Blockchain Overview and Architecture

Dr. Ruba Awadallah

Blockchain History

- **1991:** Scientists introduce Blockchain Technology by proposing time-stamping which is a Computational practical Solution (digital documents) that insure no one can temper the produced data or misdate.
- **1992:** Blockchain Technology became efficient to store several documents to be collected into one block. Merkle used a Secured Chain of Blocks that stores multiple data records in a sequence.
- **2000:** a theory of cryptographic secured chains, plus ideas for implementation has been published.
- **2004:** “Reusable Proof of Work” has been proposed this System helps others to solve the Double Spending Problem by keeping the ownership of tokens registered on a trusted server.

Blockchain History

- **2008:** Satoshi Nakamoto conceptualized the concept of “Distributed Blockchain” in his white paper: ”A Peer to Peer Electronic Cash System”. He modified the model of Merkle Tree and created a system that is more secure and contains the secure history of data exchange. His System follows a peer-to-peer network of time stamping. His system became so useful that Cryptography became the backbone of Blockchain.

- **2009:** Satoshi Nakamoto Releases Bitcoin White Paper. People who were mining Bitcoin at a low cost at the time are now millionaires.

- **2014:** 2014 was a turning point for blockchain technology. Blockchain technology was separated from currency and Blockchain 2.0 was born. Financial institutions and other industries began shifting their focus from cryptocurrency to blockchain development.

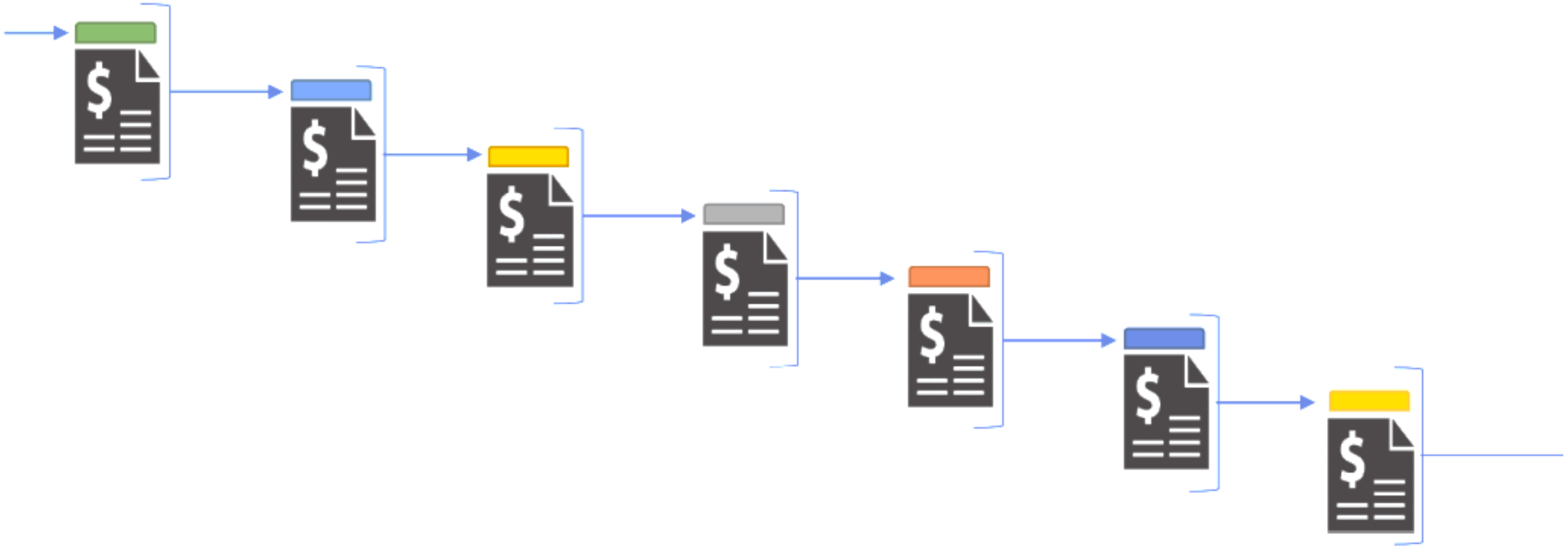
- **2015:** In 2015, the Ethereum Frontier network was launched, enabling developers to write smart contracts and decentralized applications that could be deployed on a live network.

What is Blockchain ?

Blockchains are distributed digital ledgers of cryptographically signed transactions that are grouped into blocks. Each block is cryptographically linked to the previous one (*making it tamper evident*) after validation and undergoing a consensus decision. As new blocks are added, older blocks become more difficult to modify (creating tamper resistance). New blocks are replicated across copies of the ledger within the network, and any conflicts are resolved automatically using established rules.

Note: The terms “blockchain” and “distributed ledger” are often used interchangeably.

How is It Built?



- Periodically transactions are wraps up as a block.
- Each block depends on the previous block making a chain from the origin.
- To edit a transaction in a block would require recalculation of all blocks after it.
- Normally uses a distributed ledger with a consensus system and public/private key cryptography

1- Consensus

❑ Prevents “double spend” or validation of fraudulent transactions through:

- Proof of work: miners compete to validate blocks by solving intensive cryptographic problems for rewards
- Distributed Consensus: majority validation by trusted subnetworks of peer nodes within the network.
- Proof of Stake: achieves distributed consensus by network users proving their ownership of the currency

2- The Ledger

- Often referred to as the “Blockchain”, this is a public record of all transactions stored across a distributed Peer-to-Peer (P2P) network of servers.
- Verified transactions are added to “blocks” and the history provides proof of value or assets “owned”

Reward or Incentives

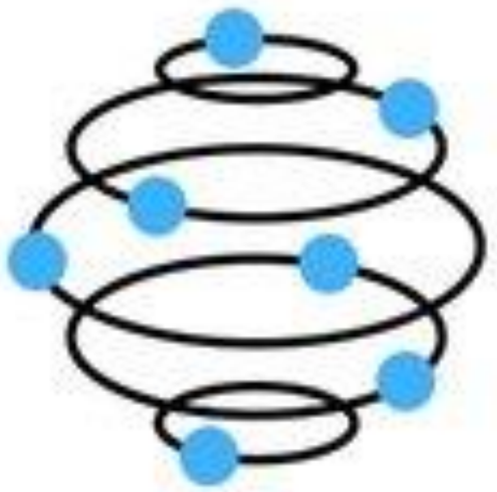
- A medium for transaction settlement within the network that rewards miners.
- Examples include “Bitcoin” – so miners are rewarded for processing transactions and providing a stable network.
- Rewards are cryptographically generated, and the protocol rules determine the issuance of the rewards.
- Rewards are required to ensure network security.

Blockchain Architectures

- Blockchain-based architectures can be integrated into many IoT applications with different requirements and restrictions.
- We will classify blockchain-based architectures according to *access and control mechanisms*.
- According to the access mechanisms, blockchains are categorized into three classes: public, private, and consortium.

Public Blockchains:

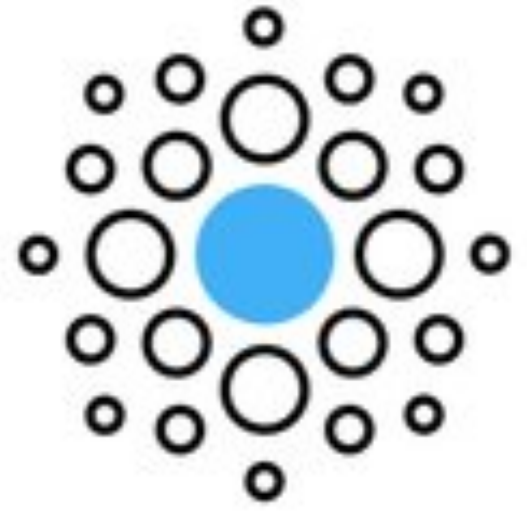
- In a public blockchain, anyone can join the network and access the transaction history recorded on the blockchain.
- Every node in the network has a copy of the distributed ledger.
- Public blockchains are resilient against attacks and node failures due to the redundancy in the network and the consensus mechanism.
- Network participants may earn economic incentives for contributing to the consensus mechanism such as proof-of-work or proof-of-stake.
- Examples of public blockchains include Bitcoin, Ethereum, and Litecoin.



Public Blockchain

Private Blockchains:

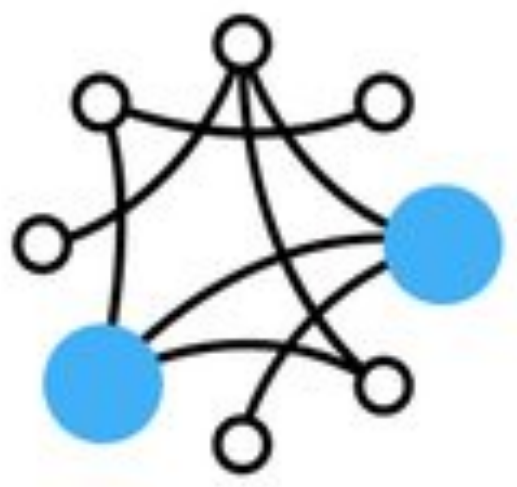
- In a private blockchain, a single organization controls the blockchain by determining the rules of the network and access permissions.
- Trust is centralized at the owner, yet there may be partial decentralization among many nodes managing blockchain that are controlled by the owner.
- By only letting the nodes with access permissions read the transactions on the blockchain, privacy of the transactions is improved.
- The consensus is established by the trusted entity, which improves the efficiency and results in faster transactions.
- The private blockchain architecture is more suitable for companies or government applications.



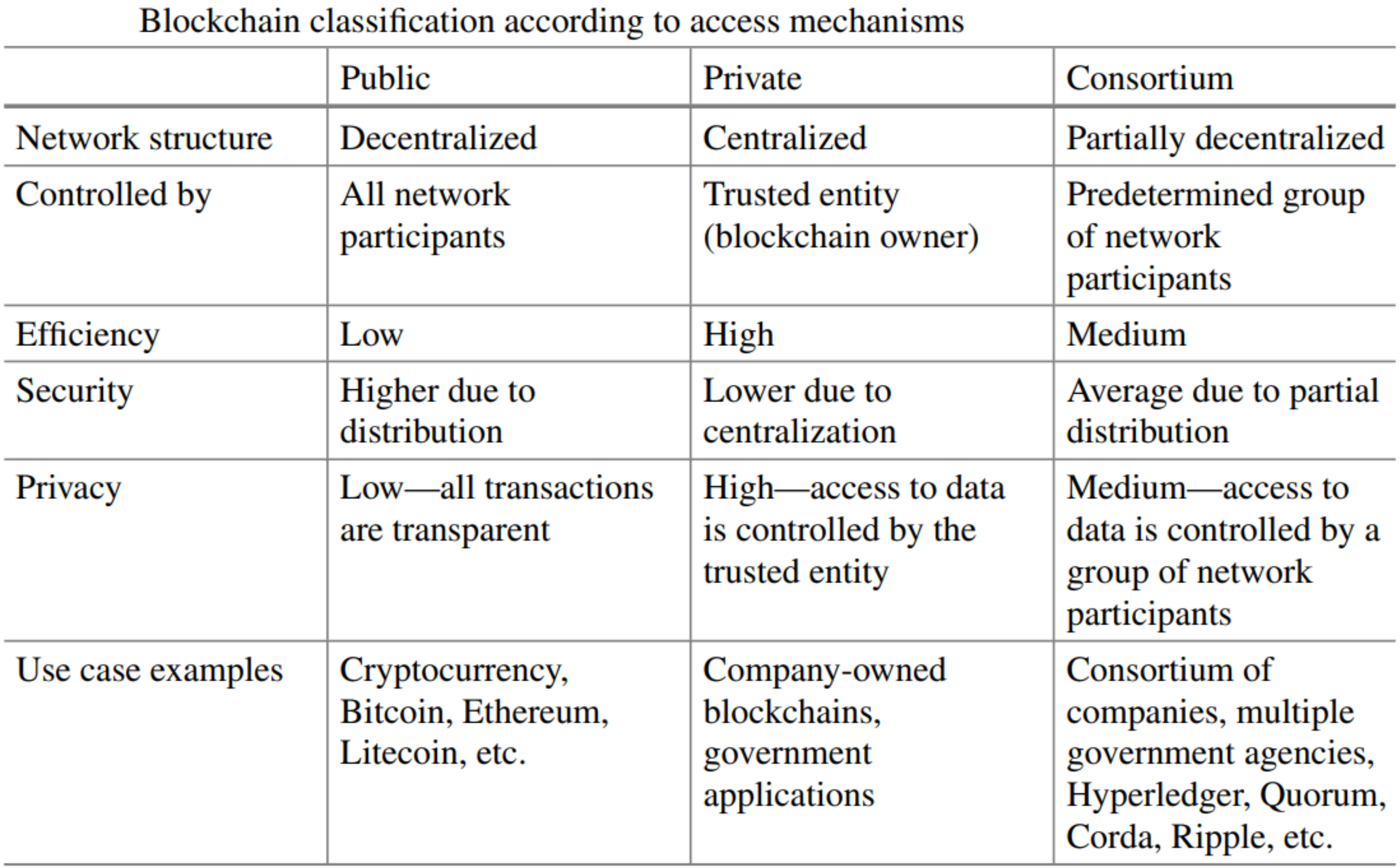
Private Blockchain

Consortium Blockchains:

- Consortium blockchains are developed for applications that involve a group of participants interacting with each other, where the consensus mechanism and maintenance of the blockchain are governed by a predetermined group of network participants.
- Consortium blockchains help the standardization of communication and transactions between the participating nodes.
- The access mechanism of the consortium blockchain defines the rules of access to the blockchain information.
- Similar to private blockchains, consortium blockchains are more efficient and provide higher transaction privacy than public blockchains.
- Consortium blockchains are suitable for applications that involve multiple companies or agencies.



Consortium Blockchain

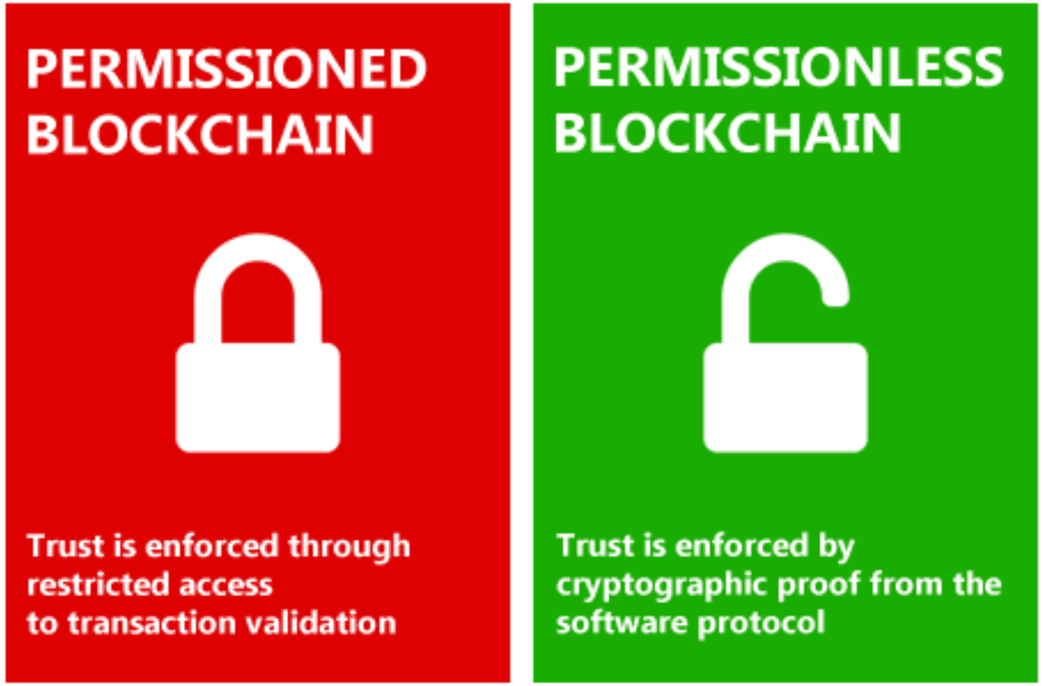


Blockchain classification according to access mechanisms

	Public	Private	Consortium
Network structure	Decentralized	Centralized	Partially decentralized
Controlled by	All network participants	Trusted entity (blockchain owner)	Predetermined group of network participants
Efficiency	Low	High	Medium
Security	Higher due to distribution	Lower due to centralization	Average due to partial distribution
Privacy	Low—all transactions are transparent	High—access to data is controlled by the trusted entity	Medium—access to data is controlled by a group of network participants
Use case examples	Cryptocurrency, Bitcoin, Ethereum, Litecoin, etc.	Company-owned blockchains, government applications	Consortium of companies, multiple government agencies, Hyperledger, Quorum, Corda, Ripple, etc.

Permissioned Versus Permissionless Participation Mechanisms

- According to their control mechanisms, blockchains can be classified as permissionless or permissioned.



PERMISSIONED BLOCKCHAIN

Trust is enforced through restricted access to transaction validation

PERMISSIONLESS BLOCKCHAIN

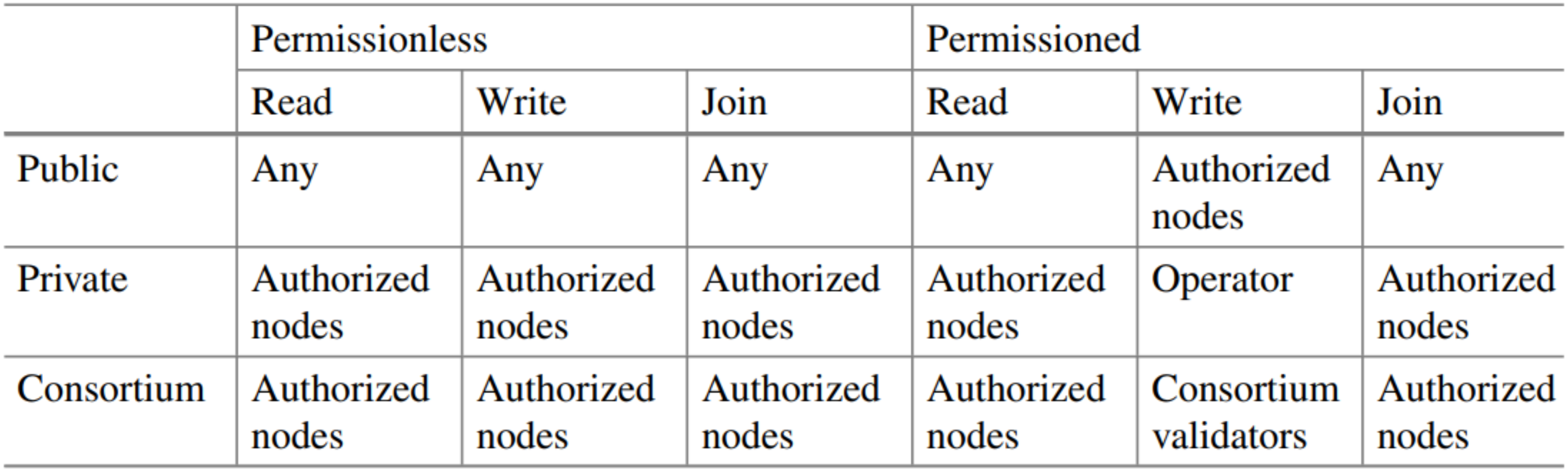
Trust is enforced by cryptographic proof from the software protocol

Permissionless Blockchains:

- Any node can join the blockchain and participate in creating and verifying transactions, contributing to the consensus mechanism.
- Permissionless blockchains use tokenized incentives for establishing consensus and network participants earn monetary or utility tokens for their contributions in the consensus mechanism.
- With no central control and distributed structure, permissionless blockchains have resilience against attacks.
- The network operation is transparent so that network participants know how the blockchain works and how consensus is achieved.
- Permissionless blockchains may have lower scalability and suffer from slower transaction times and lower throughputs. Permissionless blockchains have use cases for consumer-to-consumer and business-to-consumer interactions.

Permissioned Blockchains:

- The participating nodes are predefined, and they have permissions to participate in the blockchain.
- Permissioned blockchains allow an organization or a group of organizations to record communications, events, and transactions in an immutable manner.
- The blockchain is controlled by an organization or a group of organizations, and the level of decentralization depends on the structure of the network interactions.
- Permissioned blockchains can use consensus mechanisms that are less computationally expensive. This improves the scalability, transaction times, and network throughput when compared to the permissionless blockchains.
- Permissioned blockchains provide confidentiality of information recorded on the blockchain, which is an appealing feature for business operations. Thus, the main use case for permissioned blockchains is business-to-business interactions.



Control- and access-based blockchain classification

	Permissionless			Permissioned		
	Read	Write	Join	Read	Write	Join
Public	Any	Any	Any	Any	Authorized nodes	Any
Private	Authorized nodes	Authorized nodes	Authorized nodes	Authorized nodes	Operator	Authorized nodes
Consortium	Authorized nodes	Authorized nodes	Authorized nodes	Authorized nodes	Consortium validators	Authorized nodes

☺ Any question