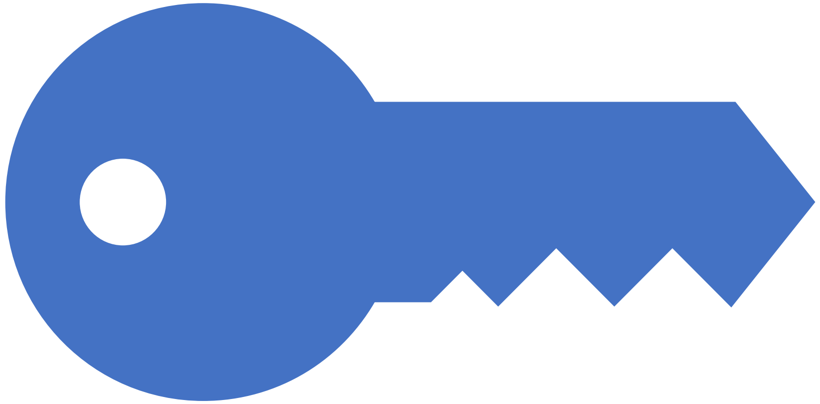
1. This document is authorized for use only by Students in Blockchain Class taught by P.T.K.Trung.
2. This document is for your personal study only. Reproduction and/or redistribution is not allowed.



Mr Pham Thai Ky Trung

Lecture1 : Introduction to Blockchain

Learning Objectives

- ○Understand a technical definition of blockchain, including its main traits
- ○Be able to describe blockchain technology as a part of the broader story of trade
- ○Explain blockchain technology to your clients, friends, and business colleagues
- ○Identify which aspects of blockchain technology seem most important and relevant to you
- ○Understand where blockchain is going, how it works, and how to start preparing for it
- ○Discuss some of the most important use cases and enterprise platforms

“BLOCKCHAIN” HAS MANY MEANINGS

○ “To understand the power of blockchain systems, and the things they can do, it is important to distinguish between three things that are commonly muddled up, namely the bitcoin currency, the specific blockchain that underpins it and the idea of blockchains in general.”

○ *The Trust Machine*, THE ECONOMIST, Oct. 31, 2015

“BLOCKCHAIN” HAS MANY MEANINGS

Phone

- The idea of a phone network
- A specific phone network (e.g., AT&T)
- A specific use of the phone network (e.g.,fax)

Blockchain

- The idea of blockchain
- The specific blockchain that underlies Bitcoin or another coin offering
- Bitcoin or another cryptocurrency

WHAT IS BLOCKCHAIN?

A technology that:

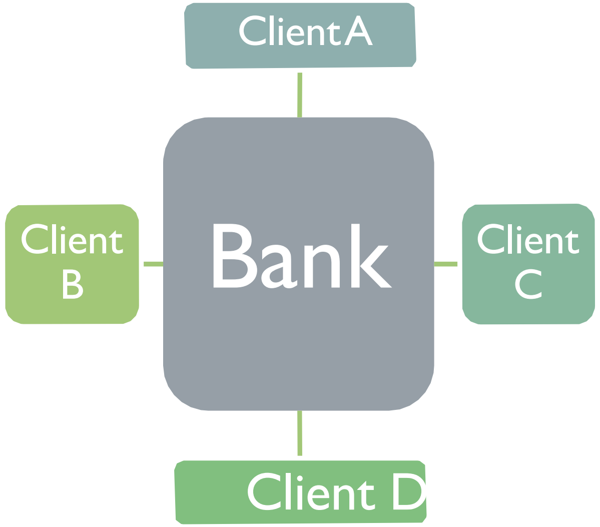
permits transactions to be gathered into blocks and recorded;

cryptographically chains blocks in chronological order; and

allows the resulting ledger to be accessed by different servers.

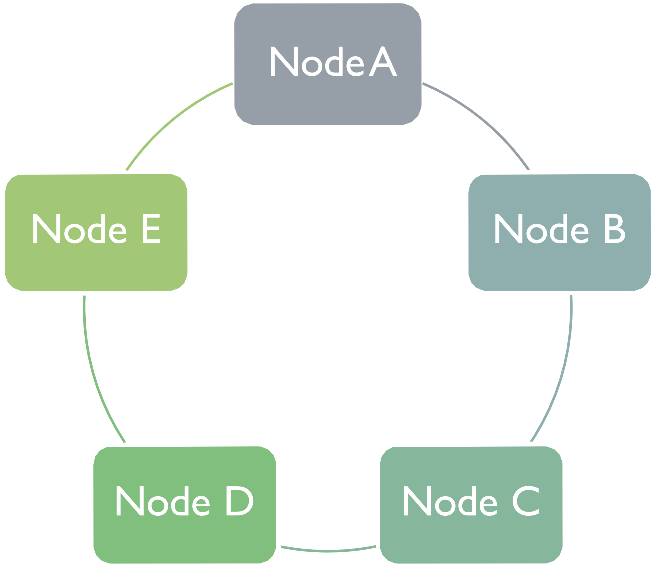
WHAT IS A DISTRIBUTED LEDGER?

Centralized Ledger



- There are multiple ledgers, but Bank holds the "golden record"
- Client B must reconcile its own ledger against that of Bank, and must convince Bank of the "true state" of the Bank ledger if discrepancies arise

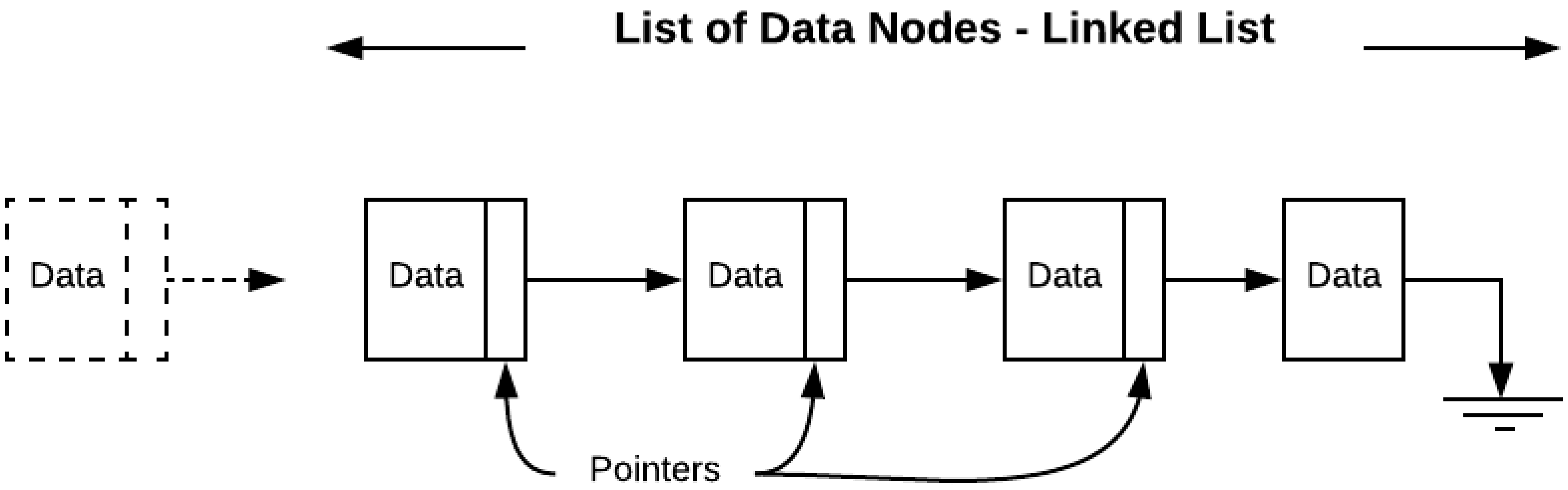
Distributed Ledger

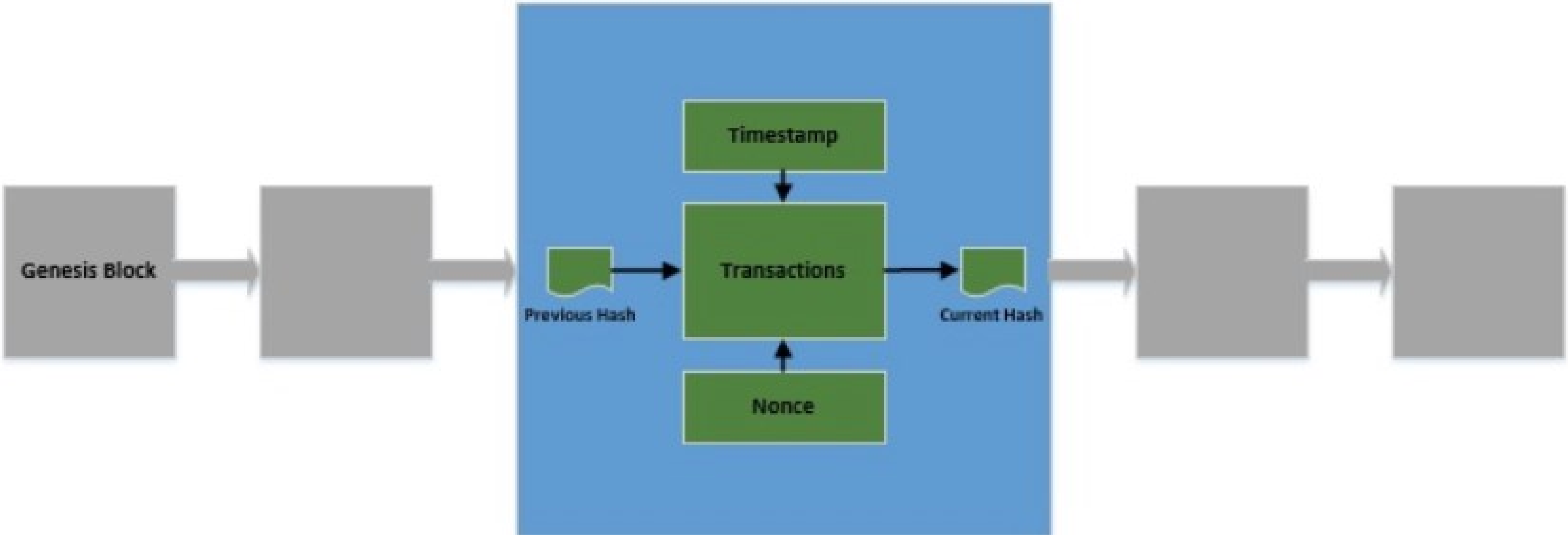


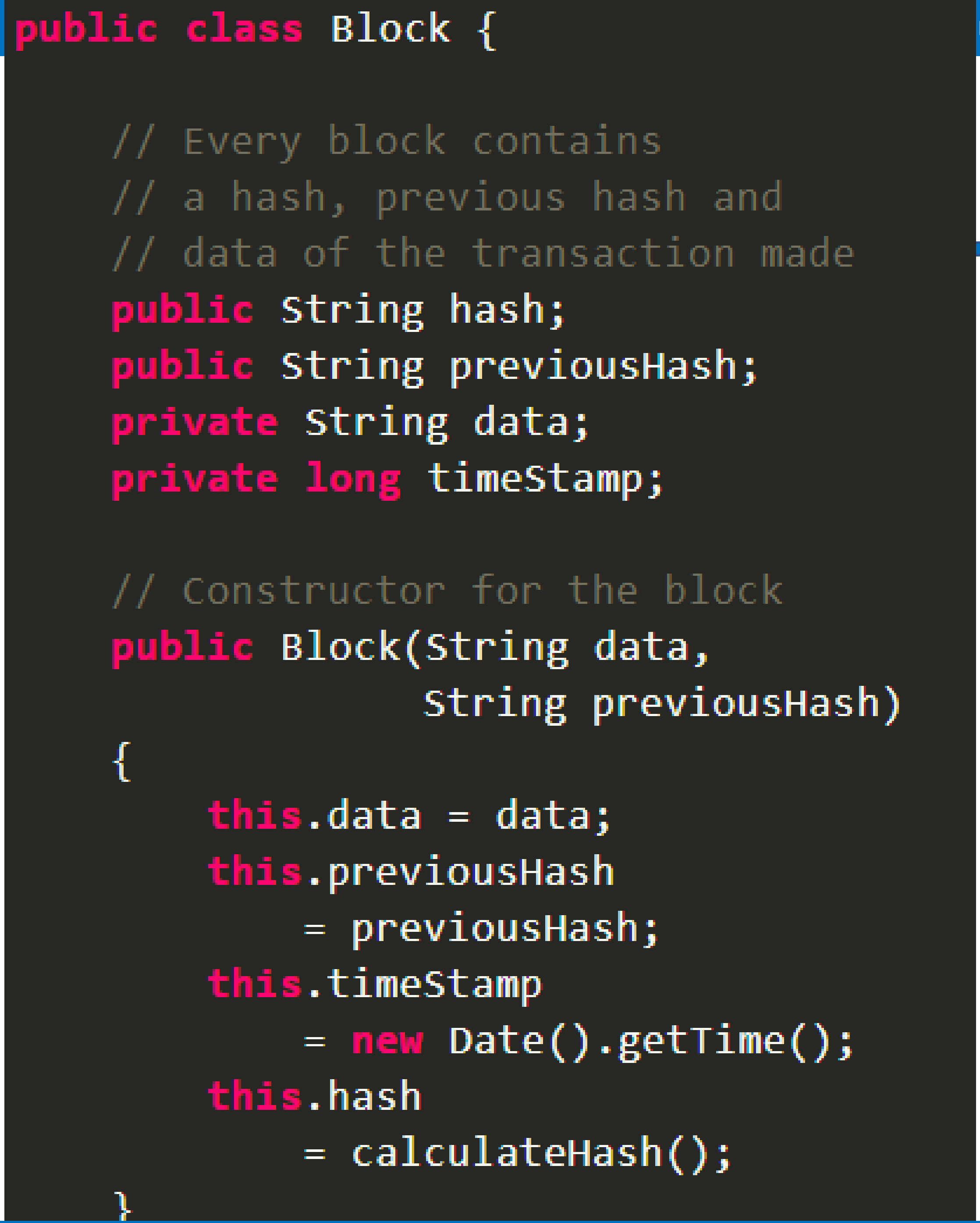
- There is one ledger. All Nodes have some level of access to that ledger.
- All Nodes agree to a protocol that determines the "true state" of the ledger at any point in time. The application of this protocol is sometimes called "achieving

Blockchain

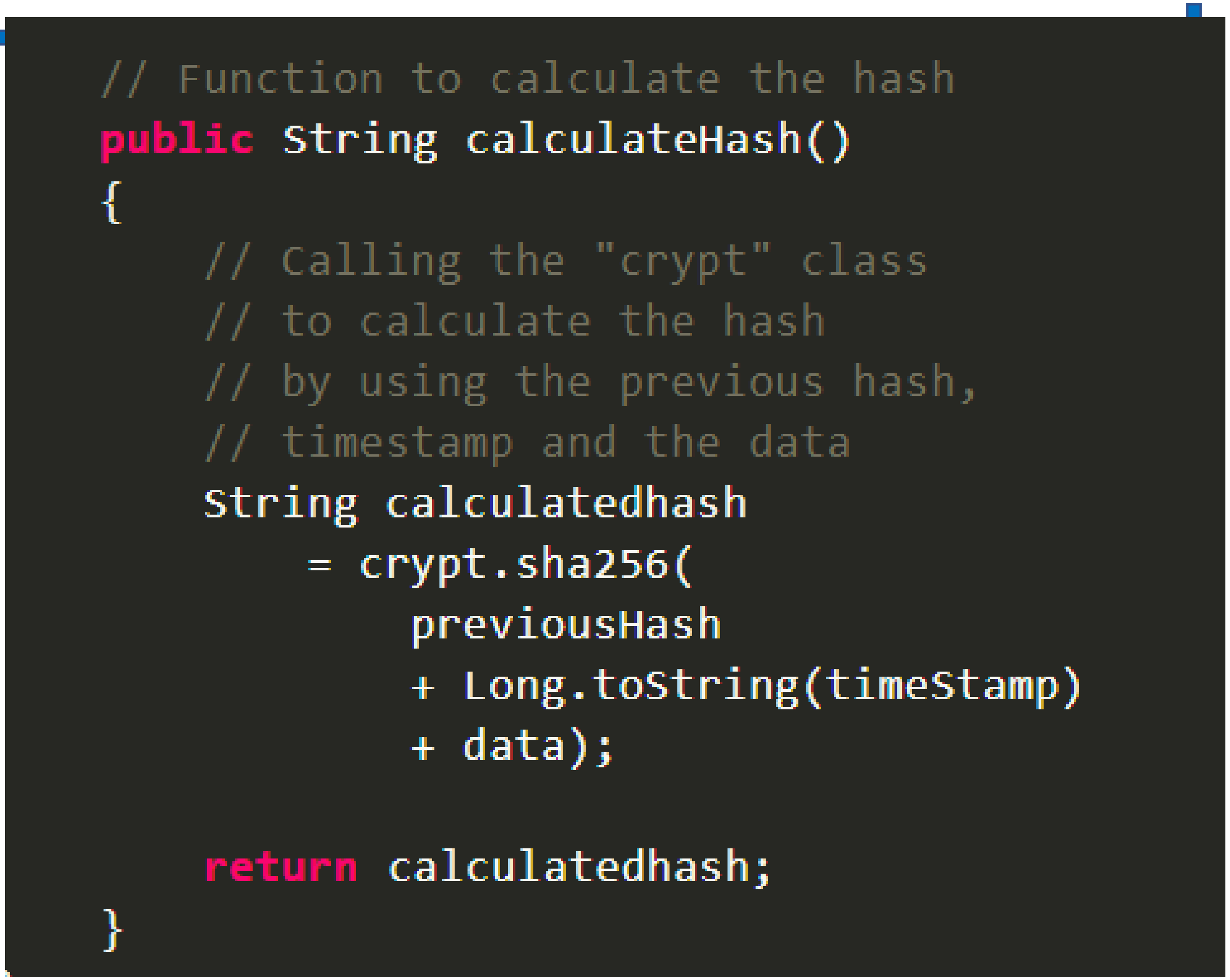
- Linked List +SHA256




Genesis Block
Timestamp
Transactions
Nonce
Previous Hash
Current Hash

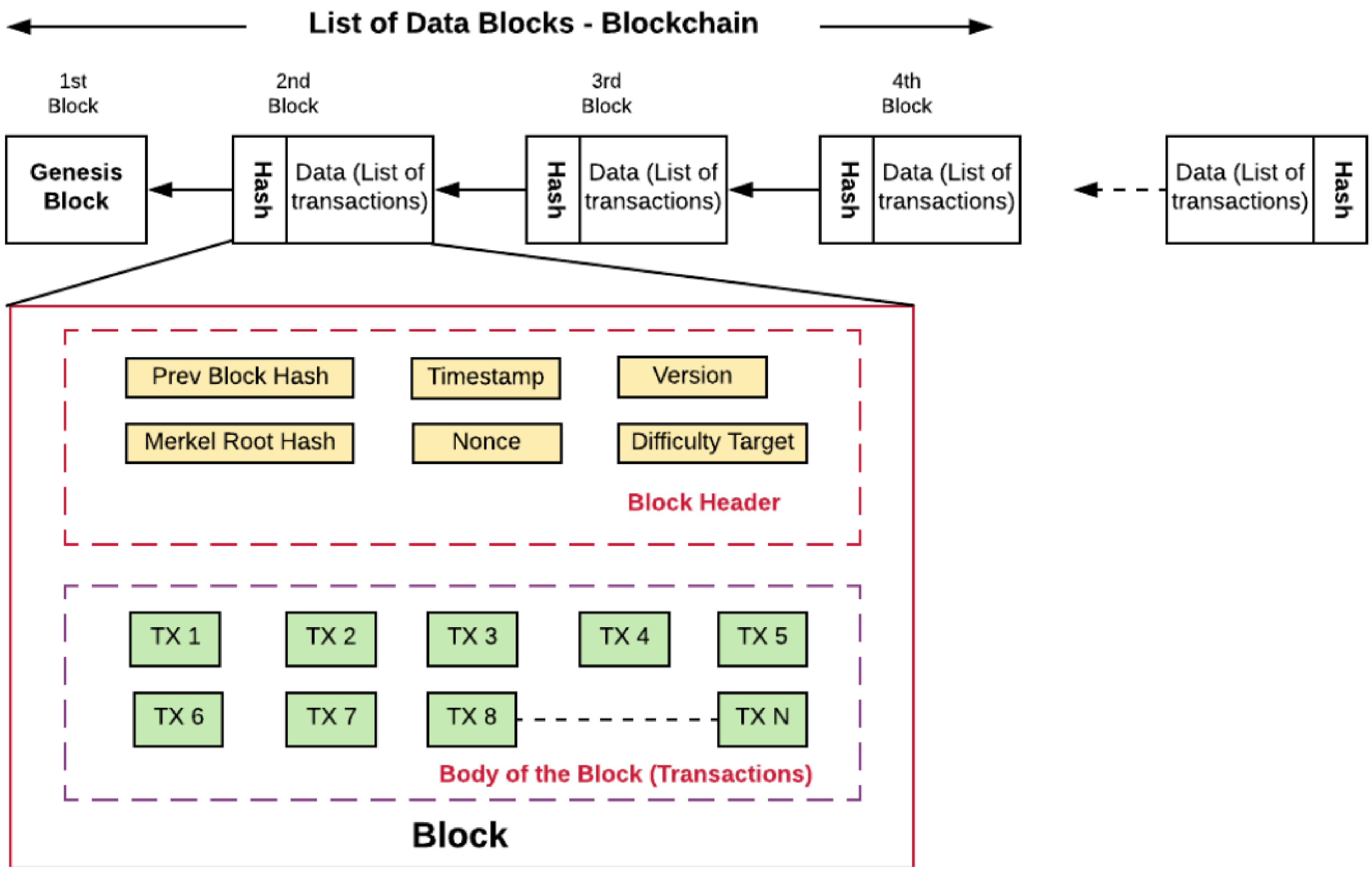


```
public class Block {

    // Every block contains
    // a hash, previous hash and
    // data of the transaction made
    public String hash;
    public String previousHash;
    private String data;
    private long timeStamp;

    // Constructor for the block
    public Block(String data,
                 String previousHash)
    {
        this.data = data;
        this.previousHash
            = previousHash;
        this.timeStamp
            = new Date().getTime();
        this.hash
            = calculateHash();
    }
```



```
    // Function to calculate the hash
    public String calculateHash()
    {
        // Calling the "crypt" class
        // to calculate the hash
        // by using the previous hash,
        // timestamp and the data
        String calculatedhash
            = crypt.sha256(
                previousHash
                + Long.toString(timeStamp)
                + data);

        return calculatedhash;
    }
```

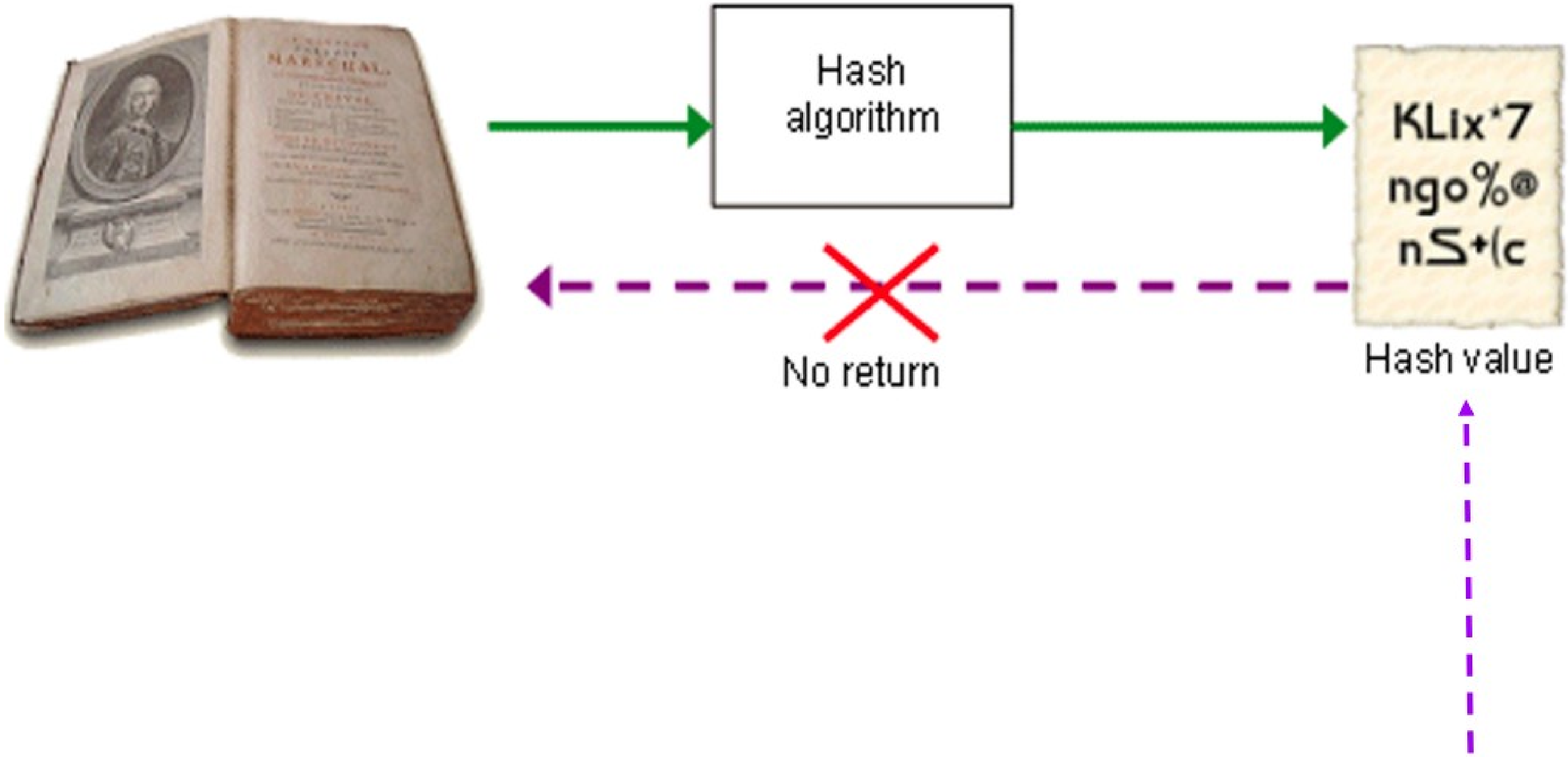
Blockchain represented as Linked List Data Structure



A linked list and A blockchain

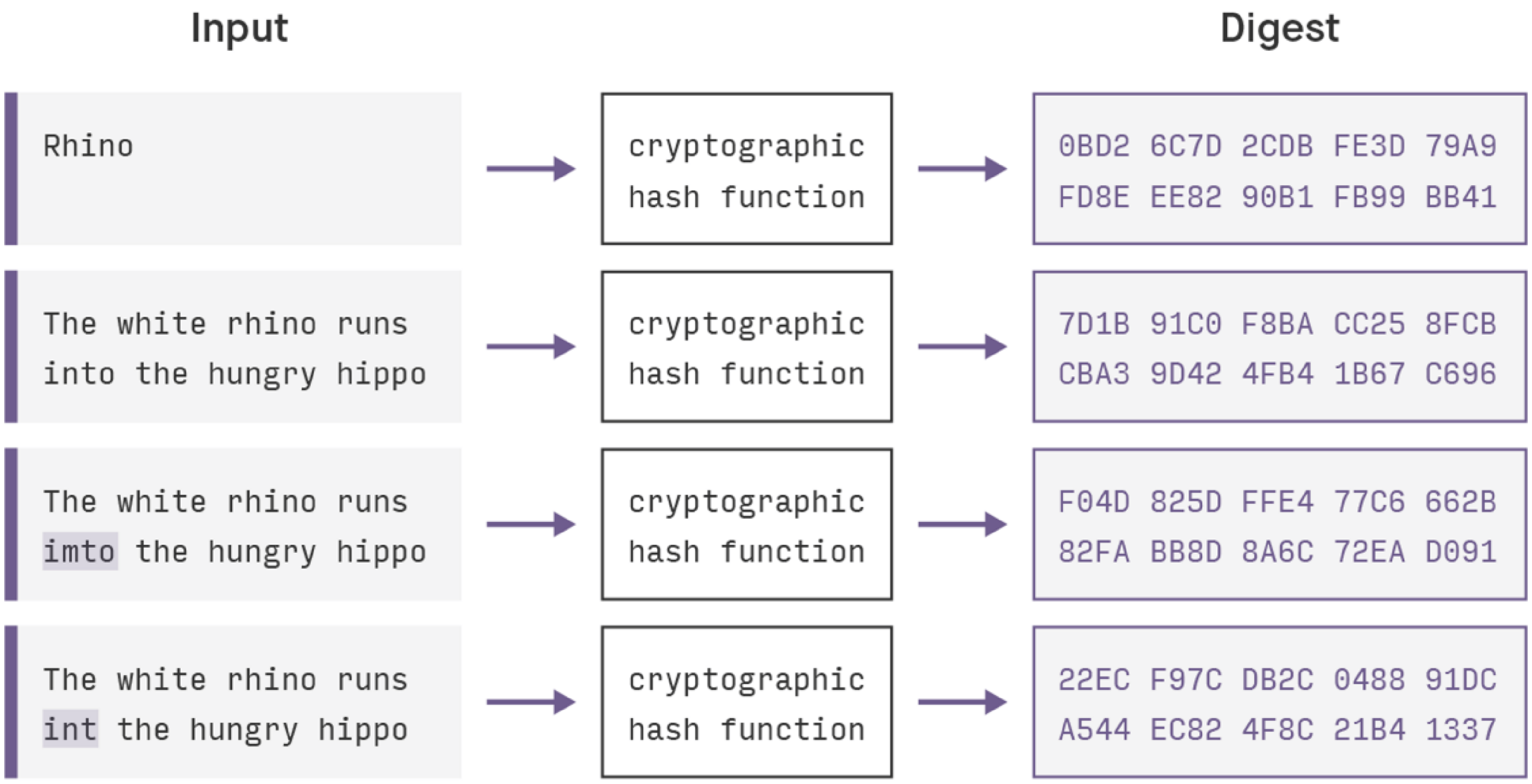
- In a linked list, data stored in a data node could be change. In Blockchain, changing a transaction would lead to re-calculation of hashes of all of the blocks.
- In a linked list, a data node can be added at any place in the list. In Blockchain, the block is added to the end of the chain (list).
- In a linked list, deleting a node would only require a link to be pointed the to previous node of the node to be deleted. In Blockchain, it is not easy to delete a block as the hash of all the block would require to be re-calculated.

The cryptographic hash function

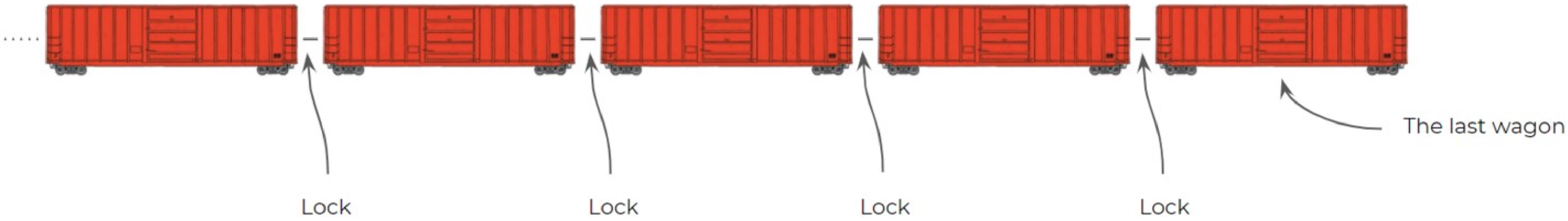


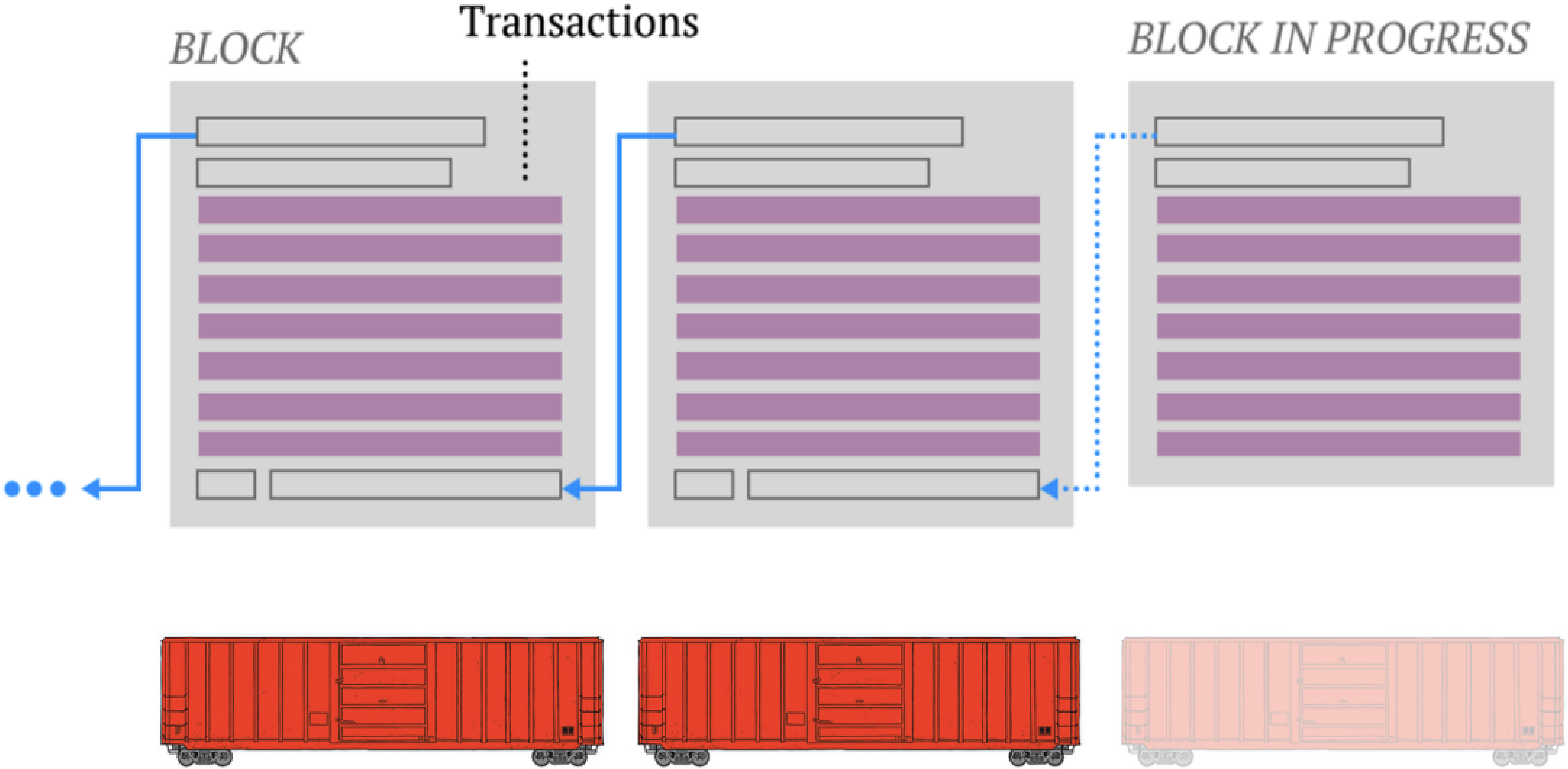
Unique for structured data

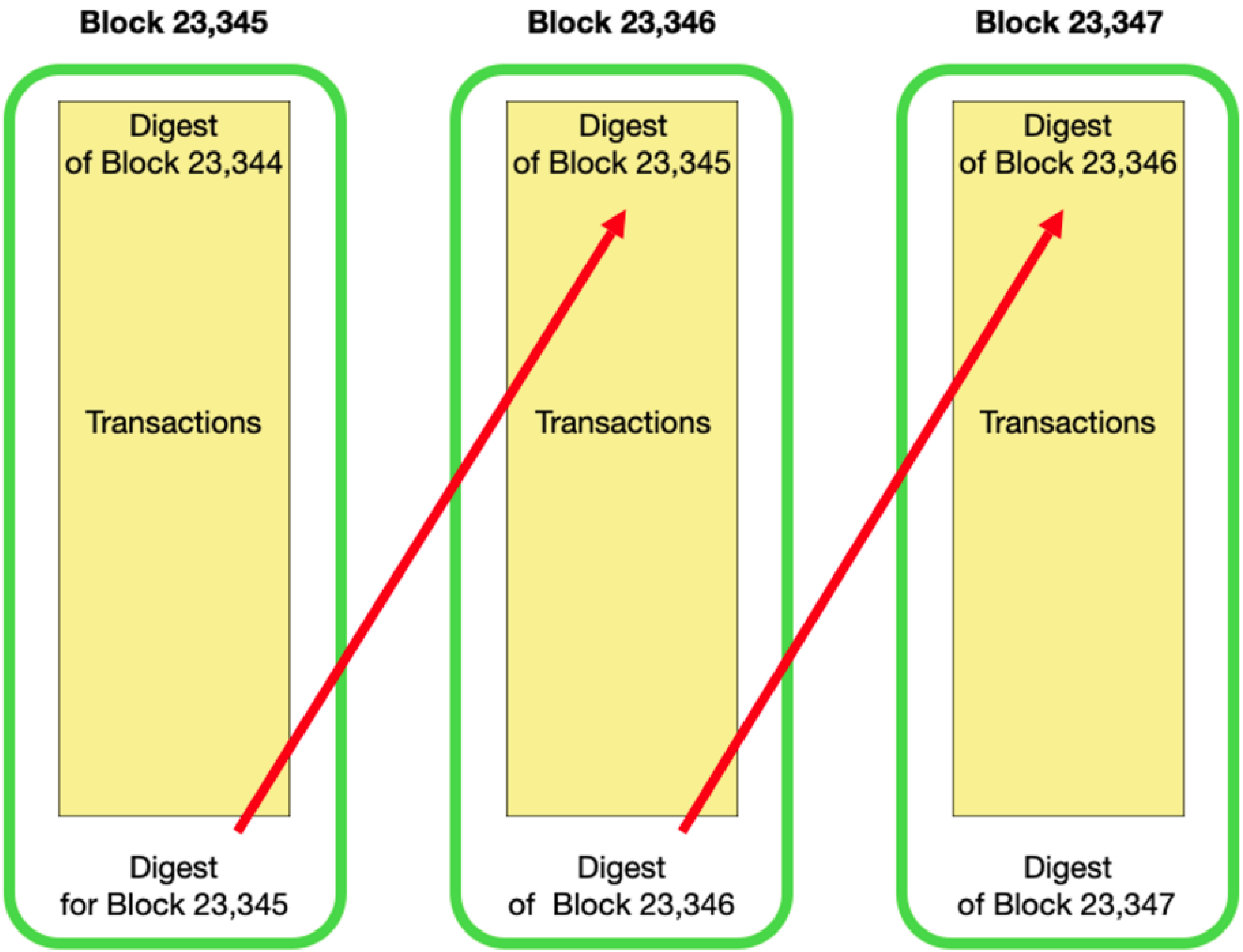
Hash Function



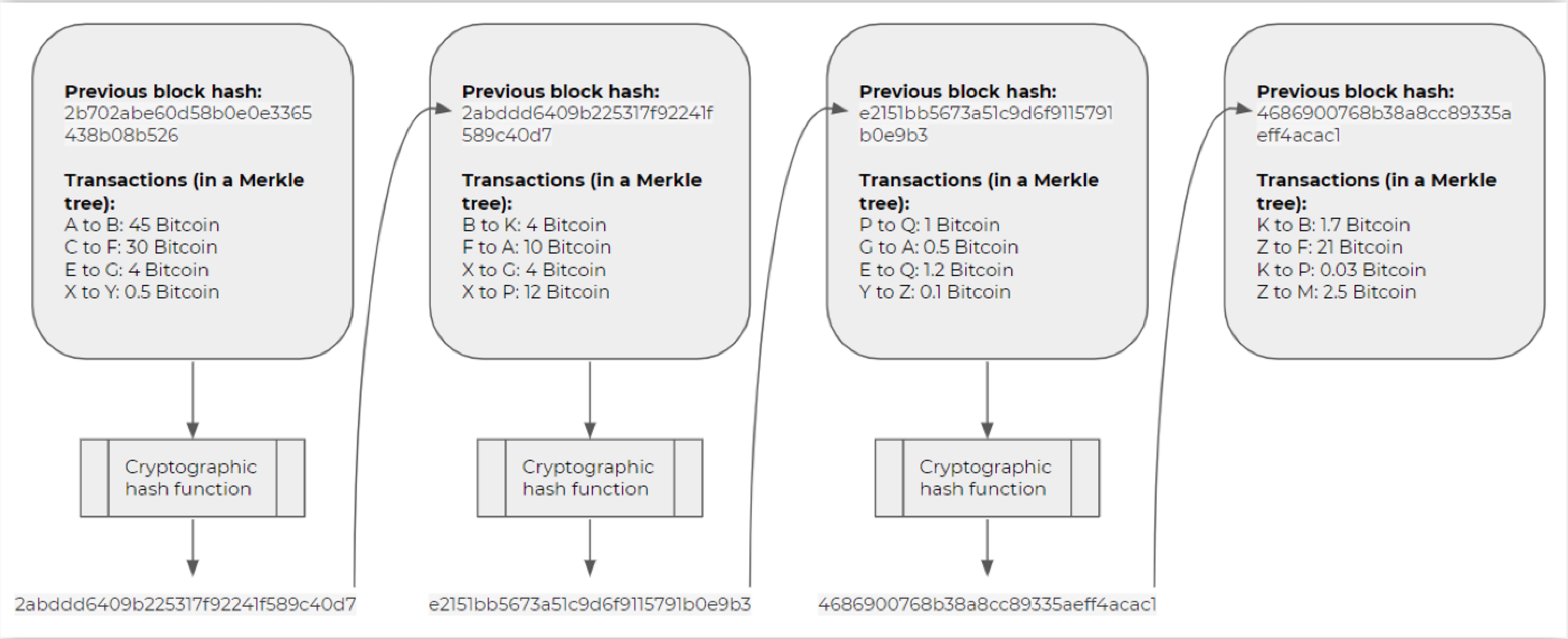
Input		Digest
Rhino	cryptographic hash function	0BD2 6C7D 2CDB FE3D 79A9 FD8E EE82 90B1 FB99 BB41
The white rhino runs into the hungry hippo	cryptographic hash function	7D1B 91C0 F8BA CC25 8FCB CBA3 9D42 4FB4 1B67 C696
The white rhino runs imto the hungry hippo	cryptographic hash function	F04D 825D FFE4 77C6 662B 82FA BB8D 8A6C 72EA D091
The white rhino runs int the hungry hippo	cryptographic hash function	22EC F97C DB2C 0488 91DC A544 EC82 4F8C 21B4 1337


. . . . .
Lock
Lock
Lock
Lock
The last wagon


BLOCK
Transactions
BLOCK IN PROGRESS


Block 23,345
Digest
of Block 23,344
Transactions
Digest
for Block 23,345
Block 23,346
Digest
of Block 23,345
Transactions
Digest
of Block 23,346
Block 23,347
Digest
of Block 23,346
Transactions
Digest
of Block 23,347

Blocks



Previous block hash:
2b702abe60d58b0e0e3365
438b08b526

Transactions (in a Merkle tree):
A to B: 45 Bitcoin
C to F: 30 Bitcoin
E to G: 4 Bitcoin
X to Y: 0.5 Bitcoin

Previous block hash:
2abddd6409b225317f92241f
589c40d7

Transactions (in a Merkle tree):
B to K: 4 Bitcoin
F to A: 10 Bitcoin
X to G: 4 Bitcoin
X to P: 12 Bitcoin

Previous block hash:
e2151bb5673a51c9d6f9115791
b0e9b3

Transactions (in a Merkle tree):
P to Q: 1 Bitcoin
G to A: 0.5 Bitcoin
E to Q: 1.2 Bitcoin
Y to Z: 0.1 Bitcoin

Previous block hash:
4686900768b38a8cc89335a
eff4acac1

Transactions (in a Merkle tree):
K to B: 1.7 Bitcoin
Z to F: 21 Bitcoin
K to P: 0.03 Bitcoin
Z to M: 2.5 Bitcoin

Cryptographic hash function
Cryptographic hash function
Cryptographic hash function
2abddd6409b225317f92241f589c40d7
e2151bb5673a51c9d6f9115791b0e9b3
4686900768b38a8cc89335aeff4acac1

- ○Block (Bitcoin blockchain: 1MB in Size, 10 mins to create) , once created , linked to previous block using an address (numbers + letters -> hash) and cryptography

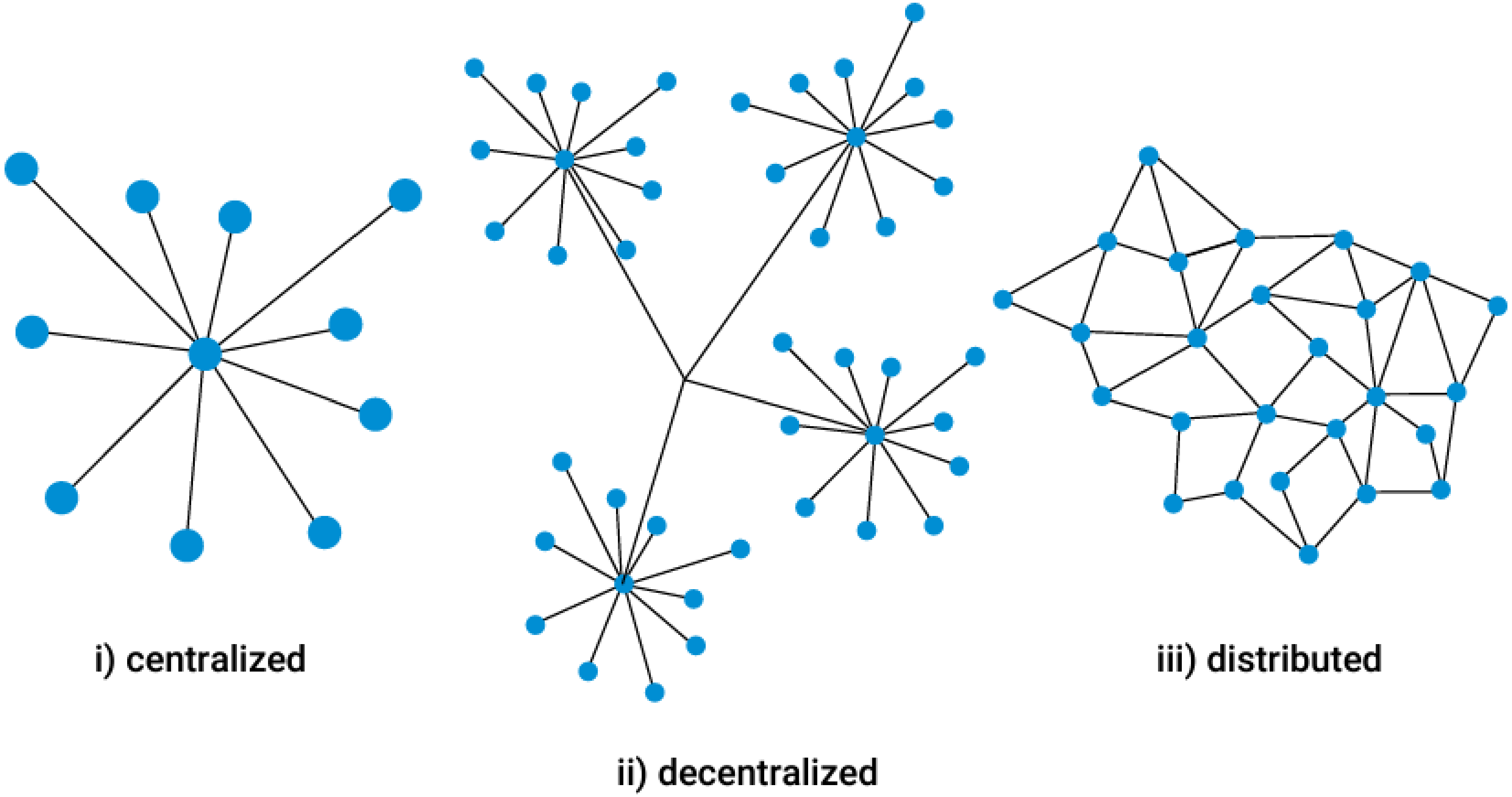
You google Blockchain

a blockchain is **a decentralized database that coordinates agreement on an append-only history of transactions across a peer-to-peer network**

Decentralized Database: A database is simply a collection of data or information. A phonebook, for example. A decentralized database is one where there is no single, centralized storage of data and no single authority or system administrator.

Decentralized databases generally have multiple readers and multiple writers such as when multiple servers on a network provide data to clients. An additional form of information architecture is a distributed database, where all the nodes on the network contain information and they are equal and have equal rights

Network Evolution



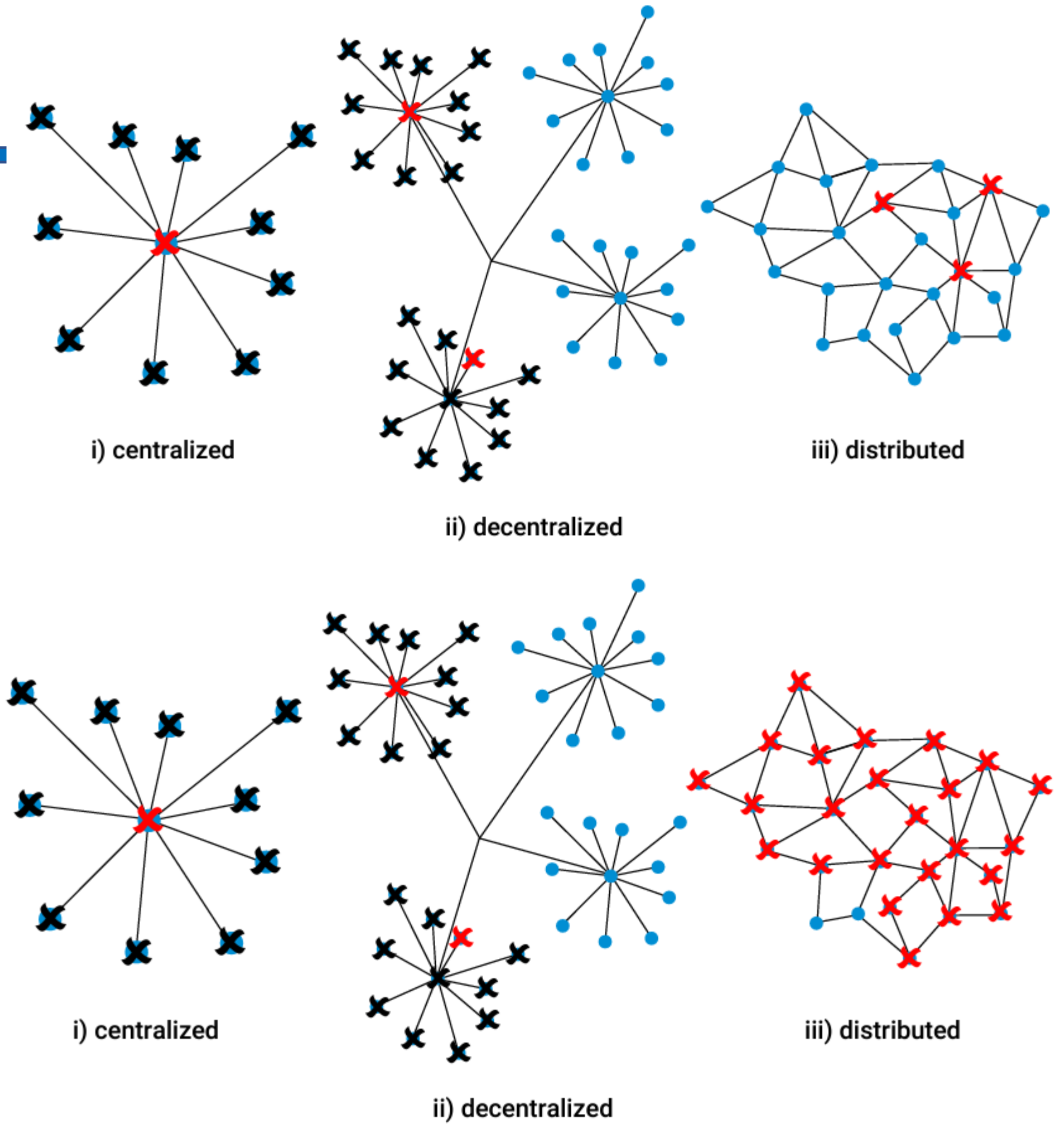
i) centralized

ii) decentralized

iii) distributed

Distributed Network

- Many, equal nodes
- Each node has multiple connections to other nodes
- Very resilient to failures, attacks
- As long as 2 nodes are up, the network is still running



Elements of a Blockchain

- Different components:
  - **Nodes** : any computer connecting to a blockchain network is a node participating in the network
  - **Community of verifiers:** you want to be more active participant in the blockchain and become a full node, you must have a computer (hardware) connected to a blockchain network and you must download a complete copy of the blockchain (software) onto your computer. (The size of Bitcoin blockchain is bout 200GB and growing -> take a several days, require CPU & RAM). One user can operate multiple nodes on a blockchain, and there also exist "partial nodes" that point to full nodes for their data.
  - **Peer-to-Peer network** : full nodes are what we referred to earlier as the "peer-to-peer network" because they have agreed to take on the role of verifying that transactions and blocks are accurate

Public and Private Keys

- Use address when transacting on a blockchain -> network verify without personal information
- Asymmetric cryptography(built in to blockchain) -> allow individual use a private key to unlock their address while sharing a public key with others involved in the transaction.
- A combination of transparency and public-key indentities -> ensure “trust” (like bank’s key (public) and the customer (private) that only the customer has access to
- To perform transactions on a blockchain -> need to digitally sign your transactions with your private key

Mining

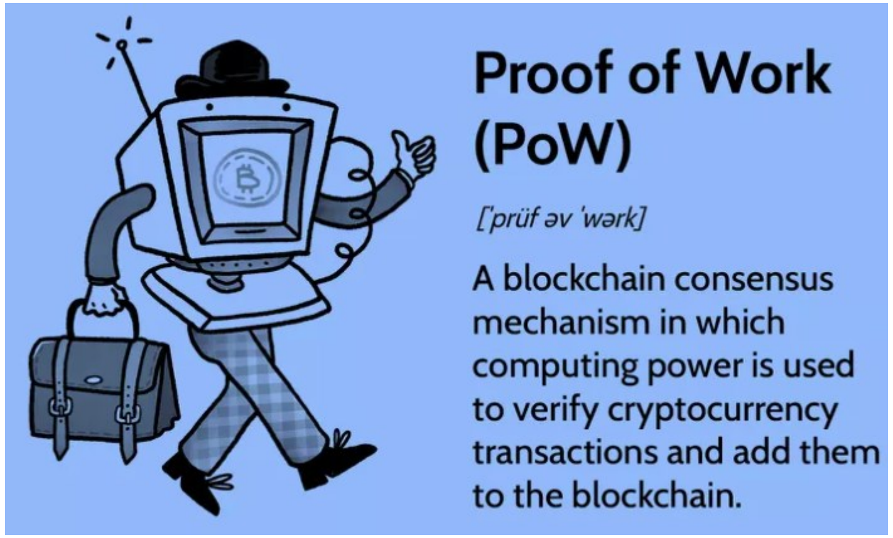
- As part of the "community of verifiers", a full node helps validate a blockchain database via a practice called **"mining"**
- **Miners** are nodes that perform a certain amount of computational work – racing with other to solve a mathematical puzzle[câu đố] to help keep the network going.
- Every time a miner successfully solves the puzzle, they win the right to contribute the newest block of transactions to the blockchain.
- The winning miner sends out a message to the entire network, and receives newly minted **tokens** as an **incentive in exchange** for the service of helping maintain the database by mining.

Tokens or Coins

- Blockchain technology was developed using some elements of game theory and economics.
- To motivate people to participate in a blockchain as a full node and help secure the history of transactions in the database, these systems include an incentive structure that uses **“digital tokens.”**
- **A digital token is just a way of representing value on a blockchain application.**

Consensus through Proof of Work

- Proof of work (PoW) is a decentralized consensus mechanism that requires network members to expend effort in solving an encrypted hexadecimal number.
- Proof of work is also called mining, in reference to receiving a reward for work done.
- Proof of work allows for secure peer-to-peer transaction processing without needing a trusted third party.
- Proof of work at scale requires vast amounts of energy, which only increases as more miners join the network

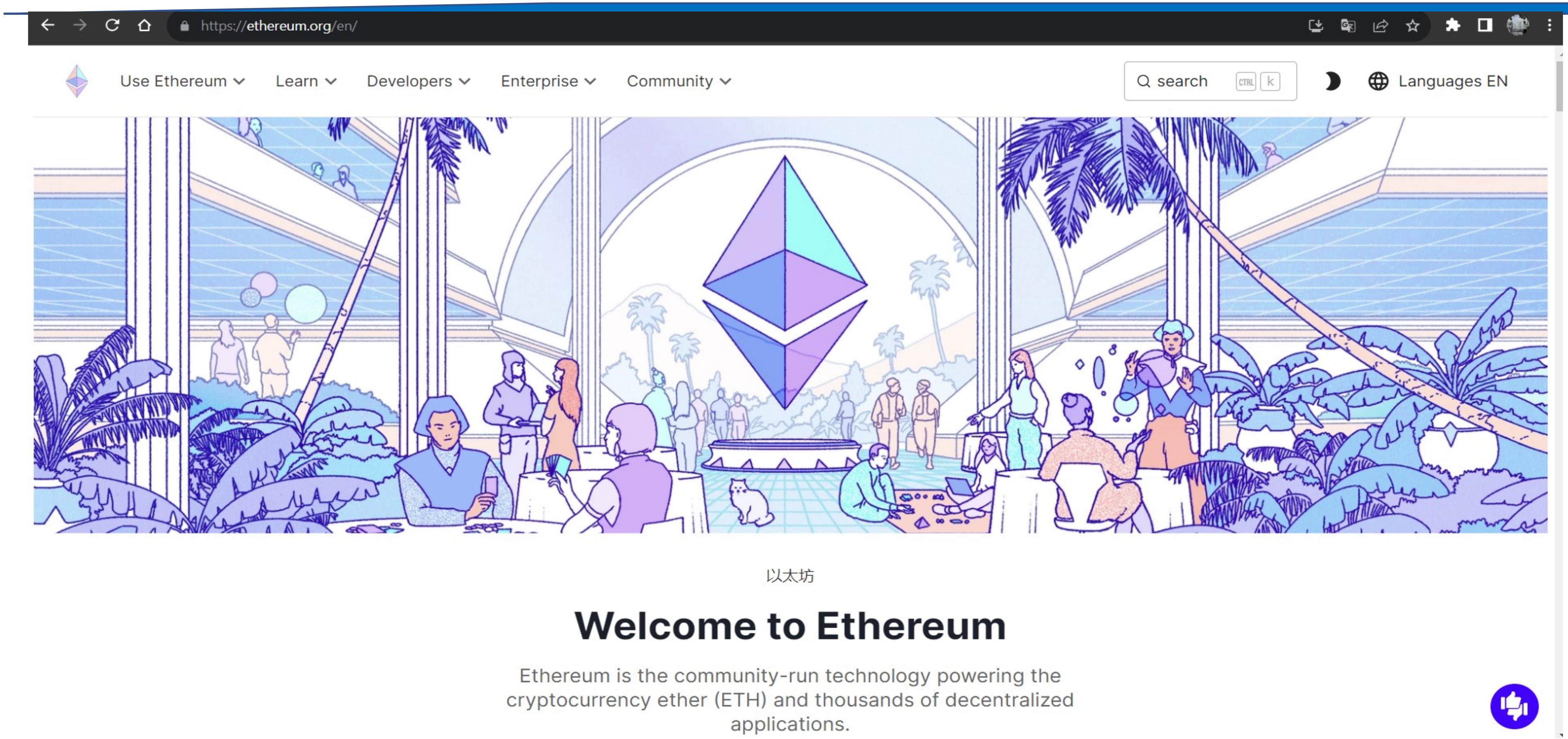


Proof of Work (PoW)

[prüf əv 'wərk]

A blockchain consensus mechanism in which computing power is used to verify cryptocurrency transactions and add them to the blockchain.

Blockchain as a platform



以太坊

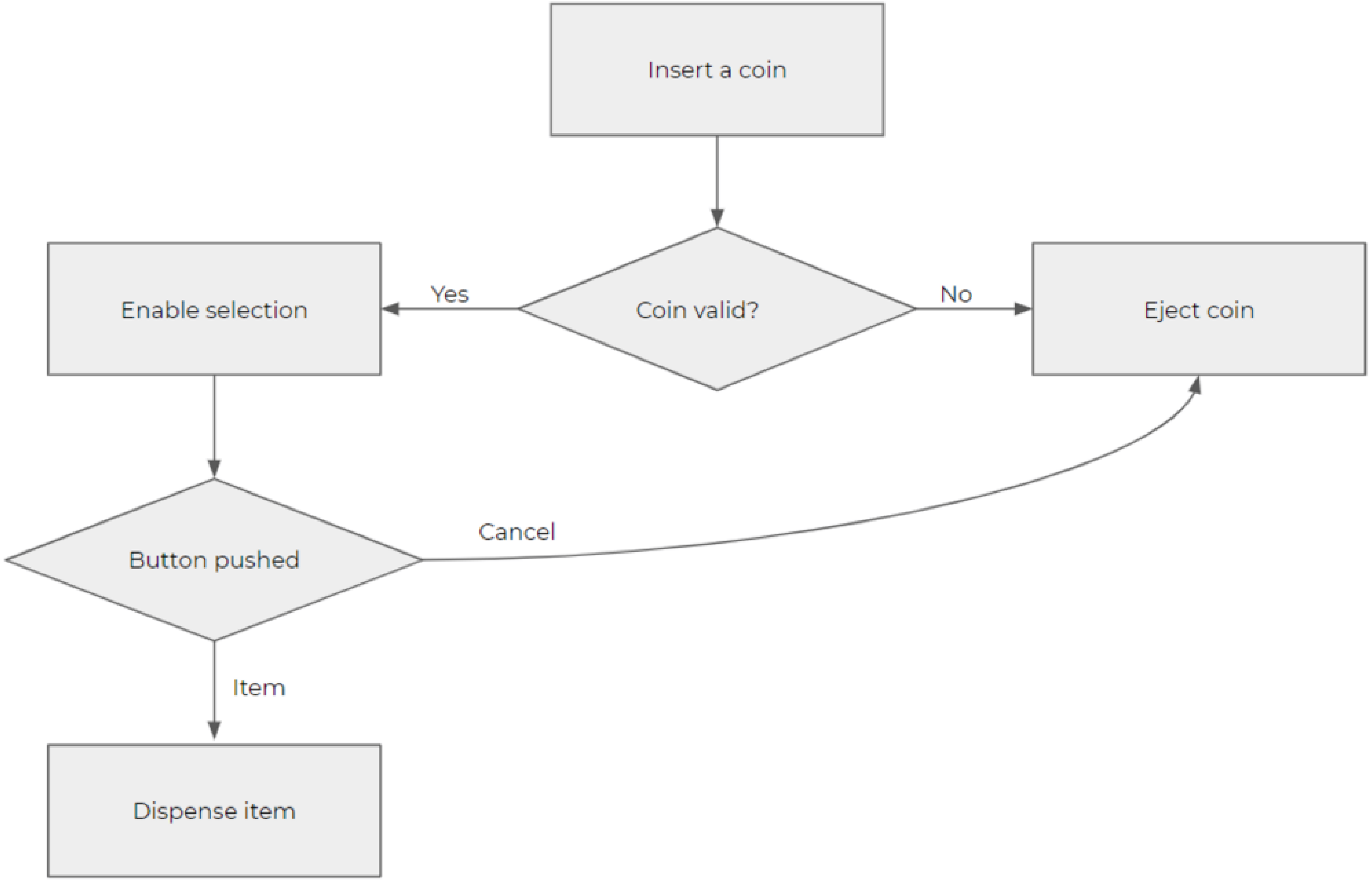
Welcome to Ethereum

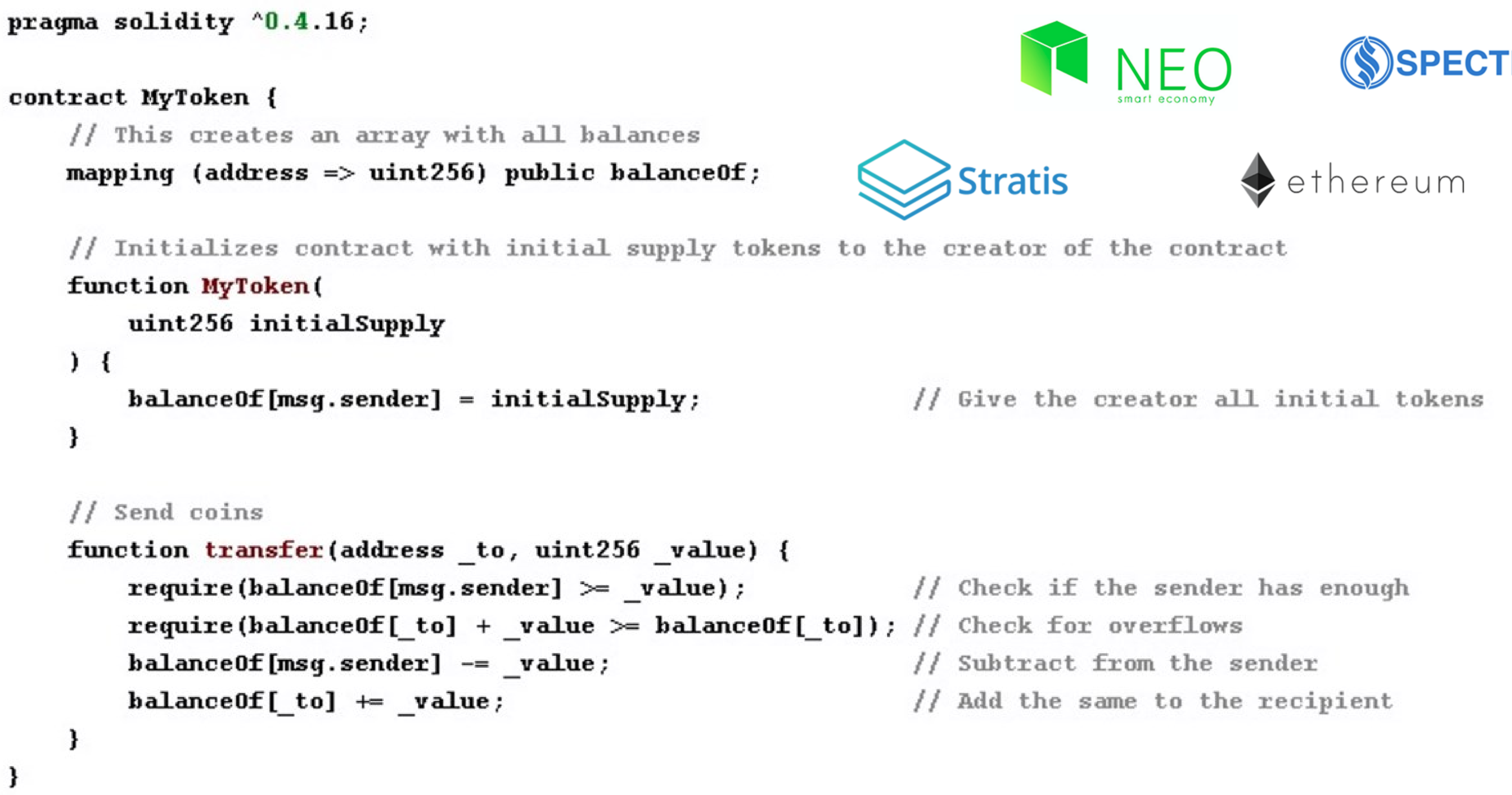
Ethereum is the community-run technology powering the cryptocurrency ether (ETH) and thousands of decentralized applications.

Features

- Tracks transactions
- Is also able to store small bits of computer code ("smart contracts")
- Code runs within the Ethereum platform and changes the state of variables (think entitlements) stored on the blockchain
- Uses the ether cryptocurrency
- Also uses gas to pay for running the computer code
- Has a much shorter confirmation time (about 15 seconds)
- "DApps" are built on top of these platforms

Smart Contract





```
pragma solidity ^0.4.16;

contract MyToken {
    // This creates an array with all balances
    mapping (address => uint256) public balanceOf;

    // Initializes contract with initial supply tokens to the creator of the contract
    function MyToken(
        uint256 initialSupply
    ) {
        balanceOf[msg.sender] = initialSupply;              // Give the creator all initial tokens
    }

    // Send coins
    function transfer(address _to, uint256 _value) {
        require(balanceOf[msg.sender] >= _value);           // Check if the sender has enough
        require(balanceOf[_to] + _value >= balanceOf[_to]); // Check for overflows
        balanceOf[msg.sender] -= _value;                    // Subtract from the sender
        balanceOf[_to] += _value;                           // Add the same to the recipient
    }
}
```

Questions & Answers

- Next lecture: Essential of BlockChain
- Email: tg_phamthaikytrung@tdtu.edu.vn