CST 428 BLOCK CHAIN TECHNOLOGIES

S8 CSE – ELECTIVE

MODULE – 2

Fundamentals of Blockchain Technology

Blockchain Definition

Layman's definition: Blockchain is an ever-growing, secure, shared recordkeeping system in which each user of the data holds a copy of the records, which can only be updated if all parties involved in a transaction agree to update.

Technical definition: Blockchain is a peer-to-peer, distributed ledger that is cryptographically secure, append-only, immutable (extremely hard to change), and updateable only via consensus or agreement among peers.

P2P - there is no central controller in the network, and all participants (nodes) talk to each other directly

allows transactions to be conducted directly among the peers without third-party involvement, such as by a bank

Blockchain Definition

Distributed Ledger - ledger is spread across the network among all peers in the network, and each peer holds a copy of the complete Ledger

Append-only

data can only be added to the blockchain in time sequential order

almost impossible to change data in block (immutable)

Blockchain Definition

- **updateable only via consensus - mutual agreement**

contains all sorts of various user level agents and programs that operate on the blockchain

provides executions services on the blockchain and performs operations such as value transfer, smart contract execution, and block generation

Ensures agreement among different participants

Ensures security of block chain

Information propagation layer

Basic communication layer

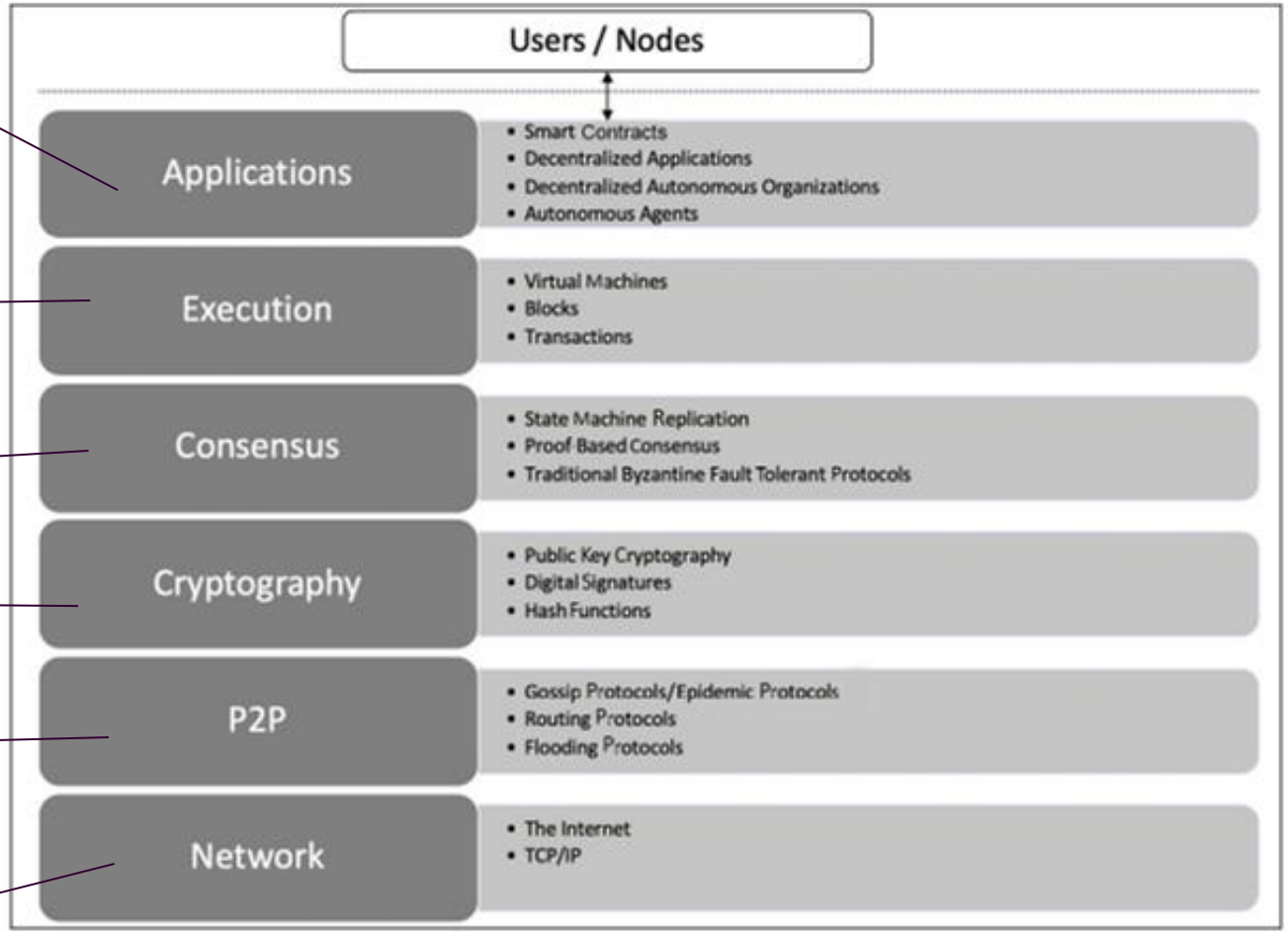


Figure 1.5: The architectural view of a generic blockchain

Blockchain - Generic Elements

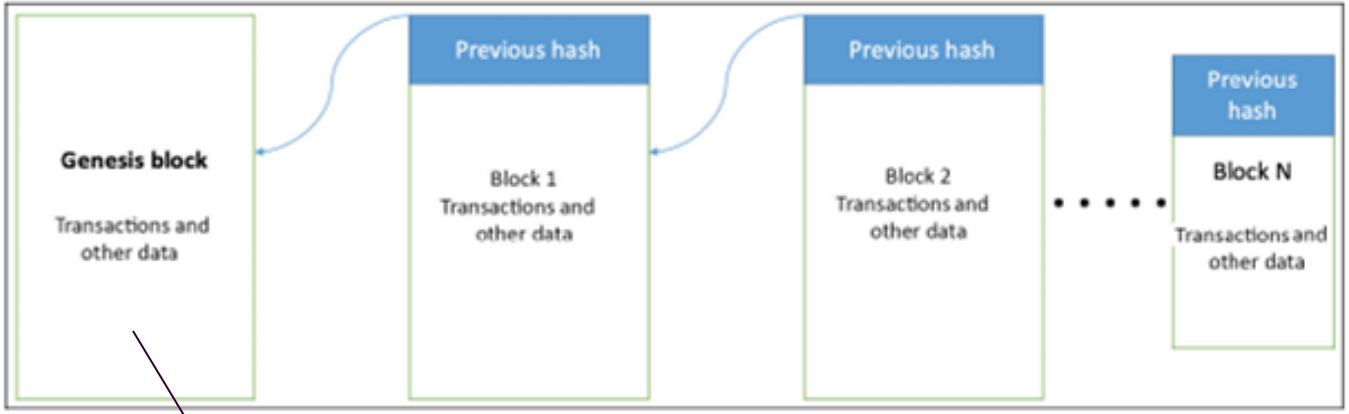


Figure 1.6: Generic structure of a blockchain

- first block in the blockchain that is hardcoded at the time the blockchain was first started
- dependent on the type and design of a blockchain

Blockchain - Generic Elements

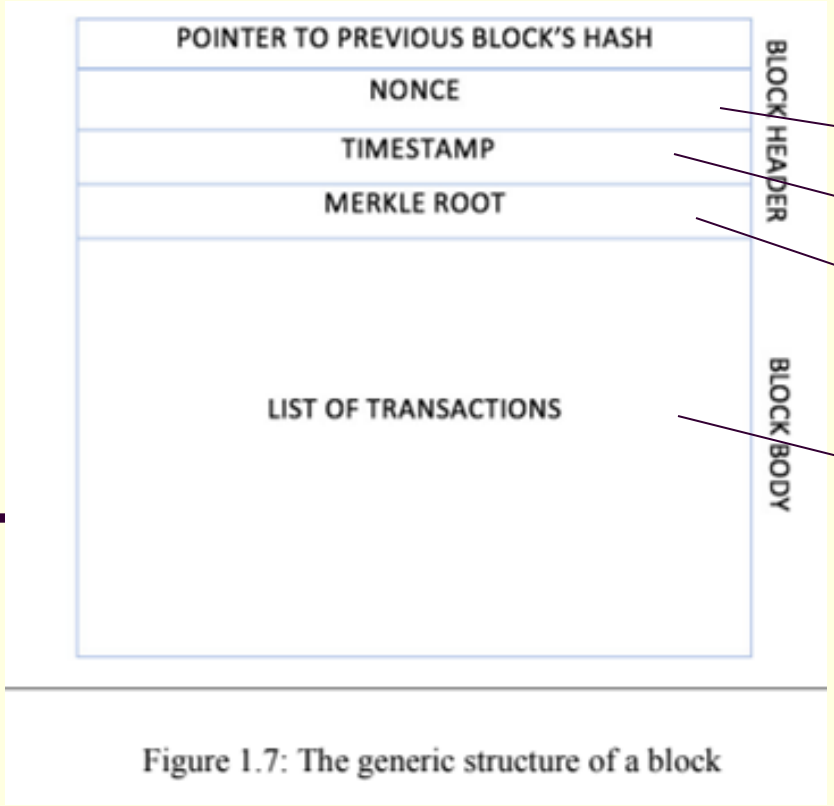


Figure 1.7: The generic structure of a block

a number that is generated and used only once

creation time of the block

hash of all of the nodes of a Merkle tree

record of an event, for example, the event of transferring cash from a sender's account to a beneficiary's account

Blockchain - Generic Elements

Address - unique identifiers used in a blockchain transaction to denote senders and recipients usually a public key or derived from a public key

Transaction: fundamental unit of a blockchain represents a transfer of value from one address to another

Block: A block is composed of multiple transactions and other elements, such as the previous block hash (hash pointer), timestamp,and nonce

Peer-to-peer network: network topology wherein all peers can communicate with each other and send and receive messages

Virtual machine: allows Turing complete code to be run on a blockchain as smart contracts whereas a transaction script is limited in its operation. Ethereum Virtual Machine (EVM) and Chain Virtual Machine (CVM)

Blockchain - Generic Elements

State machine: A blockchain can be viewed as a state transition mechanism whereby a state is modified from its initial form to the next one by nodes on the blockchain network as a result of transaction execution

Smart contracts: programs run on top of the blockchain and encapsulate the business logic to be executed when certain conditions are met. These programs are enforceable and automatically executable

Node: performs various functions depending on the role that it takes on and can propose and validate transactions and perform mining to facilitate consensus and secure the blockchain

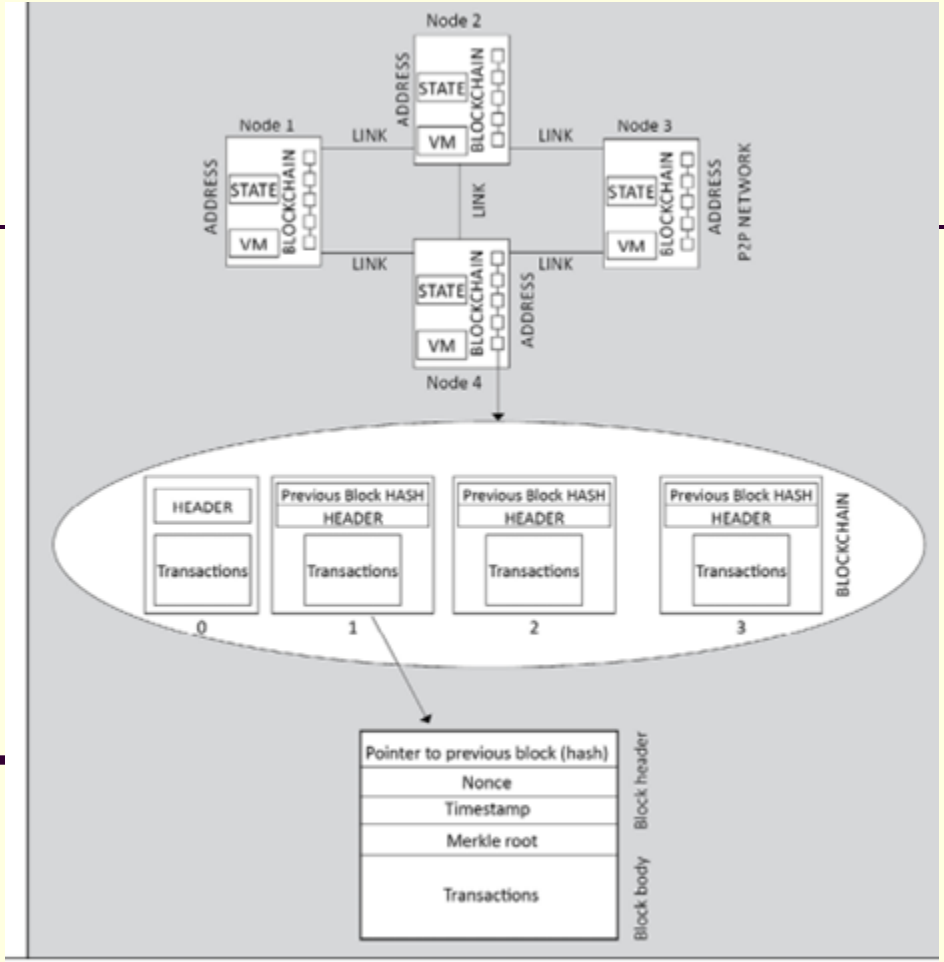


Figure 1.8: Generic structure of a blockchain network

How blockchain works?

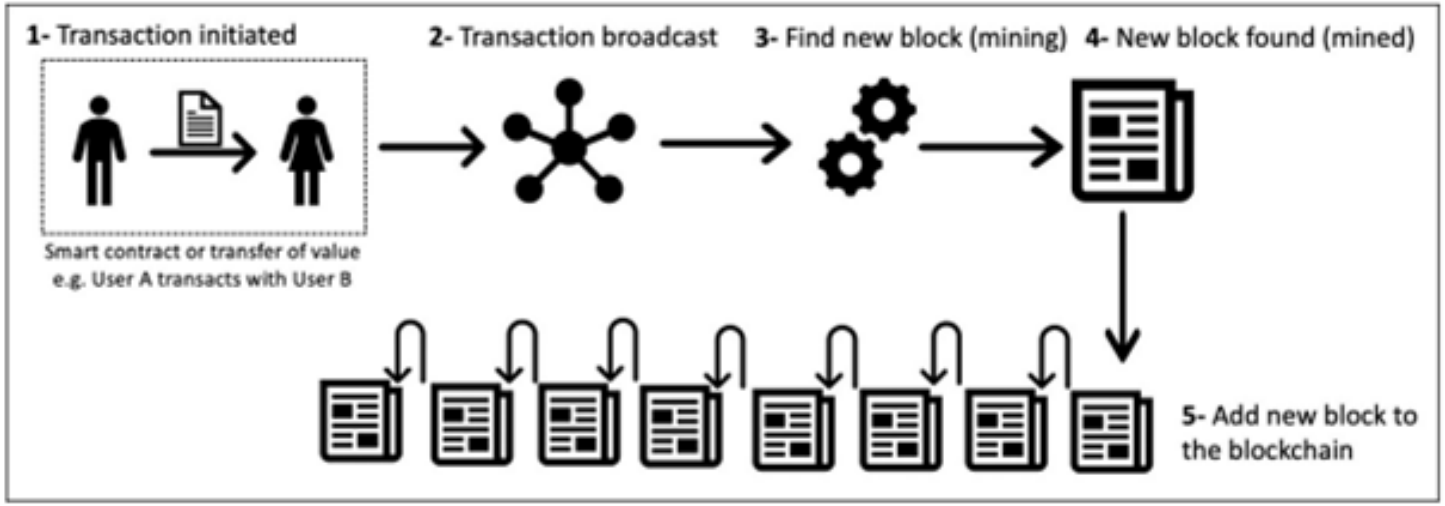


Figure 1.9: How a block is generated

Benefits and features of blockchain

Decentralization: There is no need for a trusted third party or intermediary to validate transactions; instead, a consensus mechanism is used to agree on the validity of transactions

Transparency and trust: As blockchains are shared, this allows the system to be transparent

Immutability: Once the data has been written to the blockchain, it is extremely difficult to change it back

High availability: As the system is based on thousands of nodes in a peer-to-peer network, and the data is replicated and updated on every node, the system becomes highly available

Highly secure: All transactions on a blockchain are cryptographically secured and thus provide network integrity. Any transactions posted from the nodes on the blockchain are verified based on a predetermined set of rules. Only valid transactions are selected for inclusion in a block

Benefits and features of blockchain

Simplification of current paradigms: blockchain can serve as a single shared ledger among many interested parties, this can result in simplifying the model by reducing the complexity of managing the separate systems maintained by each entity

Faster dealings: Blockchain does not require a lengthy process of verification, reconciliation, and clearance because a single version of agreed-upon data is already available on a shared ledger between financial organizations

Cost-saving: As no trusted third party or clearing house is required in the blockchain model, this can massively eliminate overhead costs in the form of the fees, which are paid to such parties

Platform for smart contracts: A blockchain is a platform on which programs can run that execute business logic on behalf of the users. It is available on newer blockchain platforms such as Ethereum and MultiChain, but not on Bitcoin

Benefits and features of blockchain

Smart property: It is possible to link a digital or physical asset to the blockchain in such a secure and precise manner that it cannot be claimed by anyone else. You are in full control of your asset, and it cannot be double-spent or double-owned. Compare this with a digital music file, for example, which can be copied many times without any controls. While it is true that many Digital Rights Management (DRM) schemes are being used currently along with copyright laws, none of them are enforceable in the way a blockchain-based DRM can be

Limitations of blockchain

Scalability: Currently, blockchain networks are not as scalable

Adoption: there is still a long way to go before the mass adoption of this technology

Regulation: Due to its decentralized nature, regulation is almost impossible on blockchain. Traditionally, due to the existence of regulatory authorities, consumers have a certain level of confidence that if something goes wrong they can hold someone accountable

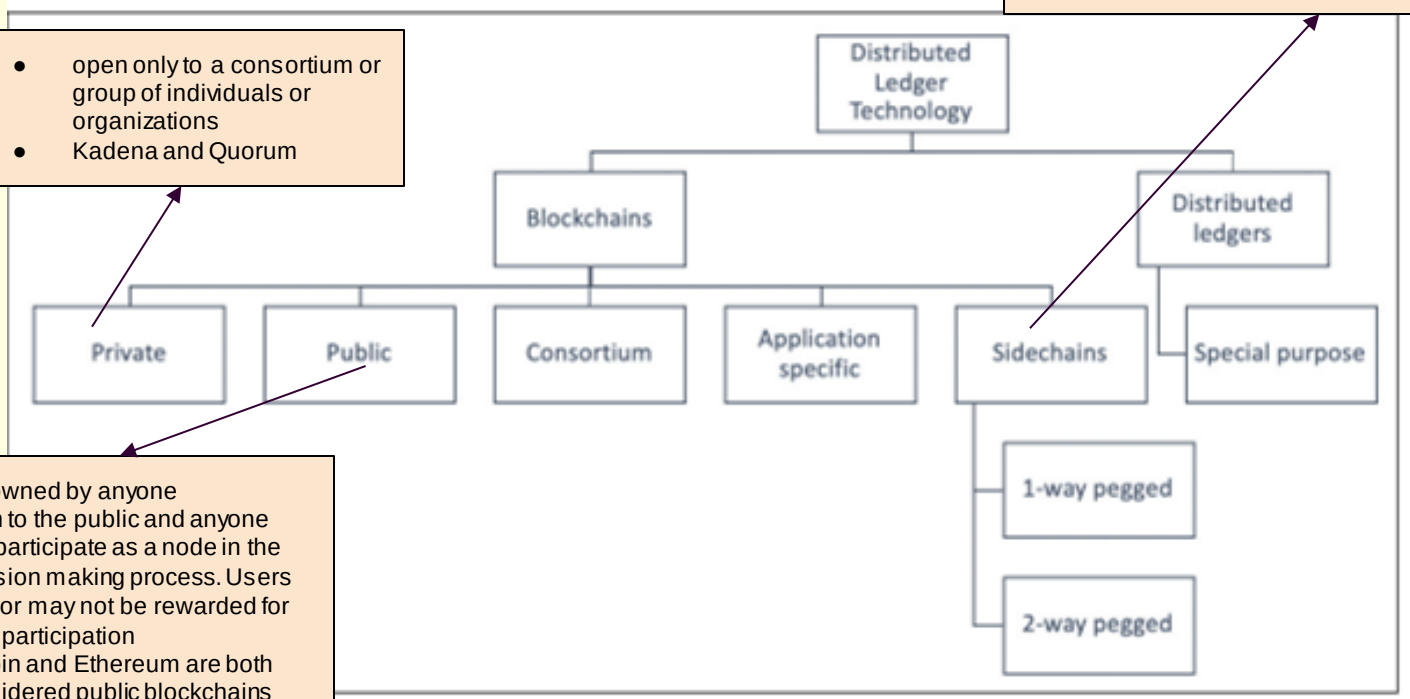
Relatively immature technology: blockchain is still a new technology and requires a lot of research to achieve maturity

Privacy and confidentiality: Privacy is a concern on public blockchains such as Bitcoin where everyone can see every single transaction. This transparency is not desirable in many industries such as the financial, law, or medical sectors

Types of blockchain

- known as "pegged sidechains"
- coins can be moved from one blockchain to another and then back again
- Typical uses include the creation of new altcoins (alternative
- cryptocurrencies) whereby coins are burnt as a proof of an adequate stake

- open only to a consortium or group of individuals or organizations
- Kadena and Quorum



- not owned by anyone
- open to the public and anyone can participate as a node in the decision making process. Users may or may not be rewarded for their participation
- Bitcoin and Ethereum are both considered public blockchains

Figure 1.10: DLT hierarchy

Types of blockchain

Permissioned ledger : blockchain where participants of the network are already known and trusted and do not need to use a distributed consensus mechanism; instead, an agreement protocol is used to maintain a shared version of the truth about the state of the records on the Blockchain

Shared ledger: any application or database that is shared by the public or a consortium. Generally, all blockchains fall into the category of a shared ledger.

Fully private and proprietary blockchains

Types of blockchain

Tokenized blockchains: standard blockchains that generate cryptocurrency as a result of a consensus process via mining or initial distribution. Bitcoin and Ethereum are prime examples

Tokenless blockchains : do not have the basic unit for the transfer of value. However, they are still valuable in situations where there is no need to transfer value between nodes and only the sharing of data among various trusted parties is required.

Consensus

- backbone of a blockchain
- provides the decentralization of control through an optional process known as mining
- choice of the consensus algorithm is governed by the type of blockchain in use
- process of achieving agreement between distrusting nodes on the final state of data

Consensus

- a set of steps that are taken by most or all nodes in a blockchain to agree on a proposed state or value
- Requirements:
  - Agreement: All honest nodes decide on the same value
  - Integrity: no node can make the decision more than once in a single consensus cycle

Consensus

- Requirements:
  - Validity: The value agreed upon by all honest nodes must be the same as the initial value proposed by at least one honest node
  - Fault tolerant: The consensus algorithm should be able to run correctly in the presence of faulty or malicious nodes
  - Termination: All honest nodes terminate the execution of the consensus process and eventually reach a decision

Types of consensus

- Proof-based consensus mechanisms:
  - nodes to compete in a leader-election lottery, and the node that wins proposes the final value
  - Eg. miner who solves the computational puzzle as proof of computational effort expended wins the right to add the next block to the blockchain

Types of consensus

- Traditional fault tolerance-based:
  - relies on a simple scheme of nodes that publish and verify signed messages in a number of phases
  - Eventually, when a certain number of messages are received over a period of rounds (phases), then an agreement is reached

Types of consensus

- Traditional fault tolerance-based:
  - Two types of faults
    - Fail-stop faults: node merely crashed
      - Paxos and RAFT protocol are used to deal
    - Byzantine faults: faulty node exhibits malicious or inconsistent behavior arbitrarily
      - Difficult to handle
      - Byzantine Fault Tolerance (PBFT) is used

Consensus in Blockchain

- used in blockchain in order to provide a means of agreeing to a single version of the truth by all peers on the blockchain network
- 1) Proof-based, leader-election lottery-based, or the Nakamoto consensus whereby a leader is elected at random (using an algorithm) and proposes a final value

Consensus in Blockchain

- also referred to as the fully decentralized or permissionless type of consensus mechanism
- used in the Bitcoin and Ethereum blockchain in the form of a PoW mechanism
- 2) Byzantine fault tolerance (BFT)-based is a more traditional approach based on rounds of votes
    - known as the consortium or permissioned type of consensus mechanism

Consensus in Blockchain

- BFT-based consensus mechanisms perform well when there are a limited number of nodes, but they do not scale well
- Leader election lottery-based (PoW) consensus mechanisms scale very well but perform very slowly

Consensus in Blockchain

- Available algorithms for consensus in context of blockchain
  - Proof of Work (PoW): relies on proof that adequate computational resources have been spent before proposing a value for acceptance by the network
    - Used in Bitcoin, Litecoin, and other cryptocurrency blockchains
    - Successful against any collusion attacks on a blockchain network, such as the Sybil attack