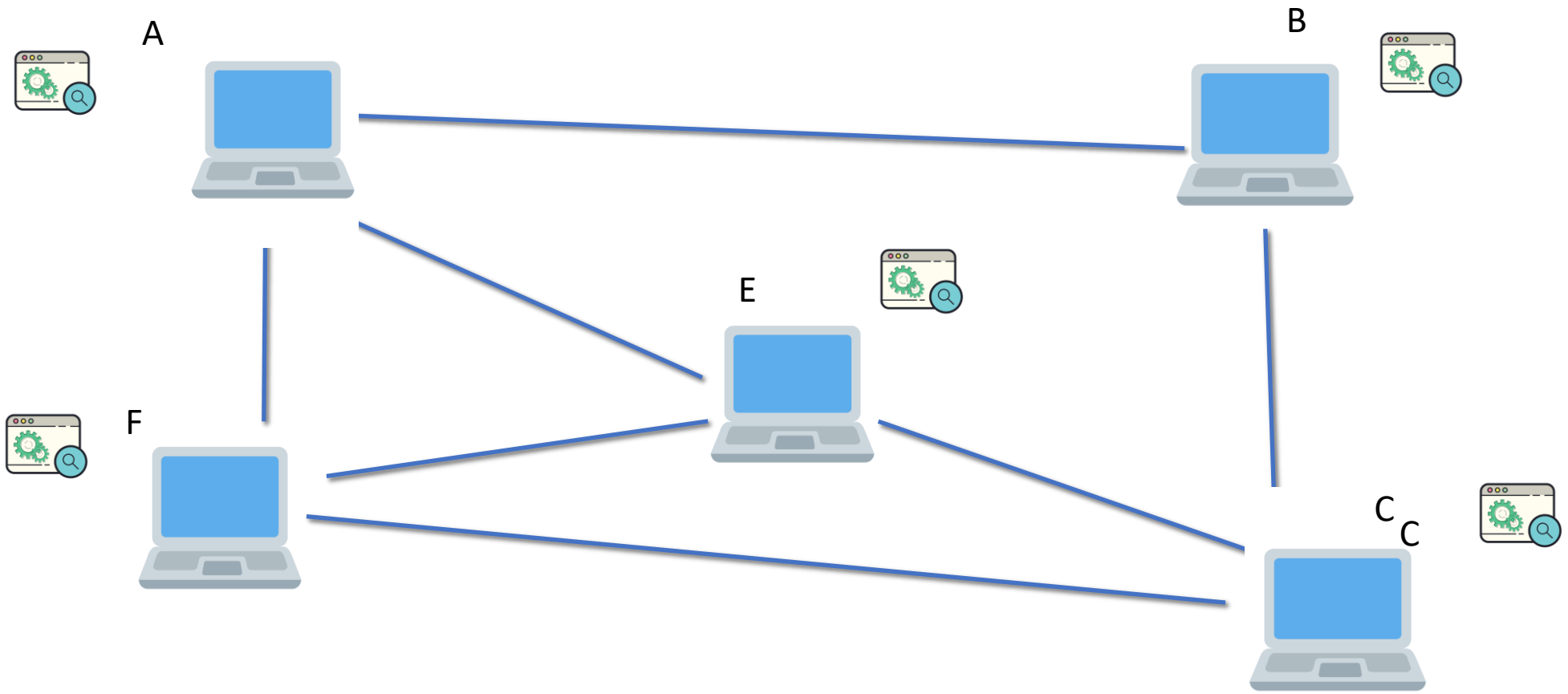
Each node has the following-:

- Current state of all smart contracts.
- History of both transaction and smart contract.



Decentralized Apps(Dapps)

Decentralized Apps(Dapps)



Decentralized Apps(Dapps)

- Applications run in a decentralized way or run in a P2P network
- Using Smart Contract for backend
- Code is transparent, everyone knows about the code
- Unlike centralized applications (Twitter, Facebook, etc.) one person cannot block another person
- Unlike centralized applications, you will be paid for advertisements in **Dapps**

Decentralized Apps(Dapps)

Decentralized Network

Smart Contract

+

Front End

Decentralized Apps(Dapps)

	Centralized Applications	Decentralized Applications
Search Engine		Presearch
Social Media		LBRY
Video Platform	YouTube	D.tube

Decentralized Apps(Dapps)

Centralized Apps	Decentralized Apps
Not Trustworthy	Trustworthy
Censorship/ Disallowance	No censorship
You pay	They pay
Go down	Can never go down