Practical Blockchain

Module 2: Crypto Assets

Scope

- What are digital assets
- Coins and Tokens
- Miners
- Wallets
- Market Makers/Exchanges
- Hands-on: Executing transactions on the Blockchain

What are Crypto Assets

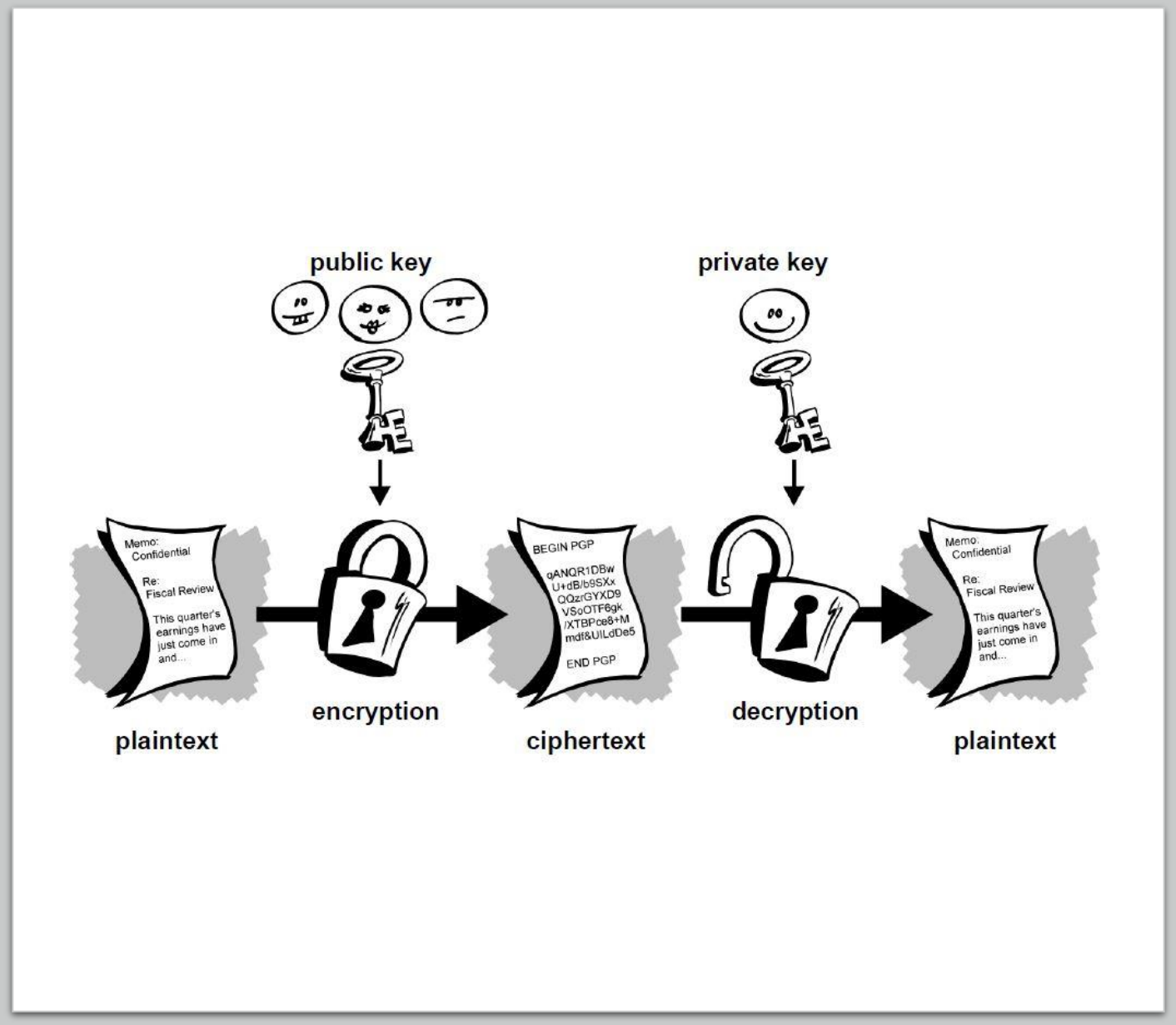
- Crypto assets, are special type of digital assets created and managed by cryptographic, peer to peer systems.
- Crypto assets are also commonly known as cryptocurrencies.
- To be exact, cryptocurrencies are only a subset of crypto assets.

What are Crypto Assets

- Crypto assets differ from other digital assets on the Internet such as music files, video, digital photos etc. as their value and ownership are being tracked as they are moved across network.

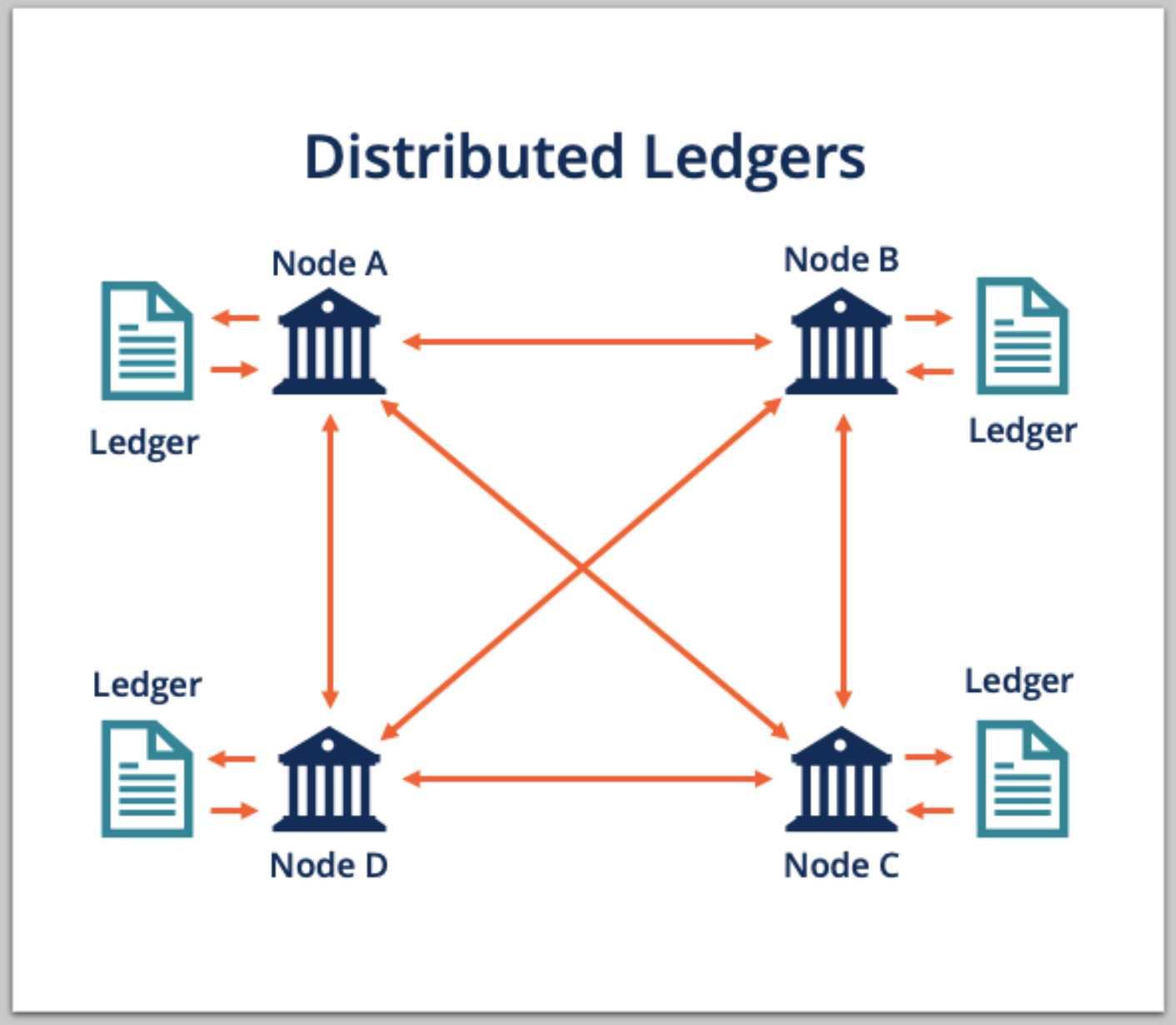
Characteristics of Crypto Assets

Use of cryptography



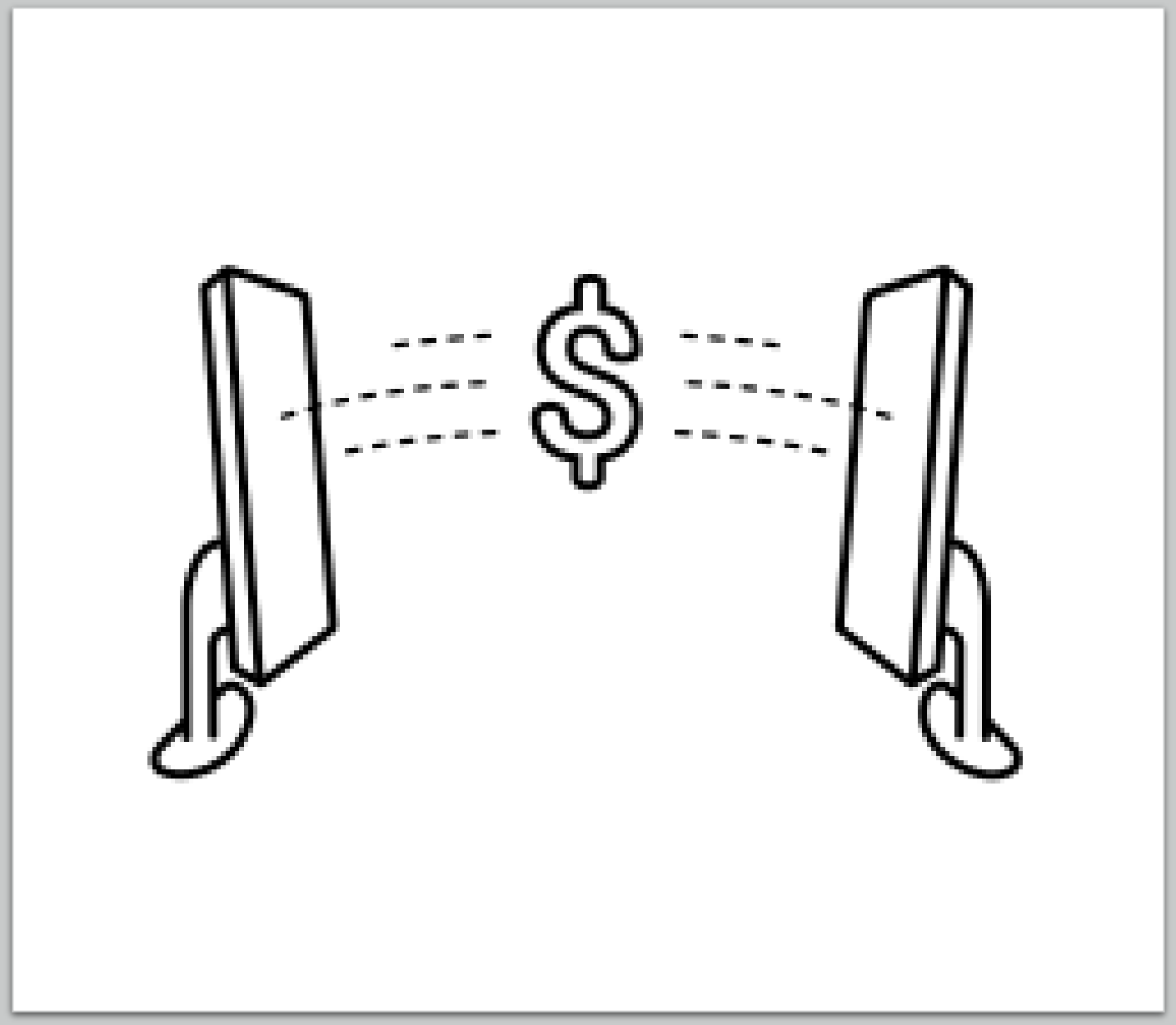
Characteristics of Crypto Assets

Depends on distributed ledger technology (DLT). One of the most famous ones is Blockchain and therefore often used synonymously



Characteristics of Crypto Assets

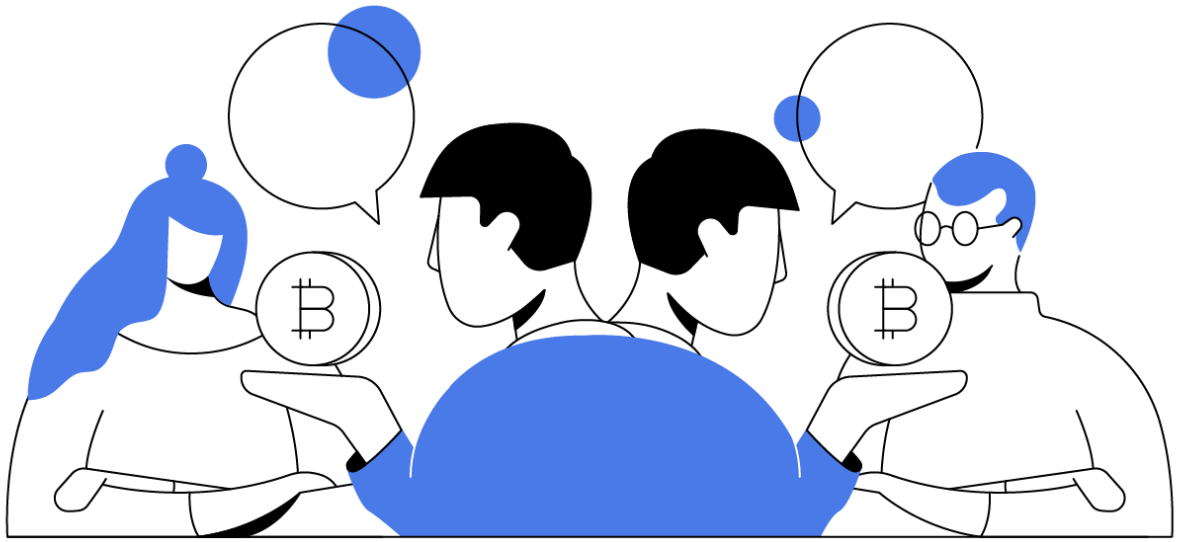
No third party like a bank or another central authority is needed to issue or exchange crypto assets such as Bitcoin



Double Spending

Double spending is the fraudulent spending of the same unit of currency more than once.

In the real world, once a bill has been handed over to a merchant, it is physically gone making it impossible to use it again.



Double Spending

In the traditional digital world, exchange of information is done by copying a file from sender to receiver.

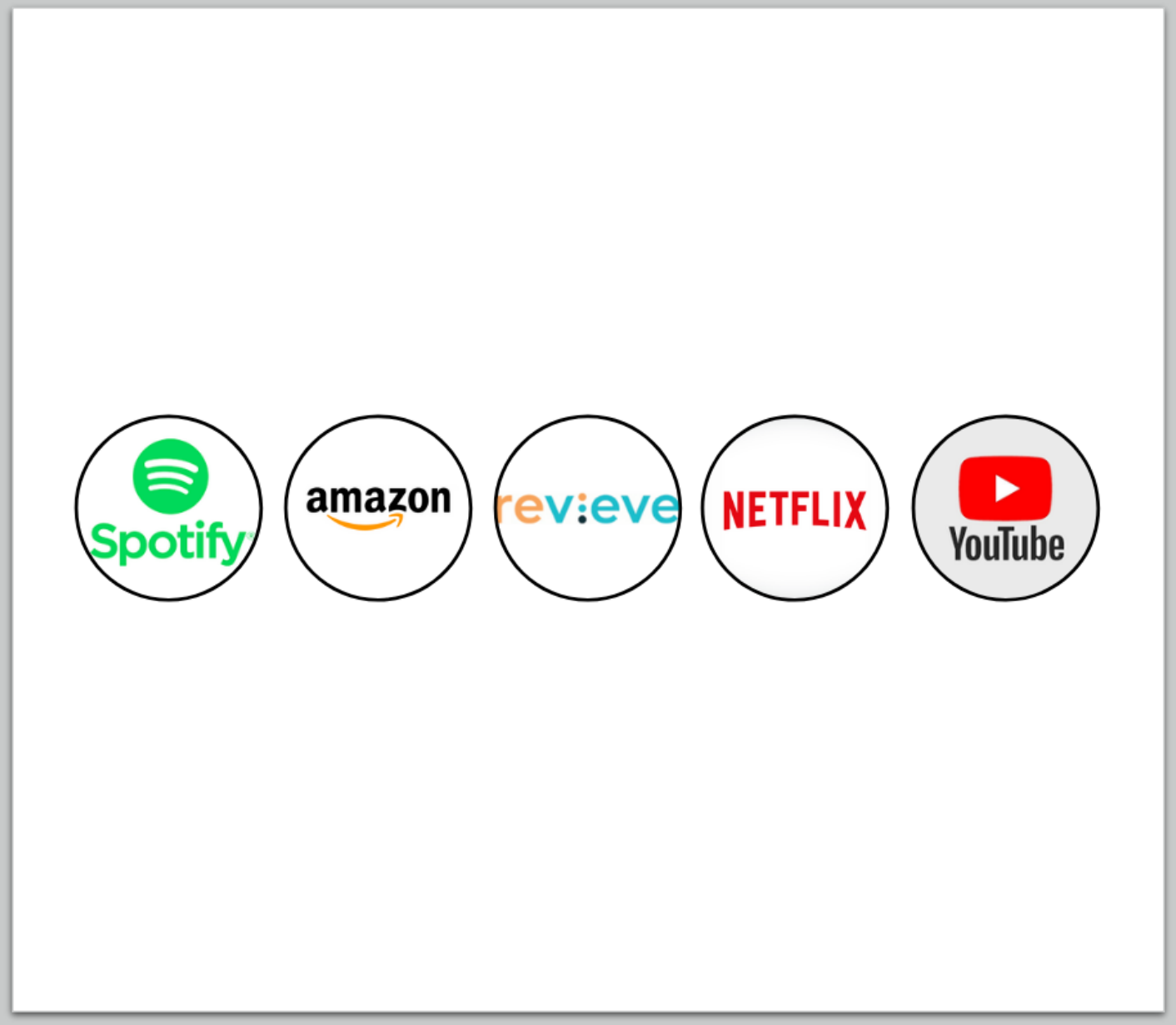
This mode of exchange doesn't fit well for exchange of valuable assets as both the sender and the receiver remains with a copy of the file making double spend possible.

Double Spending

For example, one can send a digital music file to many recipients without altering the immediate value of each individual file.

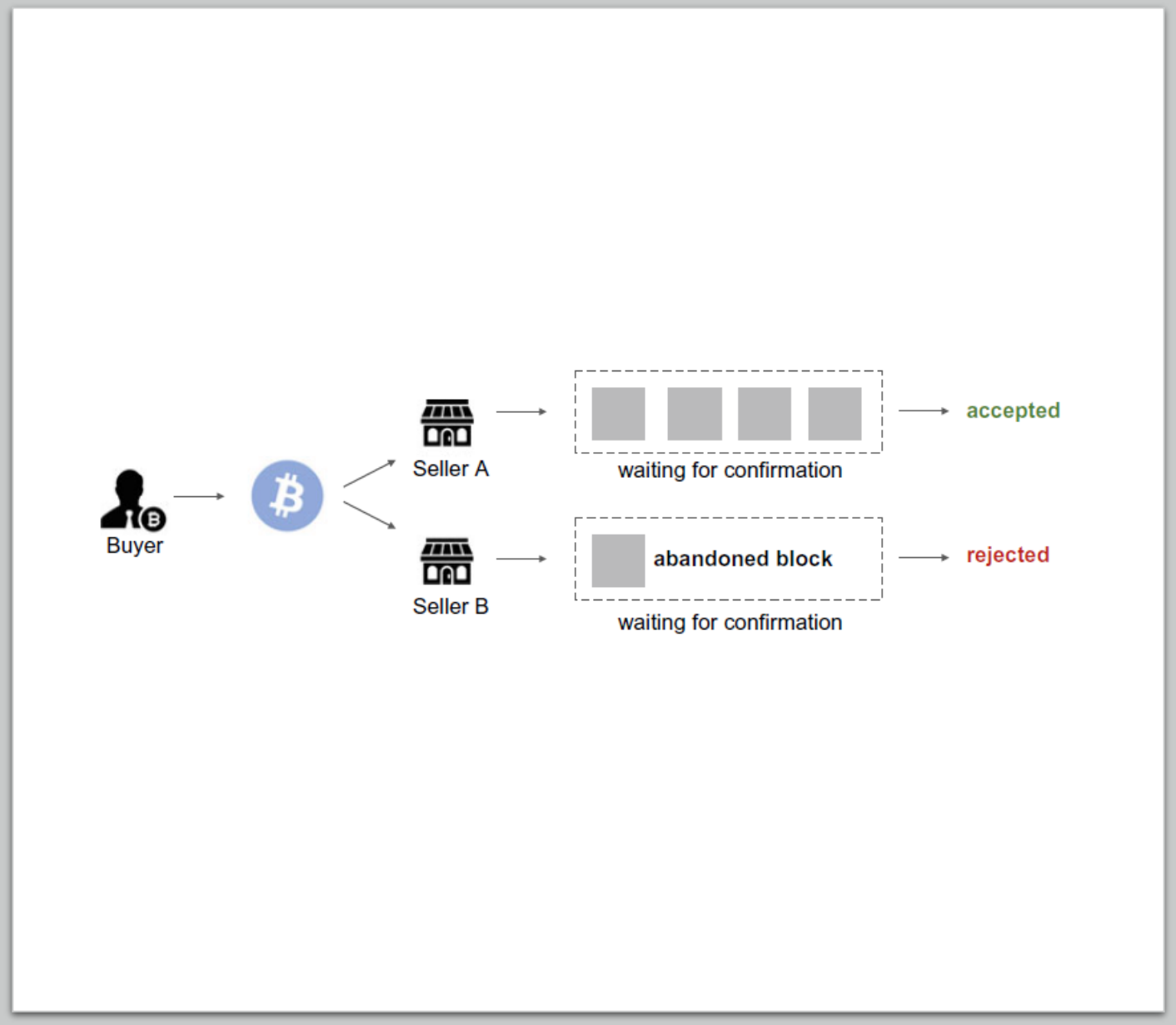
Double Spending

This scenario presented a considerable challenge for the entertainment industry at the end of the last century, disrupting the music business and resulting in new economic models



Double Spending

Crypto assets solve this problem by monitoring ownership of assets as they move across users thus omitting the need of “third parties”



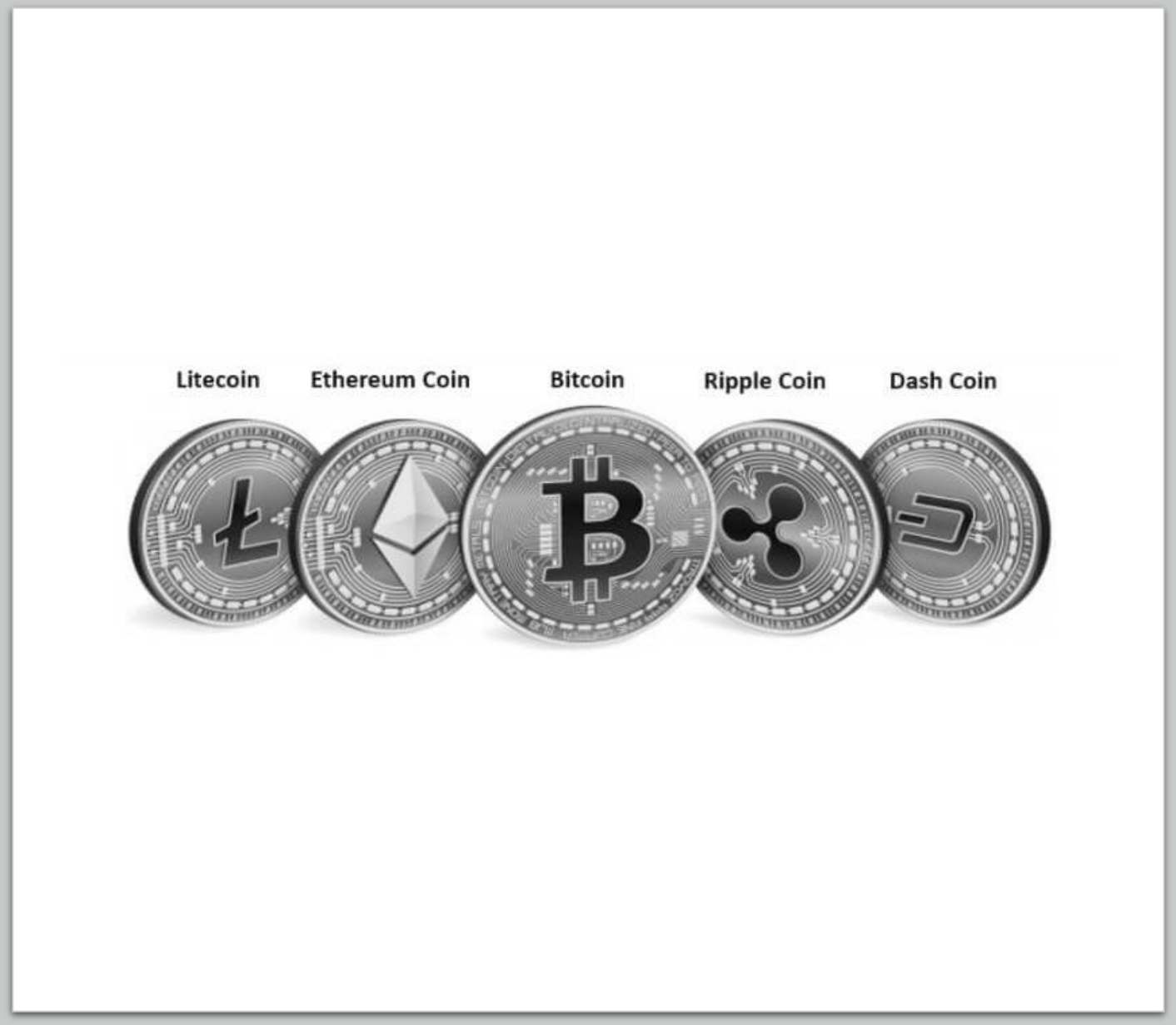
Categories of Crypto Assets

Coins

Crypto assets that fall into the category of payment are categorized as coins.

These includes Crypto currencies such as Bitcoin, Ethereum and Litecoin.

Apart from payments coins are used as investment assets.



Categories of Crypto Assets

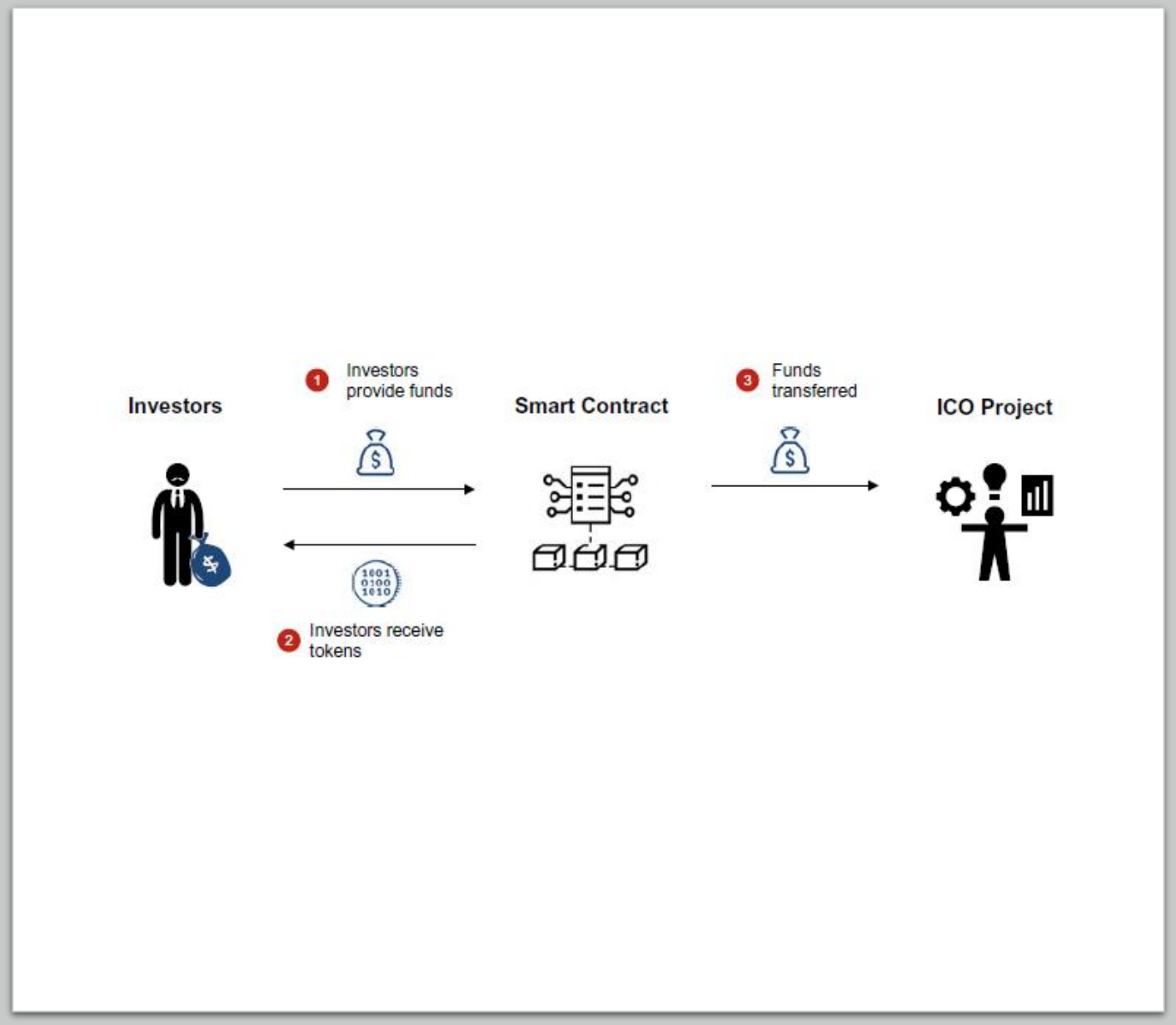
Tokens

A token is a digital asset that represents the ownership of a real-world asset such as piece of land or shares in a project.

The process of converting e.g. ownership rights of real-world items into tokens is called tokenization.

Tokens are normally created using smart contracts.

Initial Coin Offerings (ICOs) are a popular fundraising method using coins/tokens



Exercise 1: Exploring Digital Assets

Use Blockchain explorer to view Bitcoin and Ethereum coins

Crypto Asset Ecosystem

At the heart of all crypto assets there is a Blockchain. It provides the ideal infrastructure to own and exchange digital assets such as Bitcoin.

The crypto ecosystem includes the following parties

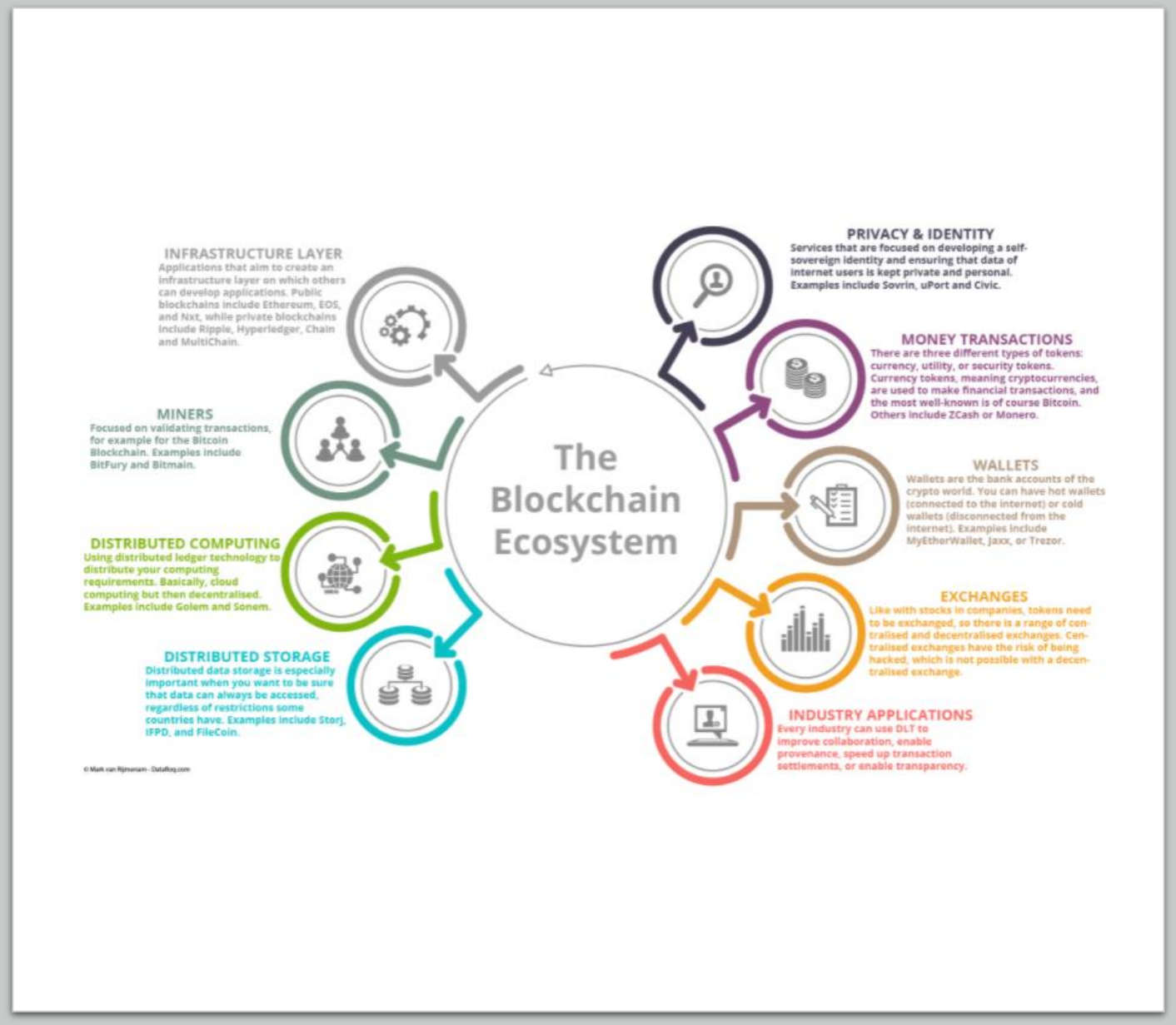
i. Distributed infrastructure

ii. Miners

iii. Wallets

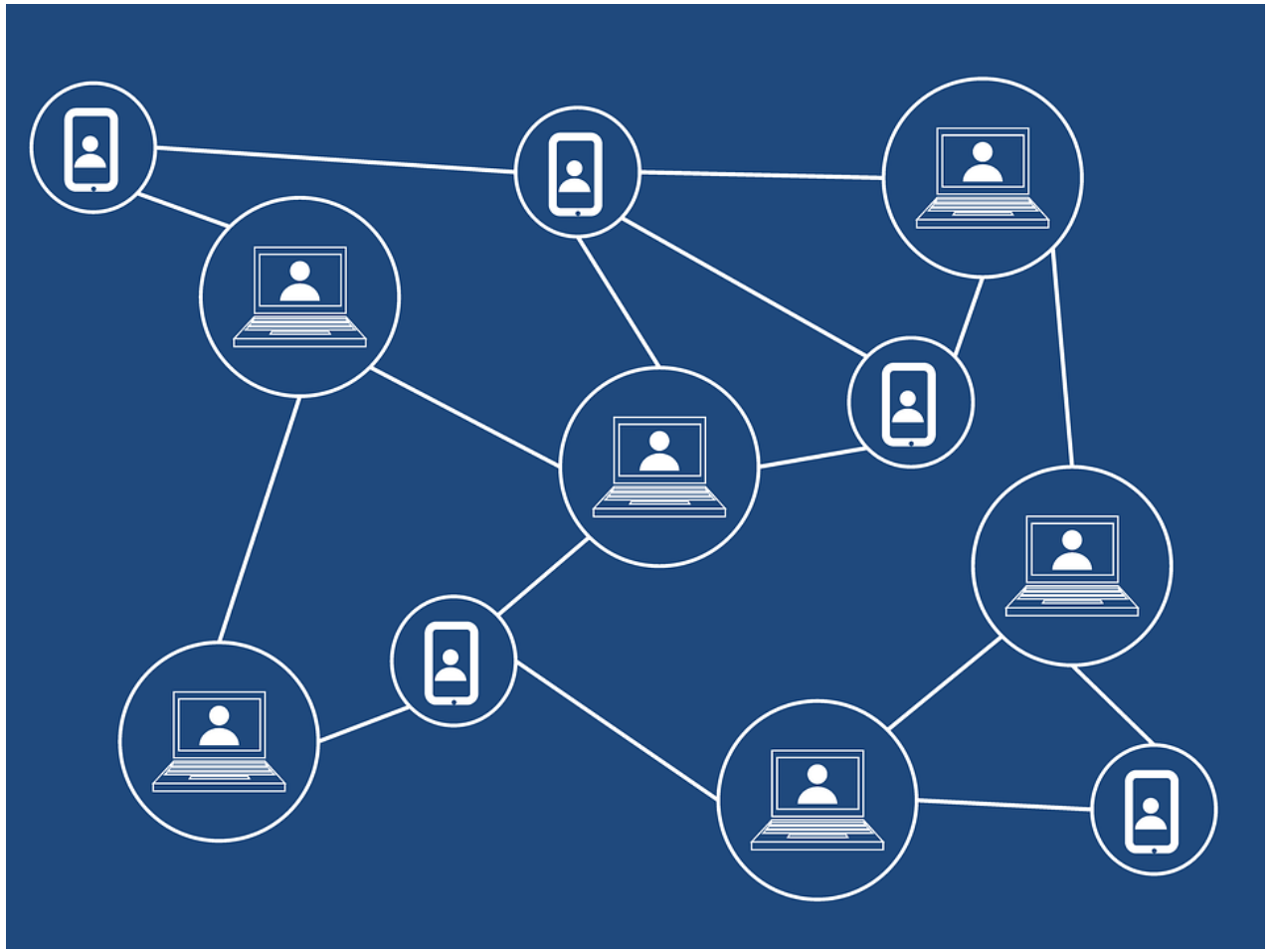
iv. Exchanges

v. ICOs



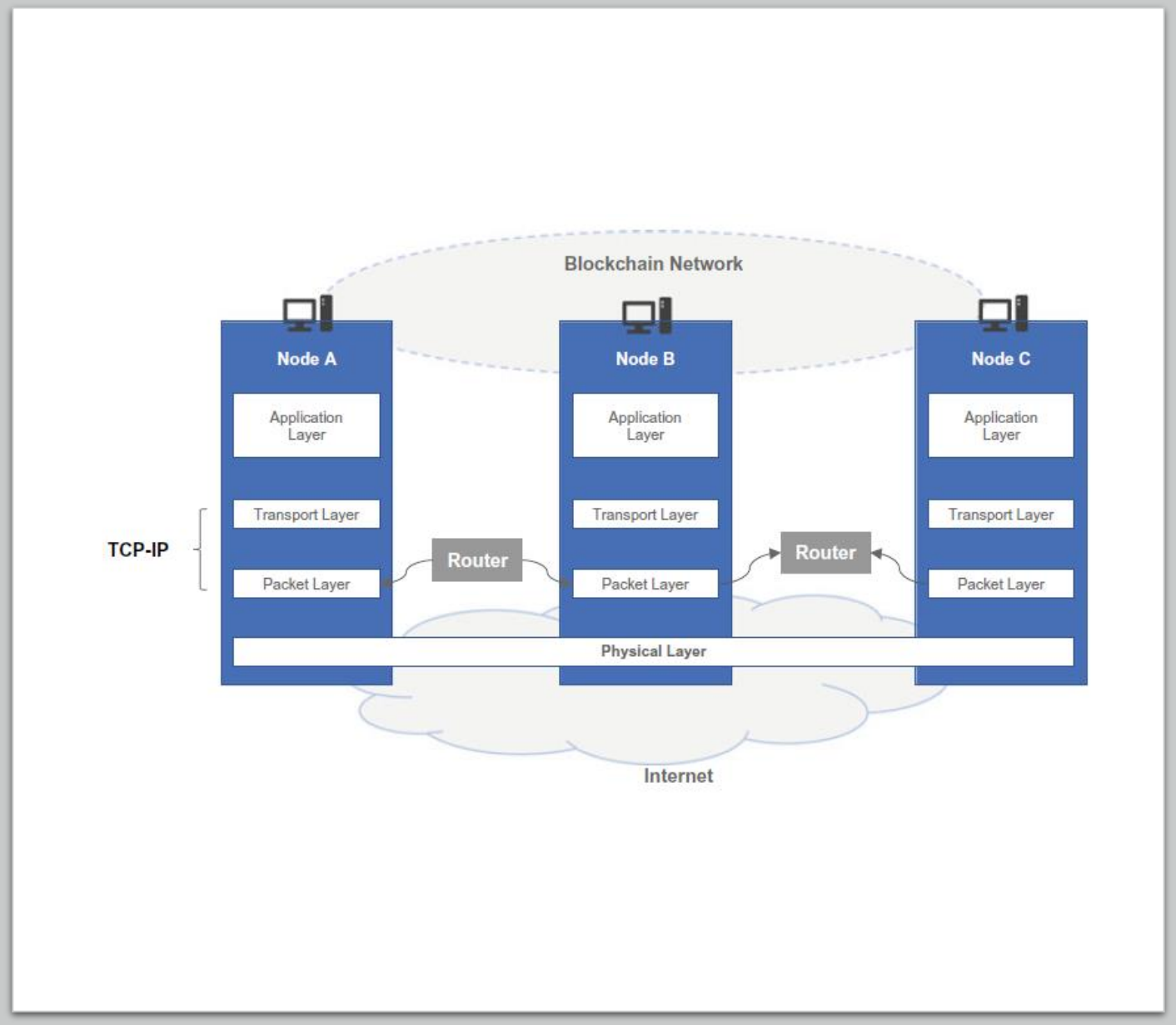
Distributed Infrastructure

A blockchain is a ledger of information (e.g., transactions, agreements) that are stored chronologically across a network of computers.



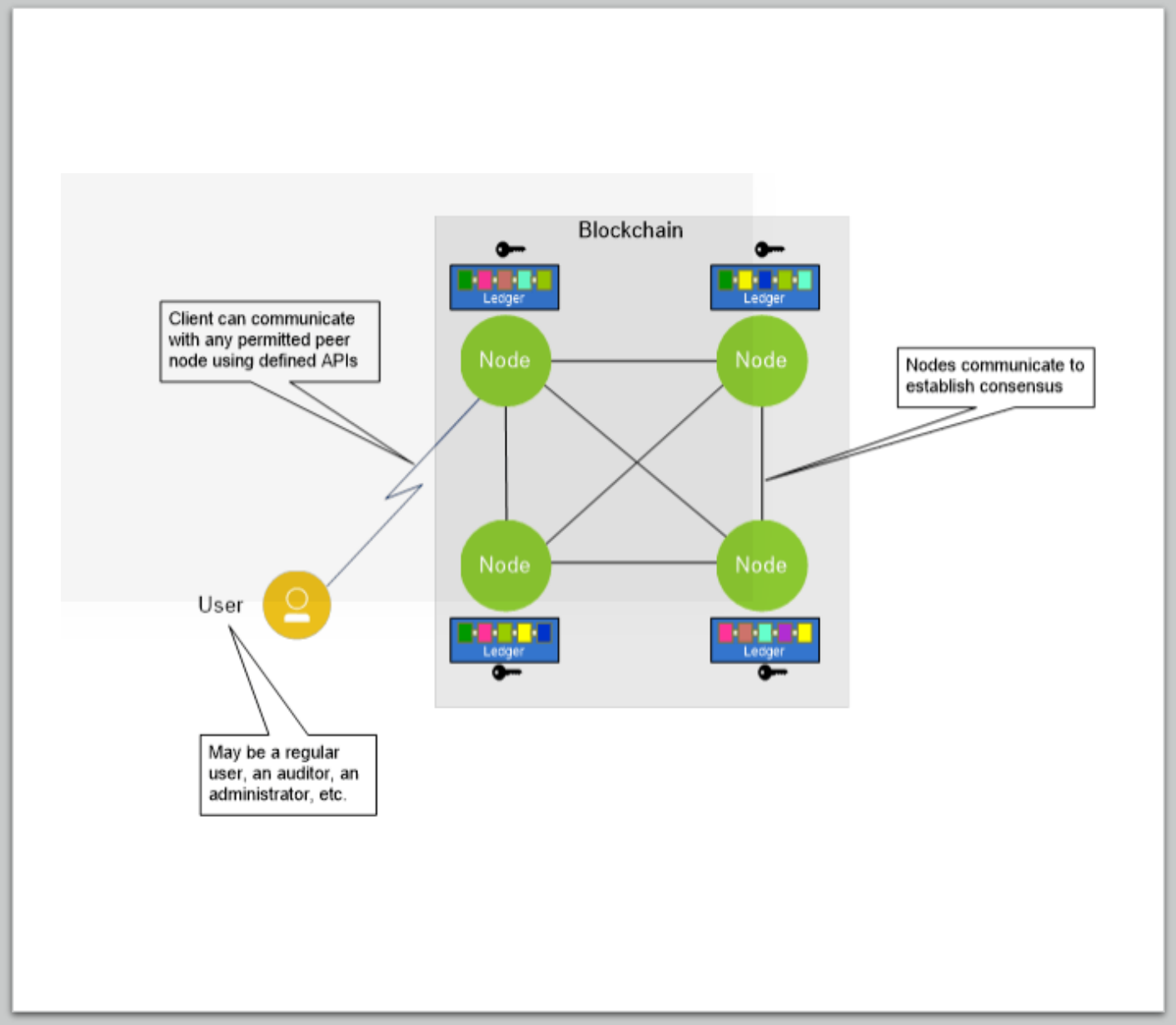
Blockchain Infrastructure

- Just as TCP-IP enables the decentralized exchange of information across the Internet, blockchains enable the decentralized exchange and control of assets.



Blockchain Architecture

- A blockchain network consist of participating members (“nodes”) that are connected via a computer network.
- Each node consists of blockchain client, a software responsible for storing and tracking the transfer of assets between nodes.



Blockchain Architecture

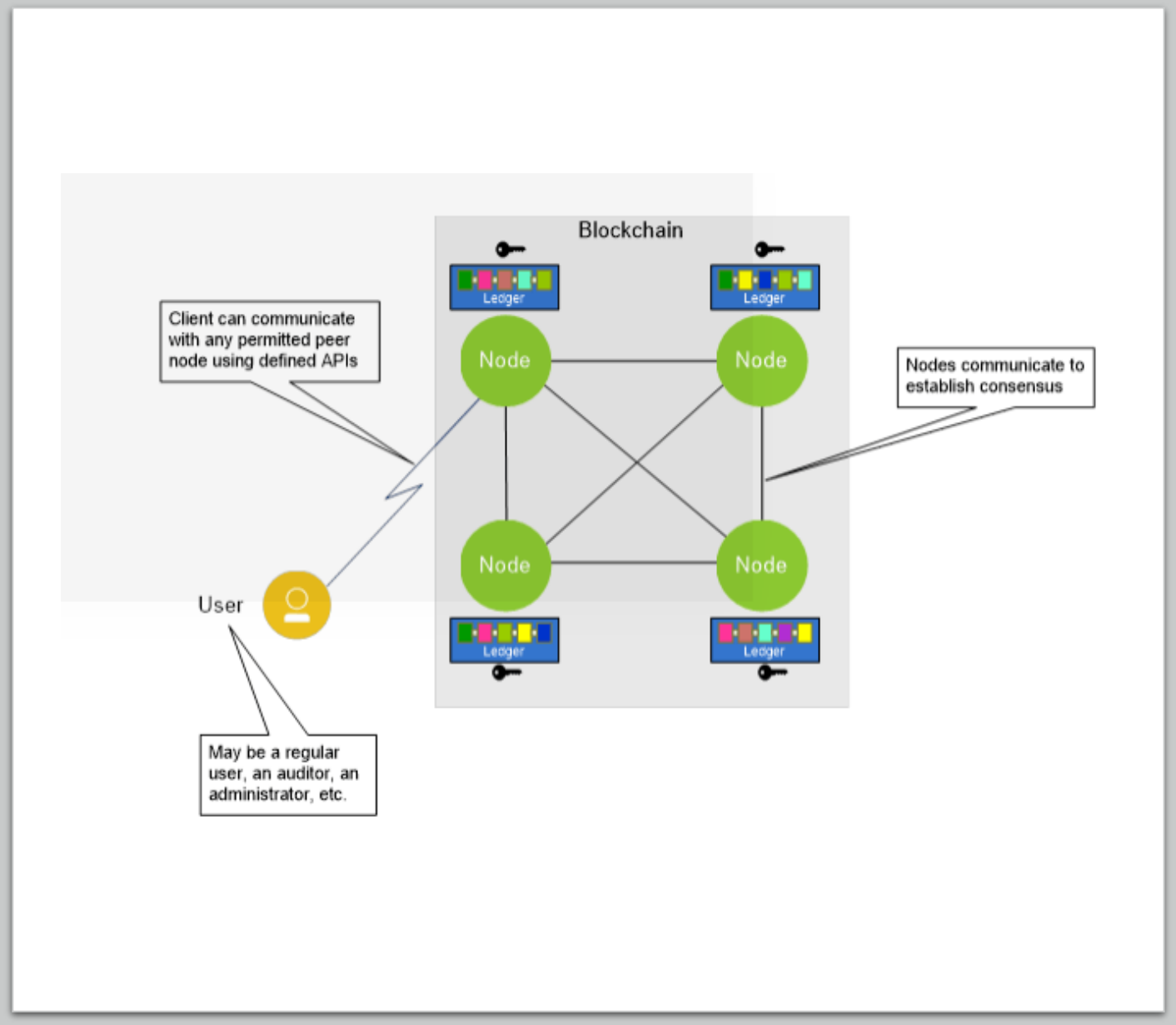
Blockchain software consist of the following components:

i. A digital account book (the “ledger”)

ii. P2P network

iii. Cryptography and

iv. Consensus protocol



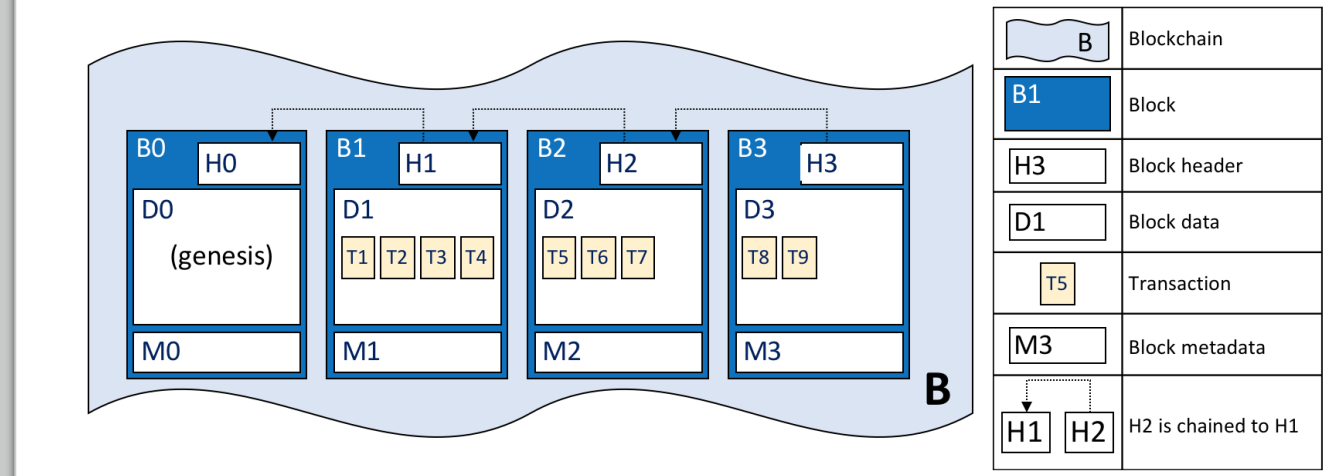
Blockchain Architecture – The Ledger

A ledger is a collection of transactions.

A blockchain network uses distributed ledger with each node keeping a copy and syncing to the same data across the network

File based

Append only

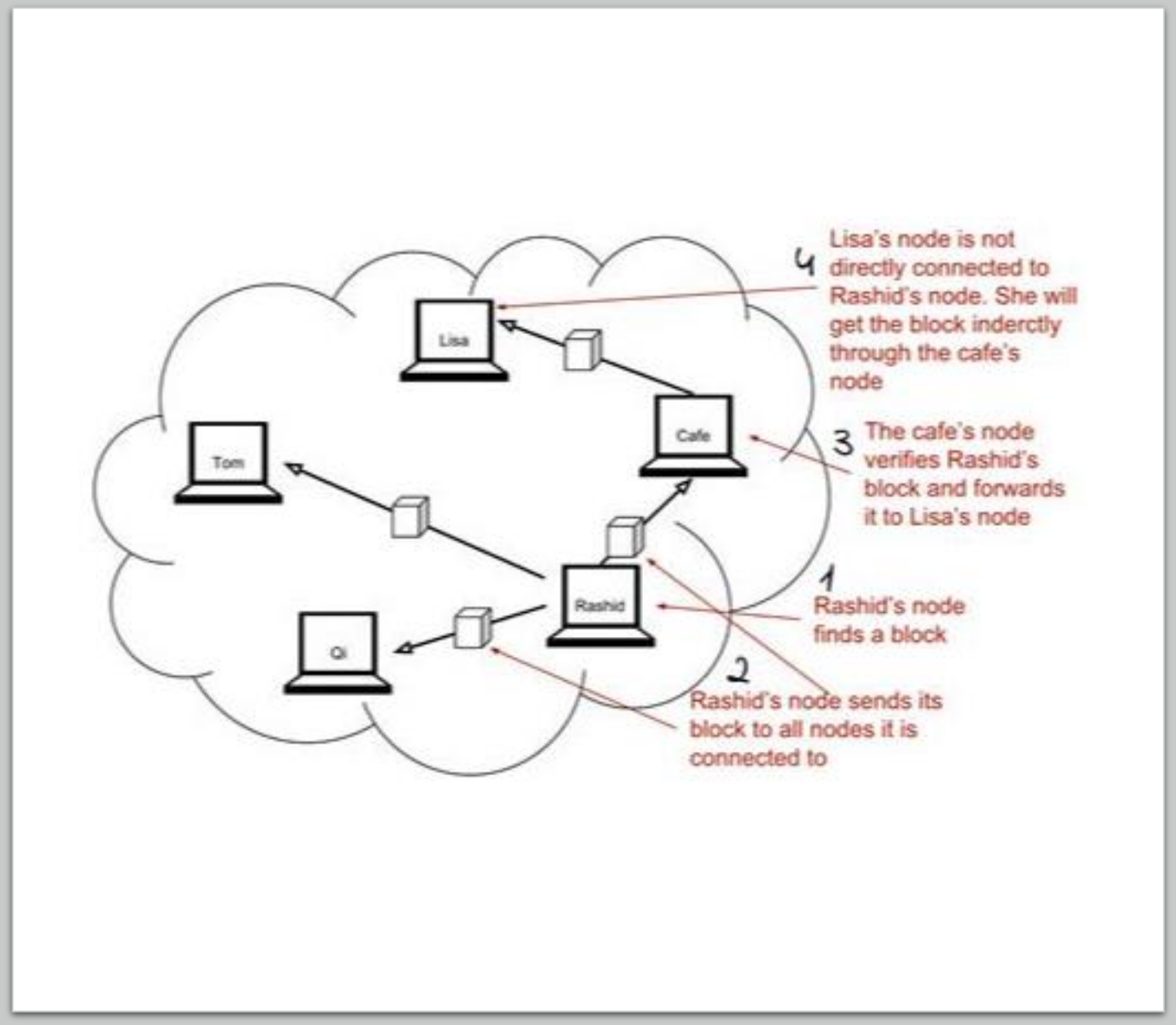


Blockchain Architecture – P2P Network

All nodes have the routing function included in order to participate in the network,

Routing function is used by a node to connect to other nodes and to propagate transactions and blocks.

Blockchain uses gossip protocol that is information is being passed from one node to another using TCP connection

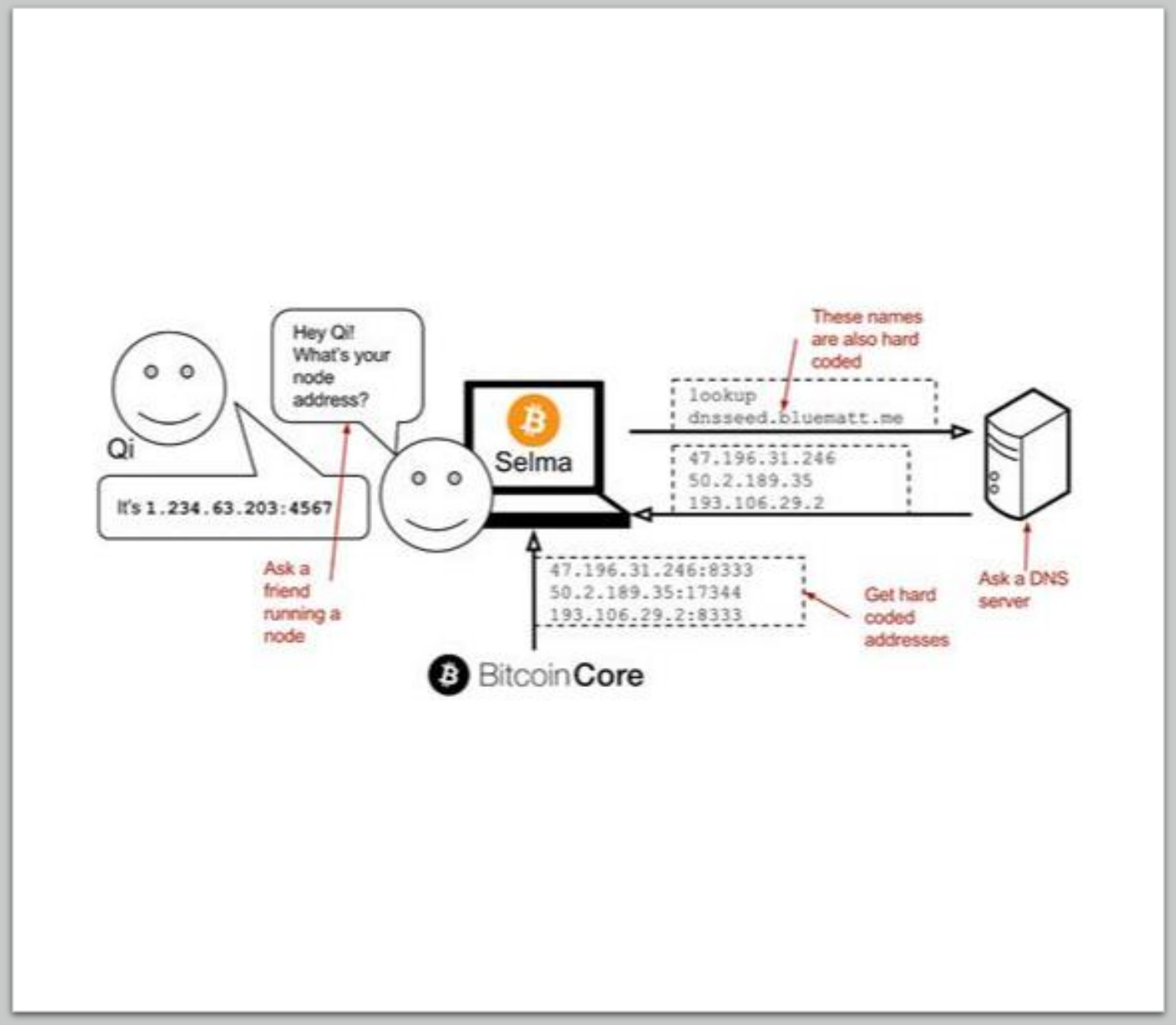


Blockchain Architecture – P2P Network

Finding initial peers

When a user first connect to the network, they find initial peer addresses through several methods the most common being DNS look up. (DNS names are hardcoded in the client software)

Other methods are configuring the node with custom addresses or hardcoding the node with known addresses.



Blockchain Architecture – P2P Network

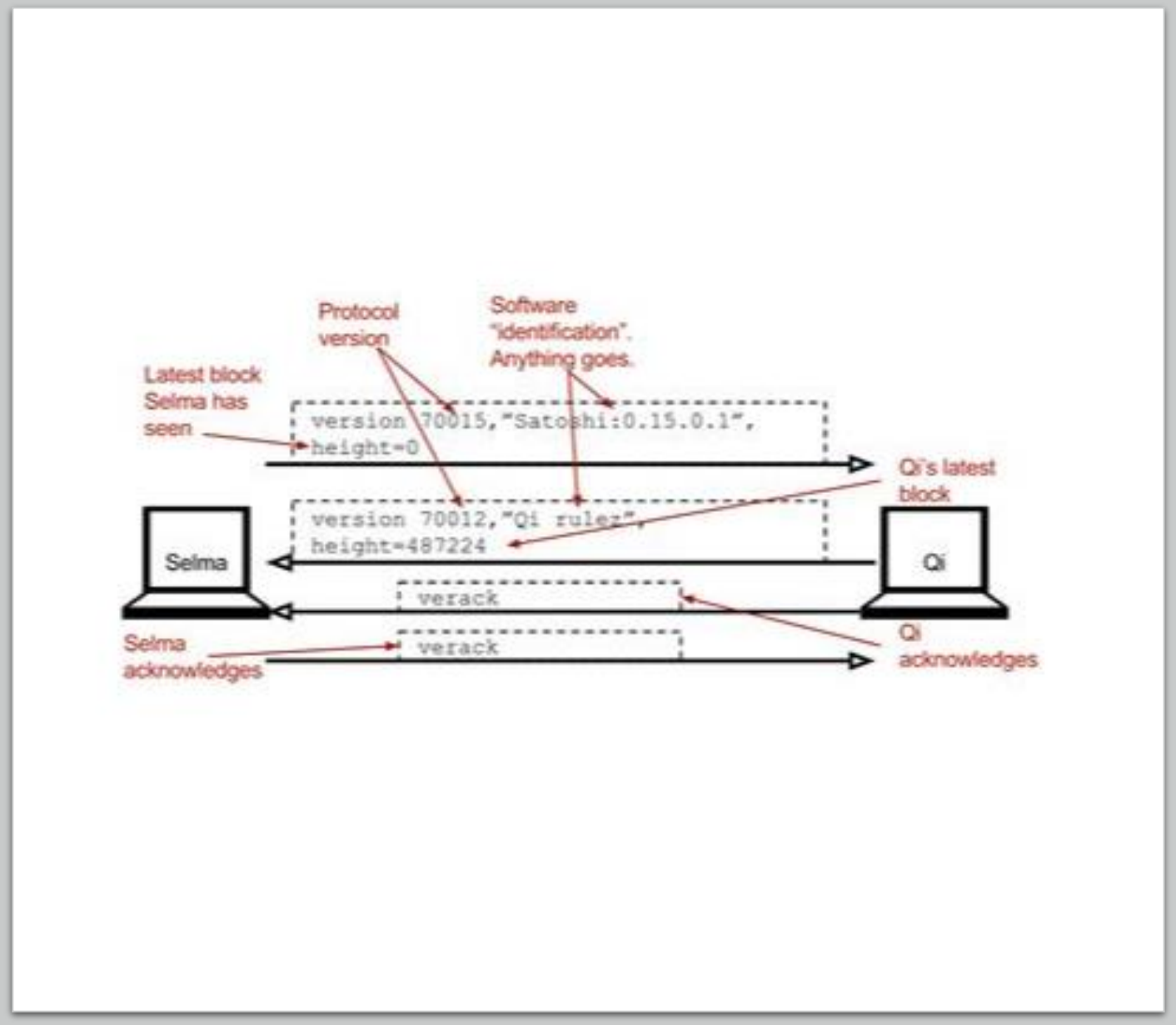
Connection handshake

Connecting node send a version message[protocol version, client software, IP, height] to peer.

Peer respond with their own version message and an ack

Connecting node respond with an ack. The handshake is done.

Connecting node ask peer for more peer addresses to connect to.



Blockchain Architecture – P2P Network

Sending transactions

Consider an example with 2 nodes, John's and Tom's

John has performed a transaction and wants to notify Tom.

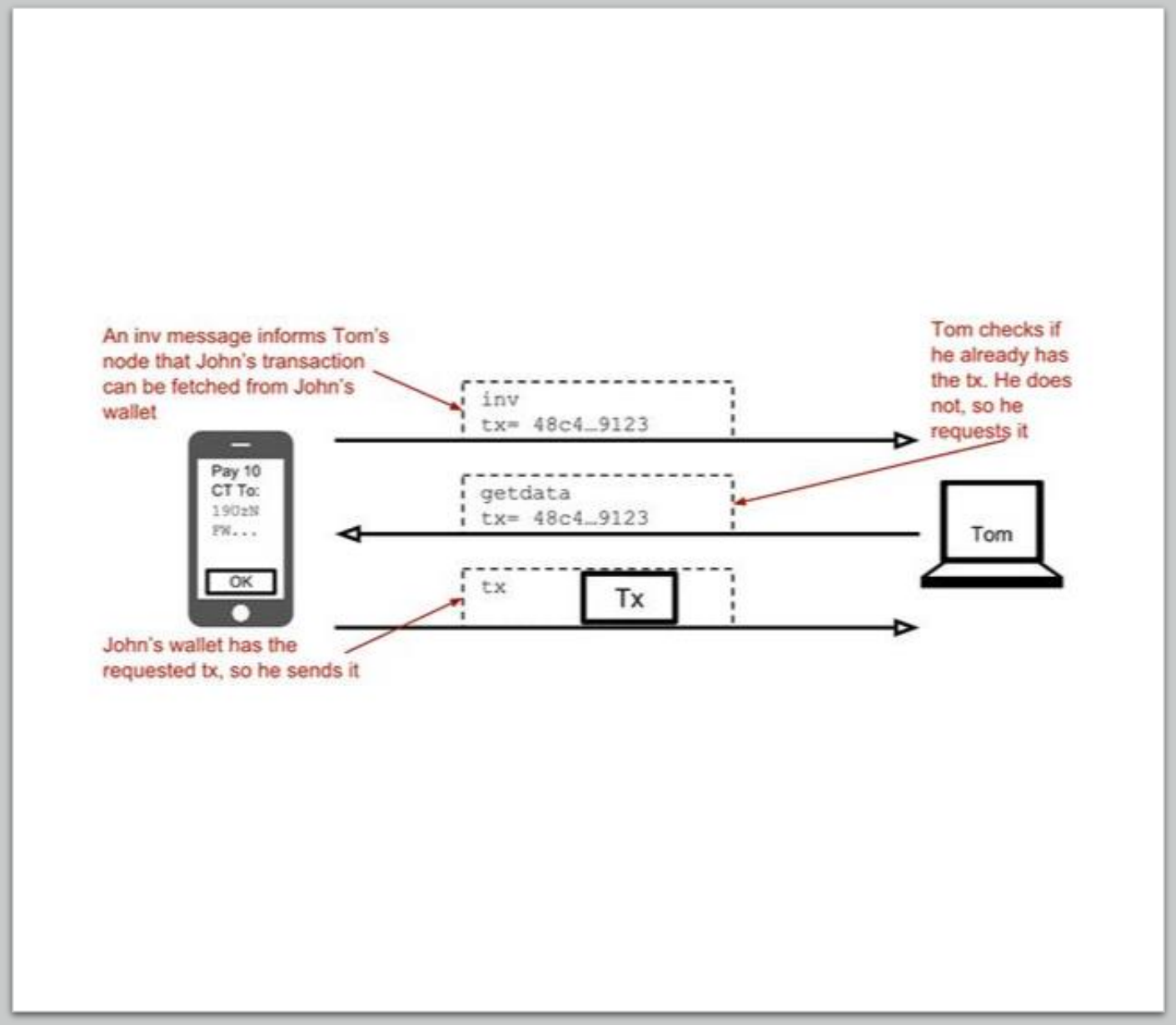
Sending the transaction to Tom will happen in 3 steps

i. John inform Tom that he has a transaction to be fetched

ii. Tom check if he doesnot have the transaction and request it

iii. John send the transaction

Tom then forwards the transaction to his peers using the same method.

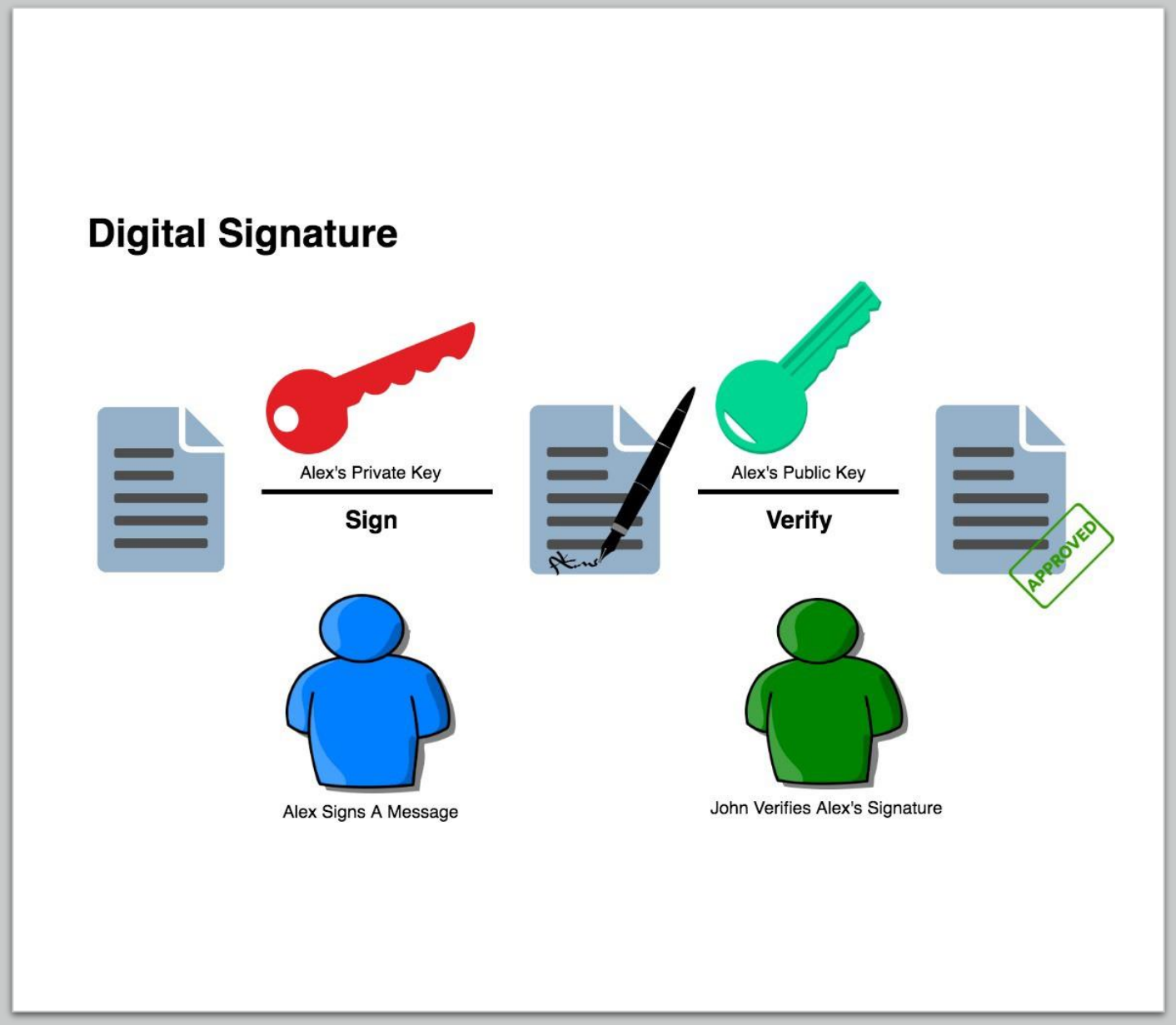


Activity 2: Blockchain Network

Explore P2P connection in a blockchain network

Blockchain Architecture – Cryptography

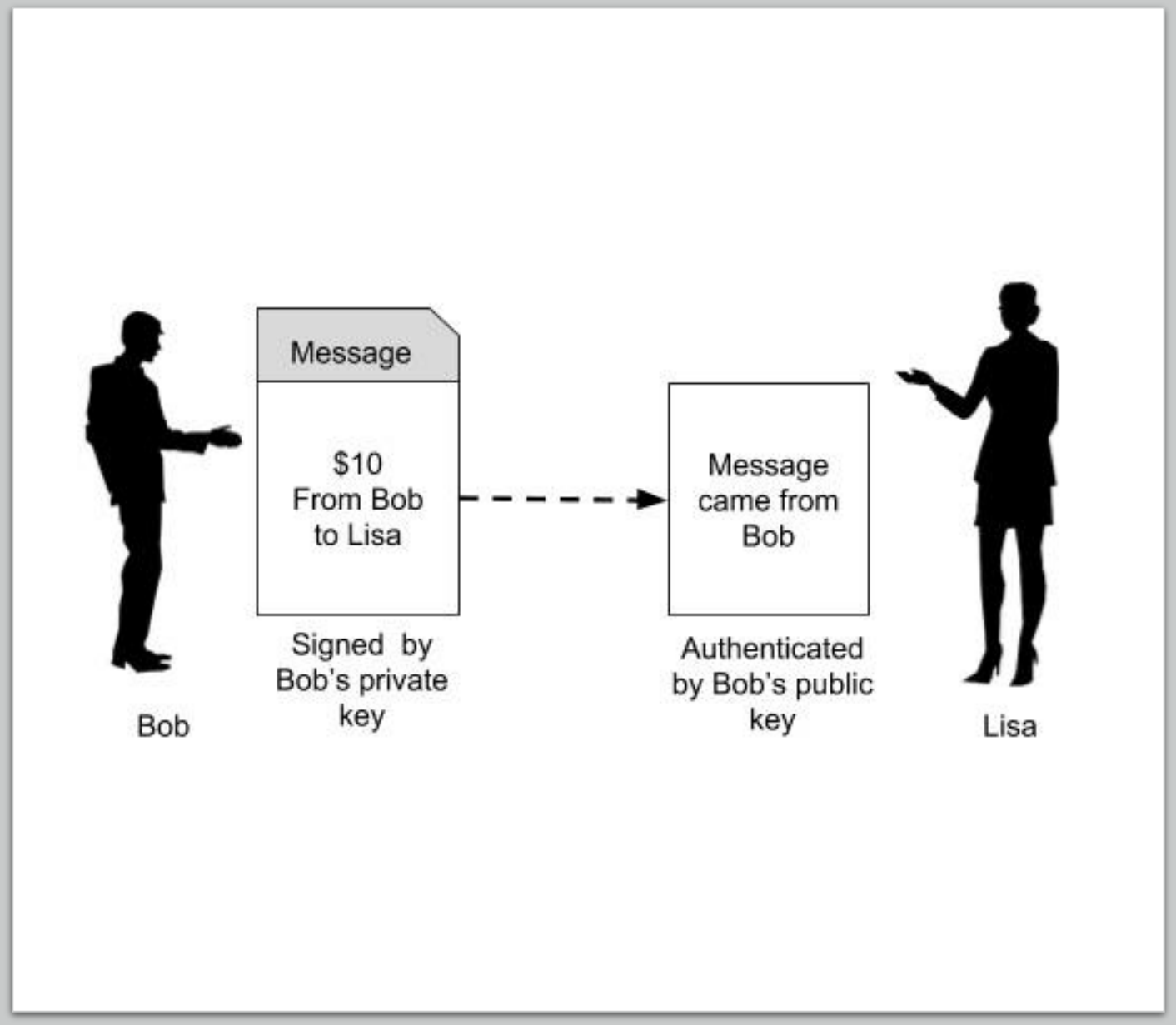
Cryptography are methods for encrypting information so it cannot be understood by unauthorized parties.



Blockchain Architecture – Cryptography

Cryptographic methods play a crucial role in ensuring the proper operations of any blockchain system

Blockchains rely on cryptography to implement security measures such as authentication, verification and integrity



Blockchain Architecture – Cryptography

Blockchains use 3 fundamental cryptographic principles for its operations

i. Public/private keys (Authentication)
ii. Digital signatures (Verification)
iii. Hashing (Integrity/mining)

Blockchain Architecture – Cryptography

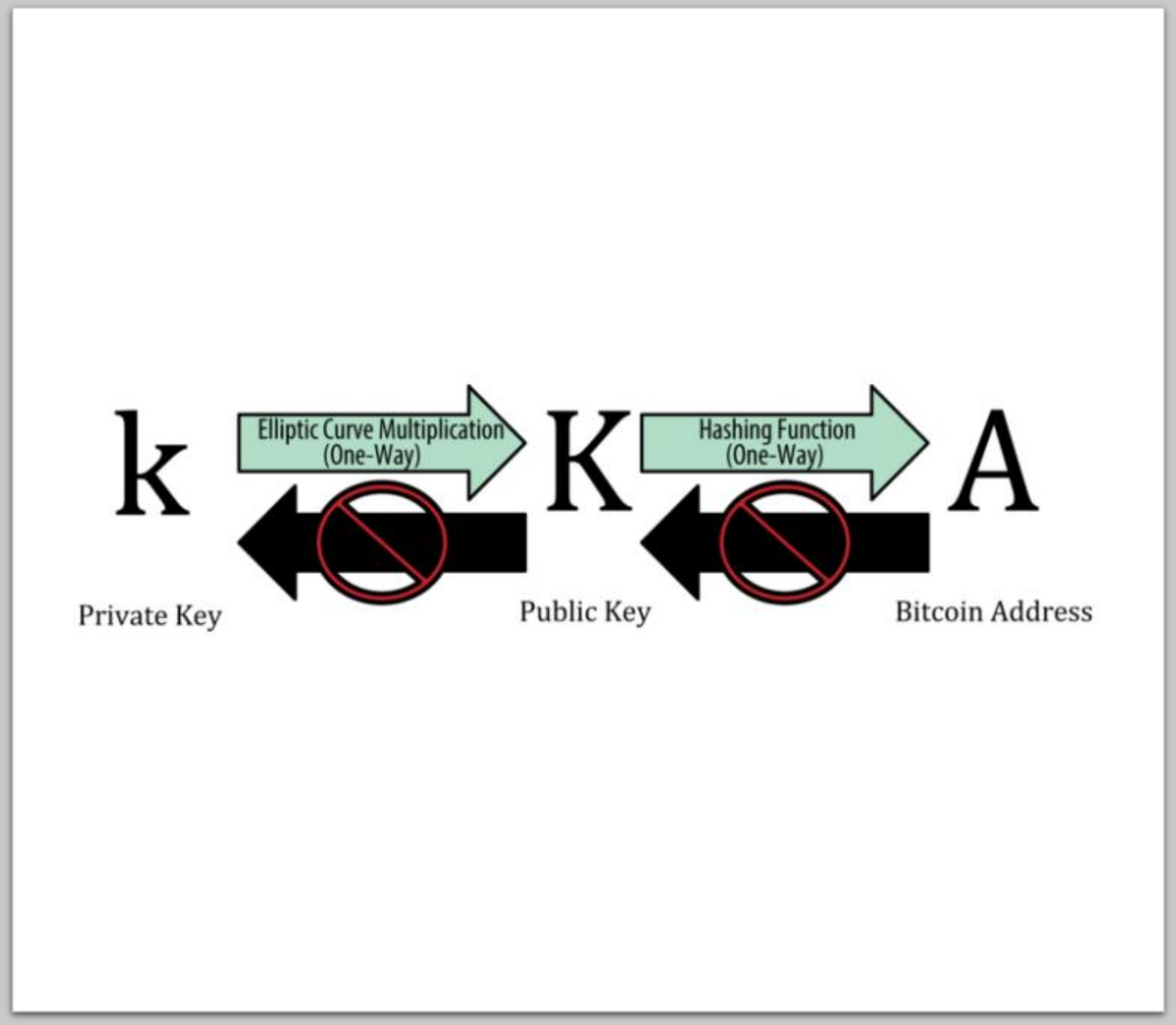
Private/Public Keys

Each account owner in a blockchain network has a public/private key pair.

A private key is created during account creation. In Bitcoin the private key is a 256-bit number.

A public key is a mathematical result of its associated private key.

In Bitcoin, the recipient address is derived from the hash of the public key

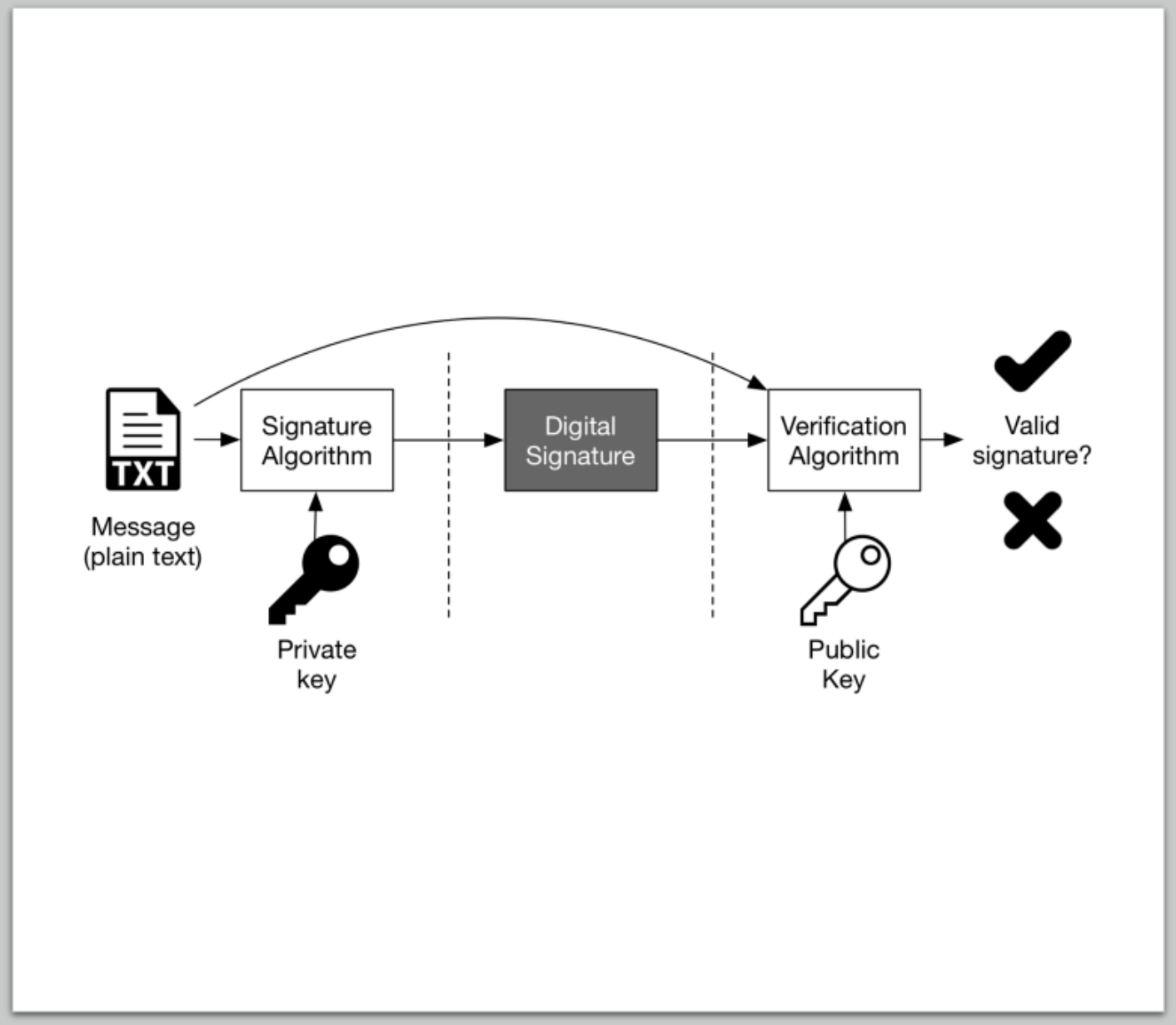


Blockchain Architecture – Cryptography

Digital Signature

Digital signature uses a mathematical function that depends both on the message (the transaction details), and sender private key.

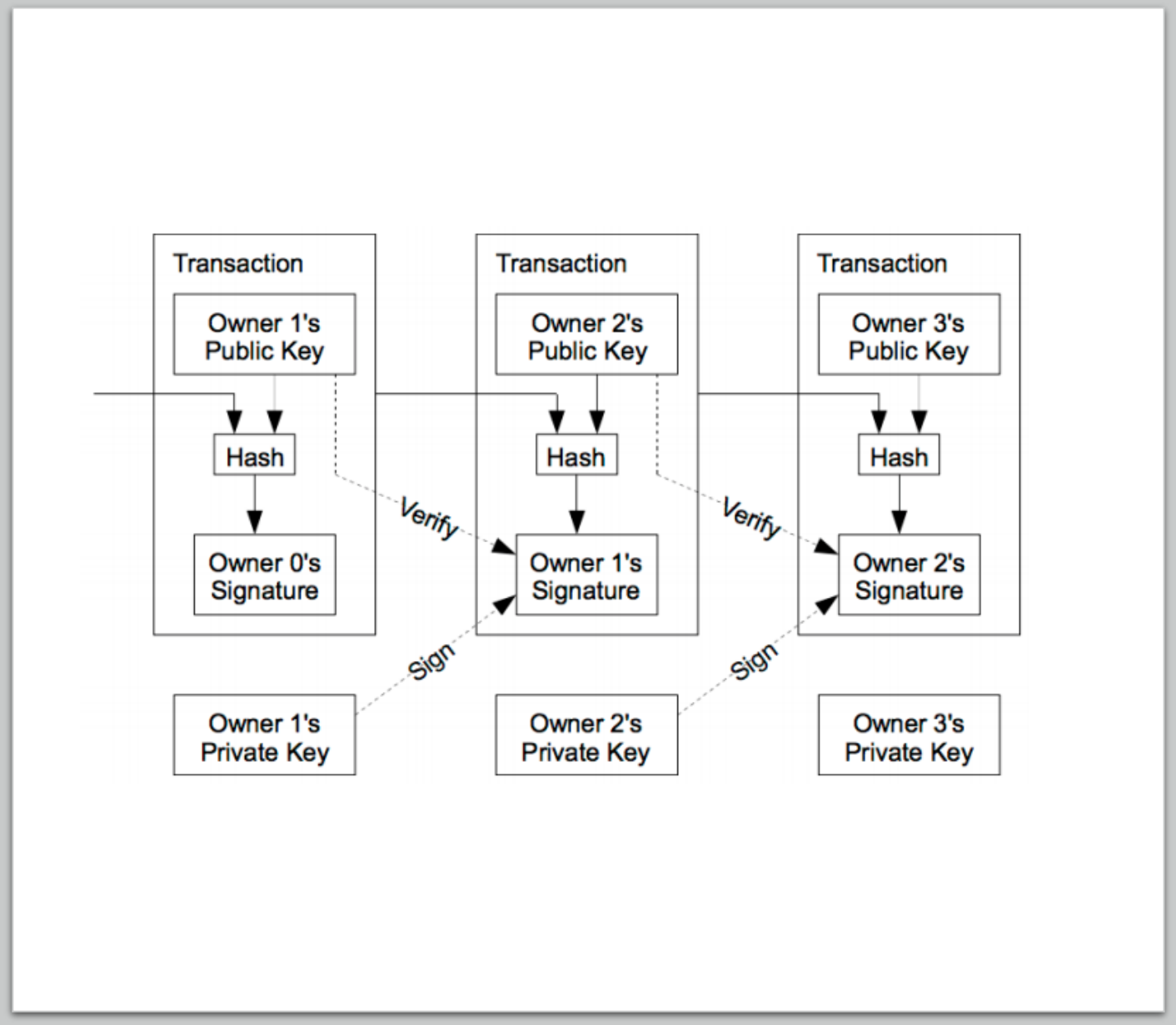
The verification determines that the transaction could have only come from someone with the private key that corresponds to their public key.



Blockchain Architecture – Cryptography

Digital Signature

1. Owner 1 creates a message transaction to send asset to owner 2: [public key (pk1), public key (pk2), amount].
2. Owner 1 signs the message using his private key (sk1): sign(message, sk1) -----> signature
3. Owner 2 verify the authenticity of the message using owner 1 public key: verify(message, signature, pk1) -----> T/F

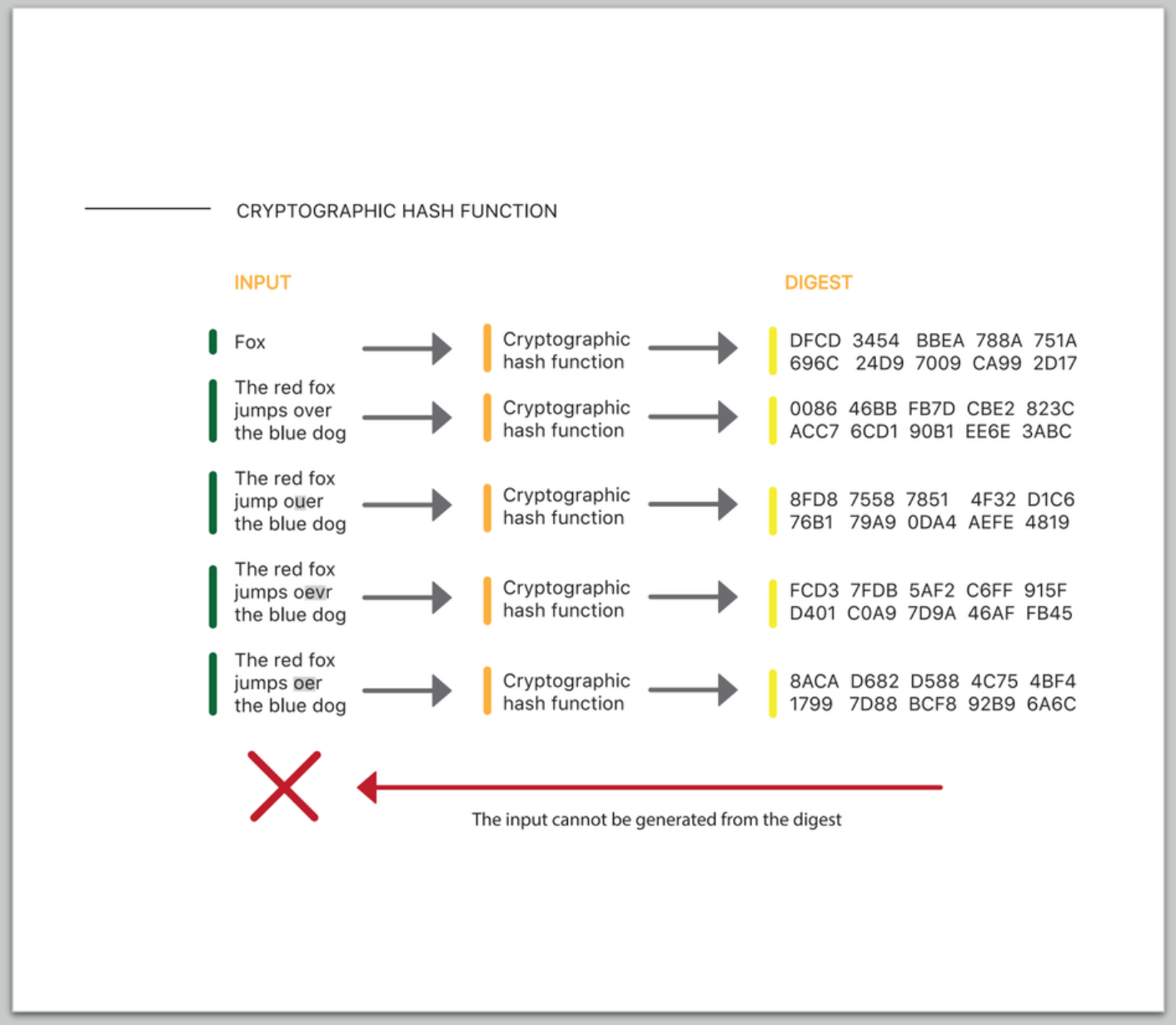


Blockchain Architecture – Cryptography

Hashing

A hash function transforms data of any size into a bit string of fixed length (32 characters for Bitcoin) called digest

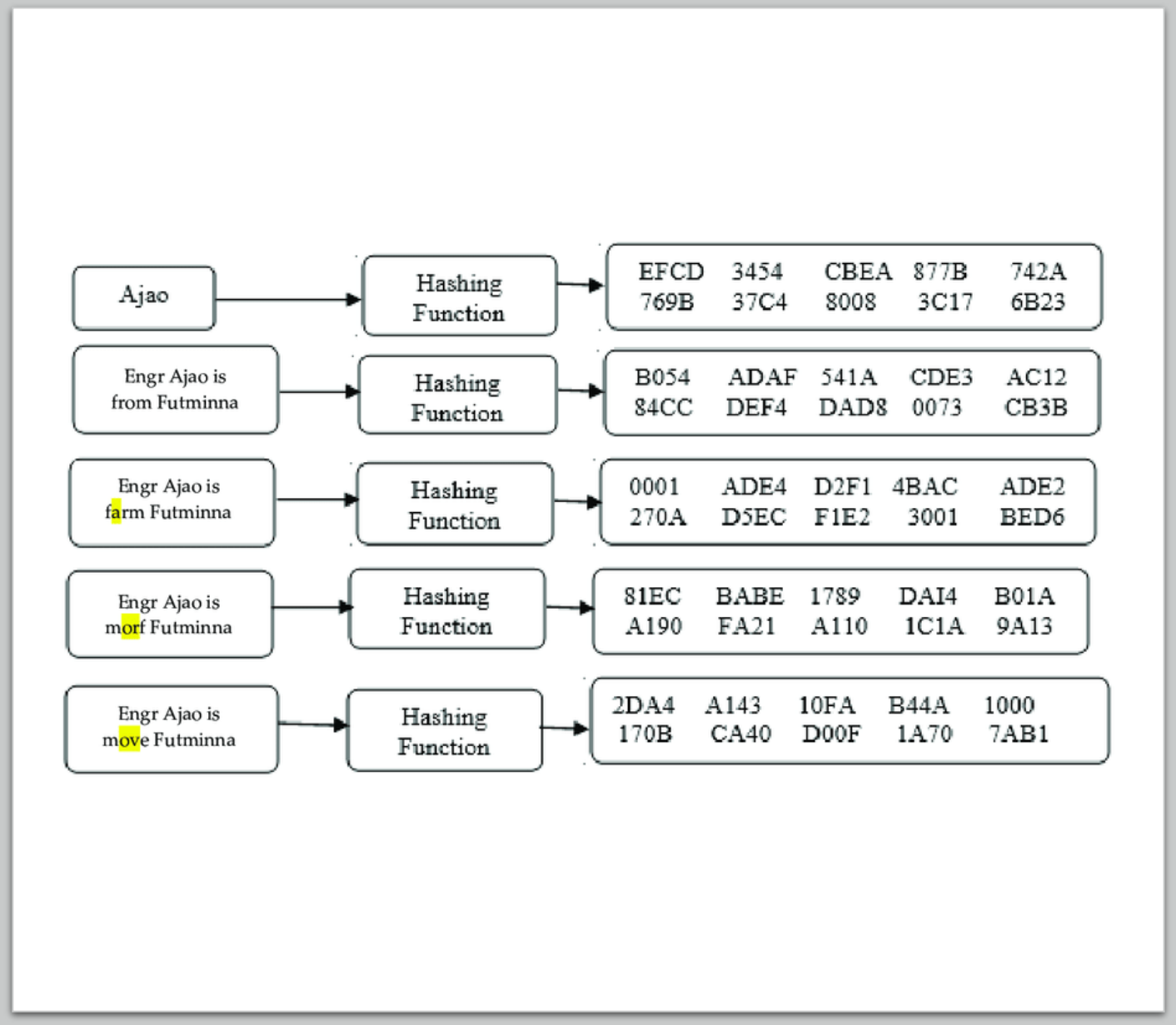
Hashing use non-decipherable one-way functions



Blockchain Architecture – Cryptography

Hashing

The power of hashing is derived from the fact that the original message differs largely from the hash. Changing even a single character in the original message, alters the results completely.



Blockchain Architecture – Cryptography

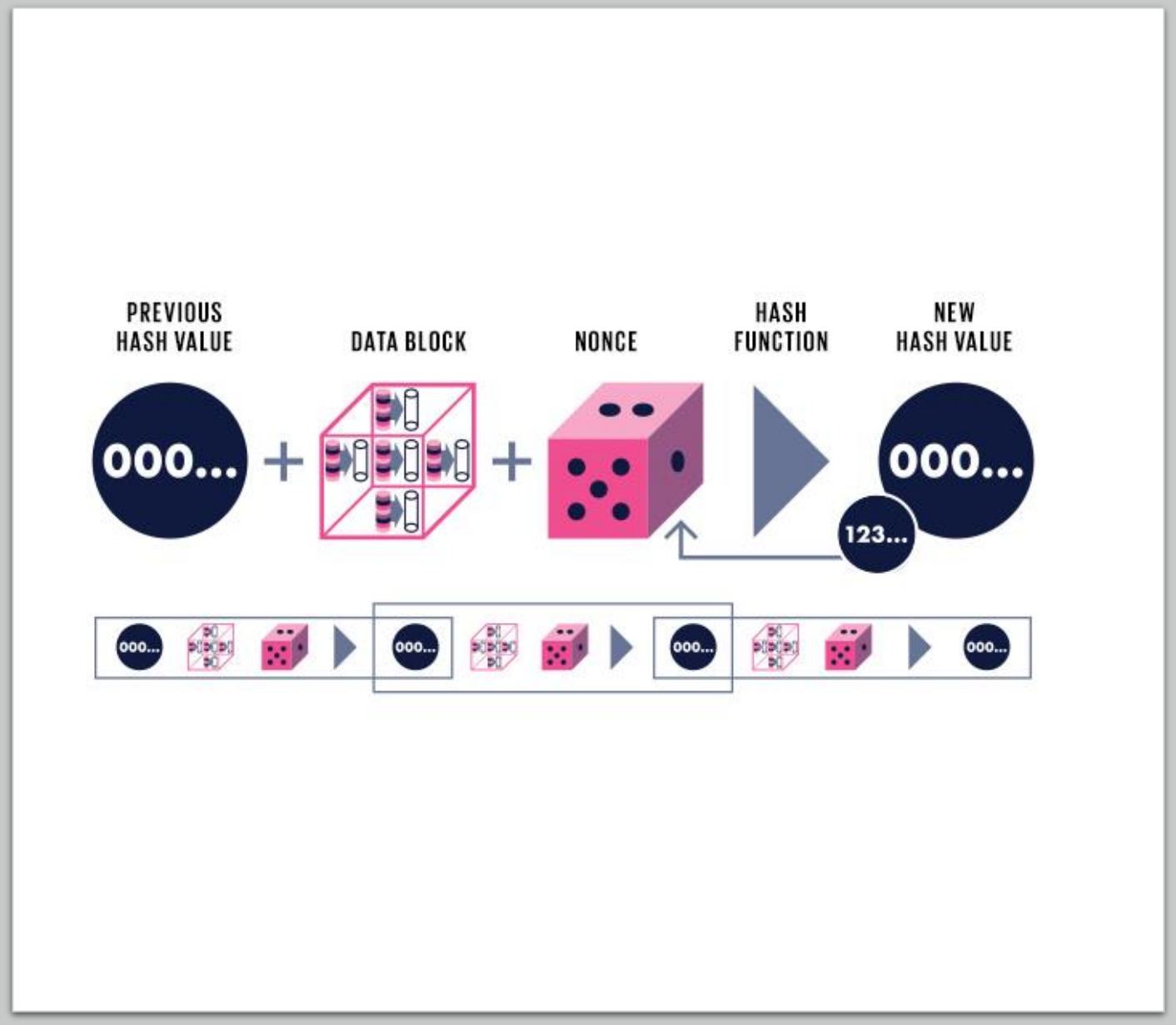
Hashing

In Blockchain, hashing is used to maintain integrity of transactions against tampering (provides ledger immutability).

When a user sends an asset to another user, the transaction is broadcasted to all the nodes in the network. Nodes assemble transactions in chronological order to form blocks.

Each block is given a unique Id which is hash of the block's data (transactions, difficulty level, timestamp, nonce, previous block hash, etc.). This hash value is also included in the next block.

Including a hash value of a block in the next block creates a chain of blocks linked together. Modifying a single transaction in one block will change its hash value and the hash of every block after it rendering the ledger invalid.



Blockchain Architecture – Cryptography

Note: Transaction messages are also encrypted using some secret key which is shared between the sender and receiver during HTTPS handshake.

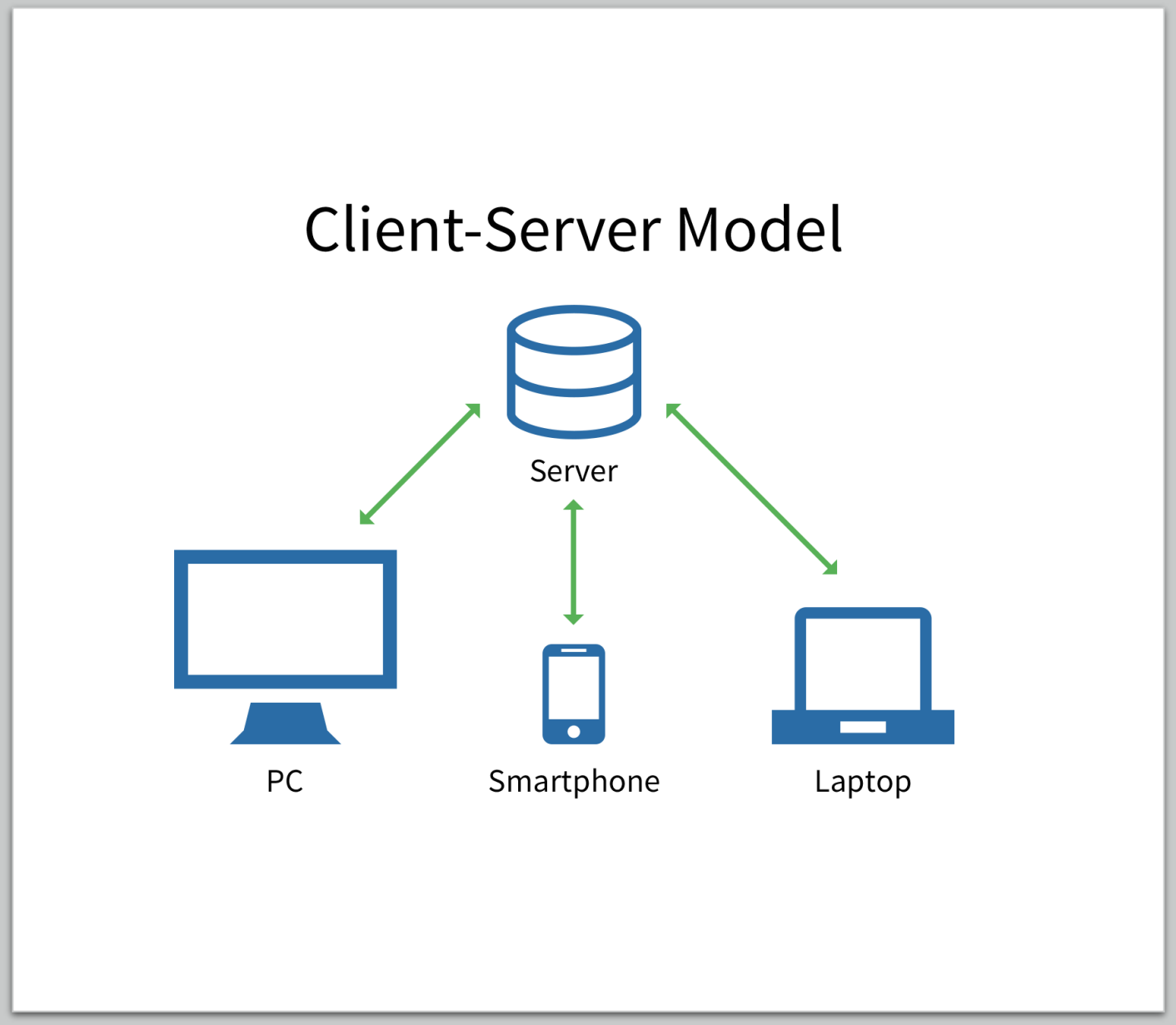
Blockchain Architecture – Consensus

Let’s try to build a system without having to depend on any organization.

The first approach would be having a public database where we save all transactions happening among us.

A digital wallet would automatically send the details of a transaction to that server.

Challenge: Who will be in charge of the db server?



Blockchain Architecture – Consensus

To remove that bit of trust we can have every participant of the network keep a copy of that database ledger on their machine.

Challenge: How can participants keep this ledger in sync? How to get everyone to agree on the same ledger?

To address this challenge, central authorities are substituted using a consensus algorithm.

There is a number of consensus algorithm out there the most common being Proof of Work (PoW) and Proof of Stake (PoS)

Blockchain Architecture – Consensus

Proof of Work (PoW) Overview

i. Each node creates a block of transactions, then they compete to generate (by guessing) a special number called an **nonce**.

ii. The **nonce** is a number which when put at the end of the transactions in the block and the block hashed, will give a 256 character output with first x (started at 30) bits equal to zero.

iii. Once a node gets this nonce it will broadcast its block to other nodes. The other nodes verify the nonce, discard the mining process and start creating a new block.

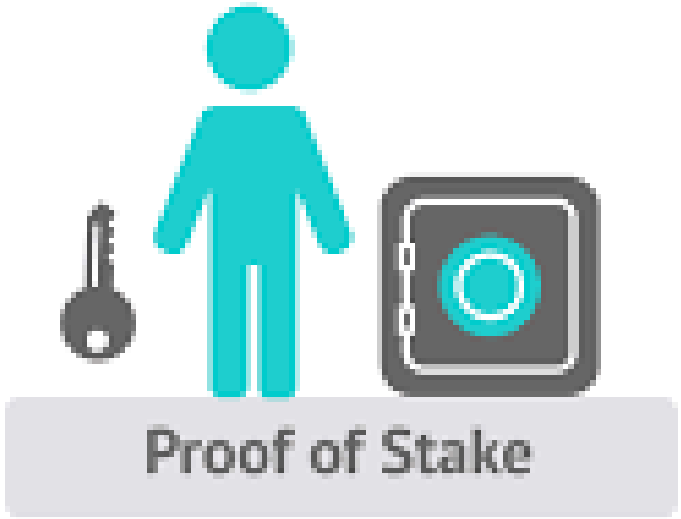
Blockchain Architecture – Consensus

Proof of Stake (PoS) Overview

Based on the idea that user with more stake (assets) in the network will less likely try to subvert it.

These blockchains uses the amount of stake a user has as a determining factor for publishing new blocks.

The choice of block publisher is weighted round robin with user owning higher stake being chosen mostly.



Miners

In PoW Blockchains, nodes designated as “miners” confirm transactions by using their computing power to solve calculations.

The mining process involves grouping transactions into blocks, validating them, and then spreading them across the network for validation by other nodes.

Miners

When other nodes confirm the validity of a block, they add its transactions to their local database, also known as a ledger.

Once more than half of the network confirms a set (block) of transactions, it becomes permanent and irreversible.

The miner who first solved the math puzzle receives a reward and applicable fees for the transactions that are included in the block.

Wallets

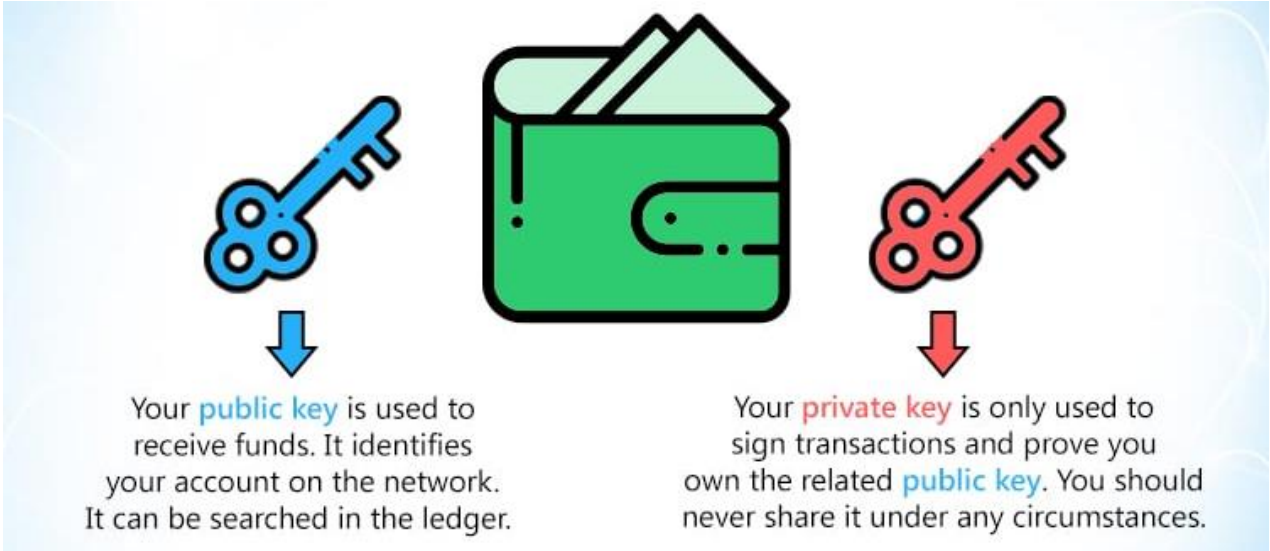
A blockchain wallet is a digital wallet that allows users to store, manage, and trade their crypto assets.

It serves as a user interface to the blockchain ledger.

It shows user's account balance and tracks incoming and outgoing transactions .

It also creates and signs transactions initiated by a user.

There are various types of wallets which varies in terms of data security, ease of use, and technical simplicity.



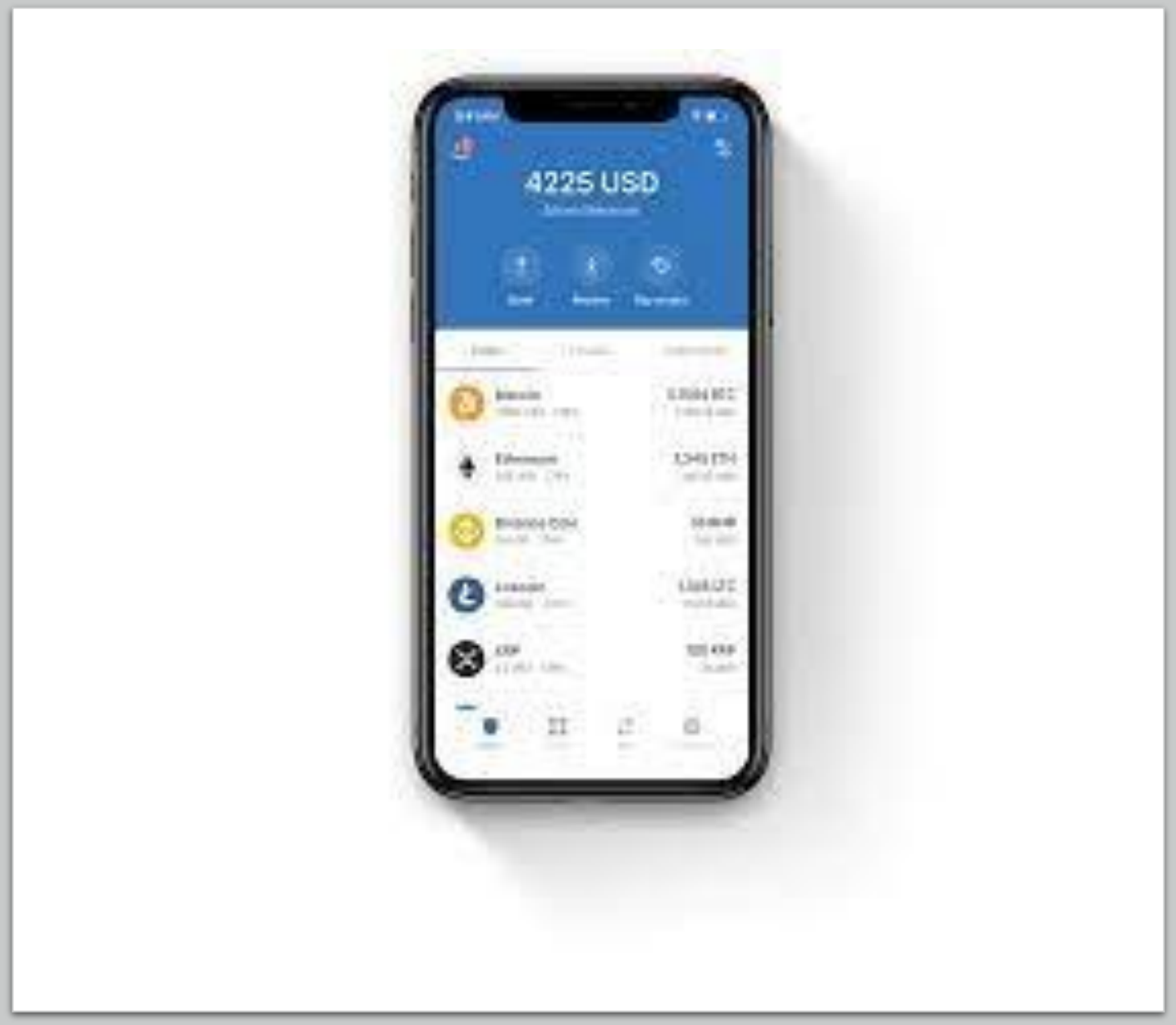
Wallets

Software/Desktop wallets

Applications that users can download and run on their workstations /mobile

Software wallets store the private keys on the user's local hard disc therefore are safer than online wallets

Examples Bitcoin core, electrum bread, geth

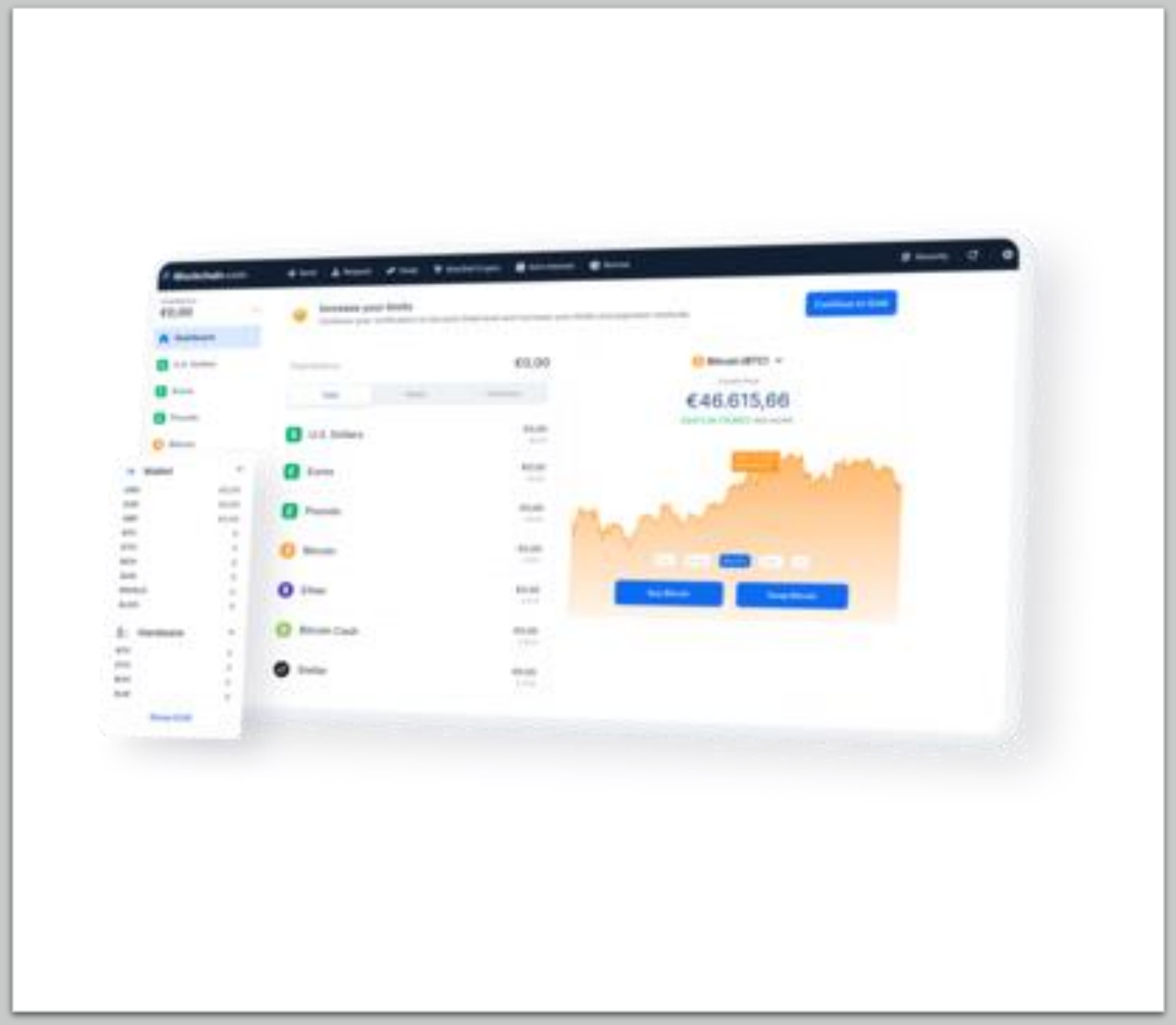


Wallets

Online wallets:

Online wallets provide access to cryptocurrencies from any device connected to the internet.

They offer convenience in that a user does not have to install software and can access the wallet via any internet browser. Online wallets store private keys on a server that is owned and operated by the companies that own the online wallet software.



Wallets

Hardware wallets:

A hardware wallet stores the private keys on secure hardware. It is the surest way to secure digital assets.

Hardware wallets uses encryption making it impossible to

read the stored keys in unencrypted form from the device. Hardware wallet devices generally use open-source software (e.g., TREZOR) for their operations, providing

additional confidence, as the public can verify the software's integrity.

Exchanges

To acquire a digital asset for the first time, one needs to buy it using traditional currency.

Exchanges provides a market place for customers to buy and sell digital assets.

Most of the exchanges are web based exchanges which can be found on the Internet. Some con

Activity 3: Wallets and Exchanges

Activity 4: Executing Transactions

Summary

- Digital Assets
- Digital Assets Ecosystem
- Distributed Ledgers
- Miners
- Wallets
- Exchanges