

Freshman seminar course

Blockchain and Applications

Danxin Wang

Qingdao Institute of Software
College of Computer Science and Technology

2023-12-8

Self-introduction

■ Danxin Wang (王丹心)

□ Research interests

- Network Security
- Data privacy preservation
- Blockchain
- Federated learning

□ Working and Education Experience

- Lecturer (06/2022-)
- Ph.D. from Wuhan University
- Visiting scholar from Florida University (12/2019-01/2022)

Self-introduction

■ Danxin Wang (王丹心)

□ Courses

- Computer Networks (Sophomore year)
- Information Security (Sophomore year)
- Blockchain Technology and Applications (Junior Year)

□ **E-mail:** wangdx@upc.edu.cn

Contents

1

Introduction

Blockchain

2

Classification

Characteristics and classification of blockchain

3

Network Structure

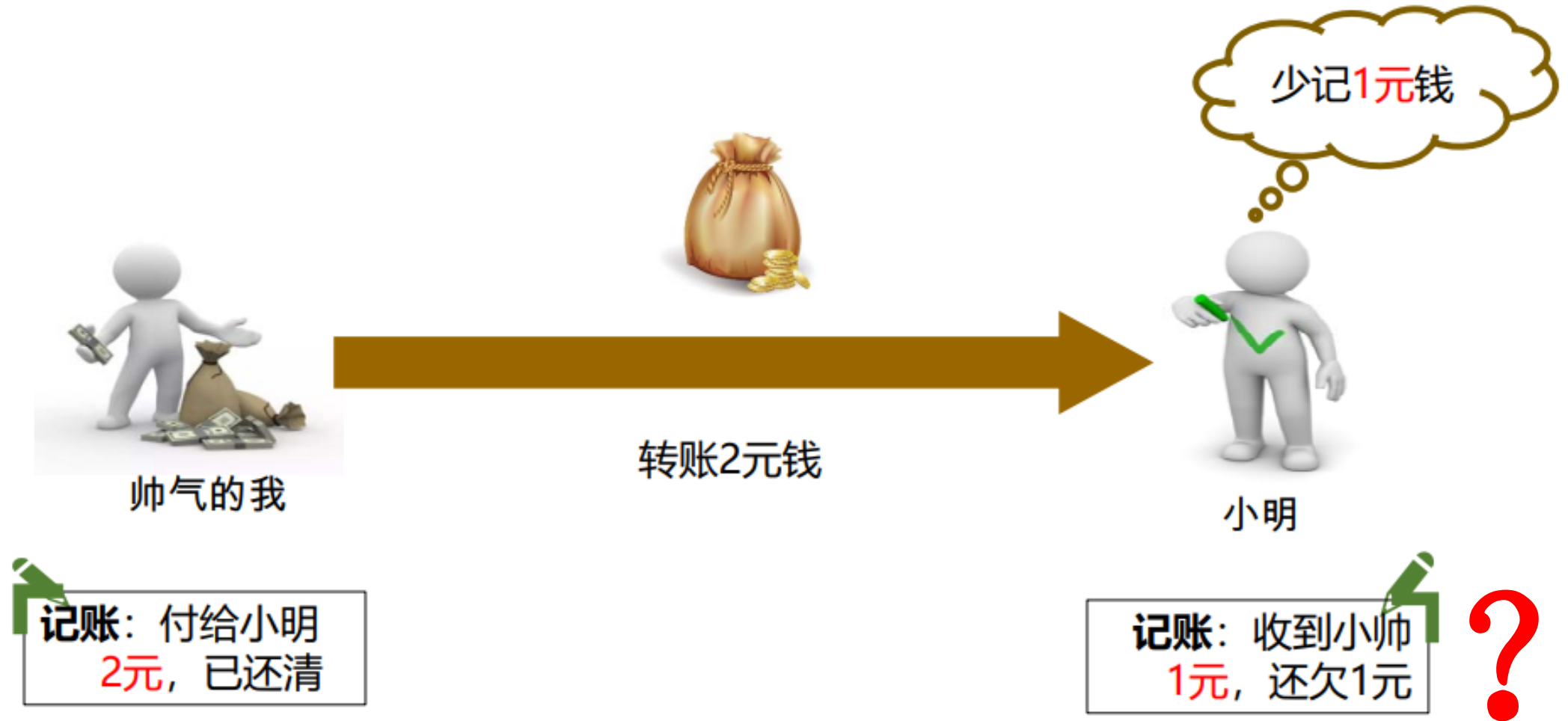
Basic knowledge

4

Applications

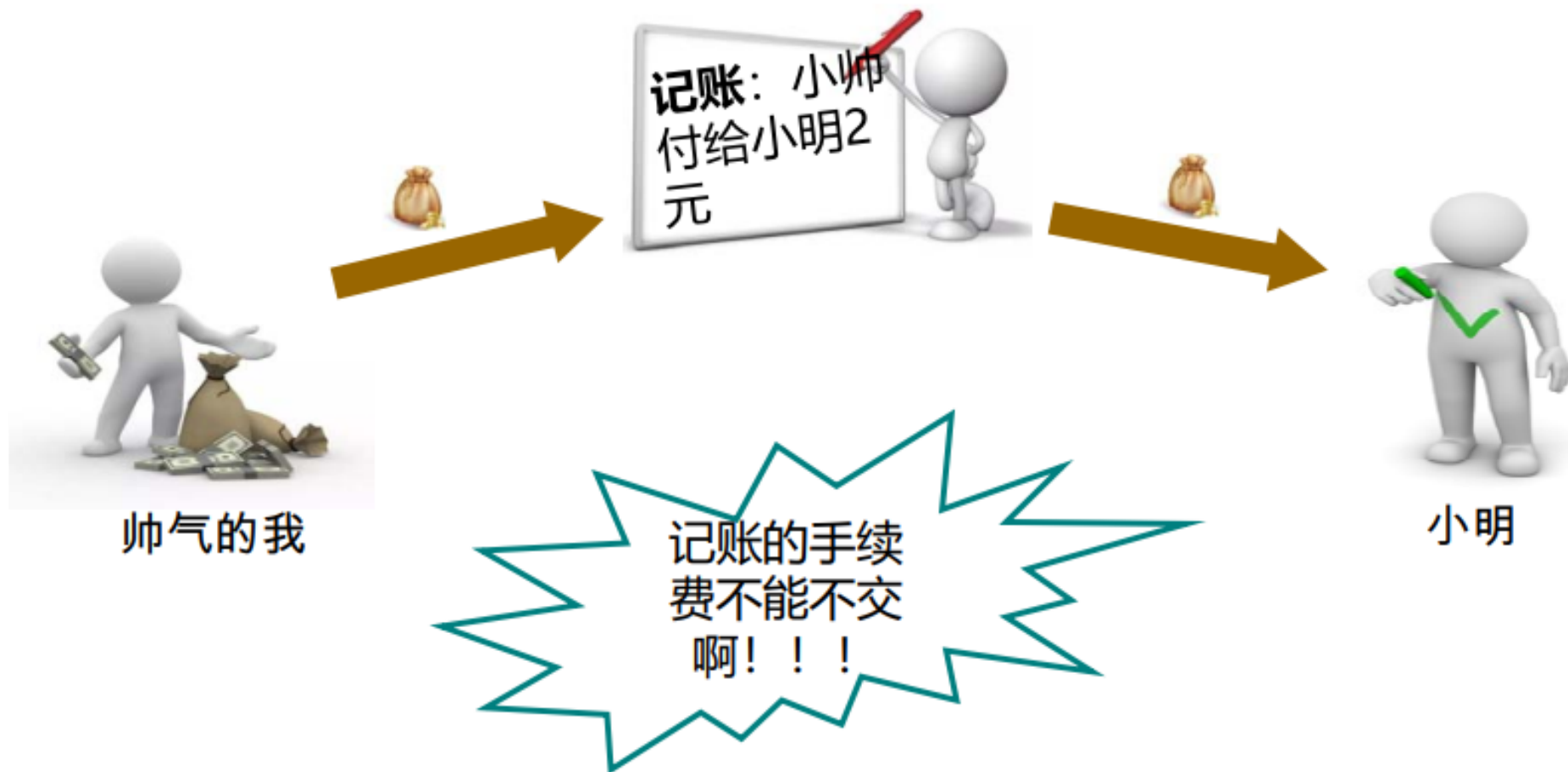
Platforms

Introduction of Blockchain

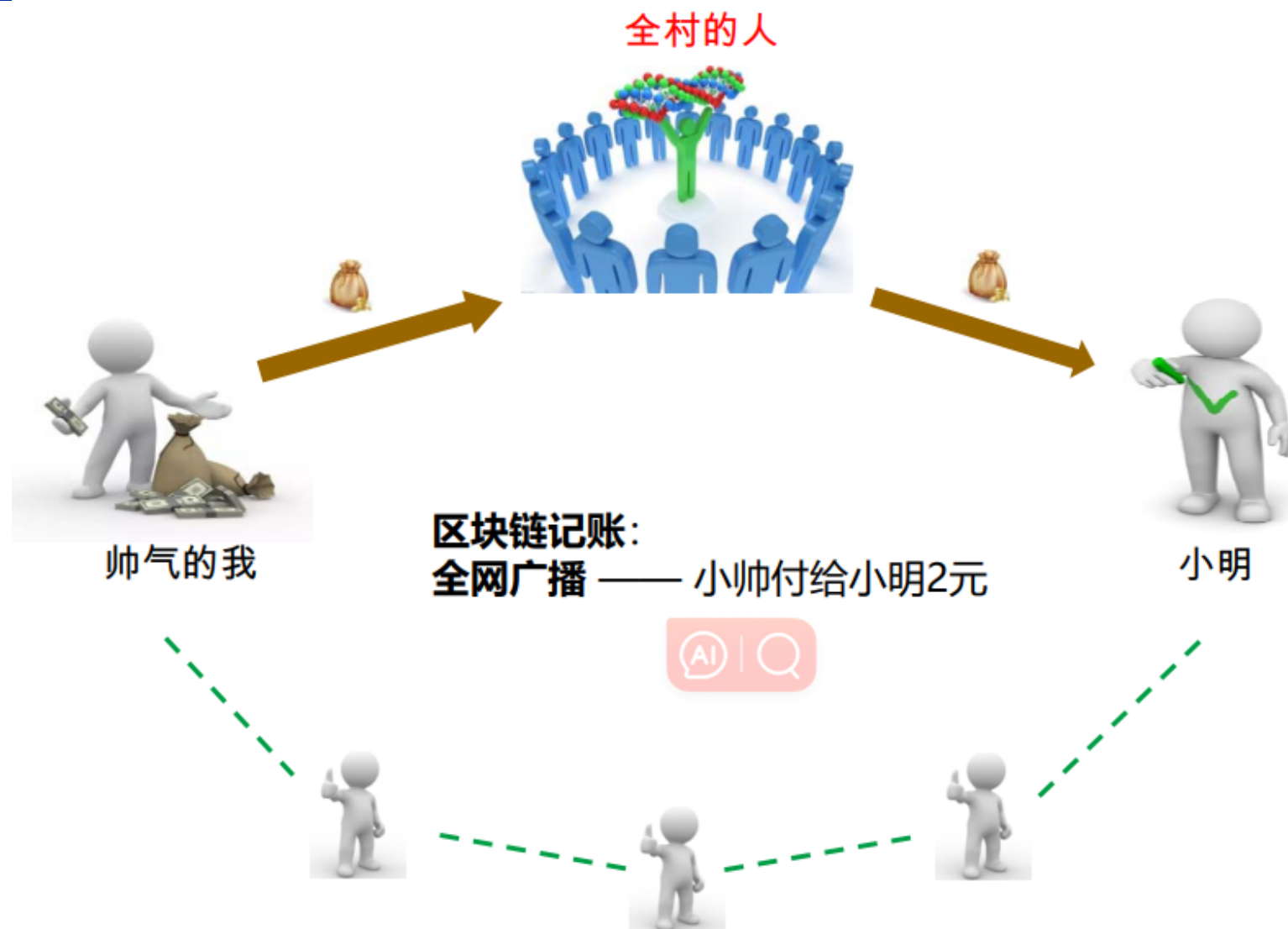


Introduction of Blockchain

银行、微信、支付宝...



Introduction of Blockchain



Introduction of Blockchain

去中介！踢开银行、第三方支付



真是个好故事



我们按照区块链的规则，
约法三章



帅气的我



小明

①每次交易，咱俩中间只能有一个人
记账；具体谁来记，咱们石头剪刀布
（工作量证明）

如果一笔交易两个人都记账，很容易记岔掉；
如果每次都是一个人记账，这个人权力太大，容易腐化堕落；
石头剪刀布最好啦，每次记账人都是随机的，公平！



帅气的我



小明

*实际区块链运转机制中用的当然不是石头剪刀布，而是让全网节点比赛，看谁先算出一个前x位都是0的随机数。谁就获得记账权。这也太难了！举个例子，整个比特币网络要10分钟才能找出一个前10位都是0的随机数。所以，可以确保同时只有一个节点记账。

②甭管谁记账，另一个人必须原封不
动照抄一遍，放进自己的账本（全网
同步备份）

把我们形成共识的记录在全网每一个角落备份，一方面可以保证
数据不会遗失，另一方面也可以对抗篡改



帅气的我



小明

*说是照抄一遍，其实交易内容是可以加密的。虽然密文全网同步备份，没有对应的私
钥还是看不到内容——确保数据私密性和安全性。

③记完账后，在字迹上盖个印章，这
样只要印章完好无损，就说明后来字
迹没有被篡改过（Merkel根）

这样一来，一旦账本记好，就不能编辑了，避免了被人篡改



帅气的我



小明

*这个“印章”是比喻区块正文的对应hash（叫做Merkel根）。只要正文被篡改哪怕一
丁点儿，hash就会变得完全不一样，“大家”也就知道正文被篡改了。于是这种篡改
内容就会被整个区块链系统无情地抛弃。

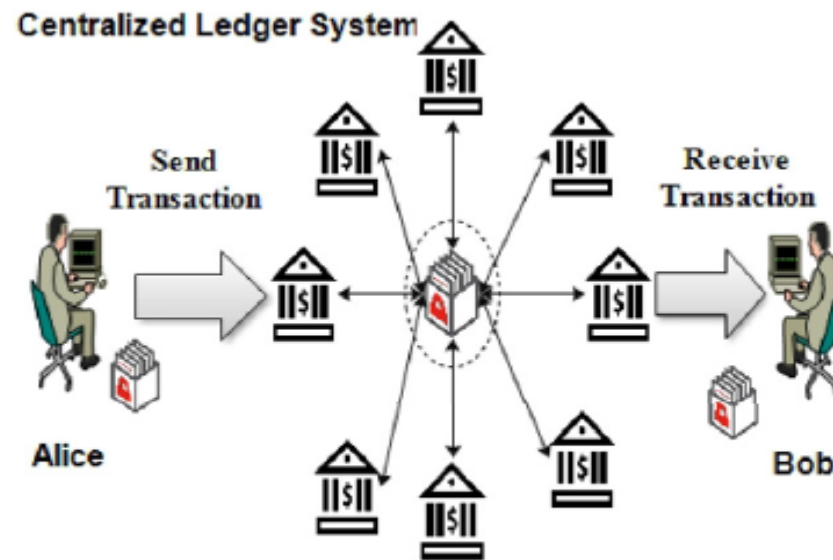
Introduction of Blockchain

■ Blockchain

- ❑ a distributed network and chain of cryptographic blocks combined together to form a Peer-to-Peer (P2P) network that is decentralized and distributed in nature.
- ❑ In blockchain, each node has its own distributed ledger for storing the history of the transactions.

Introduction of Blockchain

- Blockchain can be leveraged to achieve **authentication, authorization, accountability, security, integrity, confidentiality** and **non-repudiation** for real-time applications, which may not be provided by a centralized system efficiently.

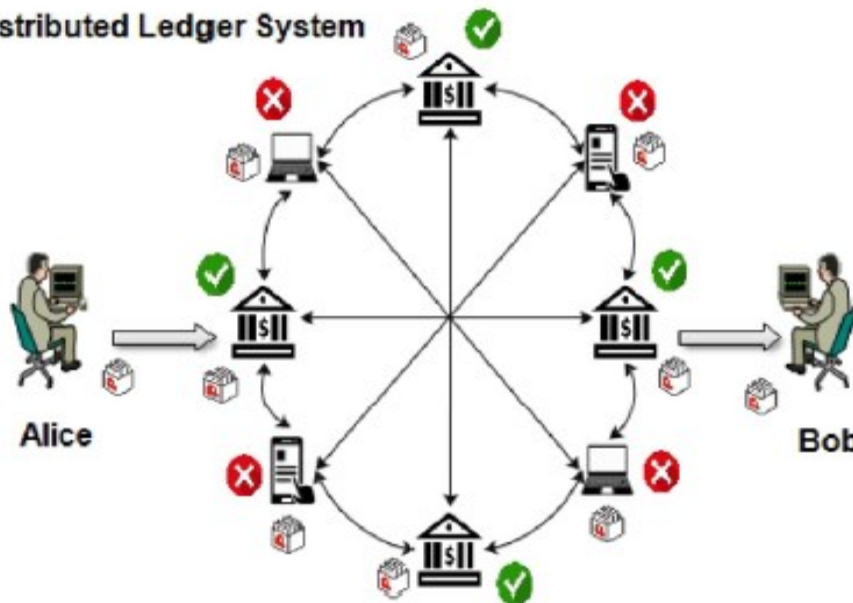


(1) Centralized Transaction System

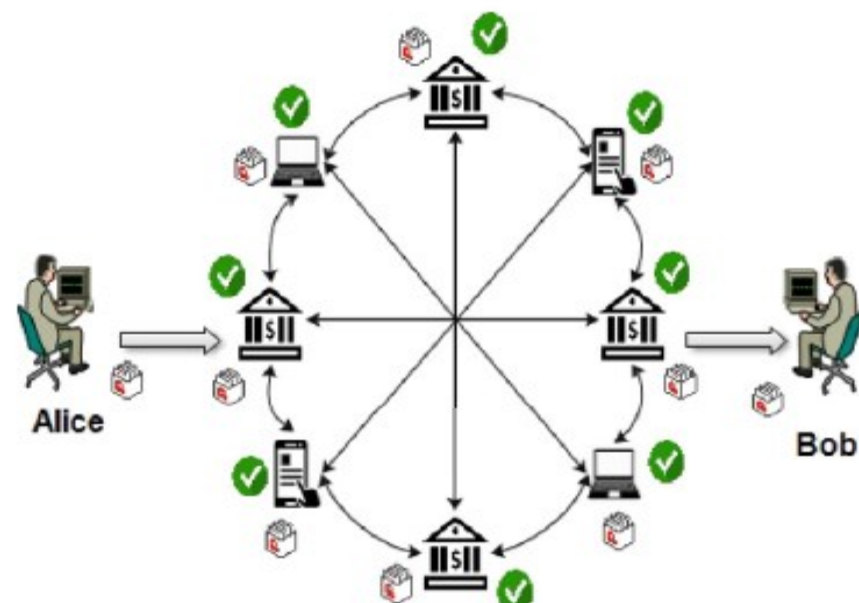
Introduction of Blockchain

- Blockchain can be leveraged to achieve **authentication**, **authorization**, **accountability**, **security**, **integrity**, **confidentiality** and **non-repudiation** for real-time applications, which may not be provided by a centralized system efficiently.

Distributed Ledger System



2 (a) Permissioned (Private)



2 (b) Permissionless (Public)

Introduction of Blockchain

■ The history of Blockchain

- ❑ Bitcoin (2009, Satoshi Nakamoto)
- ❑ Ethereum (ETH) (2013, Vitalik Buterin)
- ❑ Smart contracts
- ❑ Cryptocurrency → Web 3.0
- ❑ https://www.bilibili.com/video/BV12E411P7TT/?vd_source=b533ec11d1f387db0855d15bf81fd732

Characteristics of blockchain

■ Decentralization

- ❑ Decentralization is a **fundamental characteristic** of blockchain, where numerous nodes **form a P2P network without any centralized devices** or governing institutions. Data exchange between nodes is verified through digital signature technology, eliminating the need for mutual trust. As long as the established rules of the system are followed, nodes will not deceive each other.

Characteristics of blockchain

■ Openness and consensus (Fault tolerance)

- ❑ Openness and consensus (Fault tolerance) **allow anyone to participate in the blockchain network**, where each device can act as a node and **obtain a complete copy of the database**. Nodes maintain the entire blockchain through a set of **consensus mechanisms**, competing with each other for calculations. Even if any node fails, the remaining nodes can continue to function normally.

Characteristics of blockchain

■ Transparent and Anonymous

- ❑ Transparent transactions and anonymous operation are fundamental principles of blockchain. The rules governing the operation of the blockchain are transparent, with all data information being publicly available. As a result, every transaction is visible to all nodes in the network. Since trust is established between nodes without any prior relationship, there is no need for them to disclose their identities; hence, each participating node remains anonymous.

Characteristics of blockchain

■ Immutability and Auditability

- ❑ It means that **modifications made by individual or multiple nodes to the database cannot affect other nodes' databases** unless they can control over 51% of the nodes in the entire network simultaneously, which is highly unlikely. In blockchain, every transaction is cryptographically linked to its adjacent blocks, allowing for a traceable history of any transaction.

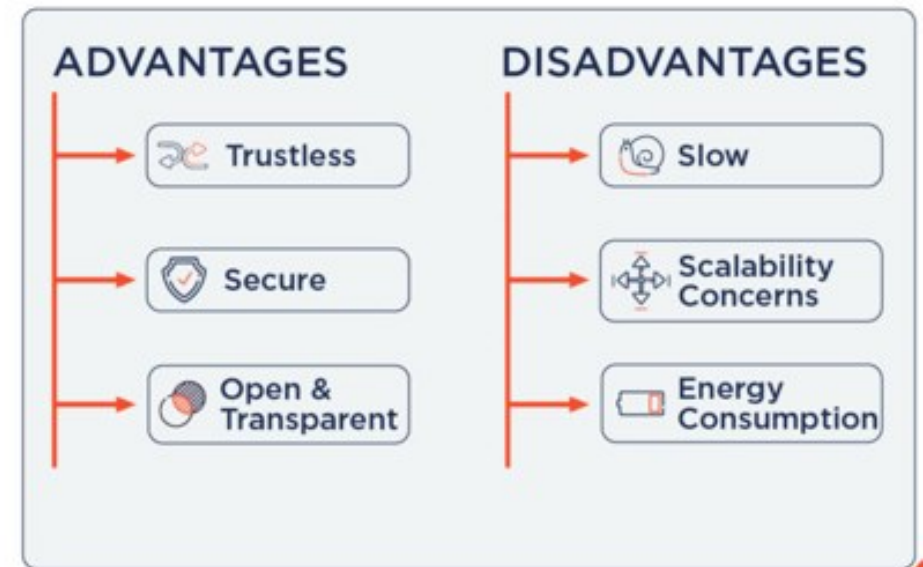
Classification of Blockchain

■ Public Blockchain (permissionless)

- which is open for anyone to read, send, or receive transactions, and allows any participant to join the consensus procedure of making the decision on which blocks contain correct transactions and get added to the blockchain.

1. PUBLIC BLOCKCHAIN

A completely open and permissionless network which stores public data.



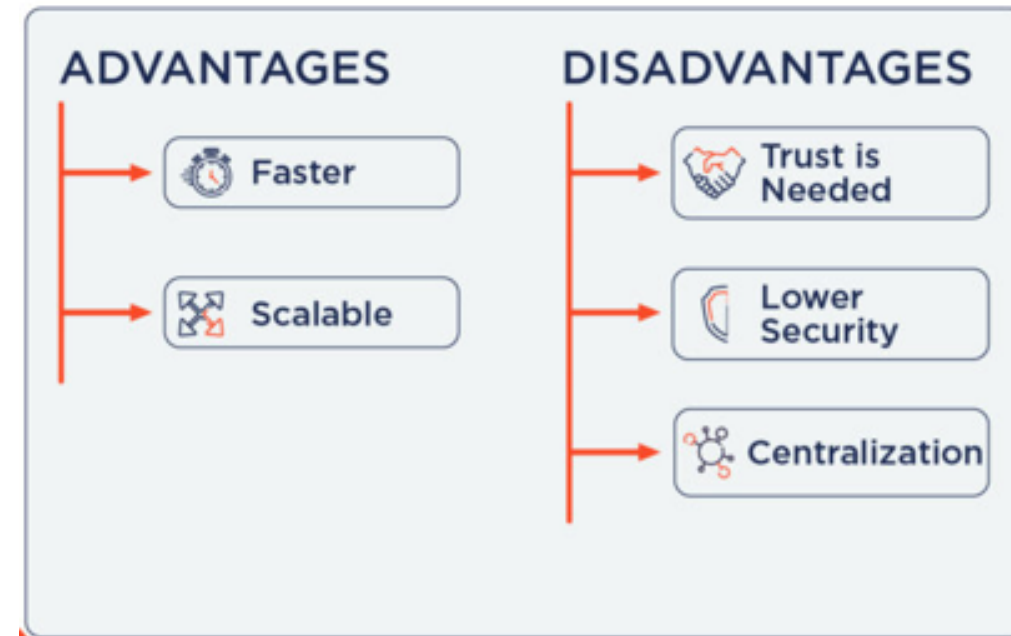
Classification of Blockchain

■ Private Blockchain (permissioned)

- whose **write permissions are restricted strictly to a single participant** (or organization), even though **its read permissions are open to the public** or constrained to a subset of participants in the network.

2.PRIVATE BLOCKCHAIN

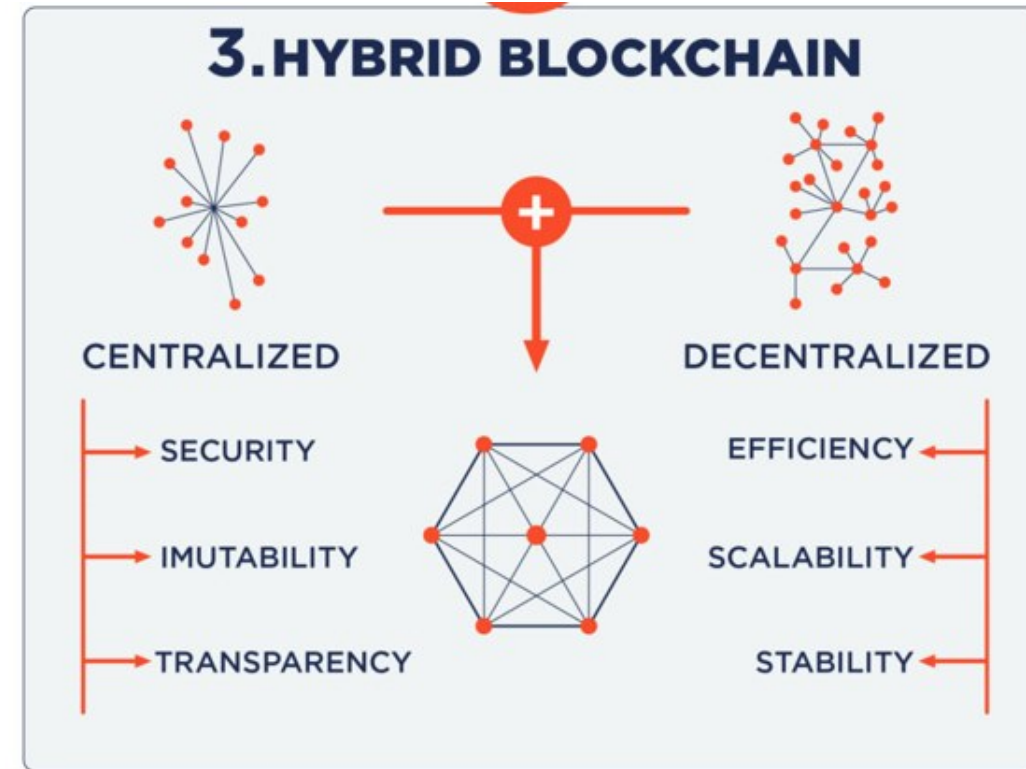
All the people in this network have permission as the it is a close and a restricted network.



Classification of Blockchain

■ Hybrid/Consortium Blockchain

- which has placed certain constraints on write permissions such that **only a pre-selected set of participants in the network can influence and control the consensus process**, even though read is open to any participant in the network.



Classification of Blockchain

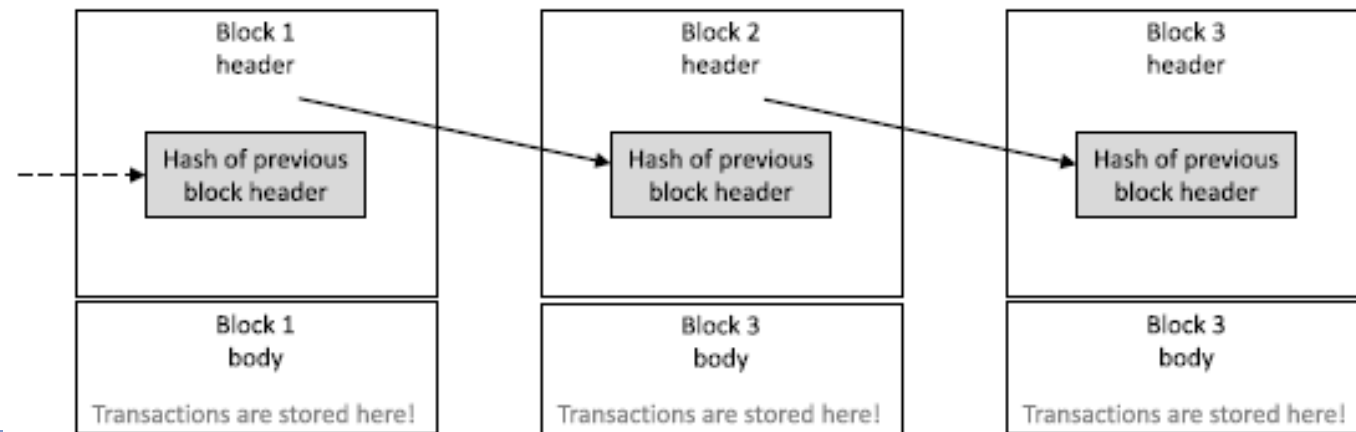
■ CAP Properties in Blockchain

- ❑ CAP theorem is a fundamental theorem for defining transactional properties in distributed systems
 - **Consistency**: all nodes keep an identical ledger with most recent updates.
 - **Availability**: any transactions generated at any time in the network will be accepted in the ledger.
 - **Partition tolerance**: even if part of the nodes fail, the network can still operate normally
- ❑ the blockchain **consistency** is not achieved **simultaneously** as availability and partition tolerance, but it is after a period of time.

Basic knowledge of Blockchain

■ Blockchain Structure

- ❑ A blockchain is made up of **blocks** containing details of **transactions** that have occurred within the network.
- ❑ The transaction information can be regarded as token transfers occurring in a network, or any manner of data exchange.

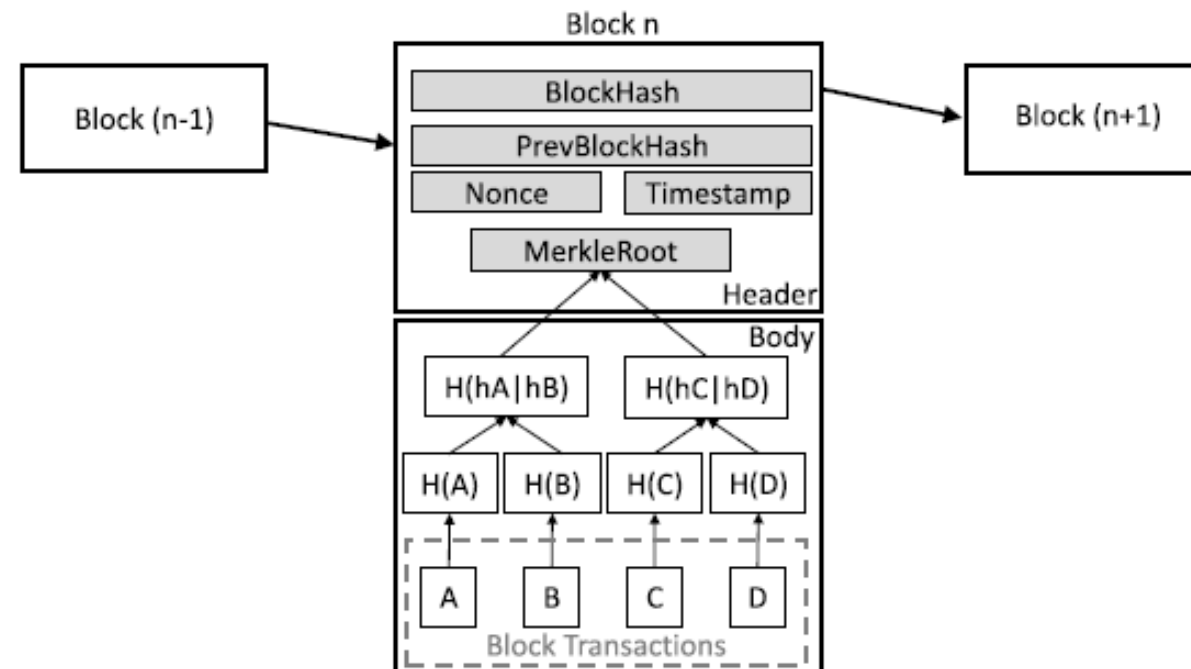


(a) Logical representation of a blockchain.

Basic knowledge of Blockchain

■ Blockchain Structure

- ❑ A blockchain is made up of **blocks** containing details of **transactions** that have occurred within the network.



(b) Block header fields and Merkle tree for storing transactions in a block.

Basic knowledge of Blockchain

■ Hash Chained Storage

□ Hash Chained Storage

- Hash pointer is a hash of the data by cryptography, pointing to the location in which the data is stored.
- A block chain is organized using hash pointers to link data blocks together

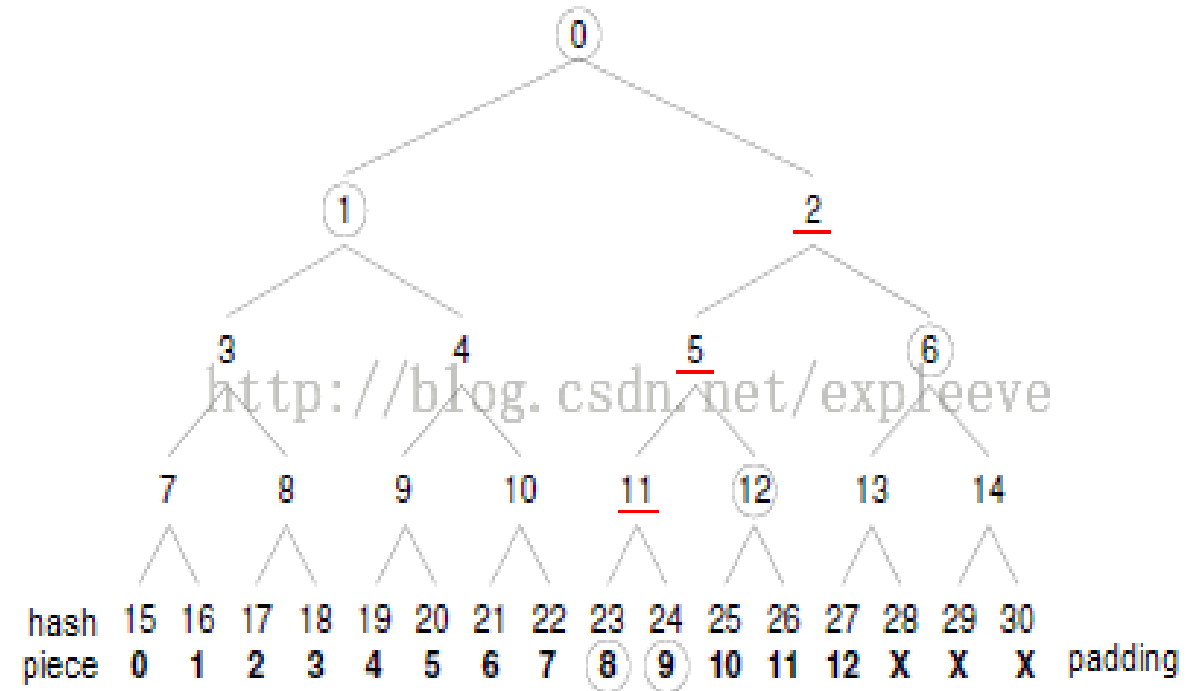
□ Merkle Tree

- A Merkle tree is defined as a binary search tree with its tree nodes linked to one another using hash pointers.
- A Merkle tree has the ability of preventing data from tampering by traversing down through the hash pointers

Basic knowledge of Blockchain

■ Hash Chained Storage

- ❑ Merkle Tree
- ❑ Hash functions
 - SHA256
 - Ethash
 - SCrypt X11
 - Equihash, RIPEMD160



Basic knowledge of Blockchain

■ Digital Signature

- ❑ A digital signature establishes the validity of a piece of data by using a cryptographic algorithm. It is also a scheme for verifying that a piece of data has not been tampered with.
 - key generation algorithm
 - signing algorithm
 - verification algorithm
- ❑ Elliptic Curve Digital Signature Algorithm (ECDSA)
- ❑ Public Keys as Pseudonyms

Basic knowledge of Blockchain

■ Digital Signature

- ❑ Elliptic Curve Digital Signature Algorithm (ECDSA)
- ❑ Edwards-curve Digital Signature Algorithm (EdDSA)
- ❑ Ring
- ❑ One-Time Signature
- ❑ Borromean Ring Signatures
- ❑ Multi-Signature

Basic knowledge of Blockchain

■ Consensus

- ❑ The consensus is employed to **seek for the majority of the network to agree upon a single state update** in order to secure the expansion of the global ledger (the blockchain) and prevent dishonest attempts or malicious attacks.
- ❑ Consensus algorithm must be **fault tolerant**, and ensure that **all nodes simultaneously maintain an identical chain of blocks** It does not rely on central authority to keep malicious adversaries from disrupting the coordination process of reaching consensus.

Basic knowledge of Blockchain

■ Timestamp server

- ❑ A timestamp server is a trusted system based on Public Key Infrastructure (PKI) technology, **providing accurate and reliable timestamp services to the public**. It utilizes precise time sources and robust security mechanisms to confirm the existence of data in a specific time and establish the relative chronological order of related operations. This serves as a fundamental service for preventing repudiation of time-related actions in information systems.

Transaction process (Bitcoin)

■ First Step: Create a transaction

- ❑ if client A wants to send some bitcoins to another client B, it will **create a bitcoin transaction** by client A.
- ❑ Client **A uses his private key to sign the previous transaction** (the source of the Bitcoin) and the Client B, attaching this signature at the end of the currency, creating a transaction record.

Transaction process (Bitcoin)

■ Second Step: Broadcast and Consensus

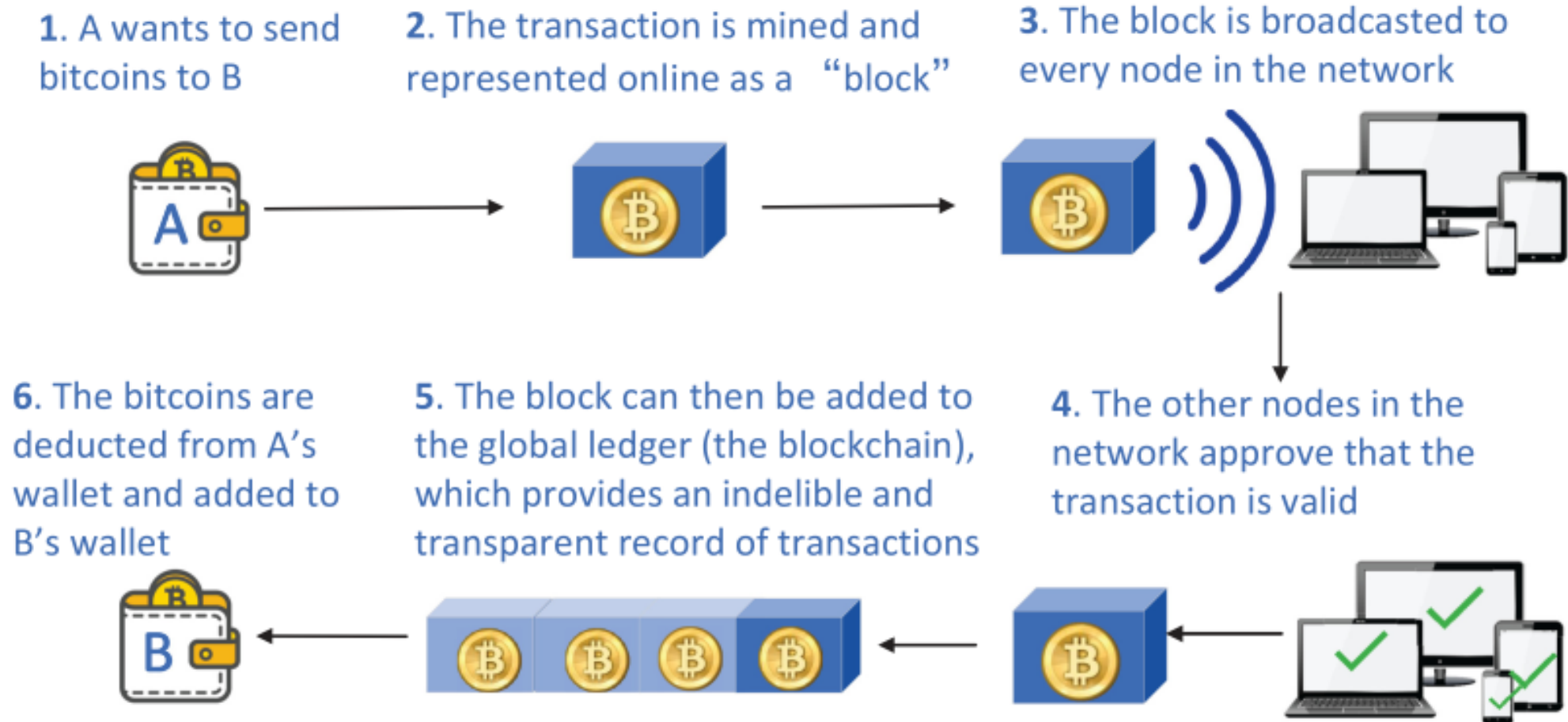
- ❑ The transaction has to be approved by miners before it gets committed by the Bitcoin network. To initiate the mining process, **the transaction is broadcasted to every node in the network**. Those nodes that are miners will collect transactions into a block, verify transactions in the block, and **broadcast the block and its verification using a consensus protocol** (a.k.a., Proof of Work) to get approval from the network.

Transaction process (Bitcoin)

■ Third Step: Verify and update

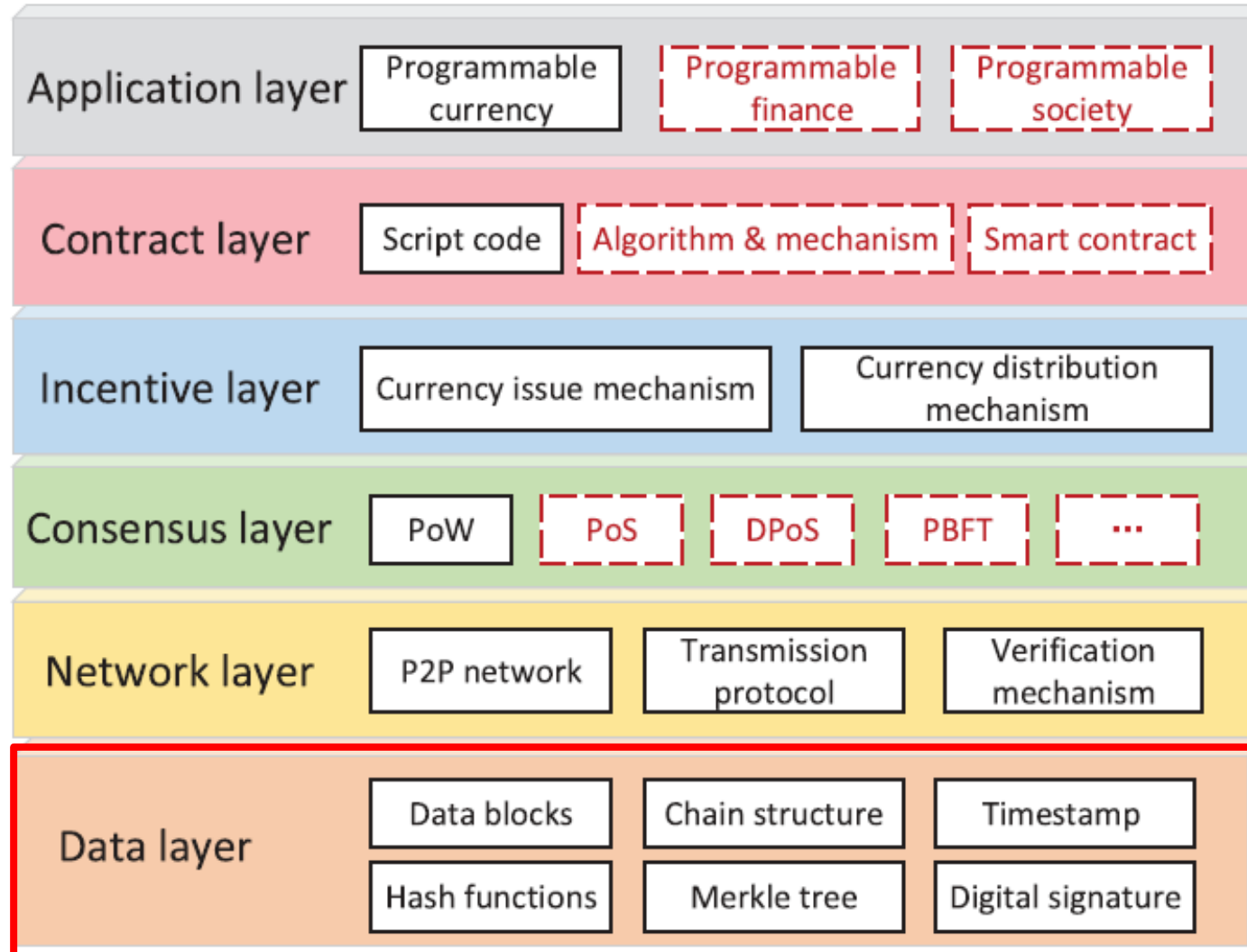
- ❑ When other nodes **verify that all transactions contained in the block are valid**, the block can be added to the blockchain. **Only when the “block” containing the transaction is approved by the other nodes and added to the blockchain**, this bitcoin transfer from A to B will become finalized and legitimate.

Transaction process (Bitcoin)



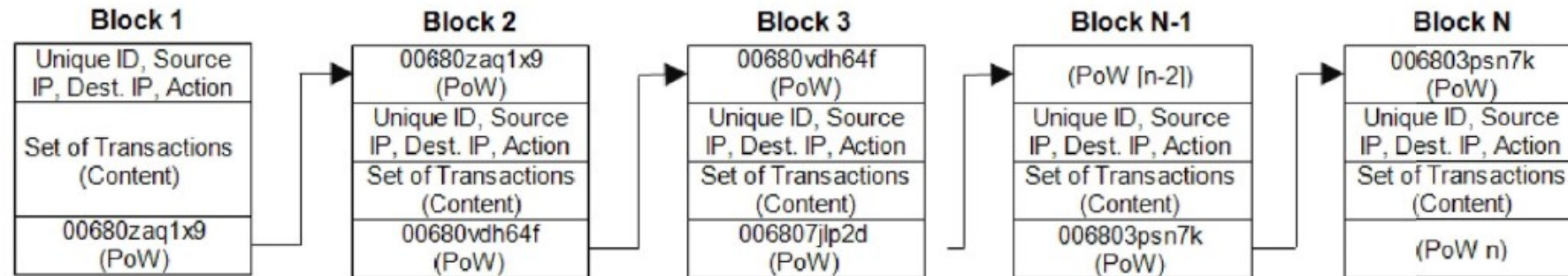
https://www.bilibili.com/video/BV1rR4y1F7VF/?spm_id_from=333.337.search-card.all.click&vd_source=b533ec11d1f387db0855d15bf81fd732

The architecture of Blockchain

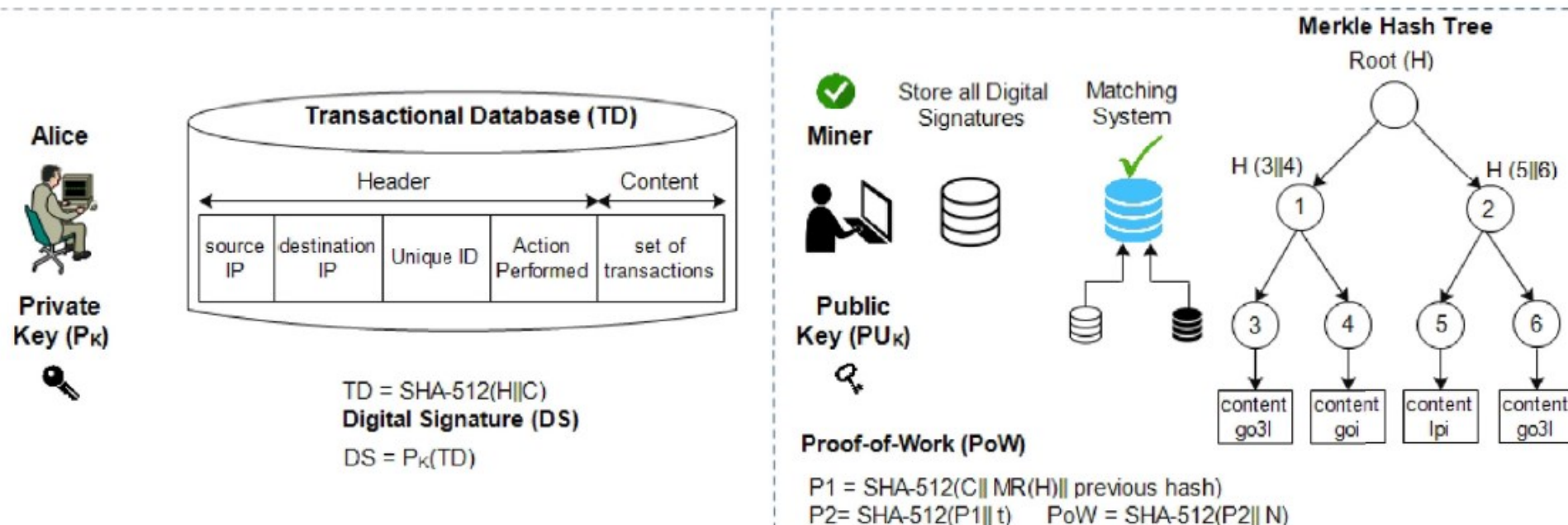


The architecture of Blockchain

■ Data Layer

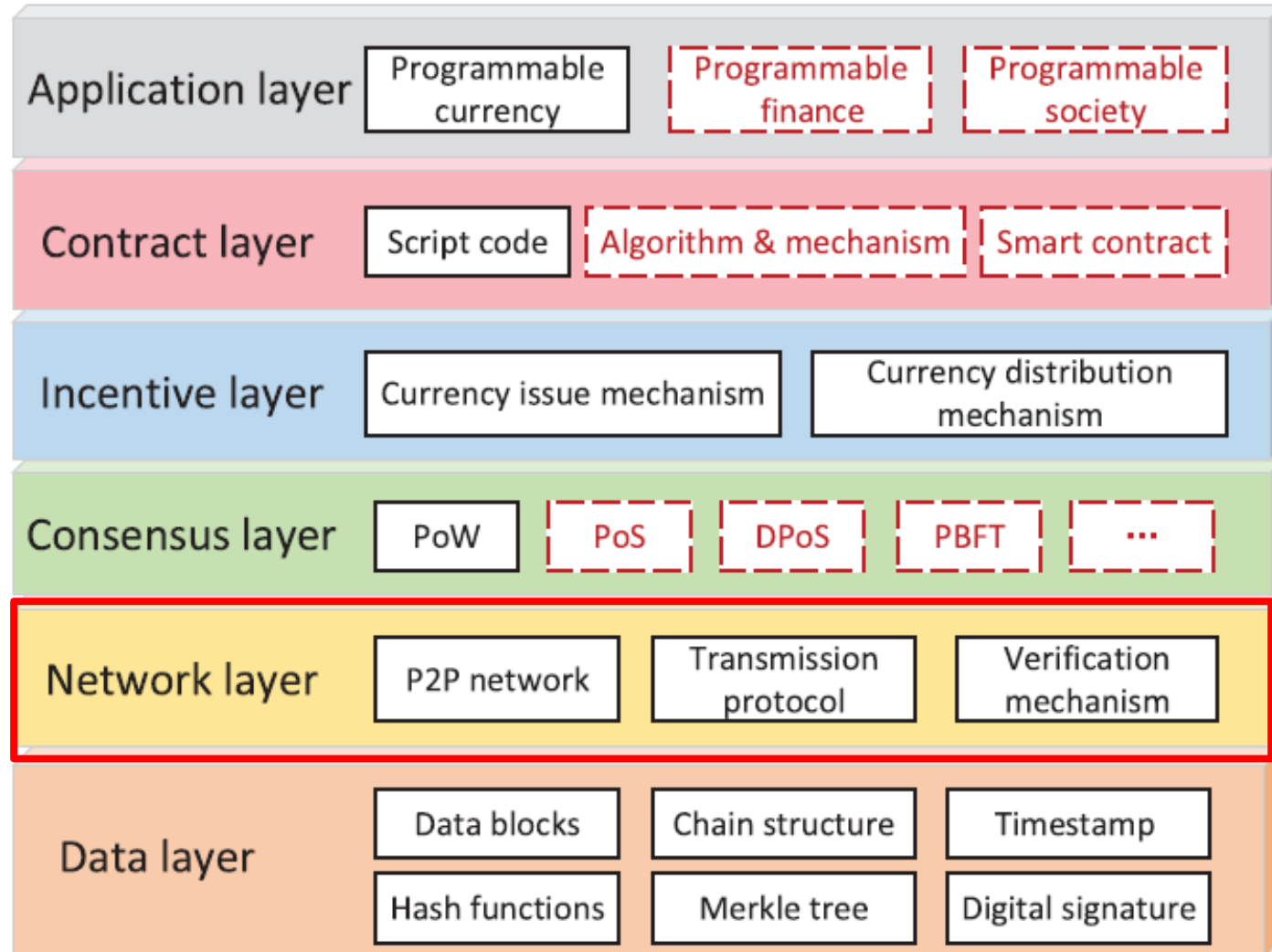


Blockchain Creation Process



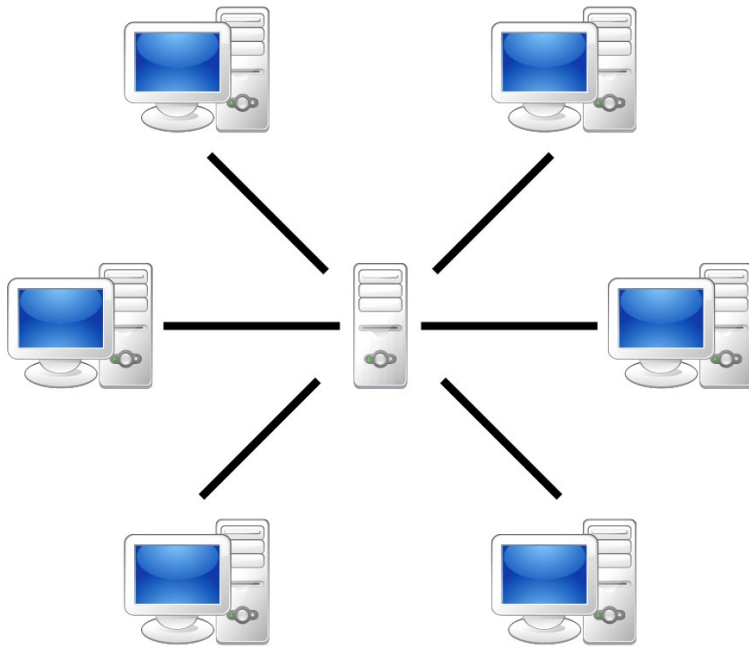
Blockchain Validation Process

The architecture of Blockchain

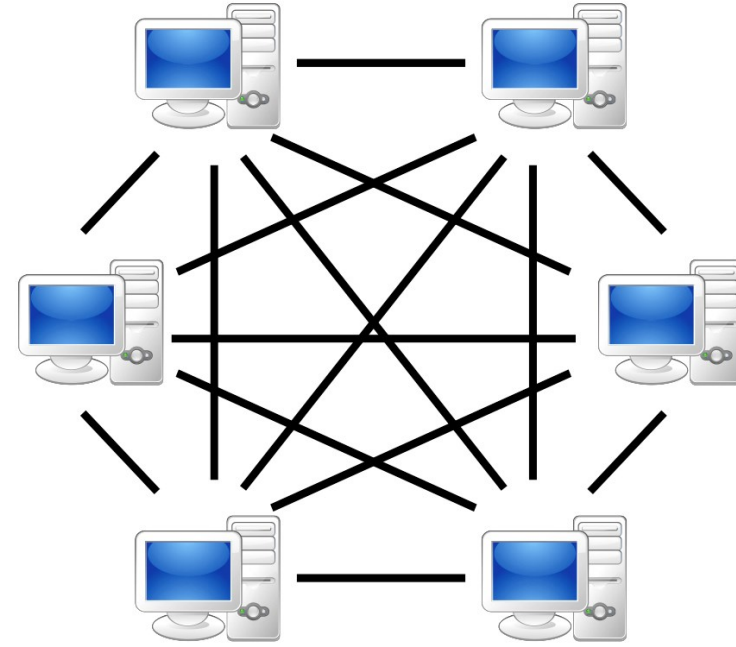


The architecture of Blockchain

■ Network Layer

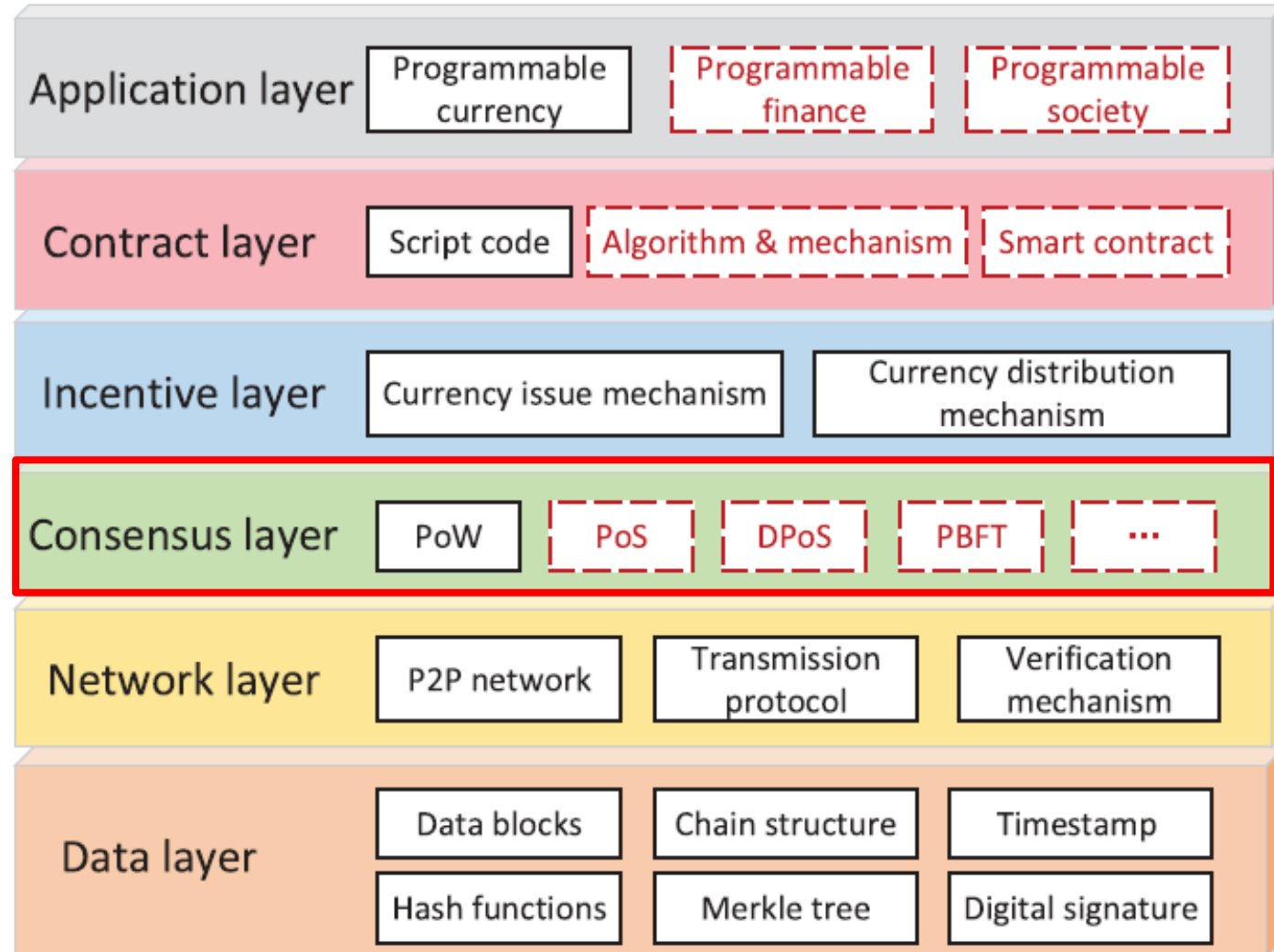


Server-based



P2P-network

The architecture of Blockchain



The architecture of Blockchain

■ Consensus Layer

- A good consensus mechanism ensures a robust transaction ledger with two important properties: **persistence and liveness**.
 - Persistence guarantees the consistent response from the system regarding the state of a transaction.
 - Liveness states that all nodes or processes eventually agree on a decision or a value

The architecture of Blockchain

■ Consensus Layer

□ Permissionless Blockchains (lottery-based selection)

- **Proof-of-Work (PoW)**
 - PoW is a costly process as the miners compete with each other to solve a mathematical problem
 - fault tolerance
 - dual properties
 - it should be difficult and time-consuming for any prover to produce a proof it should be easy and fast for others to verify the proof.
 - Liveness states that all nodes or processes eventually agree on a decision or a value

The architecture of Blockchain

■ Consensus Layer

□ Permissionless Blockchains (lottery-based selection)

- Proof-of-Work (PoW)
 - Limitations
 - the protocol is an extremely inefficient process due to high computation complexity and low probability of successful generation of the proof of work.
 - It is difficult to ensure the robustness of the PoW blockchain protocol (persistence and liveness)
 - due to the various computational capacities of participants and thus different probabilities of successful rates in generating proof of work

The architecture of Blockchain

■ Consensus Layer

□ Permissionless Blockchains (lottery-based selection)

- **Proof-of-Stake (PoS)**
 - A validator is selected in a pseudorandom fashion, with the probability of being selected proportional to the validator's share in the network
 - fault tolerance
 - In PoS, the forger node is discouraged from fraudulent transaction validation because it affects its reputation, and consequently, reducing its stake value.

The architecture of Blockchain

■ Consensus Layer

□ Permissionless Blockchains (lottery-based selection)

- Proof-of-Stake (PoS)
 - PoW - security from rewards of burning computational energy
 - PoS - security from penalties of putting up economic value-at-loss
 - Limitation
 - The richest member has a permanent advantage of putting the largest deposit at stake
 - In 2017, **Ethereum** began the process of switching from a PoW mechanism to a PoS system (DPoS)

The architecture of Blockchain

■ Consensus Layer

□ Permissionless Blockchains (lottery-based selection)

- Proof-of-Activity (PoA)
 - This is the **integration of PoW and PoS**. Computational puzzle solving in PoA only involves finding a PoW against the block header, without the transactions in the block. A random group of validators are chosen to vote on the validity of the mined block header (PoS)
 - Limitation
 - It requires higher computational power, and a naive implementation can be prone to nothing at stake attacks.

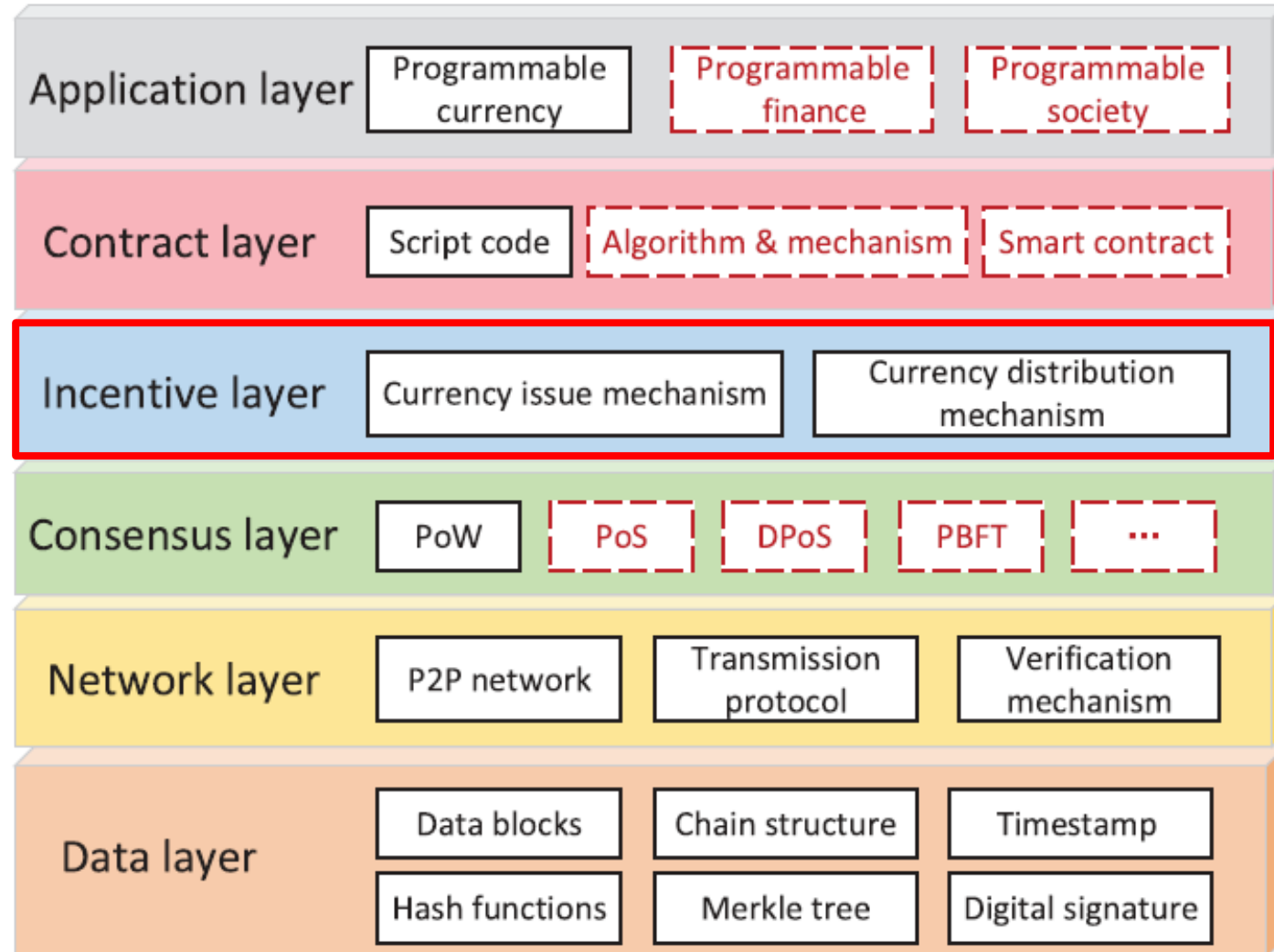
The architecture of Blockchain

■ Consensus Layer

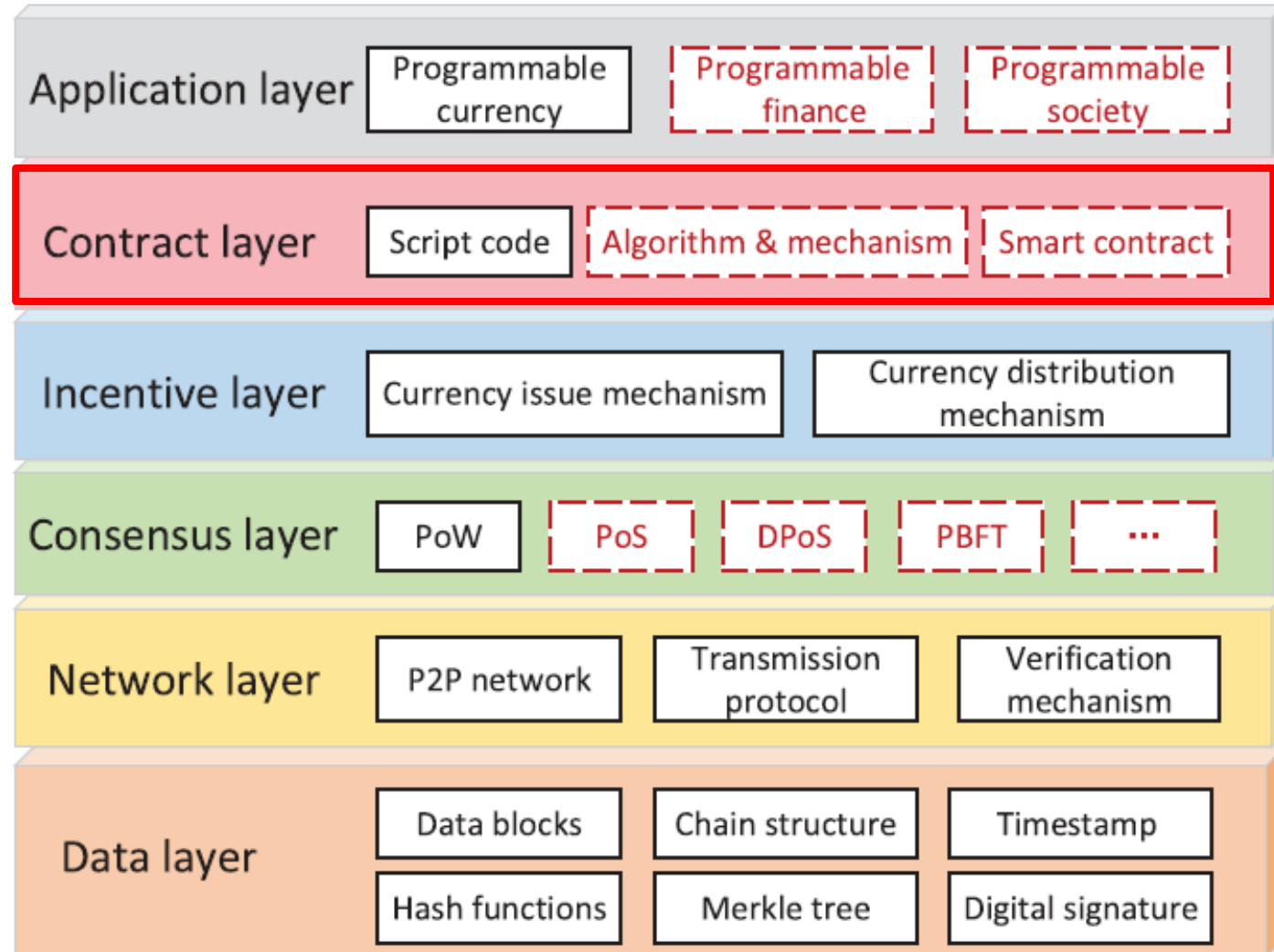
□ Permissioned Blockchains

- only a **limited number of known participants carry a copy of the entire blockchain.**
permissioned blockchains have a much higher performance than permissionless blockchains
 - **Practical Byzantine Fault Tolerance (PBFT) (Hyperledger Fabric)**
 - one node is chosen to be the “leader,” who assembles a set of ordered transactions into a block and broadcasts it to the network. It involves multiple rounds of voting by all nodes of the network, in order to commit state changes.

The architecture of Blockchain



The architecture of Blockchain



The architecture of Blockchain

■ Smart contract

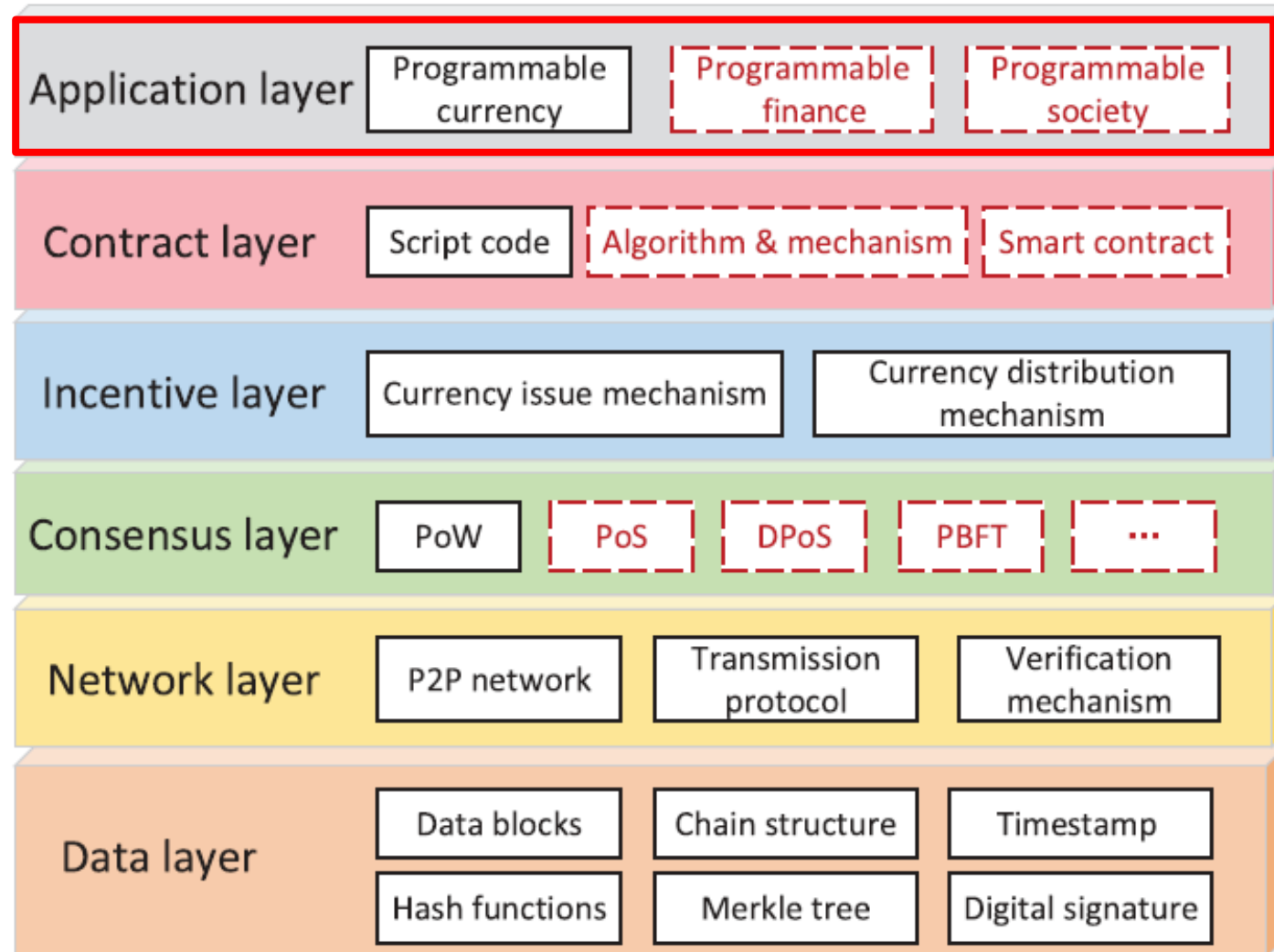
- ❑ Smart contracts are **programmable applications** stored in the blockchain, that **manage transactions under specific terms and conditions**.
- ❑ Smart contract code is stored in the blockchain, and the **functions written in the smart contract can be invoked by any participant at any time**.

The architecture of Blockchain

■ Smart contract

- Smart contracts can be utilized to perform a variety of functions within a blockchain network
 - Allowing 'multi-signature' transactions
 - Enabling automated transactions triggered by specific events
 - Providing utility to other smart contracts
 - Allowing storage space for application-specific information
 - smart contract scripting languages
 - Serpent and Solidity (Ethereum), Go (Hyperledger Fabric)
 - [Smart Contracts - EVM based Blockchain Development-part 11_哔哩哔哩_bilibili](#)

The architecture of Blockchain



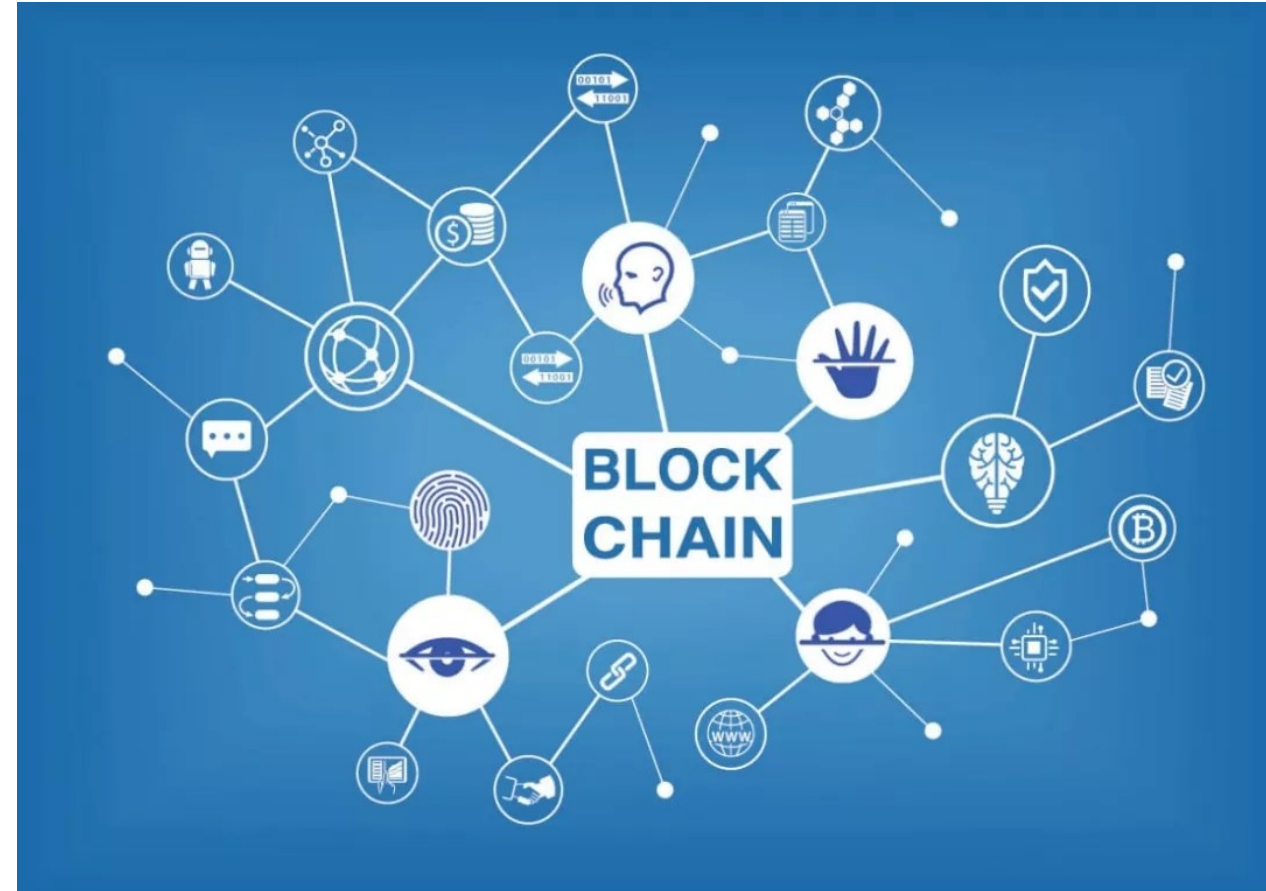
The Application of Blockchain



The Application of Blockchain

■ Criteria

- ❑ Immutability
- ❑ Visibility and Transparency
- ❑ Trust
- ❑ Identity
- ❑ Distribution
- ❑ Workflow
- ❑ Transaction
- ❑ Historical record
- ❑ Ecosystem
- ❑ Efficiency



The Application of Blockchain

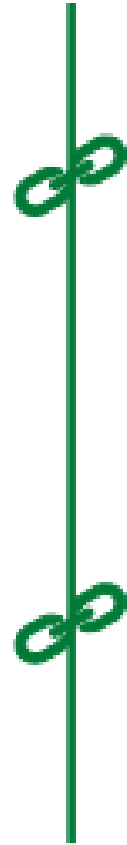
■ Criteria

1.Immutability

(不变性)

Whether support data updates?

Blockchain:
Cannot tamper the data,
Large consumption of resources

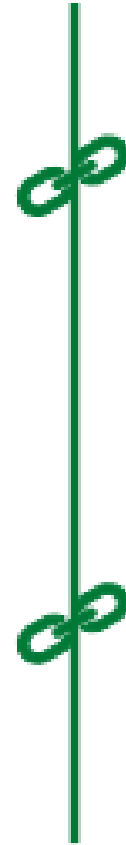


2.Visibility and Transparency

(可见性和透明性)

Whether make data transactions public?

Blockchain:
Visible and transparent,
Verified

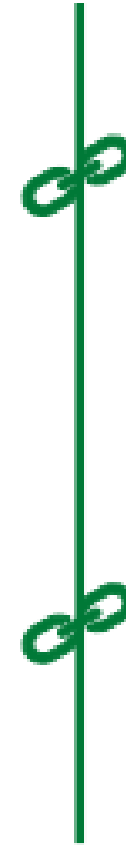


3.Trust

(信任)

Whether rely on a trust server?

Blockchain:
Decentralized, Trust,
Multi-party collaboration



4.Identity

(身份)

Whether need anonymous?

Blockchain:
Anonymity,
Digital signature

The Application of Blockchain

■ Criteria

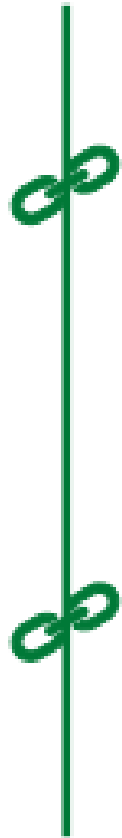
5.Distribution

(分布性)

Whether can be decentralized?

Blockchain:

Guarantee robustness, security and integrity



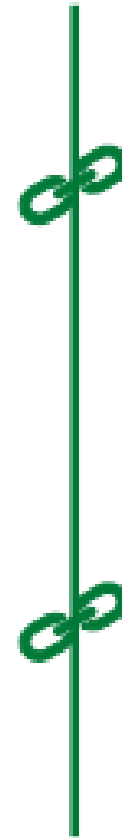
6.Workflow

(workflow)

Whether tolerant the delay, Support transaction cancellation.?

Blockchain:

Delay (Verified), cannot tamper



7.Transaction

(交易)

Whether need transaction between each other?

Blockchain:

Trade with everyone and everywhere

The Application of Blockchain

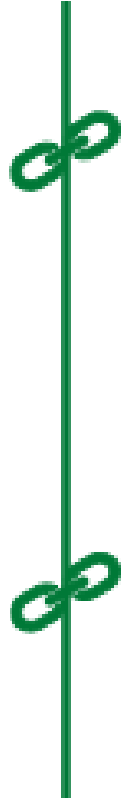
■ Criteria

8. Historical record (历史纪录)

Whether can share the log or historic records?

Blockchain:

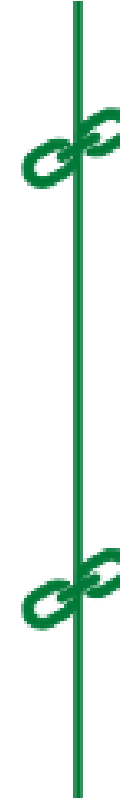
All records are public, Not suitable for storing sensitive information



9. Ecosystems (系统性)

Blockchain:

Develop a trust environment, more suitable for the system is not a single entity



10. Efficiency (效率)

Whether guarantee the efficiency?

Blockchain:

Blockchain implementation is inefficient
Complex data structures and high computational and storage overhead

The Application of Blockchain

■ Applications of blockchain in Internet of Things(IoT)

□ Issues and Challenges in the IoT

- Cybersecurity
 - IoT devices are commonly **isolated hardware** solutions
 - IoT devices have typically **limited computational power**
 - a generic **'one-size-fits-all' security model** is difficult to implement
- Privacy
 - The huge amount of data generated by IoT devices may offer detailed information about the context where users live, and about their habits (**without any explicit user consent, shared by third parties or IoT platforms**)

The Application of Blockchain

■ Applications of blockchain in Internet of Things(IoT)

□ Issues and Challenges in the IoT

- Massive Data Management
 - The volume of data generated by IoT devices can be enormous and difficult to manage in terms of elaboration, communication/transmission, and storage.
- Lack of Standardization and Interoperability
- Lack of Skills

The Application of Blockchain

■ Applications of blockchain in Internet of Things(IoT)

□ Decentralizing the IoT Through Blockchains

- The aim of the IoT is to have smart objects **communicate over the Internet** to collect comprehensive data and **provide personalized automation services**, with **little deliberate human interaction**

The Application of Blockchain

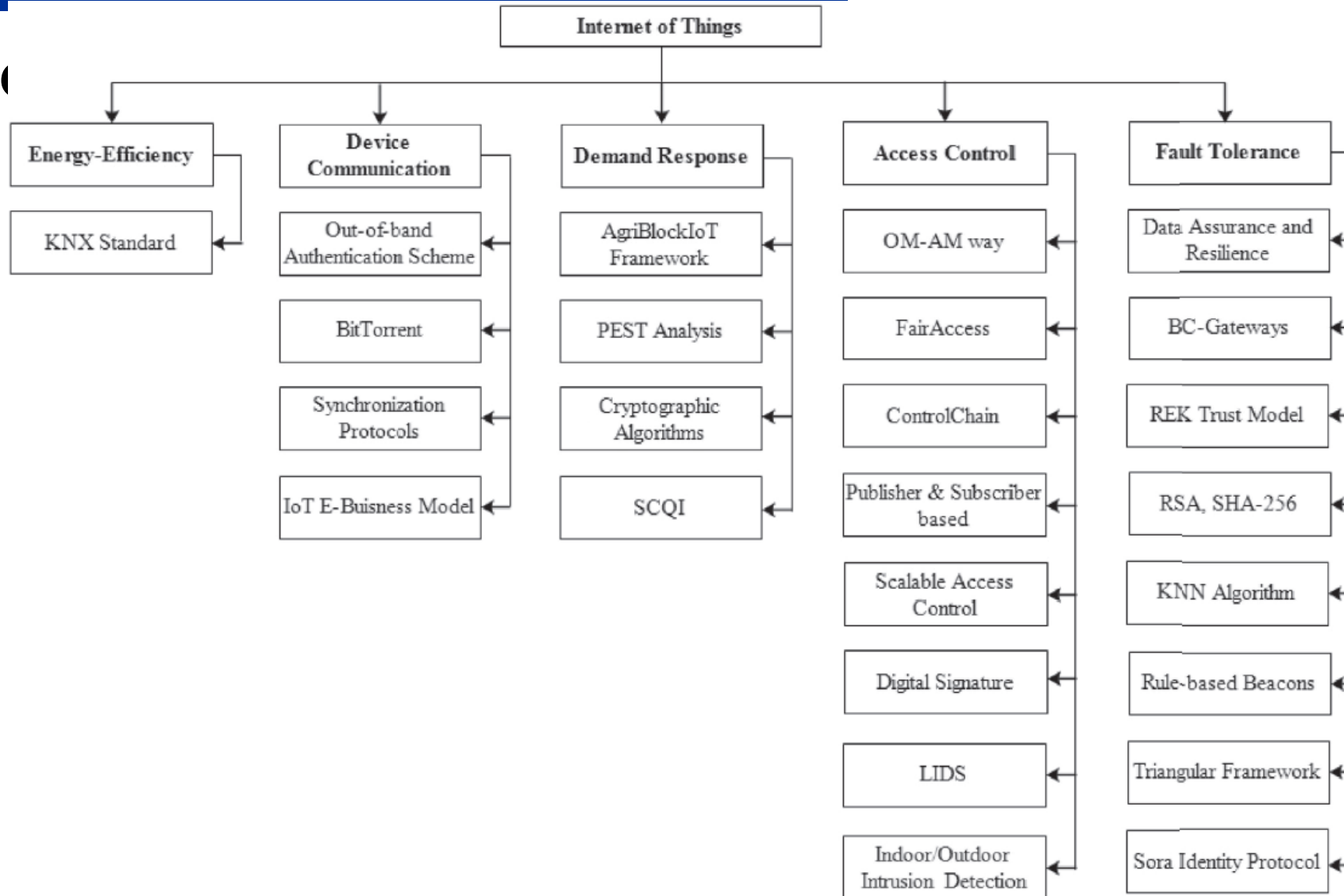
■ Applications of blockchain in Internet of Things(IoT)

□ Decentralizing the IoT Through Blockchains

- benefits and motivations
- **Resilience:** IoT applications require **integrity in the data** being transferred and analyzed, therefore IoT frameworks need to **be resilient to data leaks and breakage**.
- **Adaptability:** the heterogeneity of IoT devices and protocols **limit their interoperability**, using blockchains as the network control mechanism for the IoT will add a greater degree of adaptability to it.
- **Fault tolerance:** Network control mechanisms for the IoT **require high availability**. Blockchains are Byzantine fault tolerant record-keeping mechanisms that can **identify failures** through distributed consensus protocol.
- **Security and privacy:** blockchains have **pseudonymity in its addressing** and distributed consensus for **record immutability**.
- **Reduced maintenance costs:** Public blockchains applications utilize the **computational and storage capabilities of its participants**.

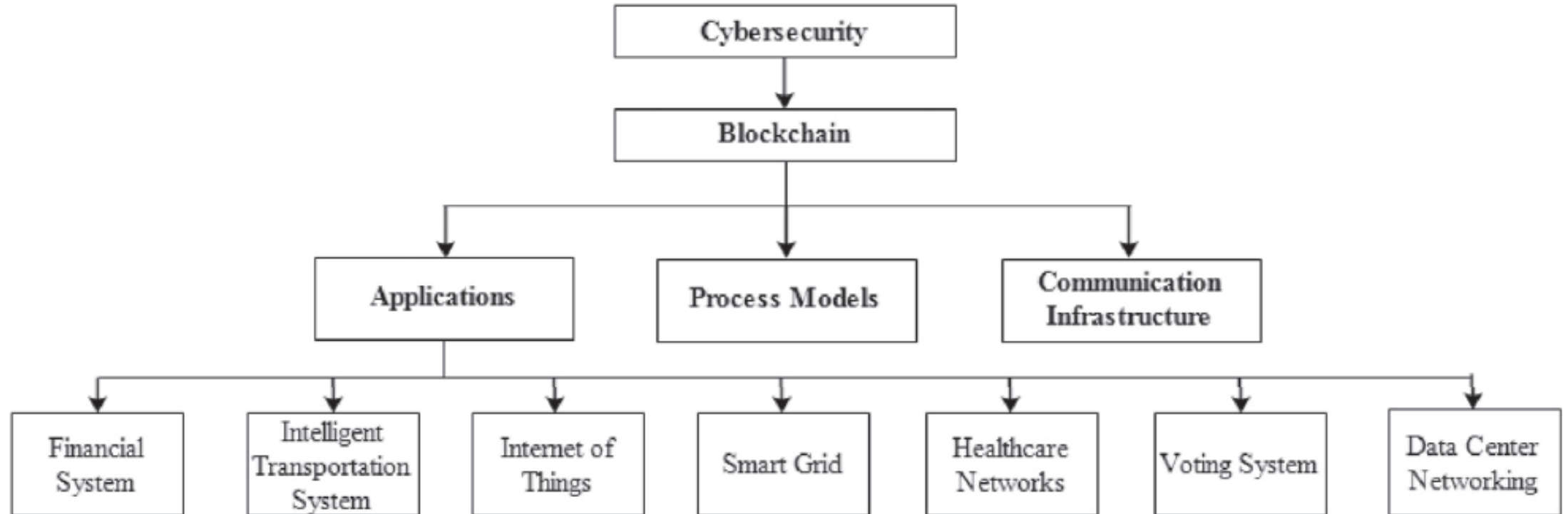
The Application of Blockchain

■ blockchain



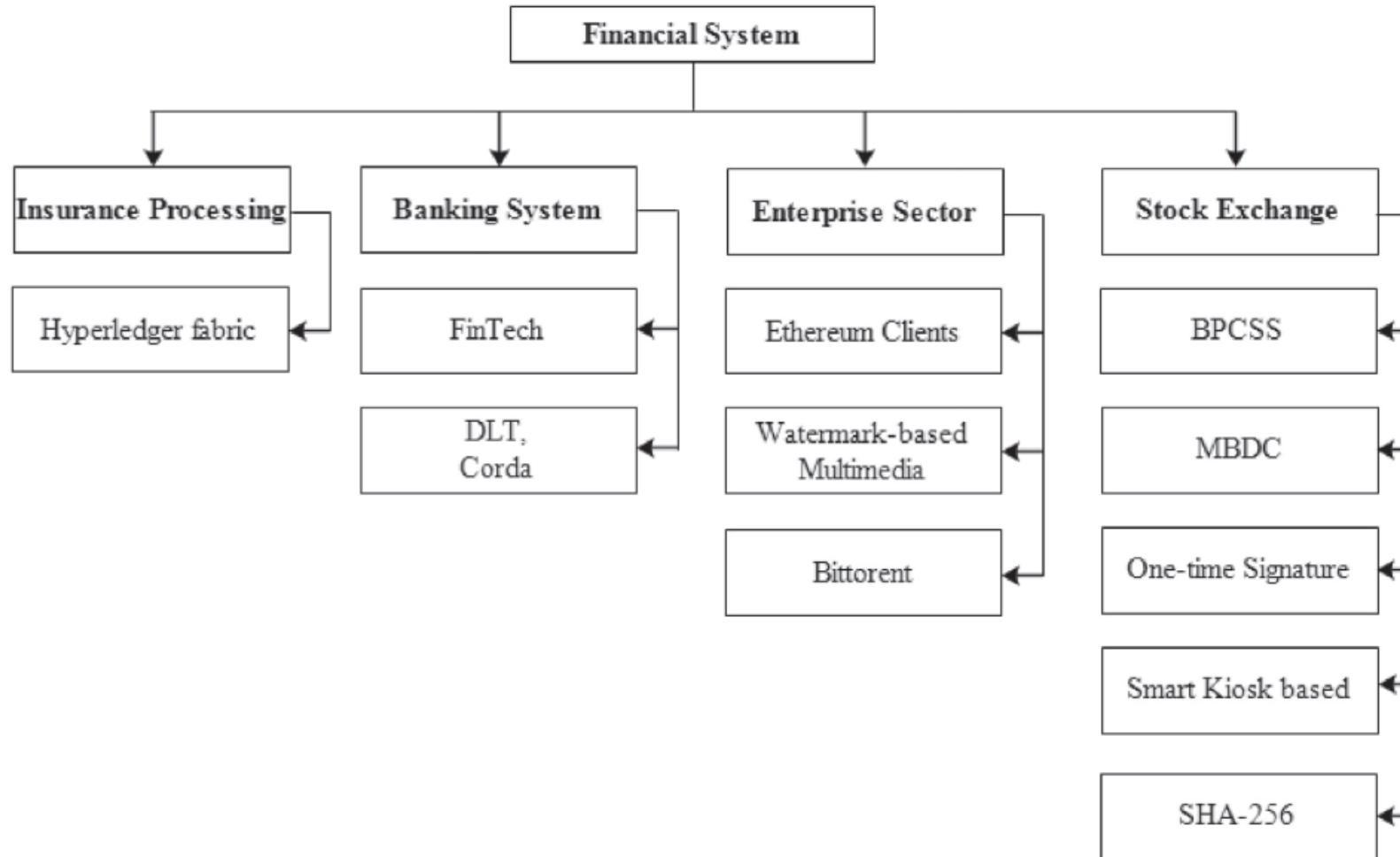
The Application of Blockchain

■ Applications of blockchain in cybersecurity



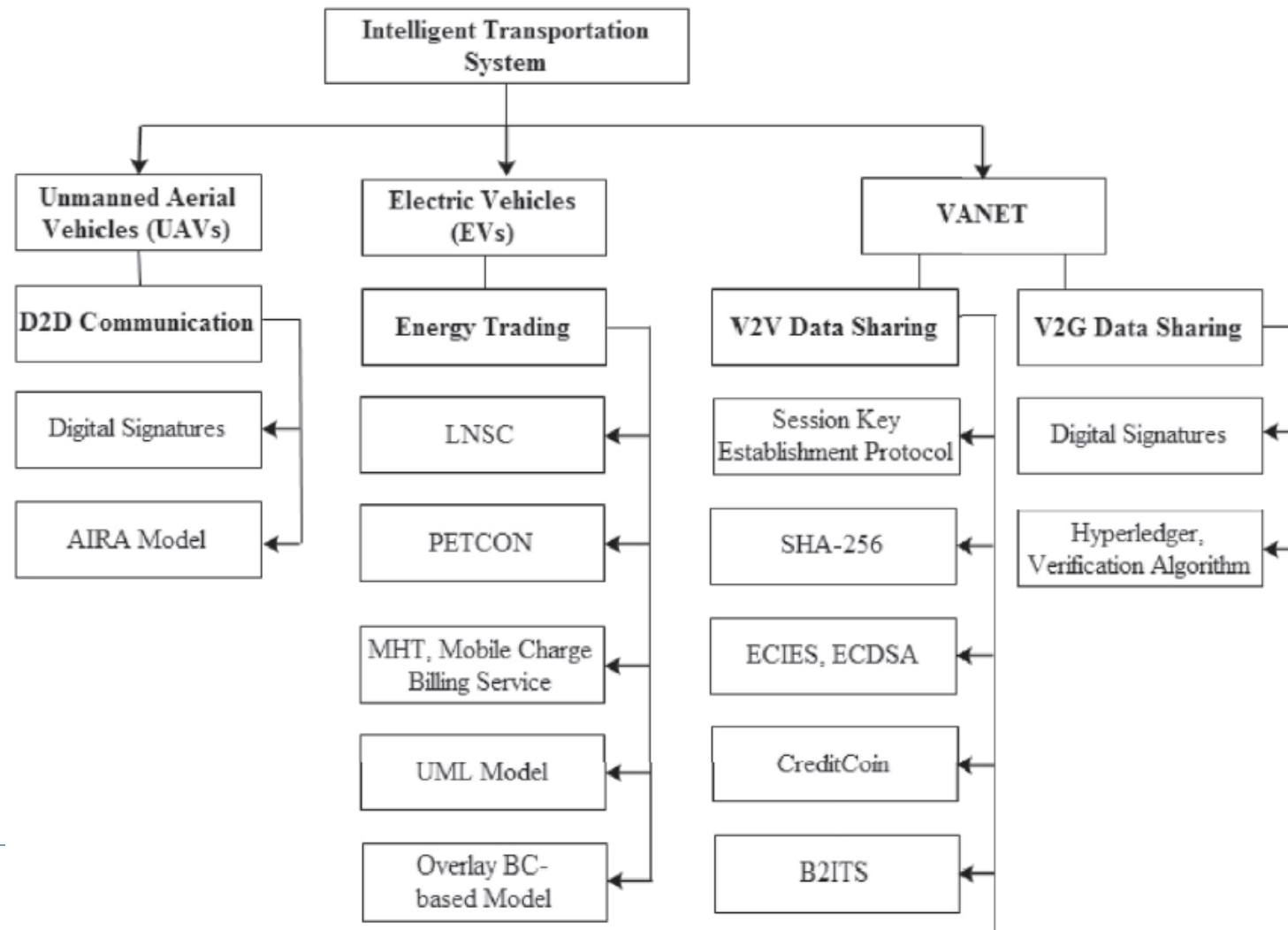
The Application of Blockchain

■ blockchain-based financial system



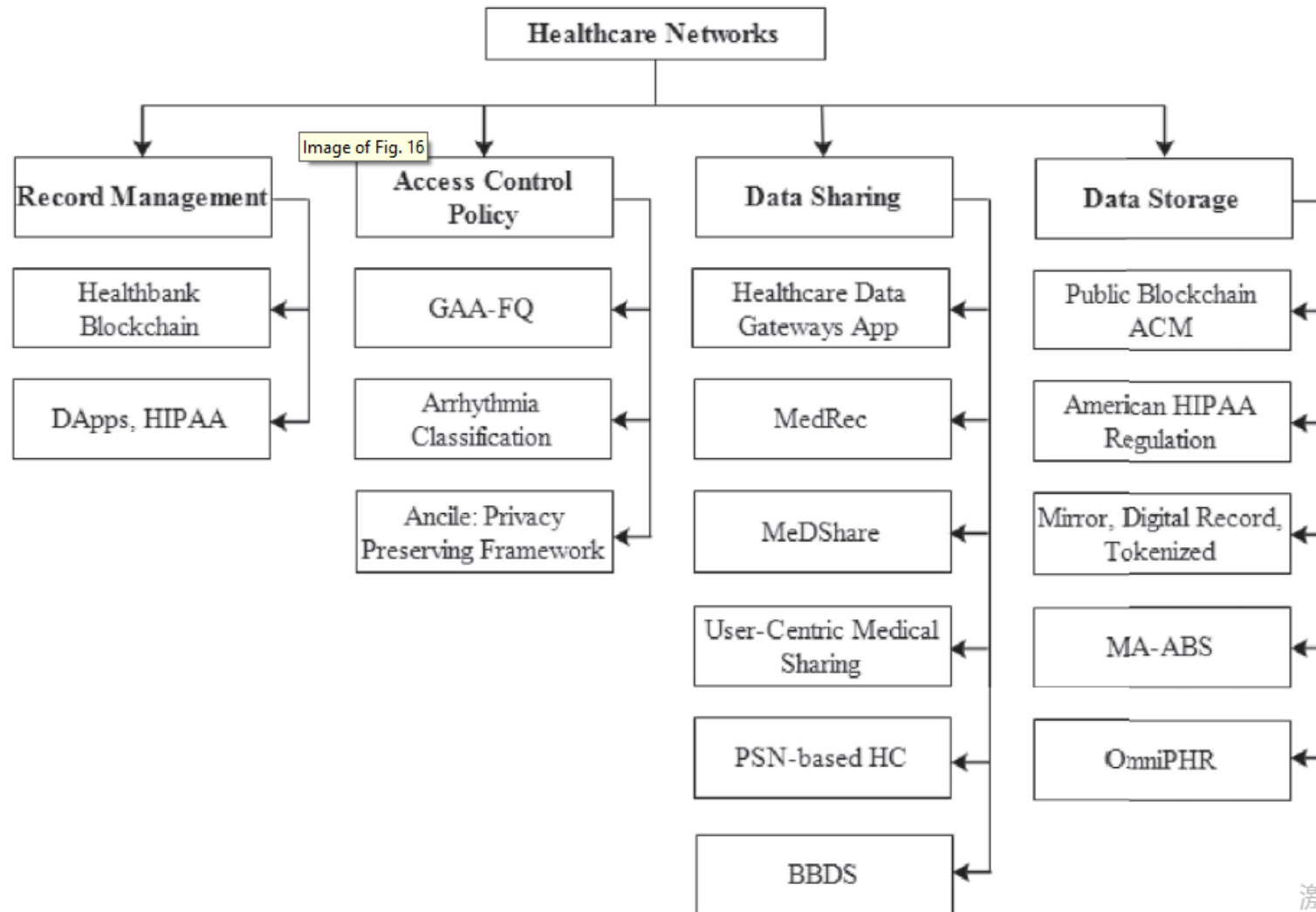
The Application of Blockchain

■ blockchain-based intelligent transportation system



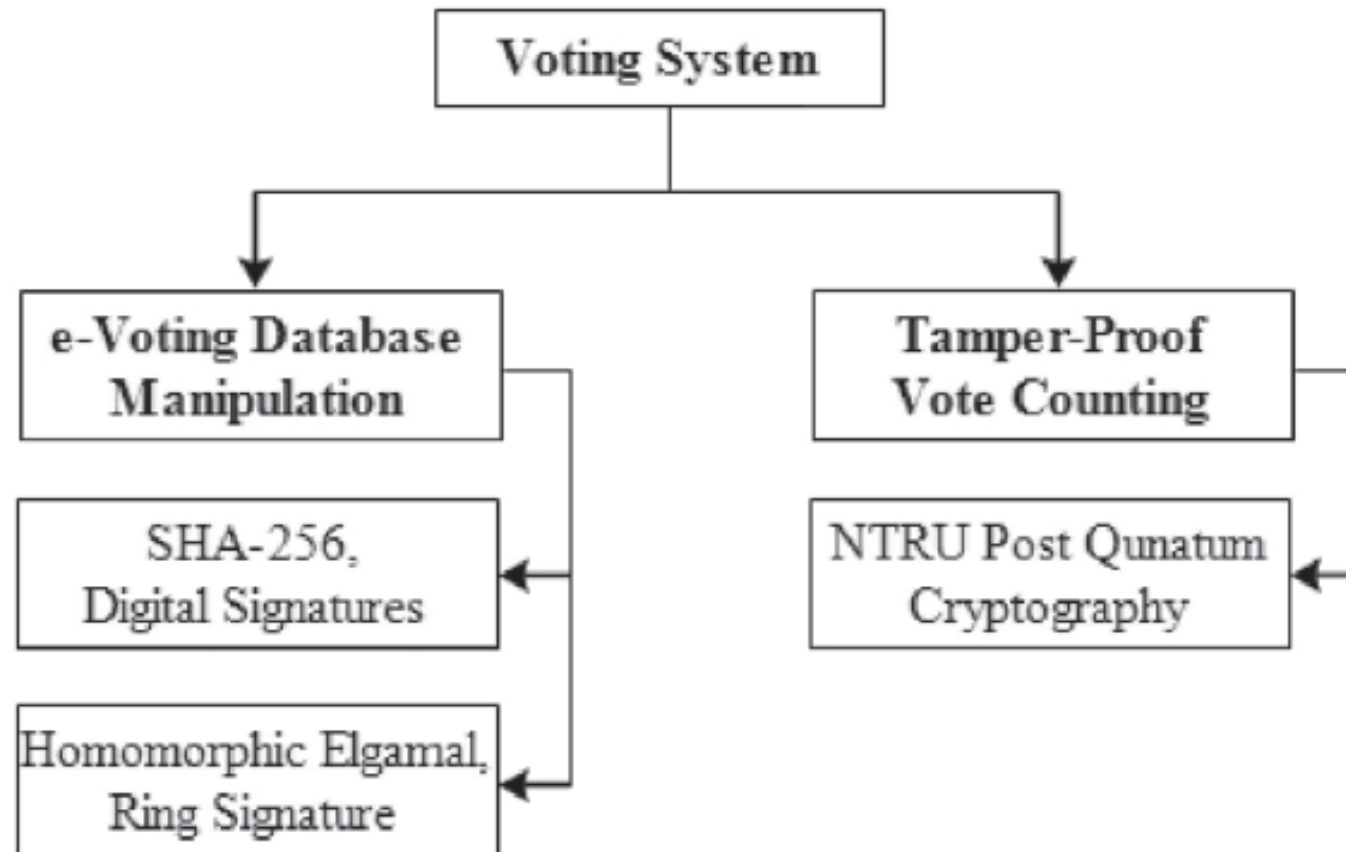
The Application of Blockchain

■ blockchain-based Healthcare Networks



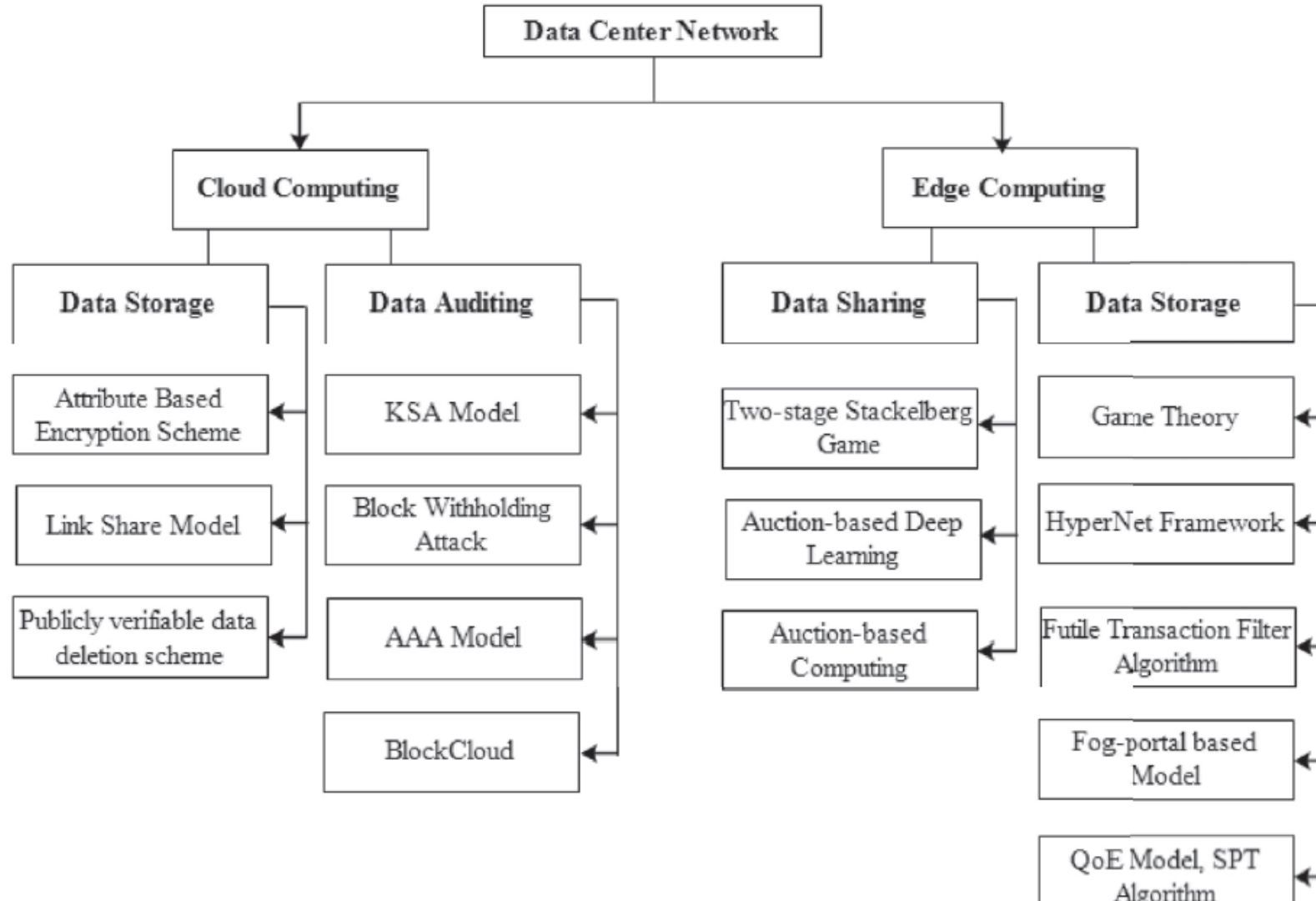
The Application of Blockchain

■ blockchain-based Voting System



The Application of Blockchain

■ blockchain-based Data Center Network



The Application of Blockchain

■ Blockchain Application Use Cases

- https://www.bilibili.com/video/BV1ss4y1X7hk/?spm_id_from=333.337.search-card.all.click&vd_source=b533ec11d1f387db0855d15bf81fd732

The Application of Blockchain

■ Blockchain Platforms

Platform	Network Type	Purpose	Prog. Language	Crypto-currency	Consensus Mechanism	Smart Contract enabled	Transaction Cost for mining	Applications
Ethereum (Ethereum Blockchain APP Platform, 2018)	public/private, permissionless	B2C businesses	Smart Contract code written in Solidity	in-built (Ether)	PoW (PoS- in future)	yes	yes (high)	banking, commodity trade finance, supply chain management, insurance, energy grid, oil & gas, real estate)
R3Corda (Corda, 2018)	private, permissioned	B2B businesses	Smart Contract code written in Kotlin, Java	not in-built	pluggable (voting process, BFT)	yes	no	banking, financial services
Hyperledger Fabric (Hyperledger, 2018)	private, permissioned	P2P, B2C operations	Chaincode written in GoLang, Java	not in-built (can be modeled in chaincode)	pluggable (PBFT)	yes	no	supply chain for pharmaceuticals, trade financing, smart energy, supply chain management
MultiChain (Multichain, 2018)	private, permissioned	B2B operations	Python, C#, JavaScript, PHP, Ruby	not in-built	PBFT	no	no	financial transactions, e-commerce
HydraChain (Hydrachain, 2019)	private, permissioned	B2B operations	Python based smart contracts	not in-built	BFT	yes	no	financial services
Openchain (Openchain, 2017)	private, permissioned	P2P, B2B operations	Javascript	not in-built	partitioned consensus	yes	no	digital asset management
IBM Blockchain (IBM, 2018)	Private, permissioned	B2B operations	GoLang, Javascript	not in-built	pluggable (PoW)	yes	yes (low)	healthcare payments, trade and supply chain finance
IOTA (IOTA, 2018)	Public	B2B operations	Python, C, Javascript	not in-built	PoW, PoS	no	no	financial, telecommunication, intelligent energy, e-healthcare
Bitcoin (Bitcoin, 2018)	public/private, permissionless	B2B, B2C operations	C++	in-built (bitcoin)	PoW	yes	yes (high)	government, financial, audit trails
Litecoin (Litecoin, 2018)	public/private, permissionless	B2B, B2C operations	C++	in-built (litecoin or LTC)	PoW	yes	yes (low)	banking, financial services
BigchainDB (BigchainDB 2.0 The Blockchain)	public/private, permissionless	B2C operations	SQL, NoSQL	no-inbuilt	BFT, federation with voting permissions	yes	no	intellectual property, human resources, identity verification, supply chain

Thanks!
