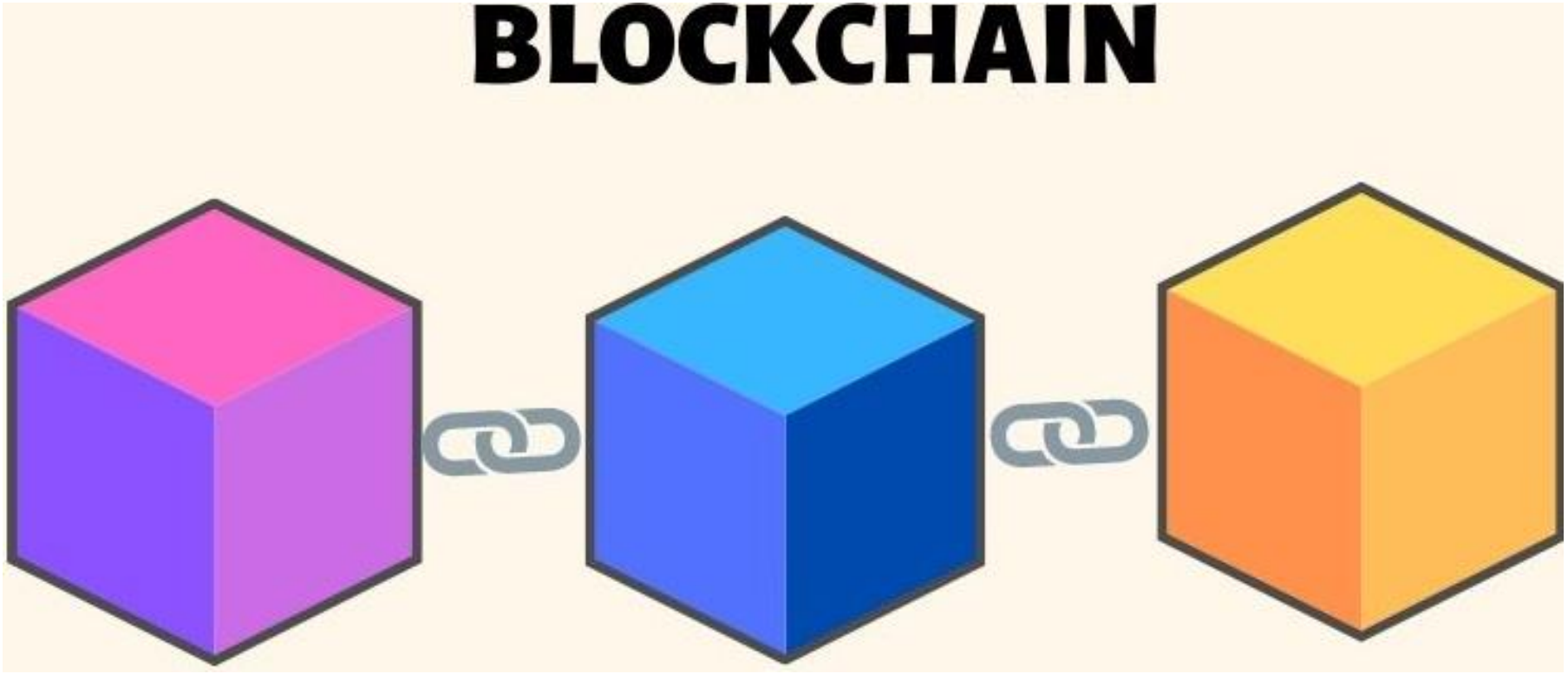
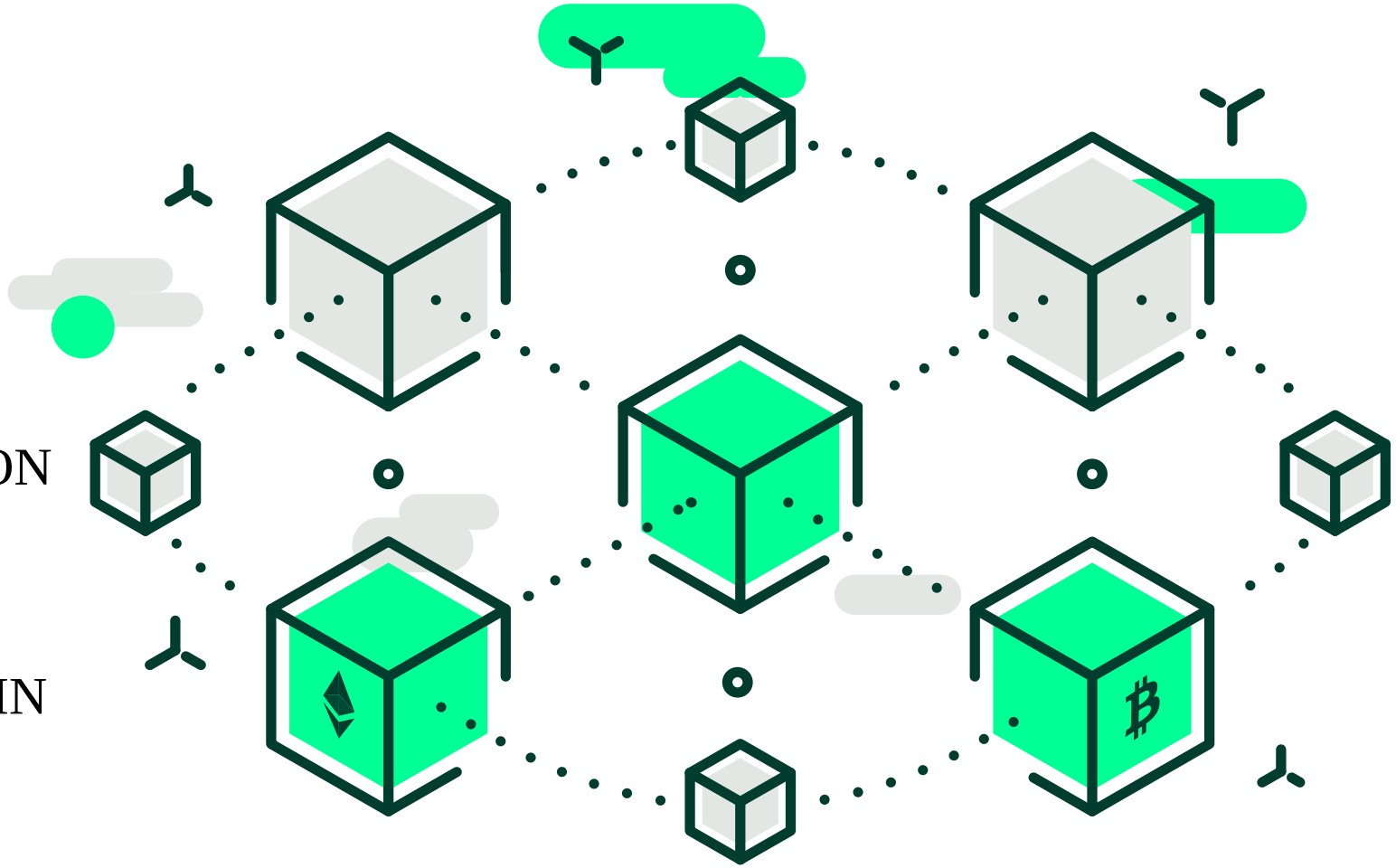


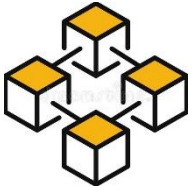
UNIT 1

GENERAL INTRODUCTION

Lecturer: Ph.D Lê Quang Huy

CONTENTS





1. INTRODUCTIONS

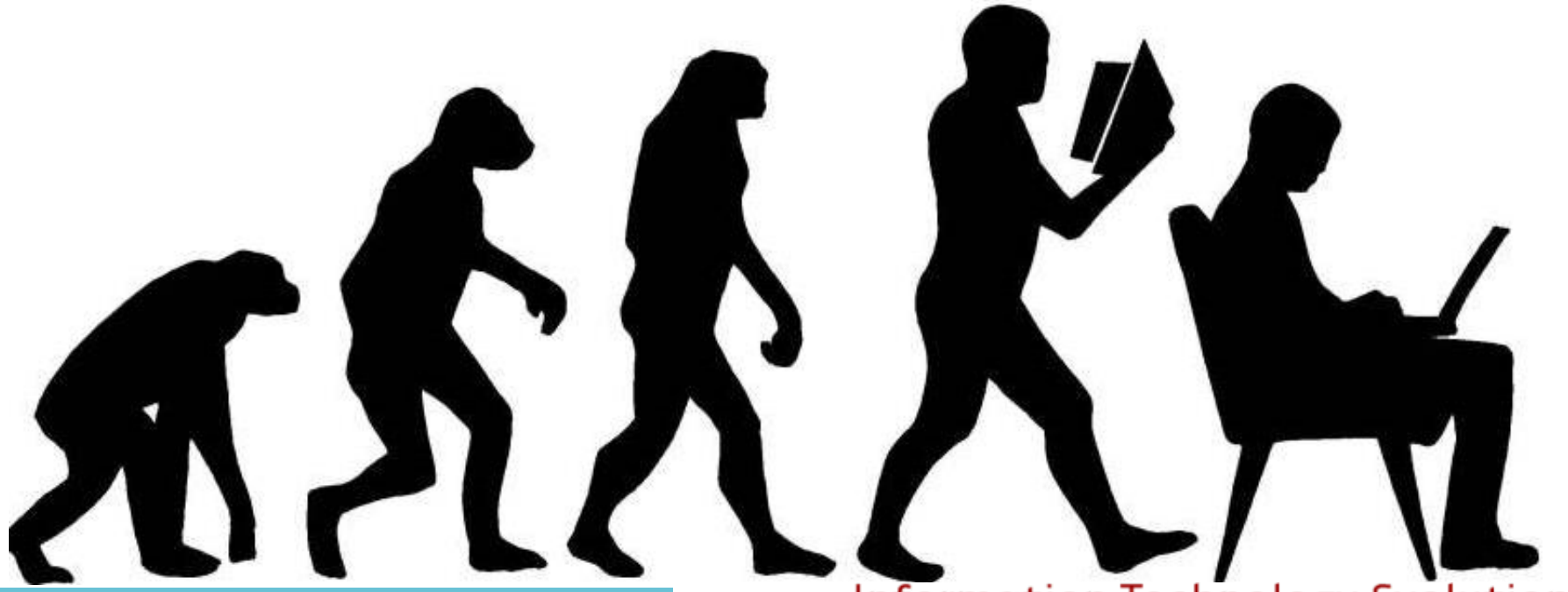
1.1. DEVELOPMENT OF INFORMATION TECHNOLOGY

1.2. SECURITY OF DATA STRUCTURES

1.3. CENTRALIZED COMPUTTING MODEL

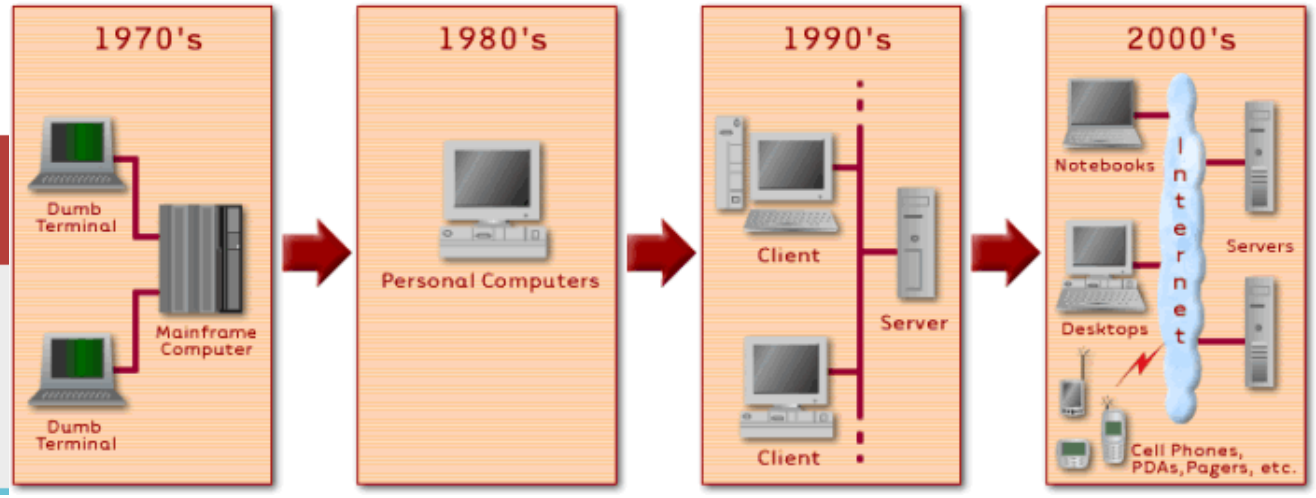
1.4. WEB APPLICATIONS

1.1. DEVELOPMENT OF INFORMATION TECHNOLOGY



Information Technology Evolution

The 1st Industrial Revolution 18th Century	The 2nd Industrial Revolution Early 19-20th Century	The 3rd Industrial Revolution Latter Half of the 20th Century	The 4th Industrial Revolution Early 21st Century -
Steam engine based mechanization revolution	Electricity based mass production revolution	Computer/Internet based knowledge and information	Big Data/AI/IoT based hyperconnectivity revolution



1.2. SECURITY OF DATA STRUCTURES

Data structure: describe objects in computer.

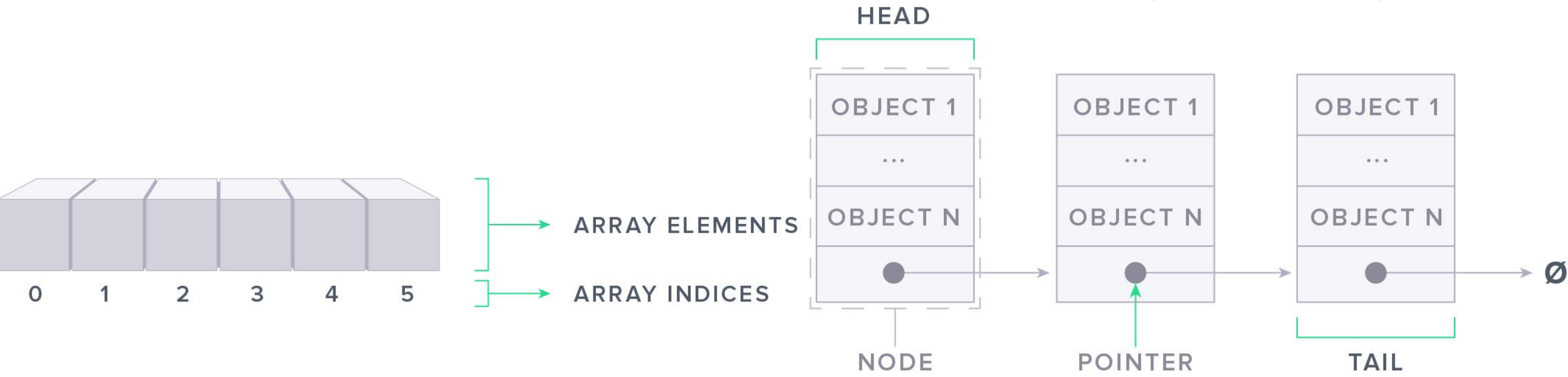
Purpose of data structure:

- Store data.
- Data manipulation: create, update, delete, save, search… eassily.

LIST TABLE

- Bread
- Milk
- Butter
- Cheese

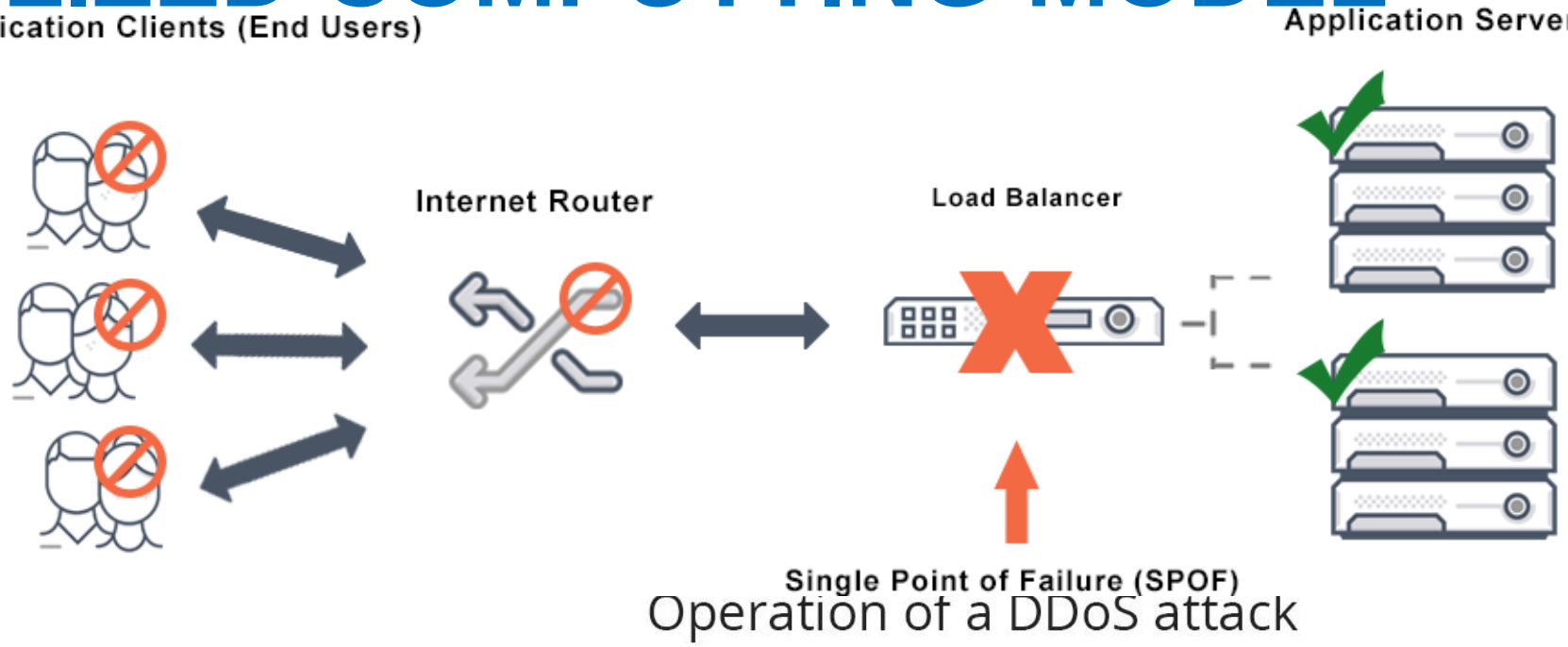
Car	Owner	Color
Ford	John	Black
Tesla	Alice	White
BMW	Bob	Red



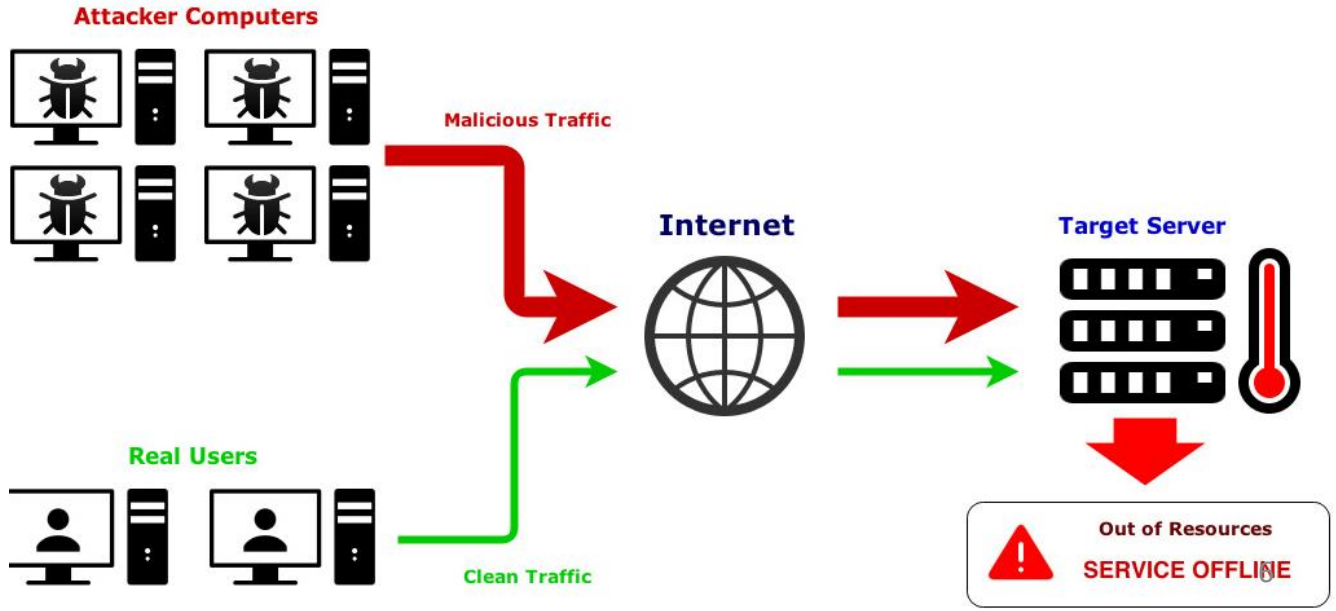
1.3. CENTRALIZED COMPUTTING MODEL

Client-Server model

- Traffic Congestion.
- Single-point of failure
- High cost of maitainance.

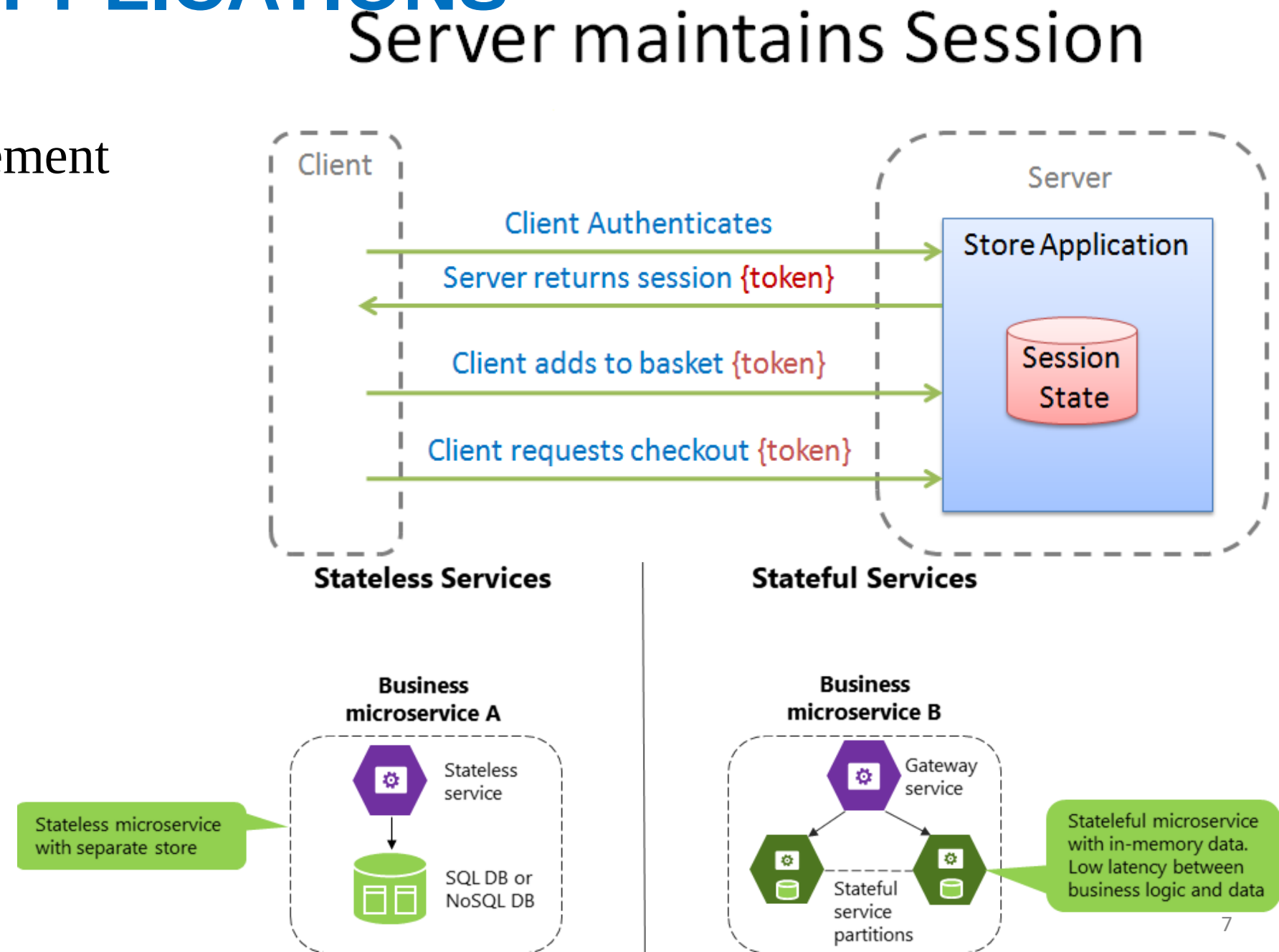


Operation of a DDoS attack

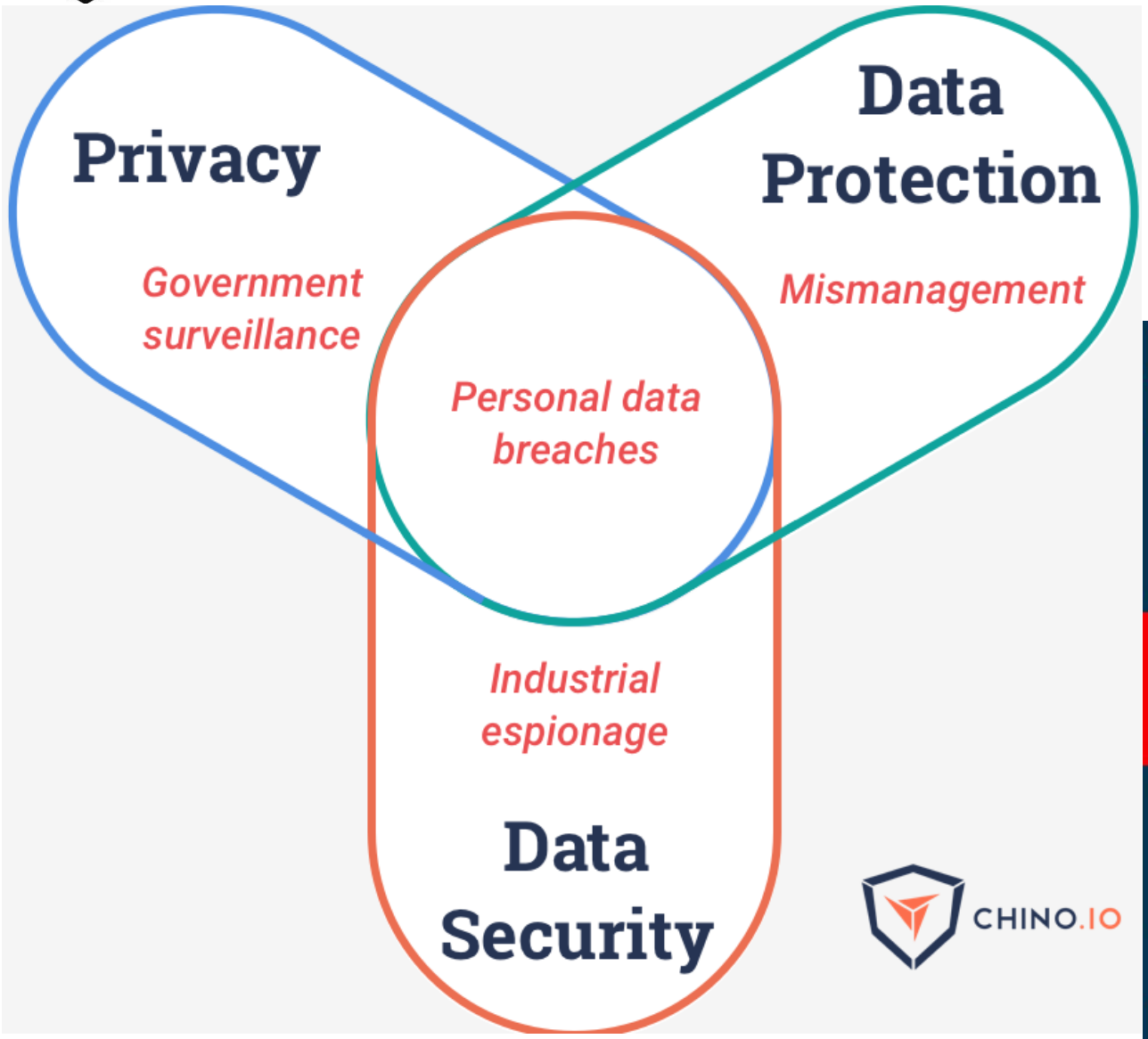


1.4. WEB APPLICATIONS

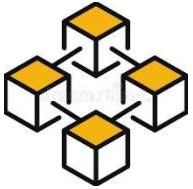
- Session state management



1.4. WEB APPLICATIONS



- Data privacy.
- Digital right.



2. BLOCKCHAIN OVERVIEW

2.1. WHAT IS BLOCKCHAIN

2.2. BLOCKCHAIN HISTORY

2.3. TECHNOLOGY COMBINATIONS

2.4. SYSTEM ARCHITECTURE

2.5. MAJOR CHARACTERISITICS

2.6. TAXONOMY

2.7. APPLICATIONS

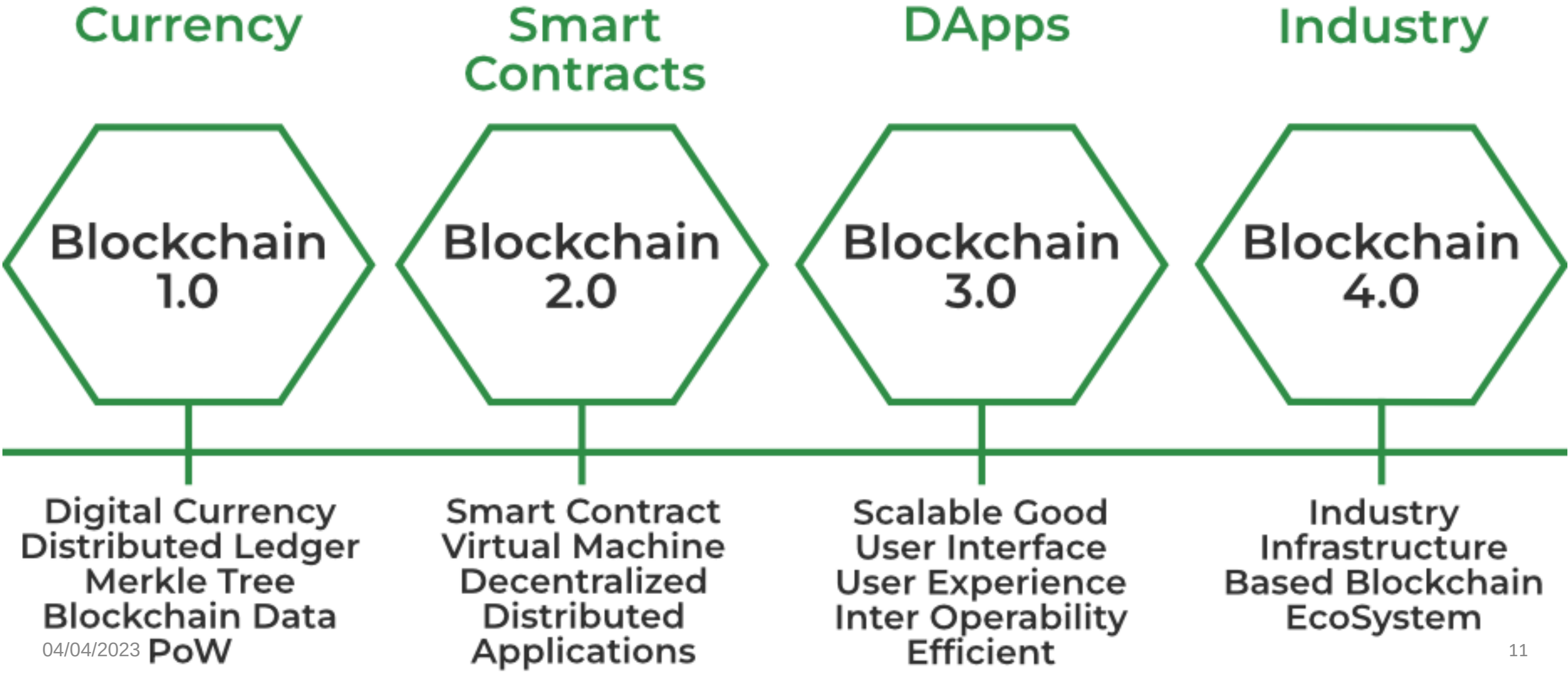
2.1. WHAT IS BLOCKCHAIN

Blockchain is:

- a type of distributed database or ledger
- record transactions in a business network

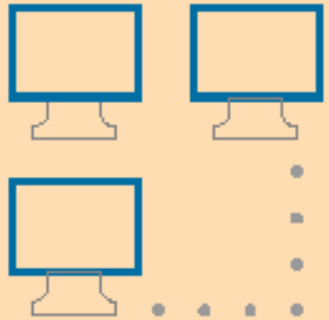
- method of managing data.
- impossible to alter, hack, defraud the system.

2.2. BLOCKCHAIN HISTORY



2.3. TECHNOLOGY COMBINATIONS

Blockchain is a combination of three concepts/technologies



Peer-to-Peer Networks

Every network paritcipant acts as both client and server

Cryptography

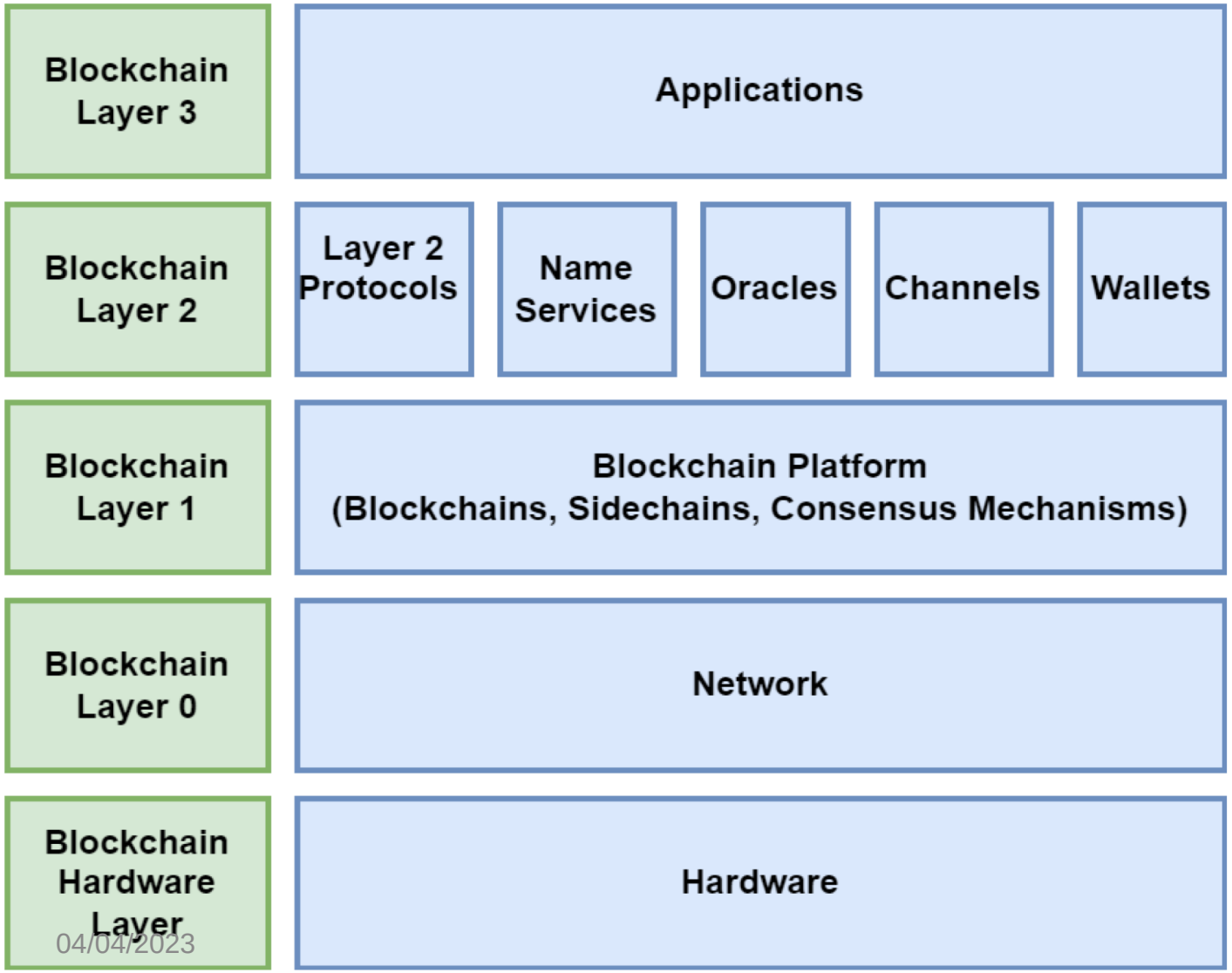
Ensures security, transparency, and privacy

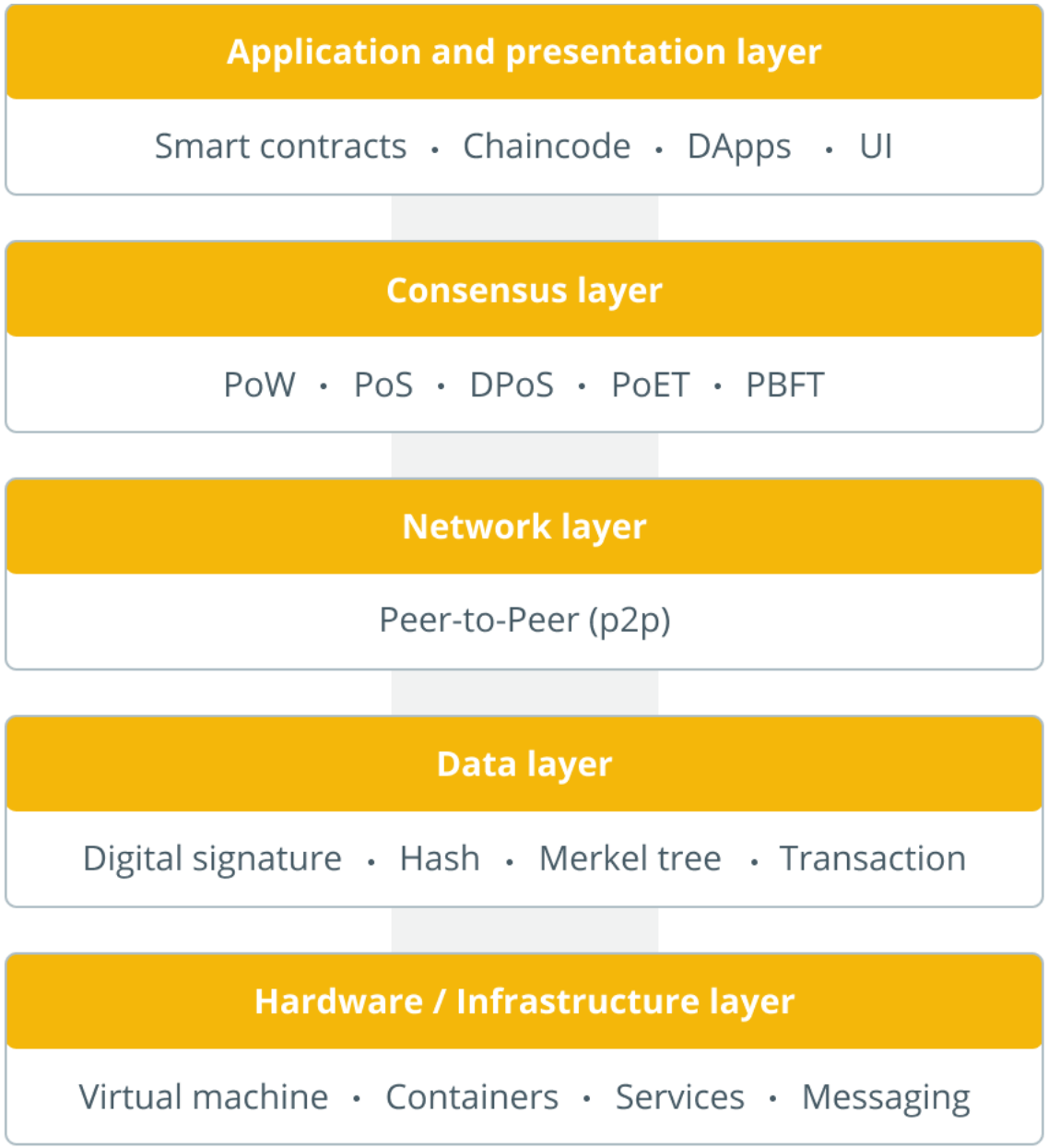
Game Theory

Creates economic incentives through reward systems

2.4. SYSTEM ARCHITECTURE

- Layer architecture





2.5. MAJOR CHARACTERISITICS

DECENTRALIZATION

TRANSPARENCY

IMMUTABILITY

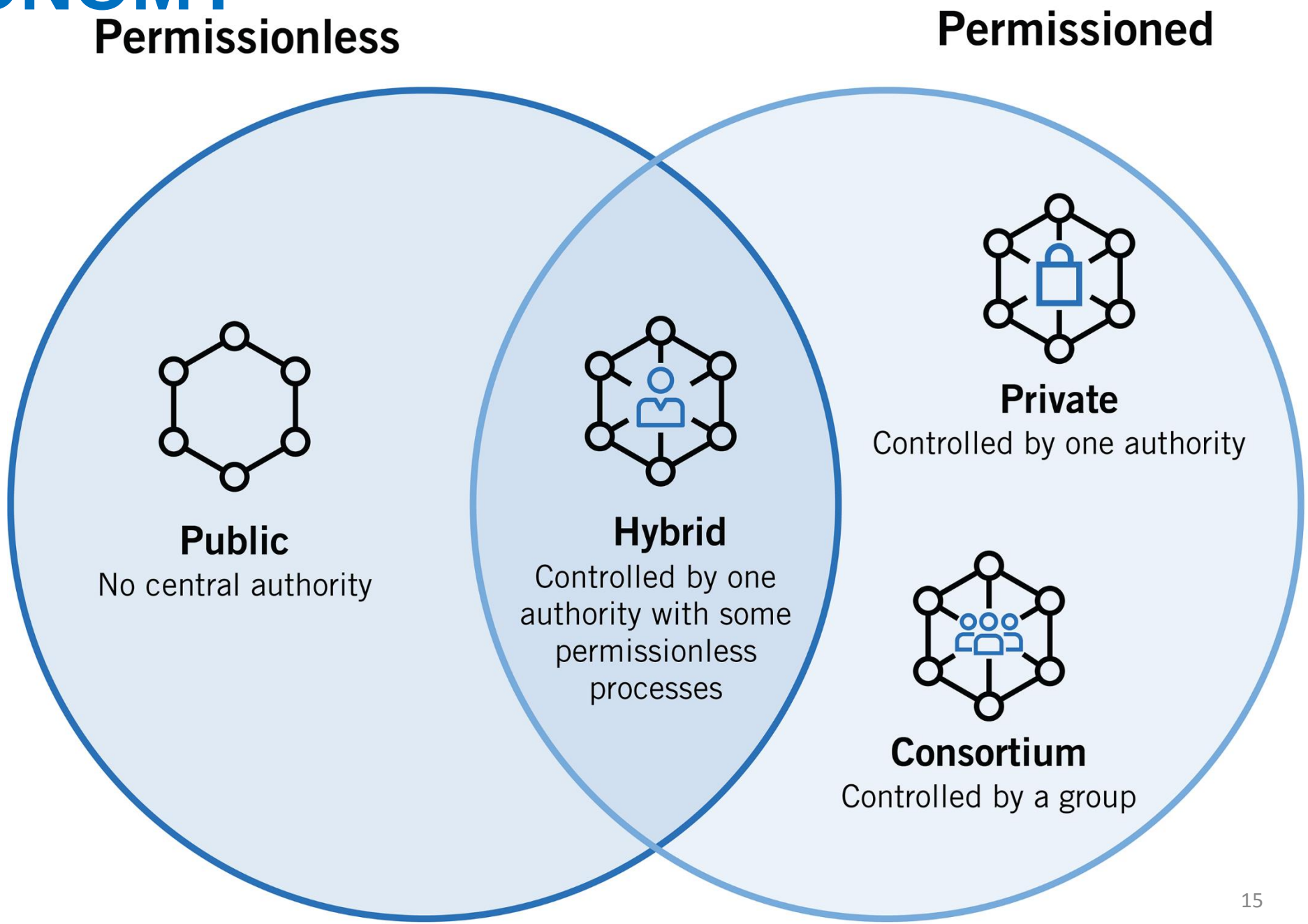
NEUTRALITY

OPEN-ACCESS

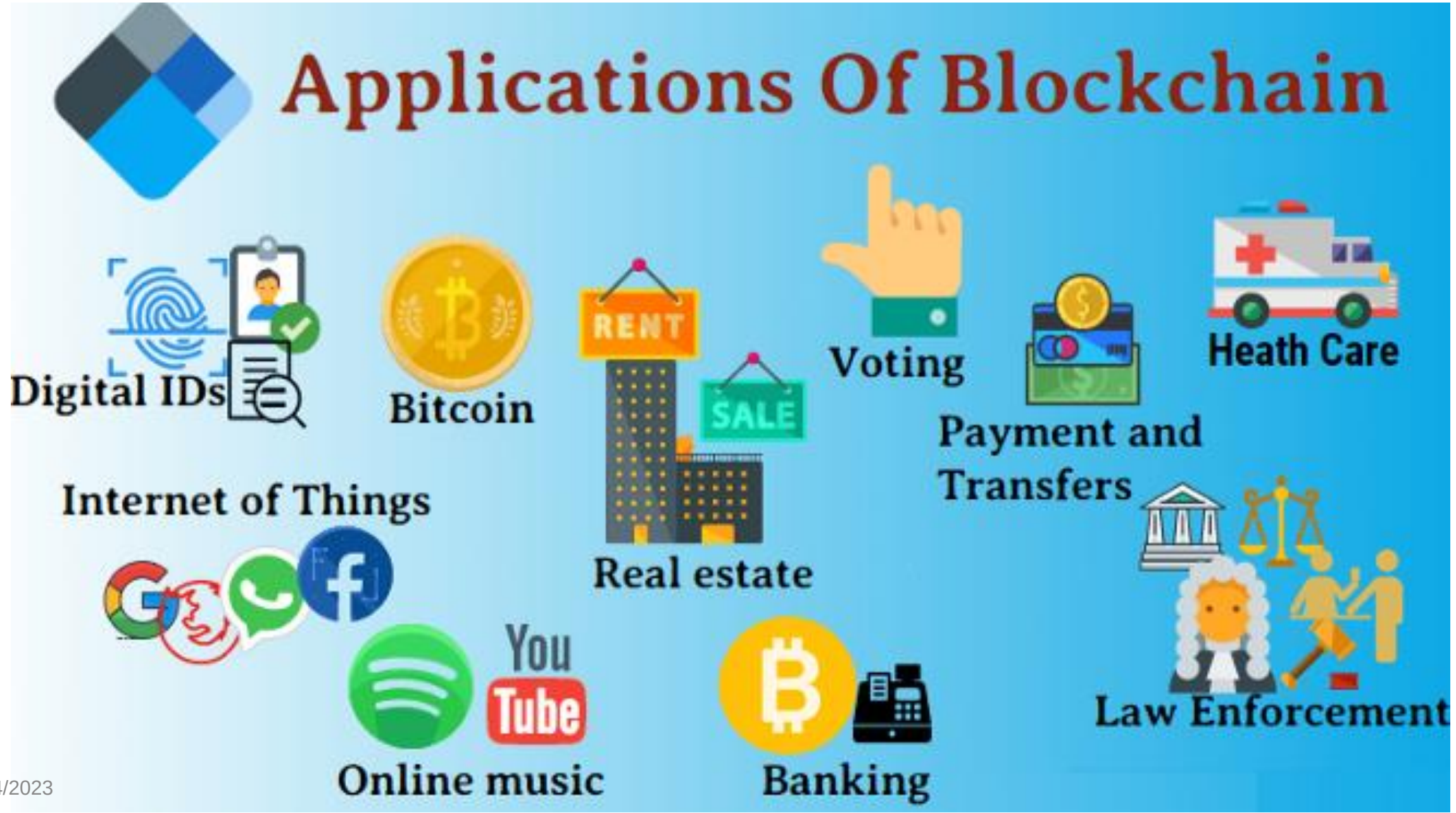
2.6. TAXONOMY

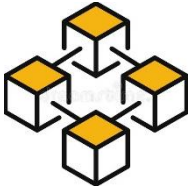
User rights:

- Read
- Write
- Vote
- ..



2.7. APPLICATIONS





3. BLOCKCHAIN DATA

3.1. IDENTITY, ADDRESS, ACCOUNT

3.2. TRANSACTIONS

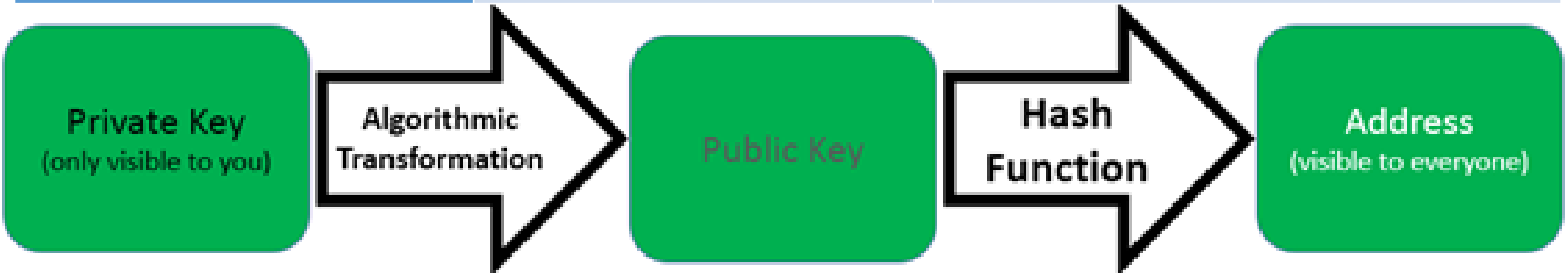
3.3. BLOCKS

3.4. BLOCKCHAIN

3.5. TRANSACTIONS ACCOUNTING MODEL

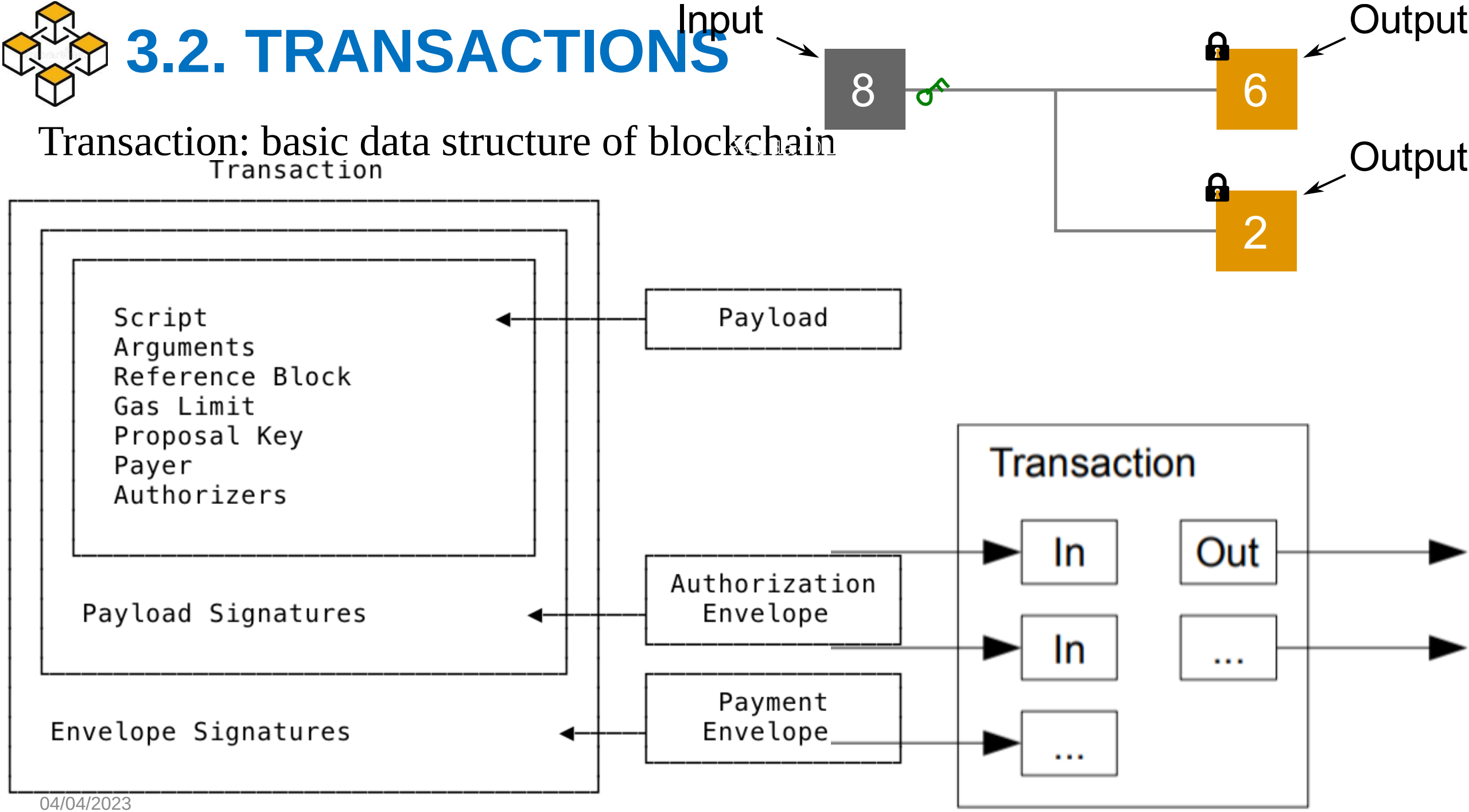
3.1. IDENTITY, ADDRESS, ACCOUNT

Identity:	Address:	Keypairs:
Information describe/identify entity	Place/site where thing is sent to/received from	Sign transactions Owner aggree to do transactions



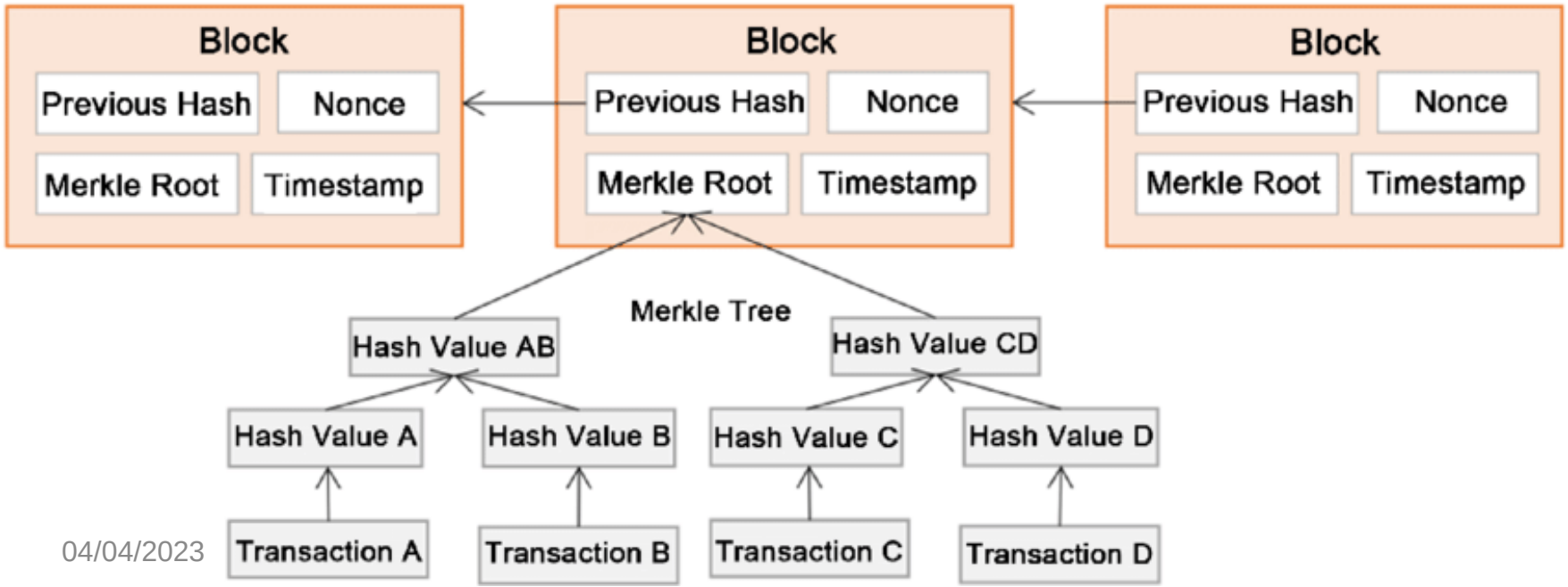
3.2. TRANSACTIONS

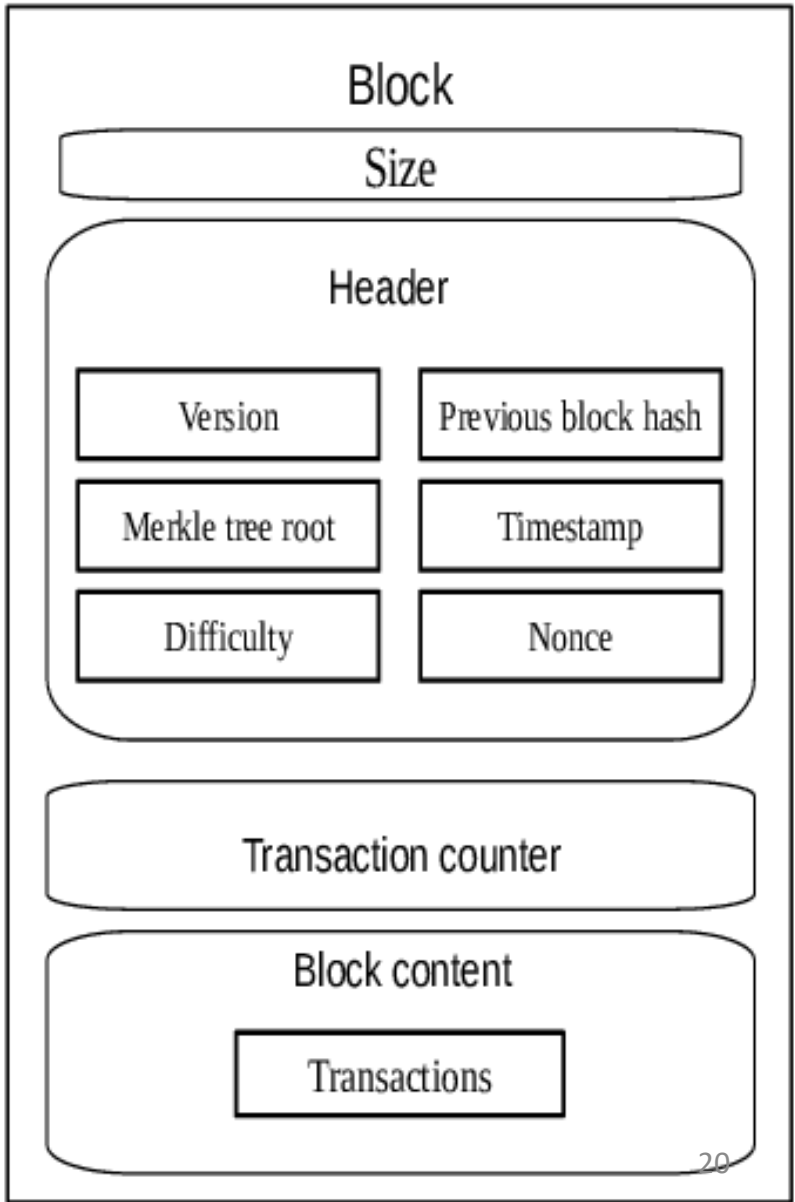
Transaction: basic data structure of blockchain



3.3. BLOCKS

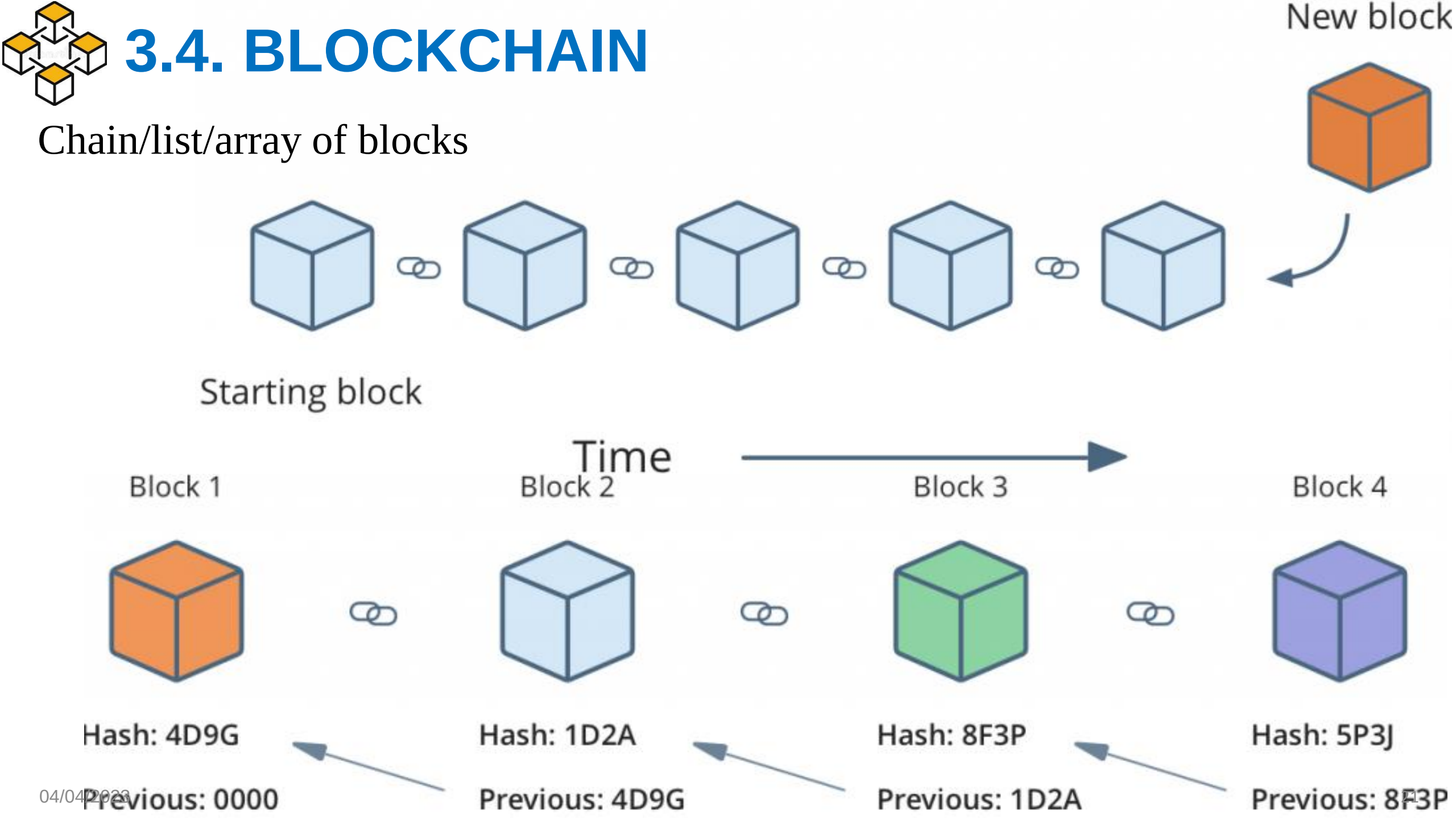
Block: group/bundle of transactions





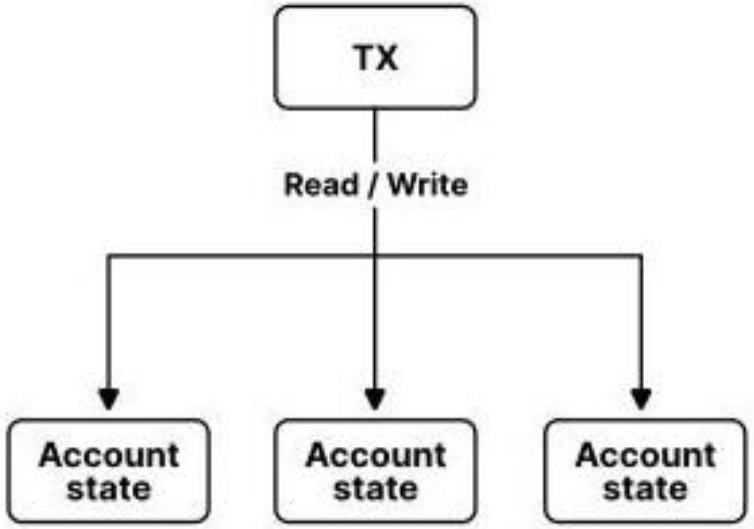
3.4. BLOCKCHAIN

Chain/list/array of blocks

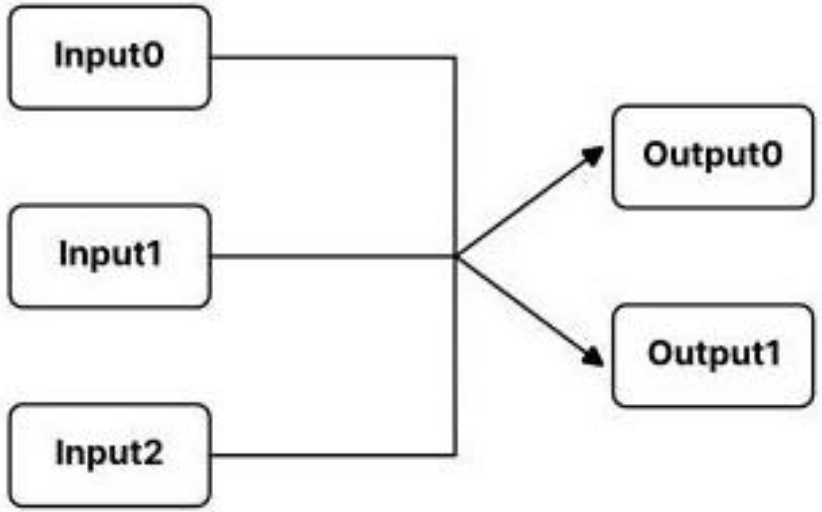


3.5. TRANSACTIONS ACCOUNTING MODEL

Account Model



UTXO Model



Pros

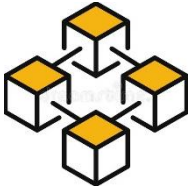
- The programming model is dev friendly
- Expressive and flexible with direct state access
- Smaller TX size

- UTXO directly owned by users
- Explicit inputs & outputs, good for verification
- Better parallelism, scalability

Cons

- Mutable state creates more room for bugs
- Harder to execute in parallel

- Concurrency issue if two TXs consume the same UTXO
- Learn a new programming model



4. BLOCKCHAIN NETWORK

4.1. NETWORK ARCHITECTURE

4.2. BLOCKCHAIN NODES

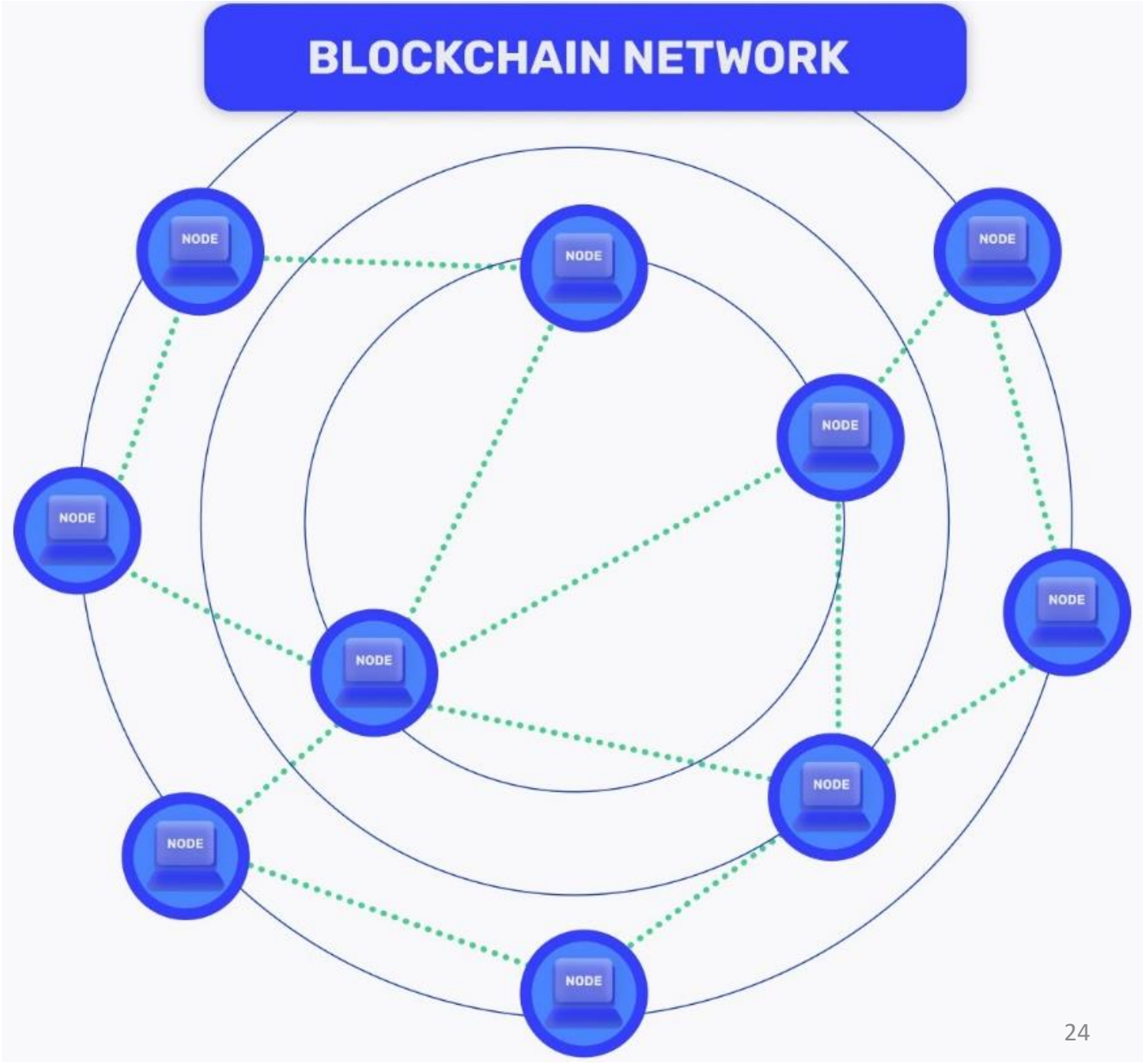
4.3. BLOCKCHAIN PROTOCOLS

4.4. BLOCKCHAIN WORKING PRINCIPLES

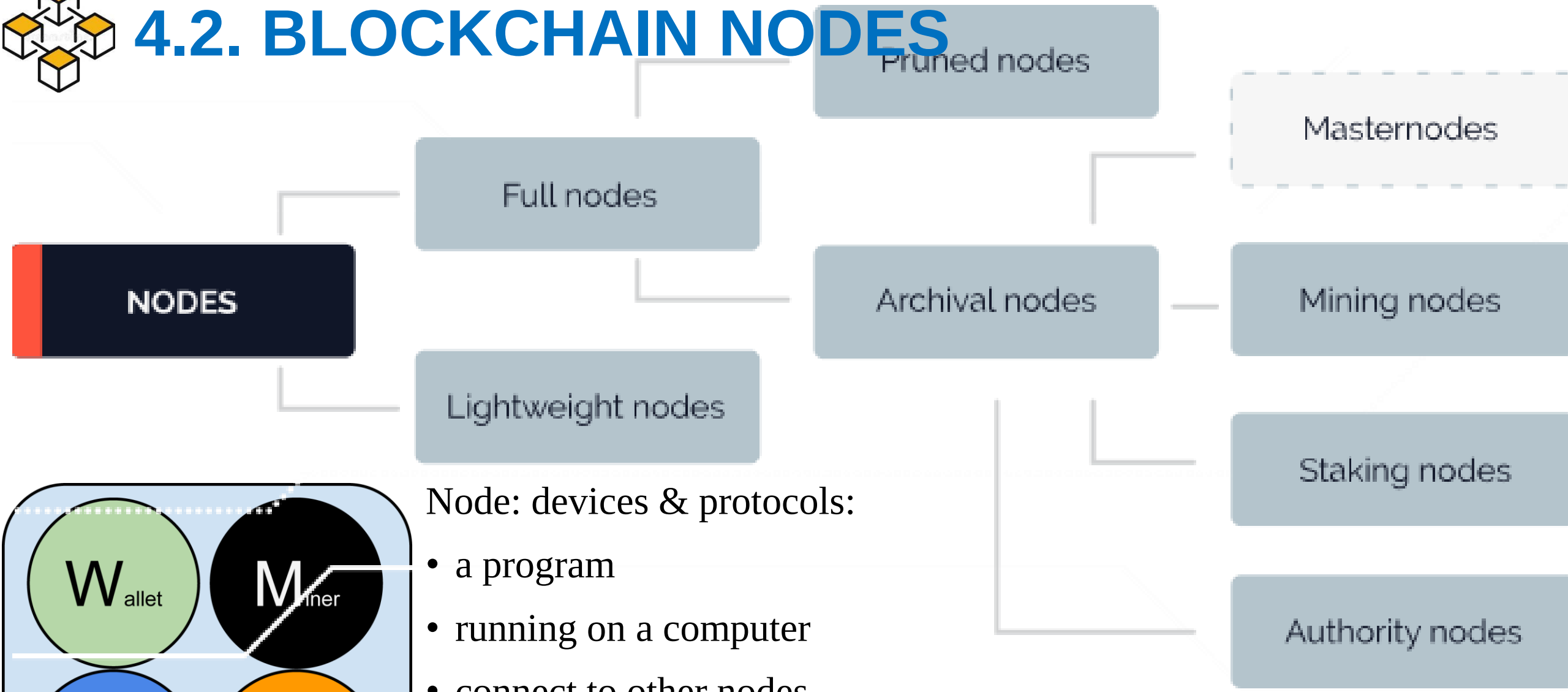
4.1. NETWORK ARCHITECTURE

Blockchain network:

- Nodes: devices
- Architecture: P2P network
- Protocol: procedures, peers reach agreement about present state of data in network



4.2. BLOCKCHAIN NODES



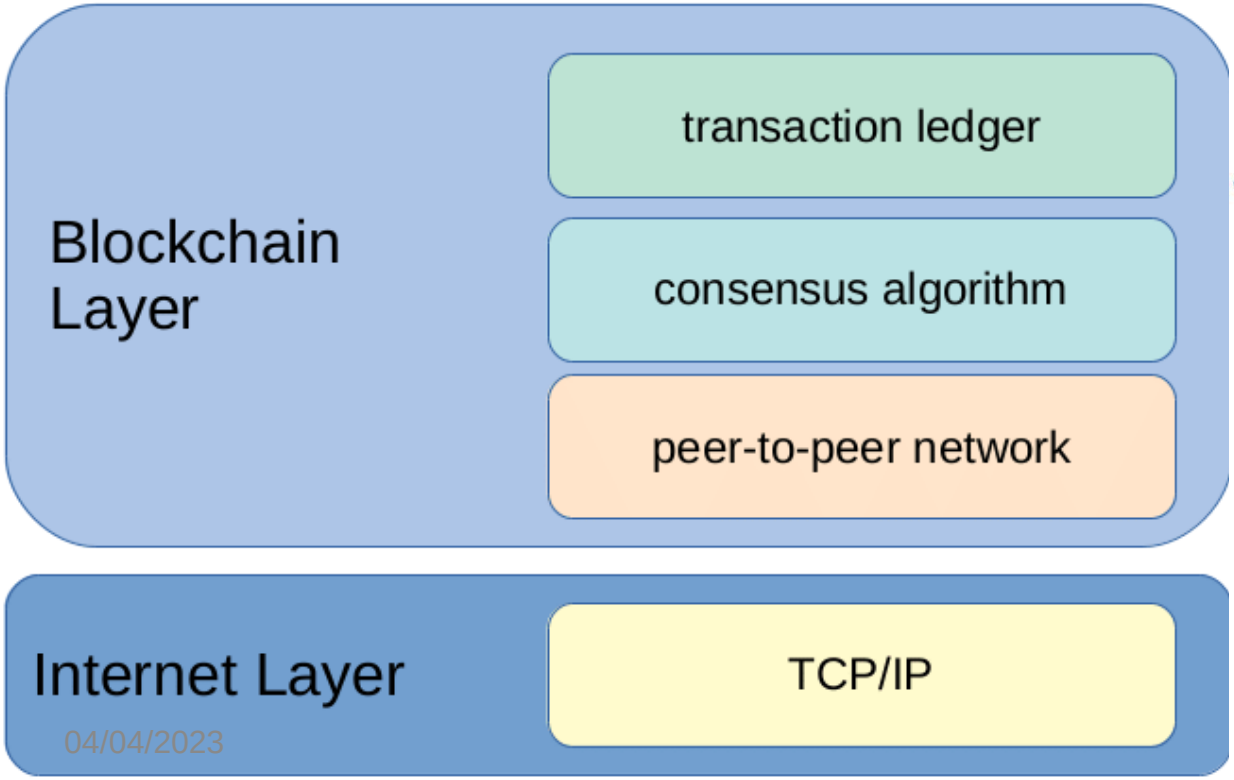
Node: devices & protocols:

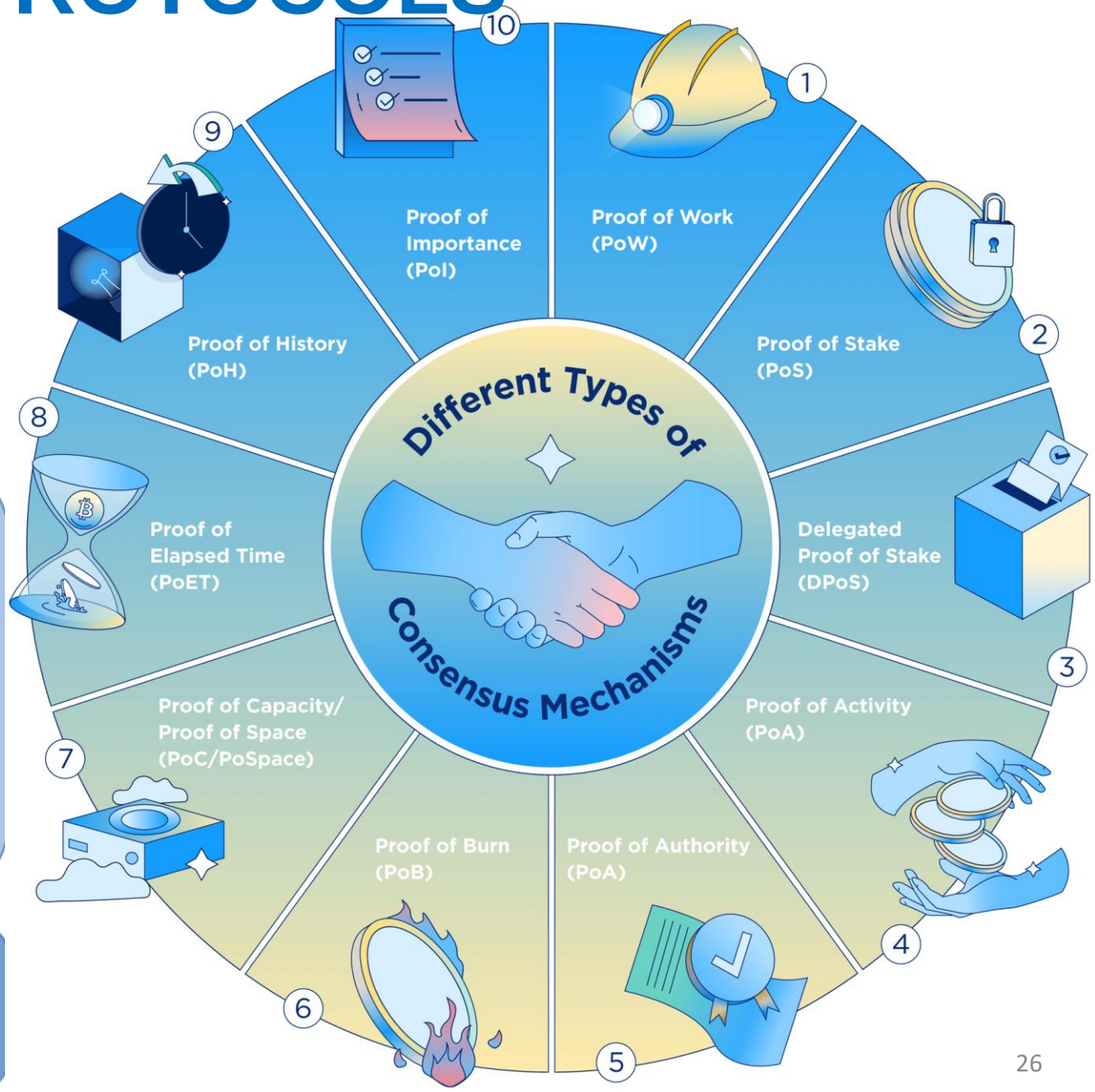
- a program
- running on a computer
- connect to other nodes

Node functions: maintain consensus of ledger

4.3. BLOCKCHAIN PROTOCOLS

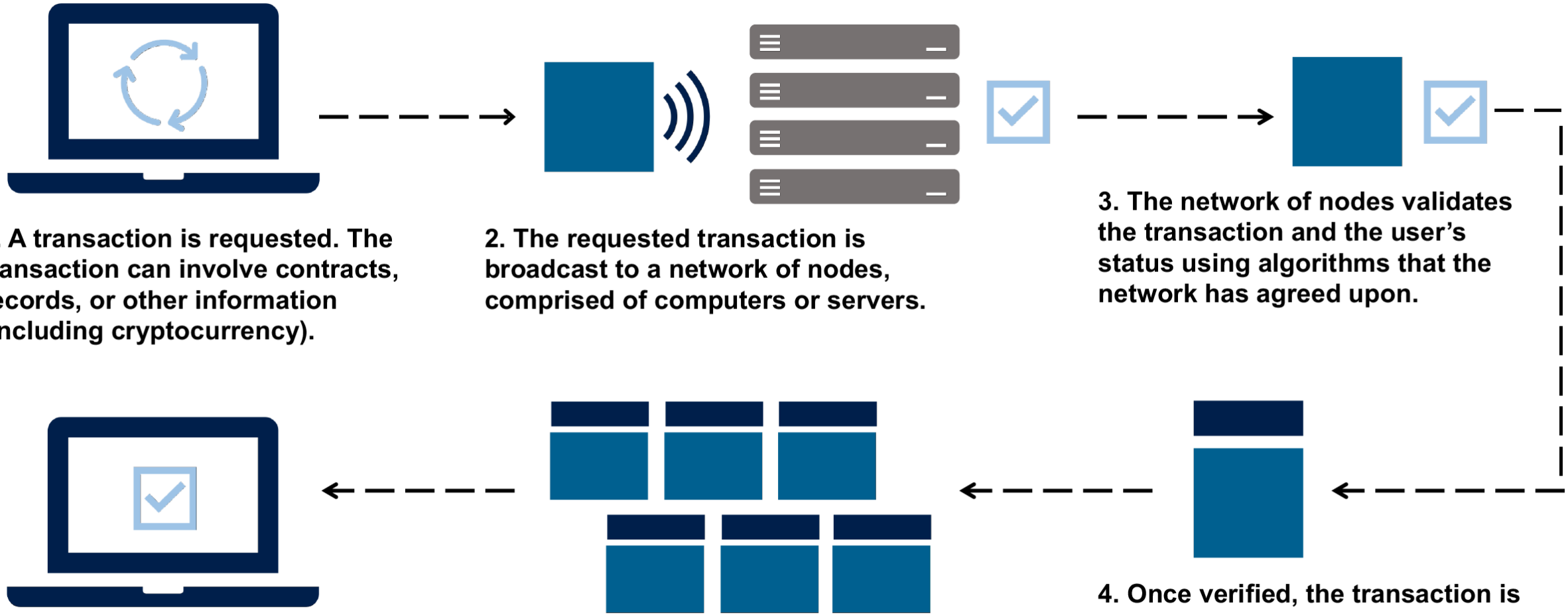
Concensus mechanism:





4.4. BLOCKCHAIN WORKING PRINCIPLES

How Blockchain Works



1. A transaction is requested. The transaction can involve contracts, records, or other information (including cryptocurrency).

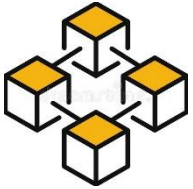
2. The requested transaction is broadcast to a network of nodes, comprised of computers or servers.

3. The network of nodes validates the transaction and the user's status using algorithms that the network has agreed upon.

4. Once verified, the transaction is combined with other transactions to create a new block of data for the ledger.

5. The new block is added to the existing blockchain. It is distributed through the network, with the other blocks ensuring that the information is not altered.

6. The transaction is completed.



5. DECENTRALIZED APPICATIONS

5.1. DECENTRALIZED APPICATIONS

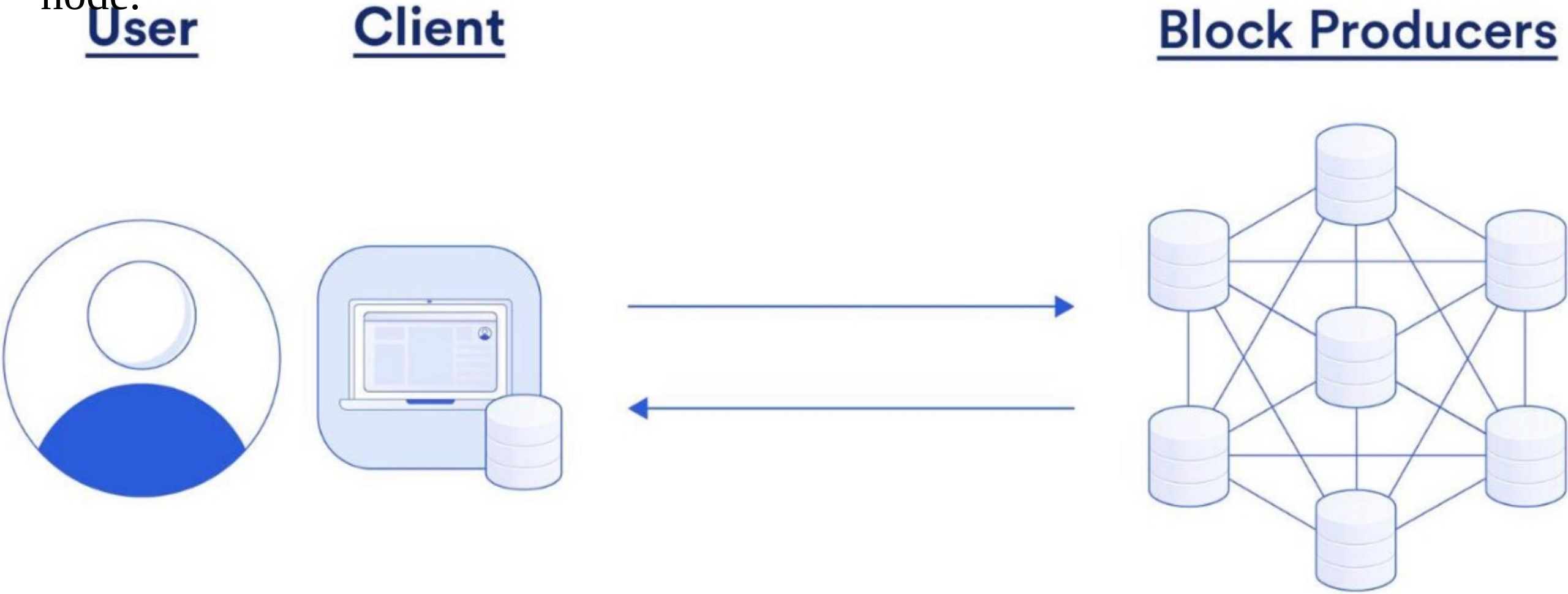
5.2. SMART CONTRACTS

5.3. CRYPTO WALLET

5.4. DECENTRALIZED AUTONOMOUS ORGANIZATION

5.1. DECENTRALIZE APPICATIONS

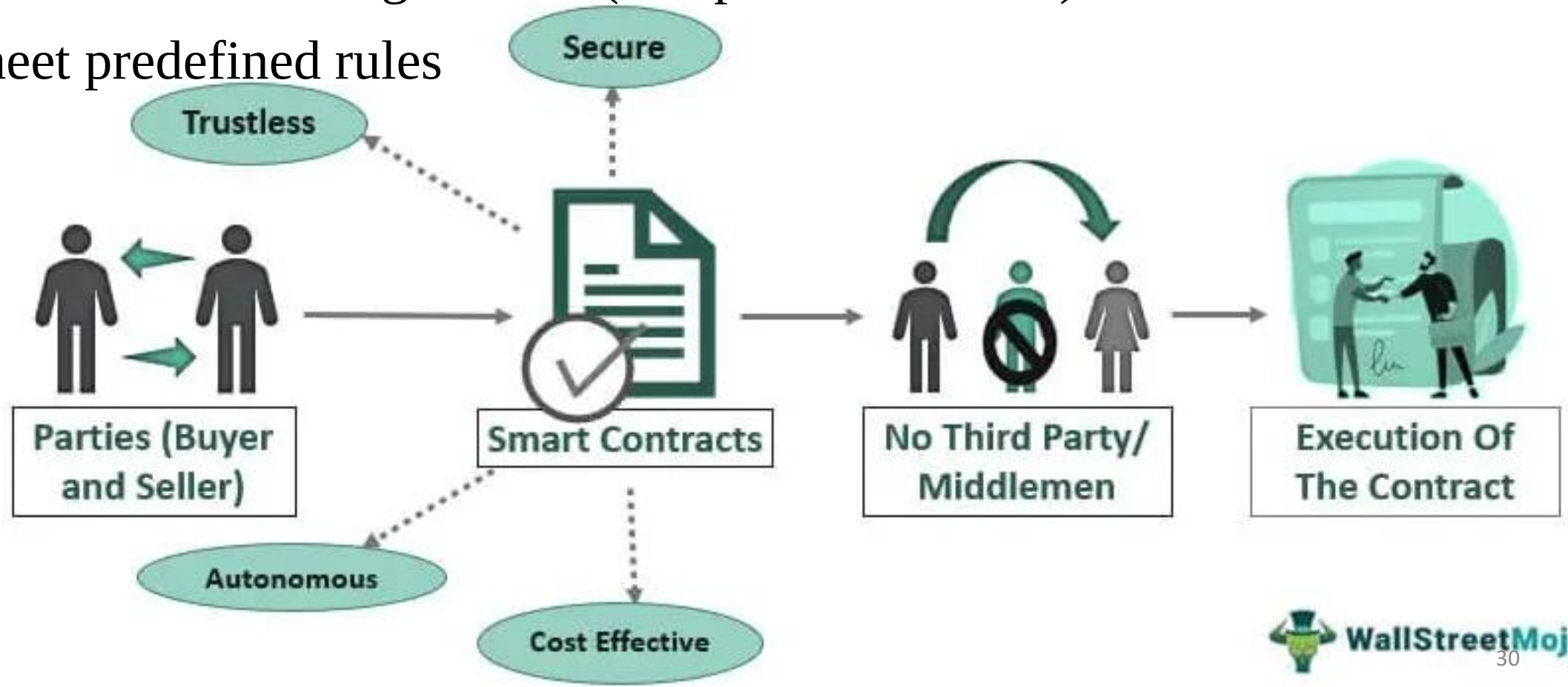
Decentralized Applications (DApp): digital application interact with blockchain node.



5.2. SMART CONTRACTS

Smart contracts:

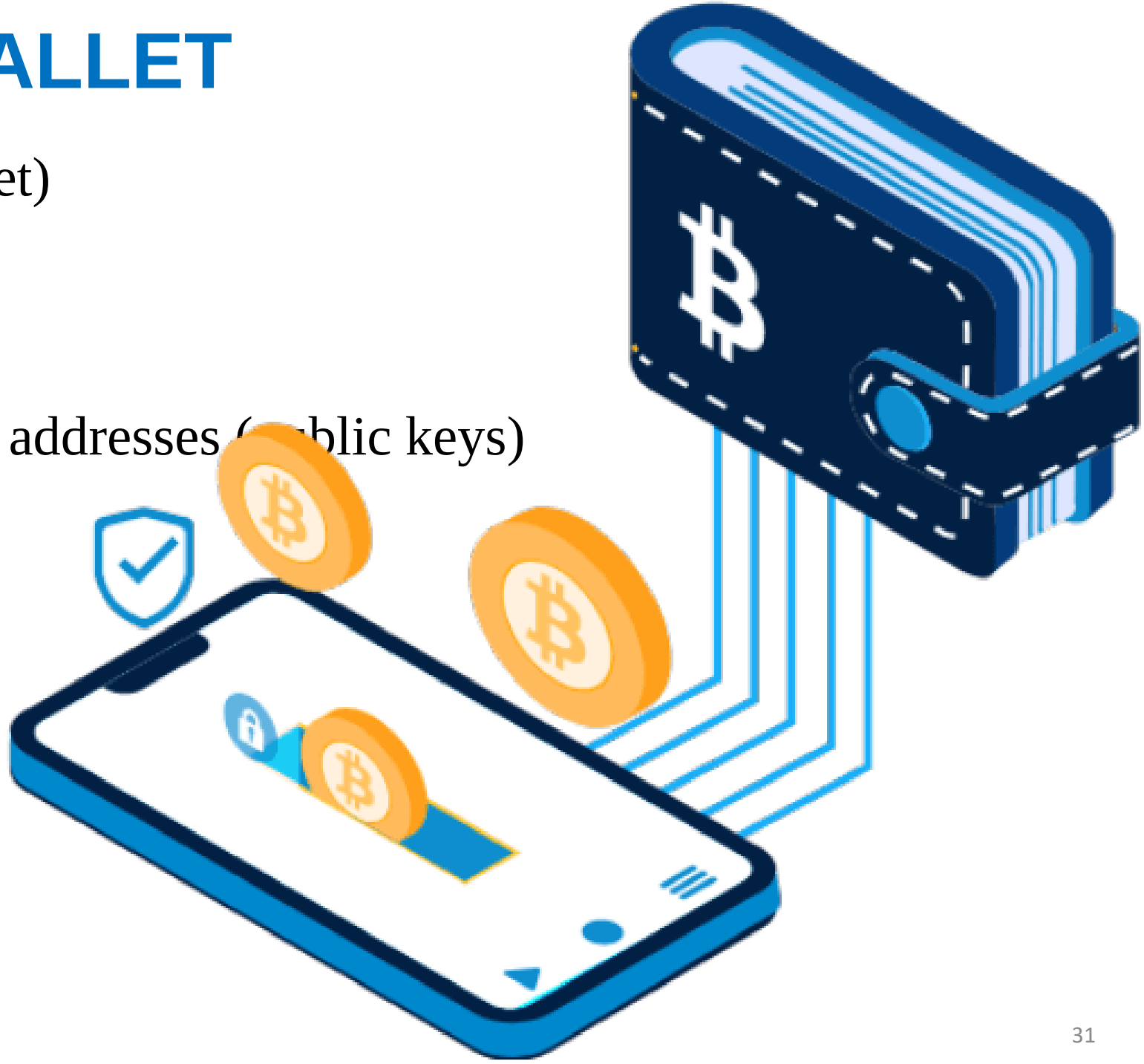
- Digital transaction protocols
- Invoked or self-execute an agreement (computerized codes)
- if parties meet predefined rules



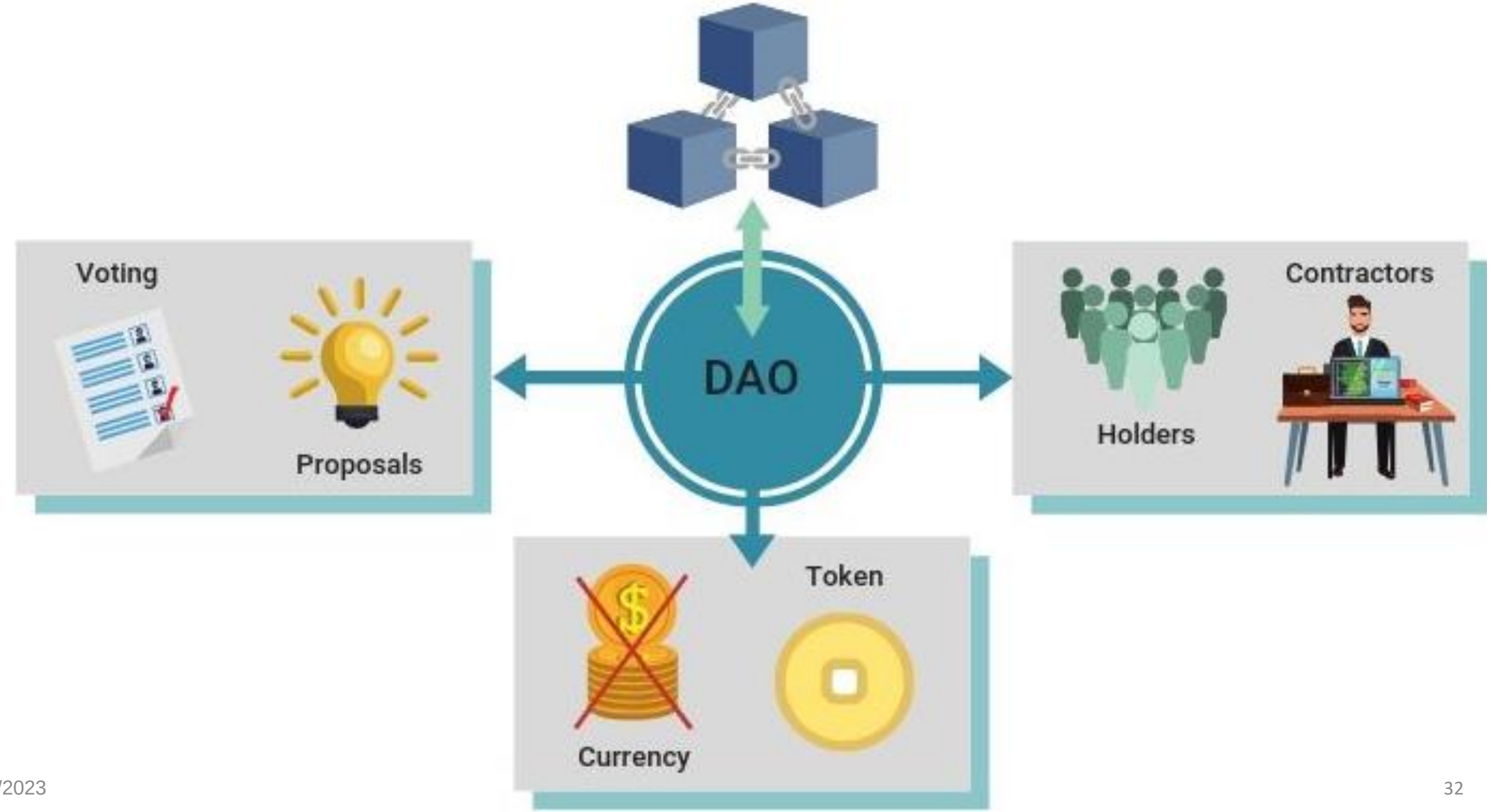
5.3. CRYPTO WALLET

Blockchain wallet: (crypto wallet)

- Digital softwares/programs
- Stores private/public keys.
- Tracks transactions relating to addresses (public keys)



5.4. DECENTRALIZED AUTONOMOUS ORGANIZATION



6. BLOCKCHAIN OPENNESS

6.1. BLOCKCHAIN INFRASTRUCTURE

6.2. BLOCKCHAIN TRILEMMA

6.3. BLOCKCHAIN INTEROPERABILITY

6.4. BLOCKCHAIN GOVERNANCE

6.1. BLOCKCHAIN INFRASTRUCTURE

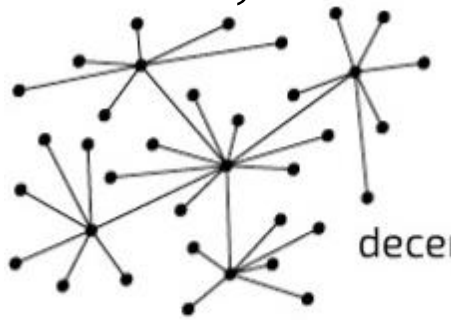
Infrastructure: encompasses services, facilities necessary

Blockchain infrastructure:

- Resources
- Underlying framework
- to function accurately

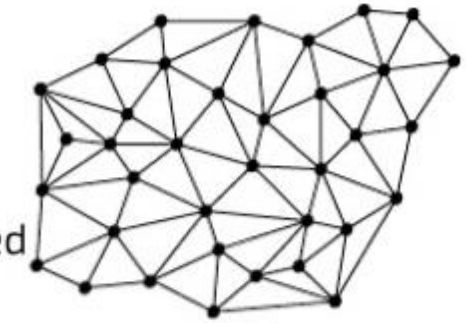
Components:

- **Storage:** token, database, file system/blobs
- **Processing:** business logic, high performance compute
- **Communications:** networks of data, of value, of state



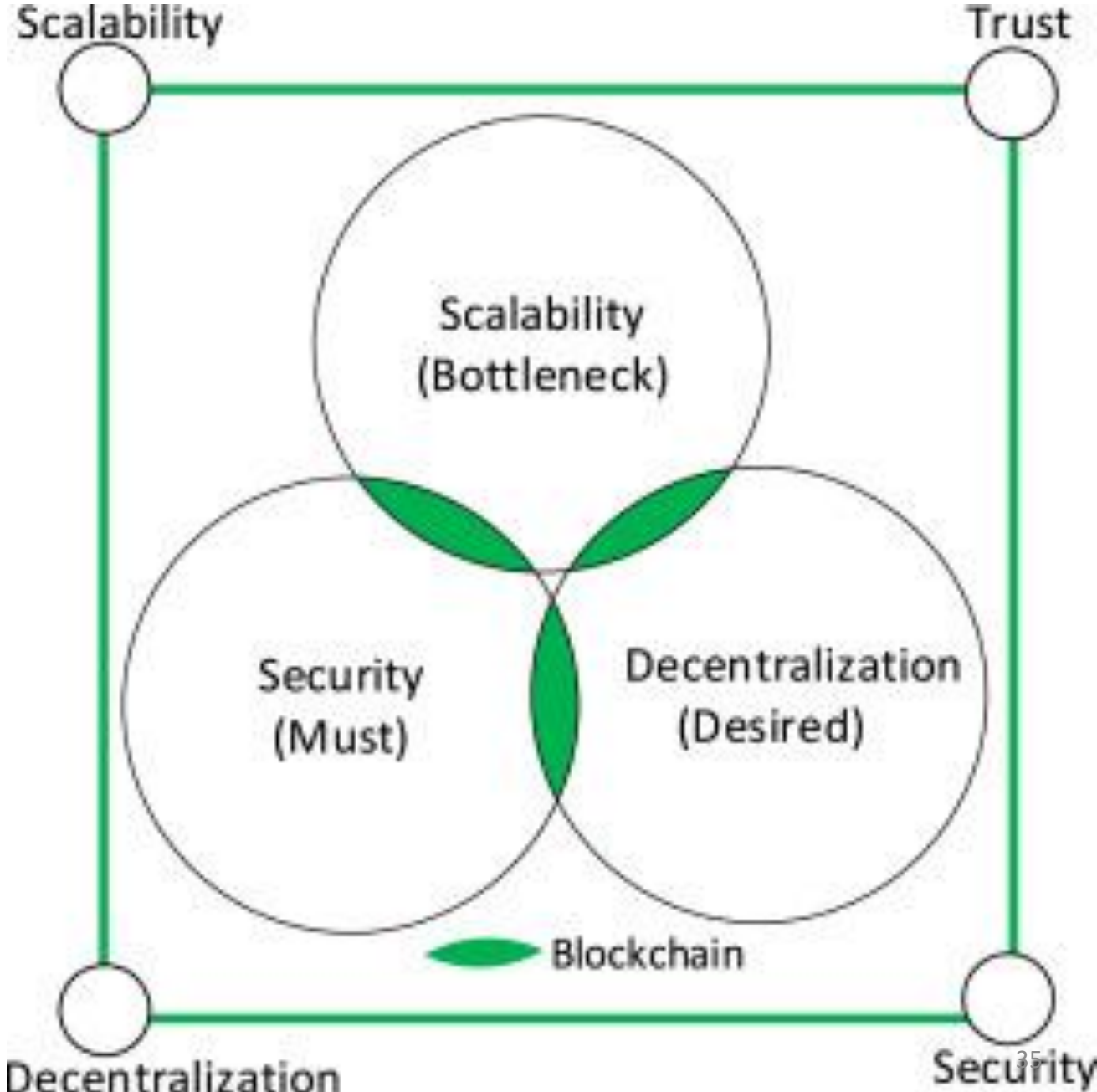
decentralized

distributed



6.2. BLOCKCHAIN TRILEMMA

- Decentralization: blockchain control central entity to group.
  power to govern blockchain.
- Security:
  - Inner: network (51%)
  - Outter: manipulate transactions to steal.
- Scalability: network grow:
  transaction speed and output.



6.3. BLOCKCHAIN INTEROPERABILITY

- Interoperability: sharing and use of data/resources between systems.
- Blockchain Interoperability: ability to exchange data with external systems.
  - Between different blockchains: Cross Chain…
  - Between other systems: Oracle…. .
- Extend blockchain capabilities:
  - combining with off-chain systems

6.4. BLOCKCHAIN GOVERNANCE

The need for blockchain governance:

- All global things we use are under governance.
- Earlier blockchain (governance-free), next to governance
- government cannot control something, it forbids the thing.

7. APPLICATION OF BLOCKCHAIN

7.1. CRYPTO CURRENCY

7.2. DECENTRALIED FINANCE

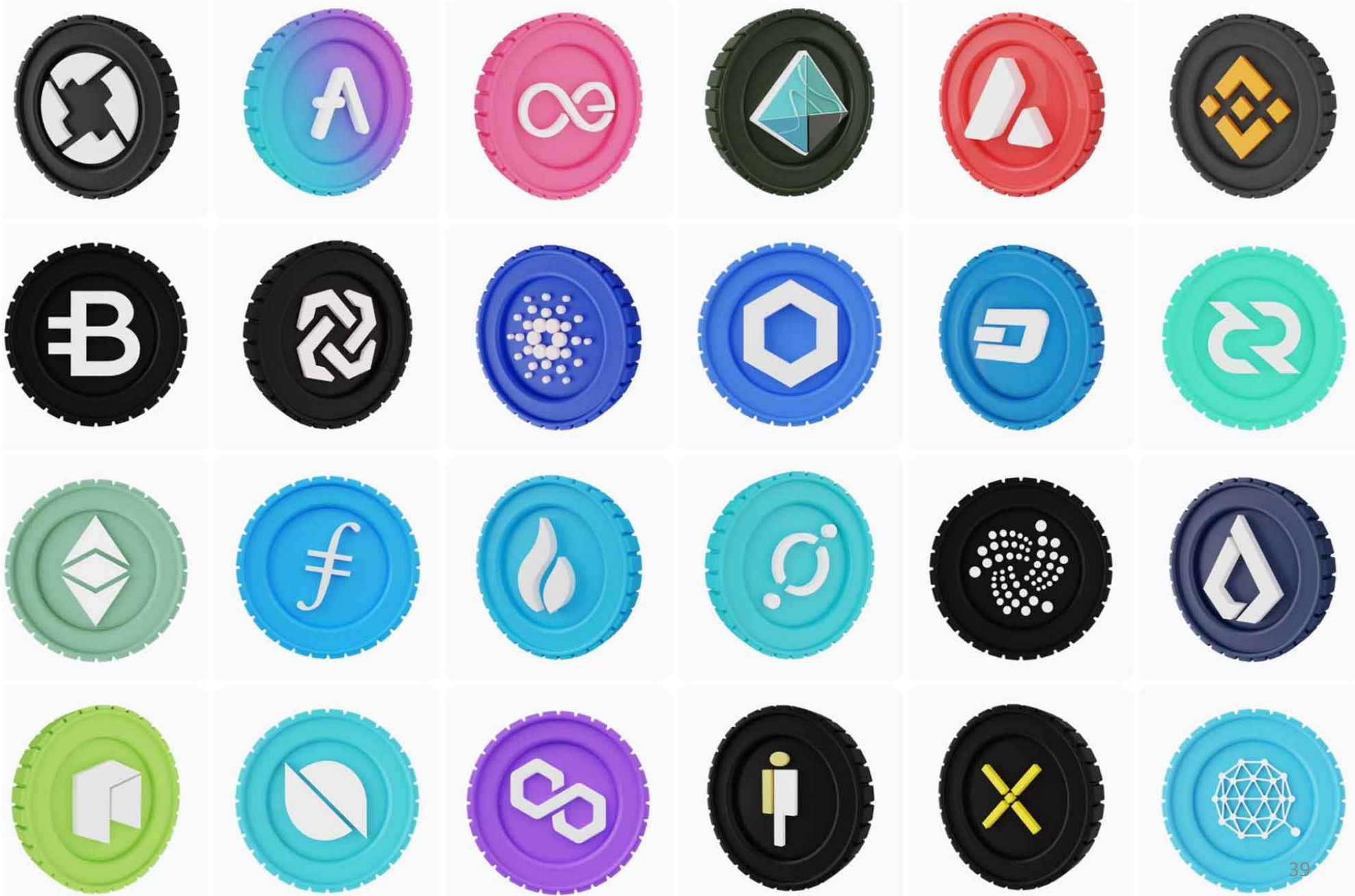
7.3. CRYPTO TOKEN

7.4. DATA MANAGEMENT

7.5. SELF-SOVEREIGN IDENTITY

7.1. CRYPTO CURRENCY

Cryptocurrency

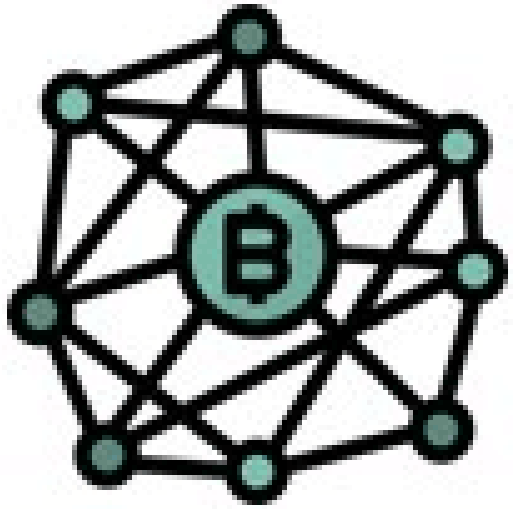


7.2. DECENTRALIED FINANCE

D

7.3. CRYPTO TOKEN

Crypto Token

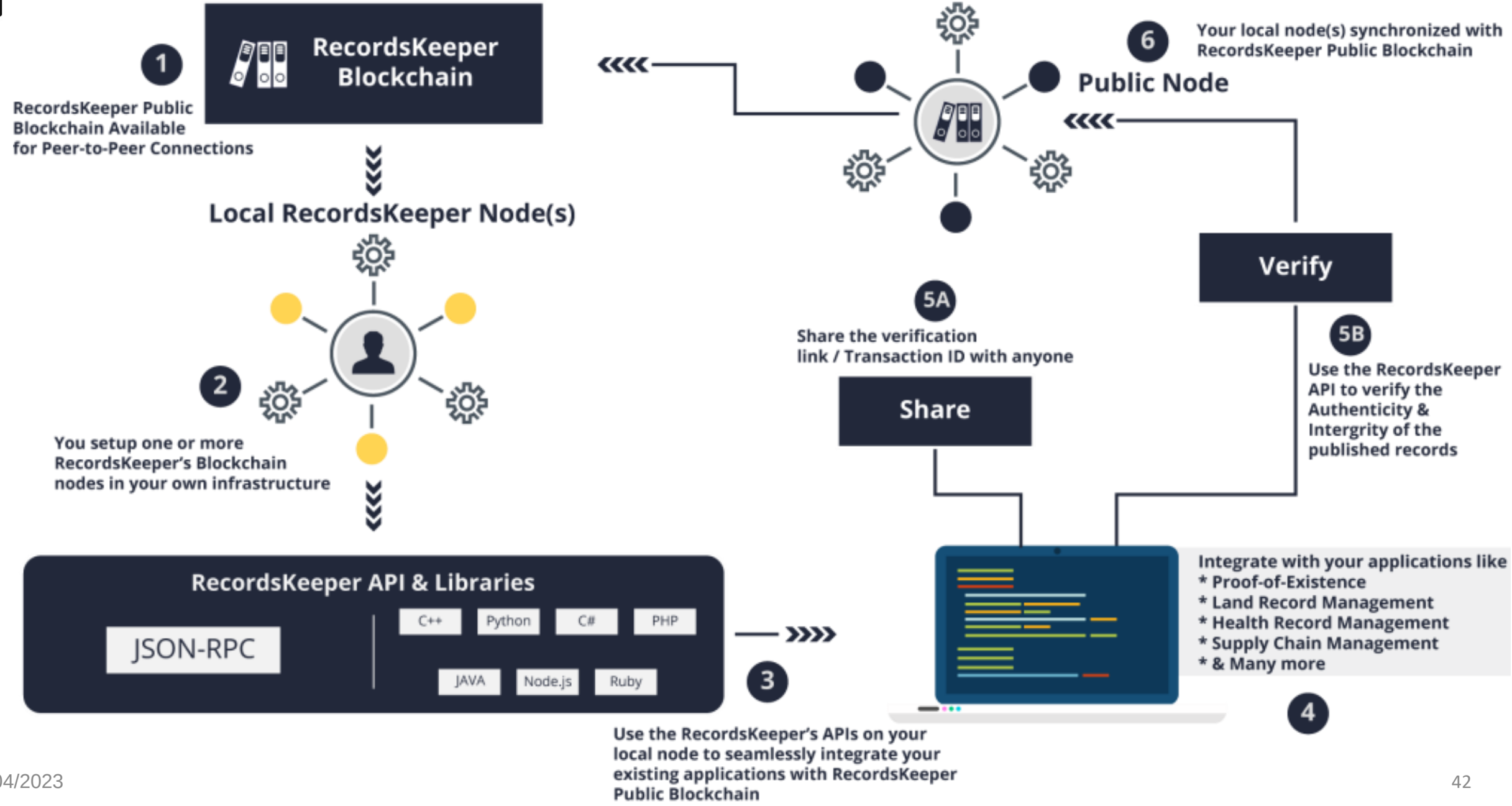


A digital asset

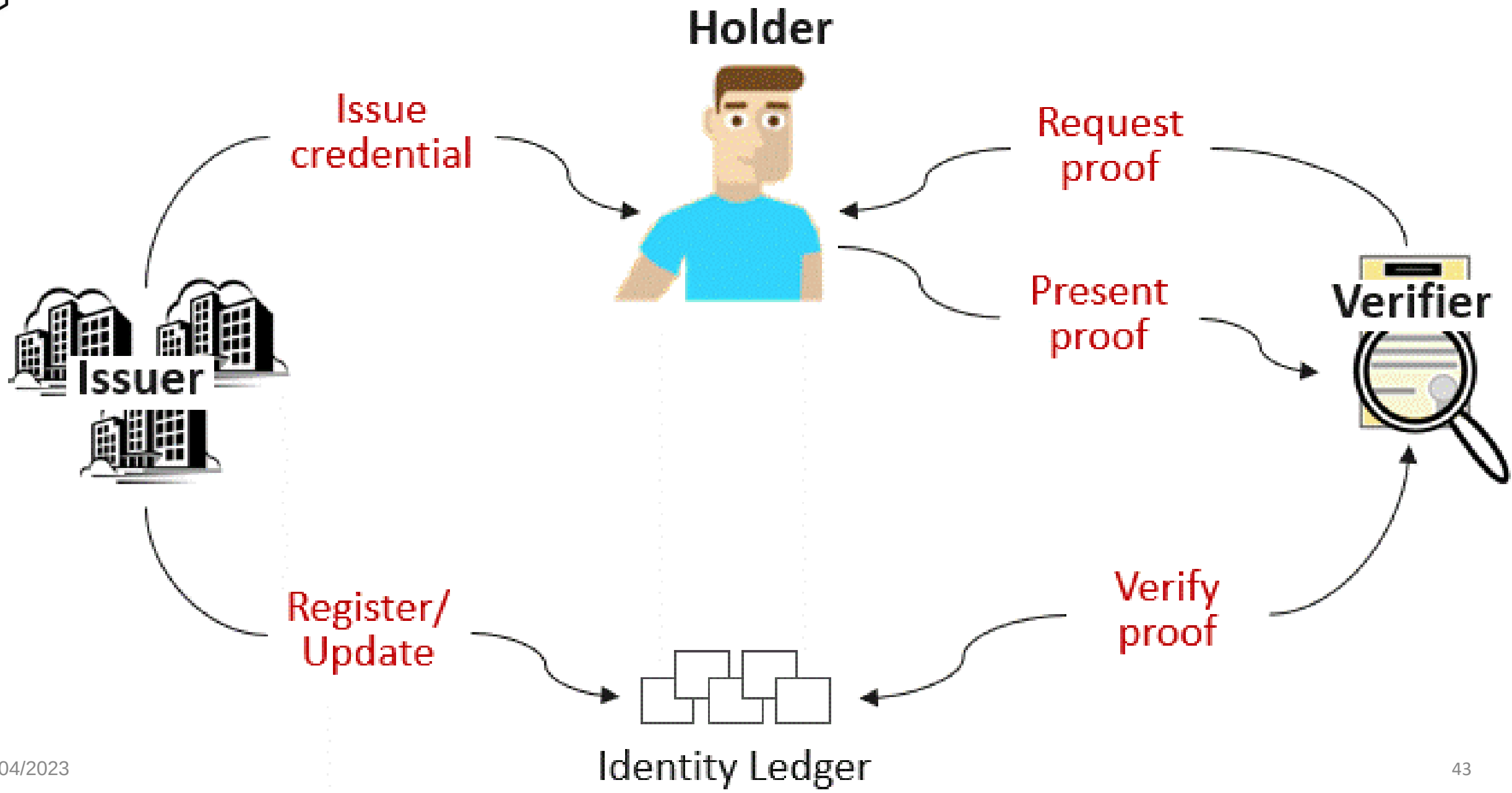
operating on

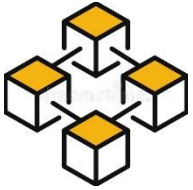
A crypto coin's blockchain

7.4. DATA MANAGEMENT



7.5. SELF-SOVEREIGN IDENTITY

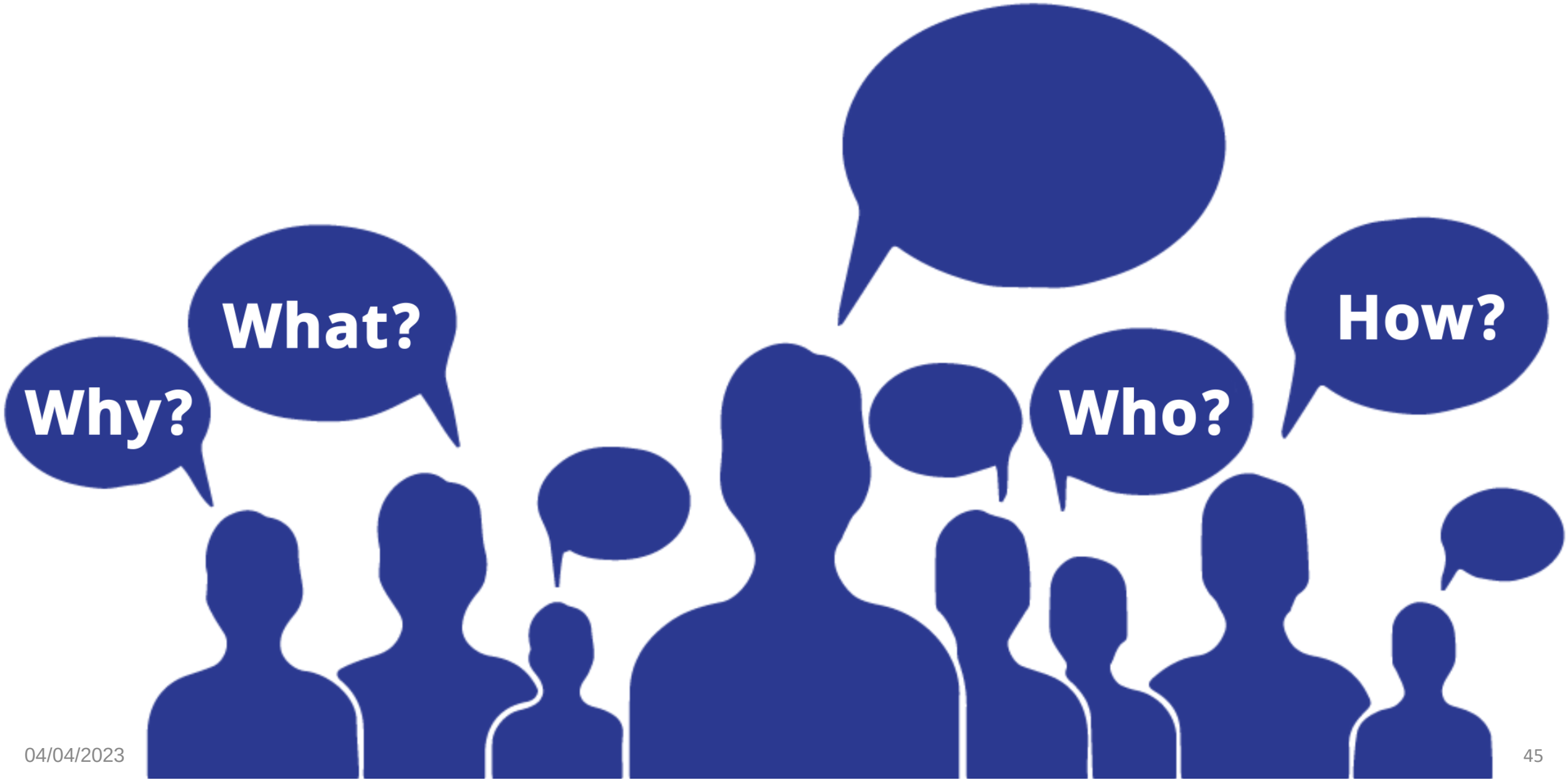




8. SUMMARY

- Blockchain: a decentralized platform (database, ledger …).
- Data: identity (address), blockchain, block, transaction, accounting model
- Network: node, architecture, protocols.
- Decentralized Application: Dapp, smartcontract, wallet, DAO
- Openness: Infrastructure, trilemma, interoperability, governance
- Applications: currency, finance, token, security, SSI….

9. DISCUSSION



FINISH