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**

Blockchain Demo (andersbrownworth.com)

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

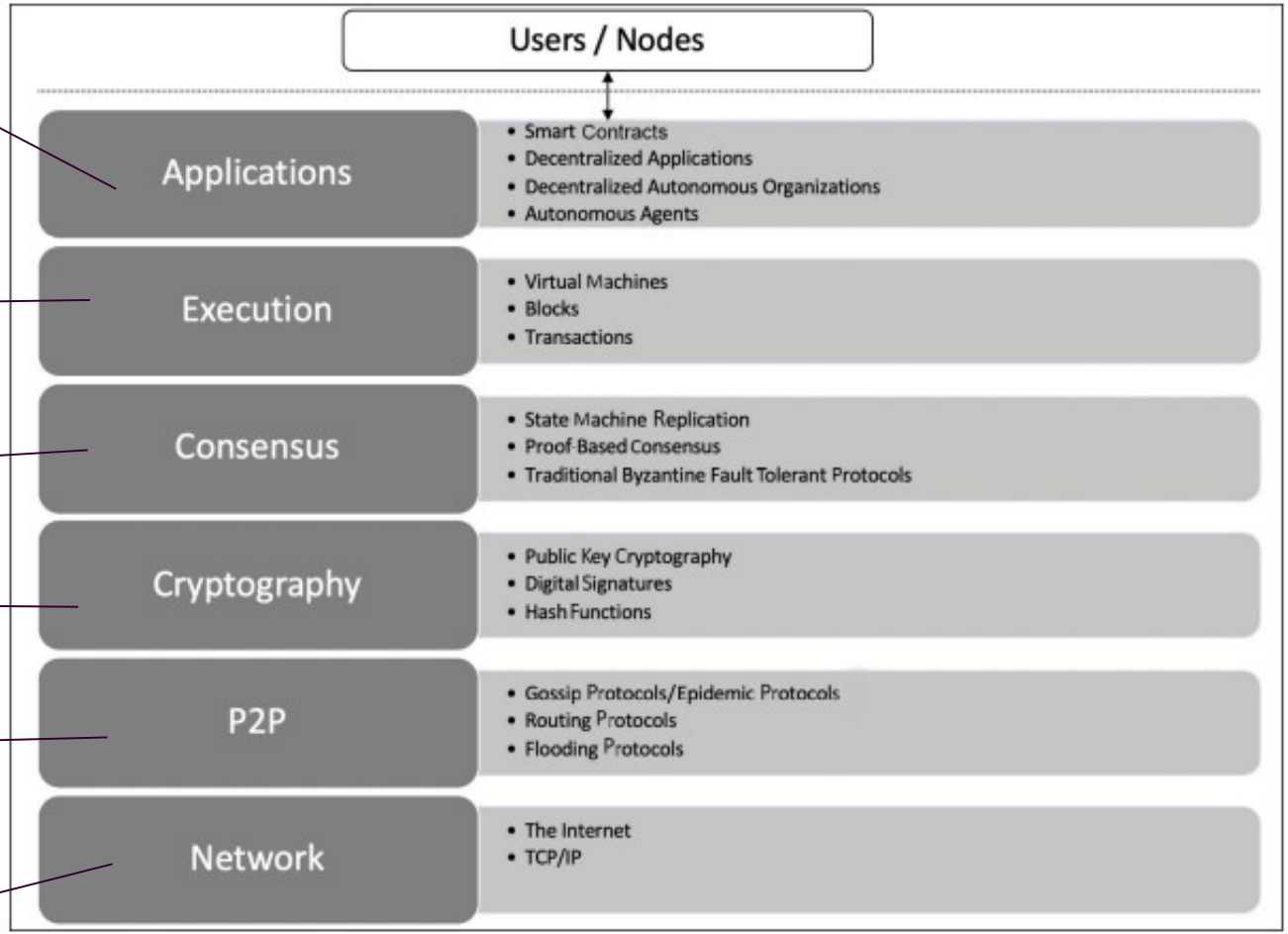


Figure 1.5: The architectural view of a generic blockchain

Blockchain - Generic Elements

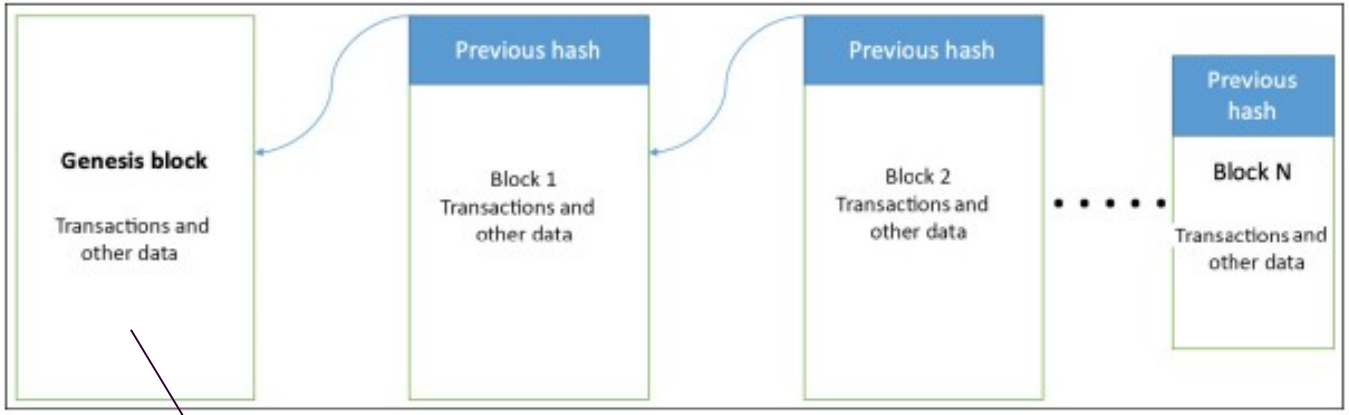


Figure 1.6: Generic structure of a blockchain

- 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

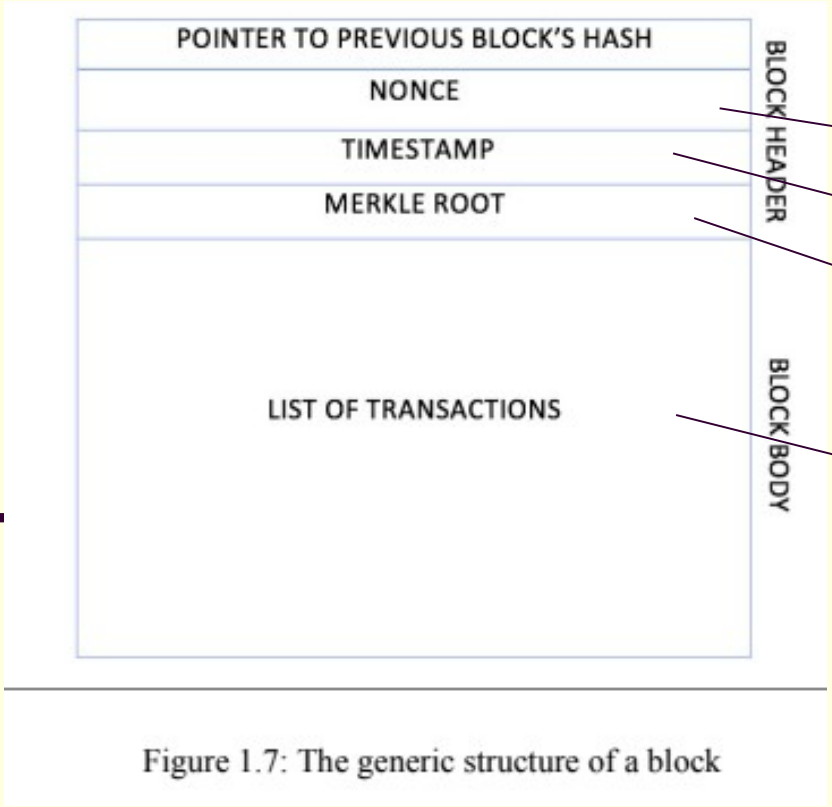


Figure 1.7: The generic structure of a block

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

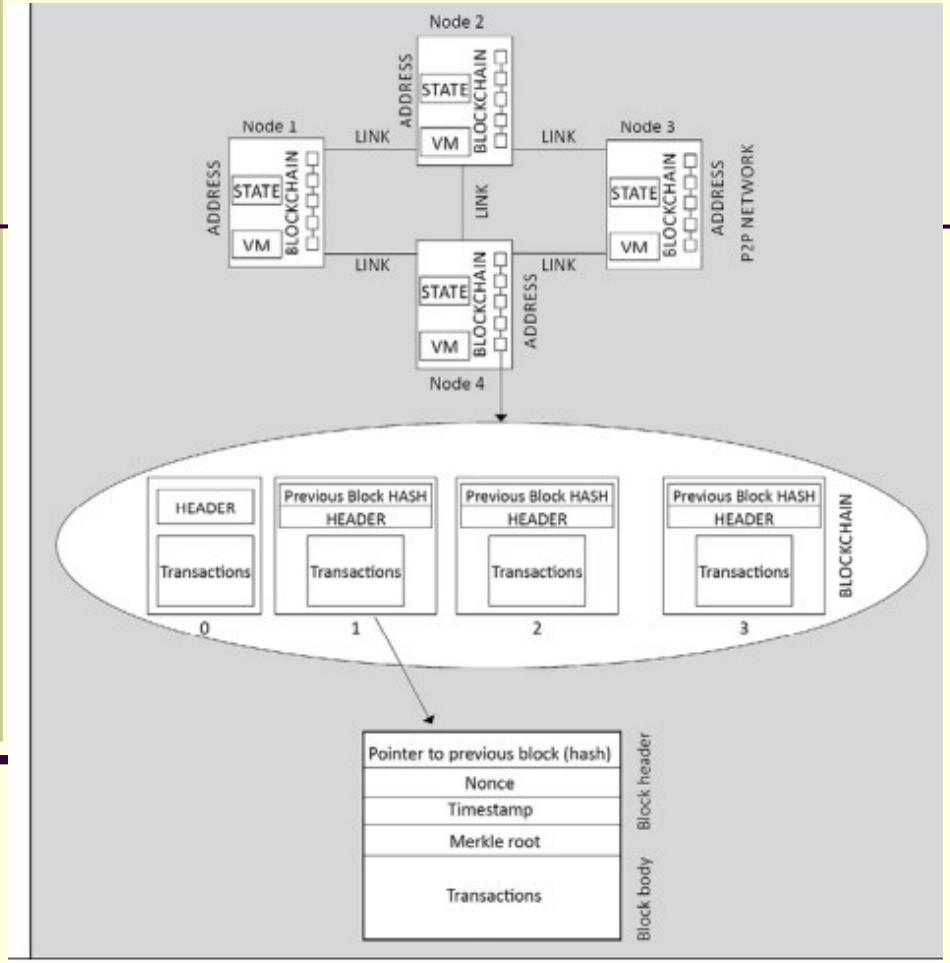


Figure 1.8: Generic structure of a blockchain network

How blockchain works?

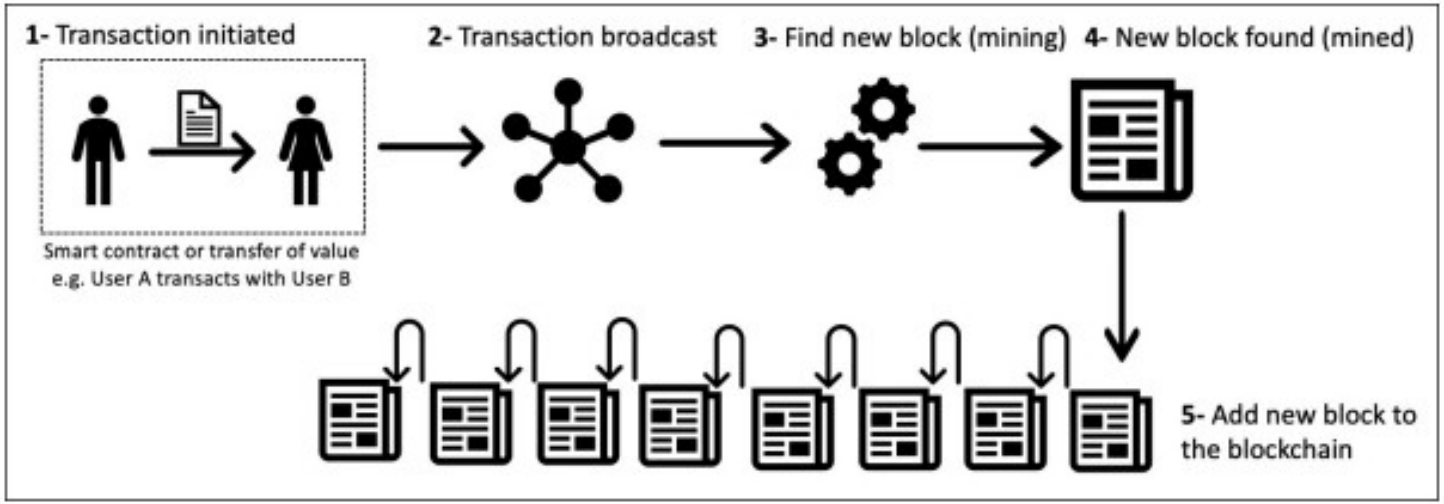


Figure 1.9: How a block is generated

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

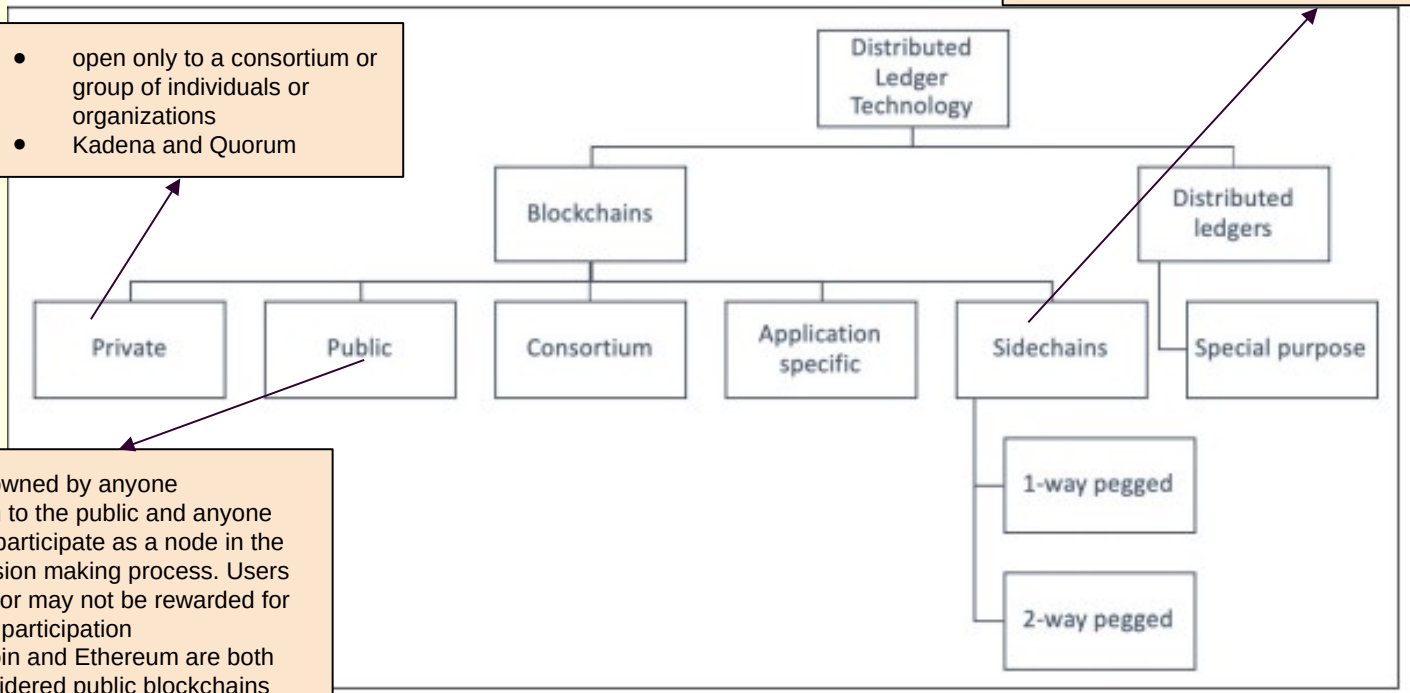
Relatively immature technology: blockchain is still a new technology and requires a lot of research to achieve maturity

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

Consensus in Blockchain

01	Proof of Work (PoW)	• proof that adequate computational resources have been spent • Used in Bitcoin, Litecoin and other cryptocurrency • Successful against Sybil Attack
02	Proof of Stake (PoS)	• node or user has an adequate stake (invest) in the system so that any malicious attempt outweigh the benefits of performing such an attack on the network • first introduced by Peercoin • used in the Ethereum blockchain version Serenity

Consensus in Blockchain

03	Delegated Proof of Stake (DPoS)	• innovation over standard PoS • each node that has a stake in the system can delegate the validation of a transaction to other nodes by voting • used in the BitShares blockchain
04	Proof of Elapsed Time (PoET)	• uses a Trusted Execution Environment (TEE) to provide randomness and safety in the leader-election process via a guaranteed wait time
05	Proof of Deposit (PoD)	• nodes that wish to participate in the network have to make a security deposit before they can mine and propose blocks • used in the Tendermint blockchain

Consensus in Blockchain

06	Proof of Importance (PoI)	• monitors the usage and movement of tokens by the user in order to establish a level of trust and importance
07	Federated consensus or federated Byzantine consensus	• used in the stellar consensus protocol • Nodes retain a group of publicly-trusted peers and propagate only those transactions that have been validated by the majority of trusted nodes
08	Reputation-based mechanisms	• a leader is elected by the reputation it has built over time on the network • based on the votes of other members

Consensus in Blockchain

09	Practical Byzantine Fault Tolerance (PBFT)	• provides tolerance against Byzantine nodes • used in many different implementations of distributed systems and blockchains
10	Proof of Activity (PoA)	• combination of PoS and PoW • ensures that a stakeholder is selected in a pseudorandom but uniform fashion • more energy-efficient mechanism
11	Proof of Capacity (PoC)	• uses hard disk space as a resource to mine the blocks • also known as hard drive mining • First introduced in the BurstCoin cryptocurrency

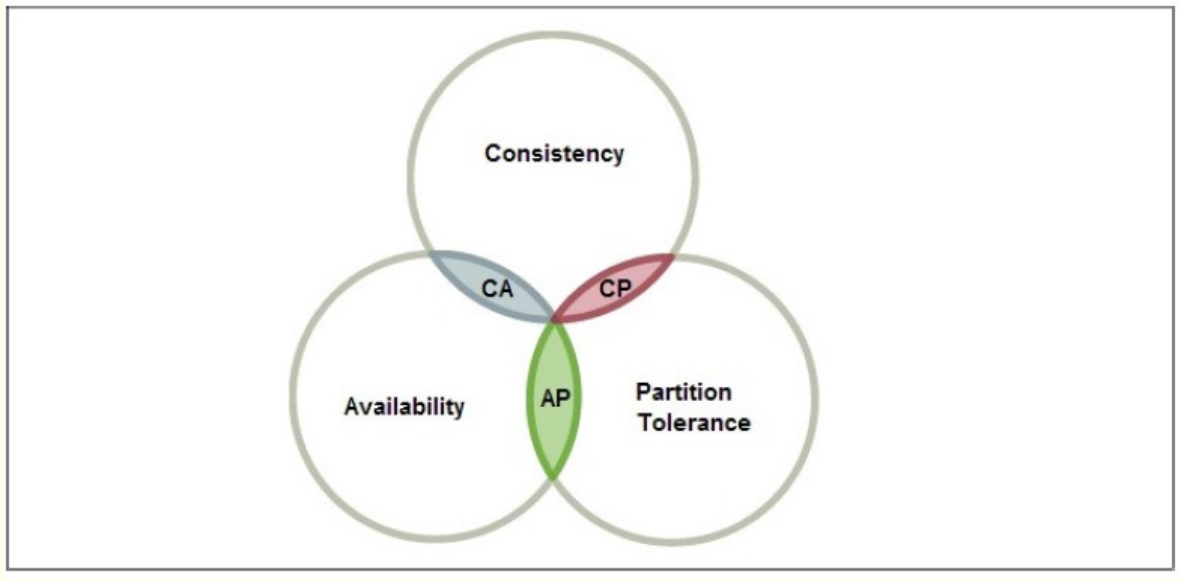
Consensus in Blockchain

12	Proof of Storage	• allows for the outsourcing of storage capacity • based on the concept that a particular piece of data is probably stored by a node, which serves as a means to participate in the consensus mechanism
13	Proof of Authority (PoA)	• utilizes the identity of the participants called validators as a stake on the network • Validators are known and have the authority to propose new blocks • Validators propose the new blocks and validate them as per blockchain rules

CAP Theorem

- Also known as Brewer’s Theorem
  - ***Any distributed system cannot have consistency, availability and partition tolerance simultaneously***
    - **Consistency** : property that ensures all nodes in a distributed system have a single, current and identical copy of data
    - **Availability** : data is available at each node and the nodes are responding to requests
    - **Partition Tolerance :** ensures that if a group of nodes is unable to communicate with other nodes due to network failures, the

CAP Theorem



Only Two properties at a time can be achieved : Either AP, CA or CP

CAP Theorem

- Choice is between consistency or availability as network partition cant be ignored.

Imagine a distributed system with two nodes. Due to partition nodes cant communicate with each other.

Consistency?

Availability?

Partition Tolerance?

Blockchain Manages to achieve all these

CAP Theorem & Blockchain

- Consistency is achieved over time as a result of validation from multiple nodes over time.
- There can be temporary disagreements between nodes on final state but it is eventually agreed upon.
- Ex : Bitcoin
  - Multiple transaction confirmation required to achieve good level of confidence that transactions are not rolled back in future
  - Consistent view of transaction history available to all nodes

Decentralization

- core benefit and service provided by blockchain technology
- allows anyone to compete to become the decision-making authority
- consensus mechanism governs this competition, and the most famous method is known as Proof of Work (PoW)
- applied in varying degrees from a semi-decentralized model to a fully decentralized one depending on the requirements and circumstances

Decentralization

Not dependent on a single master node control is distributed among many nodes

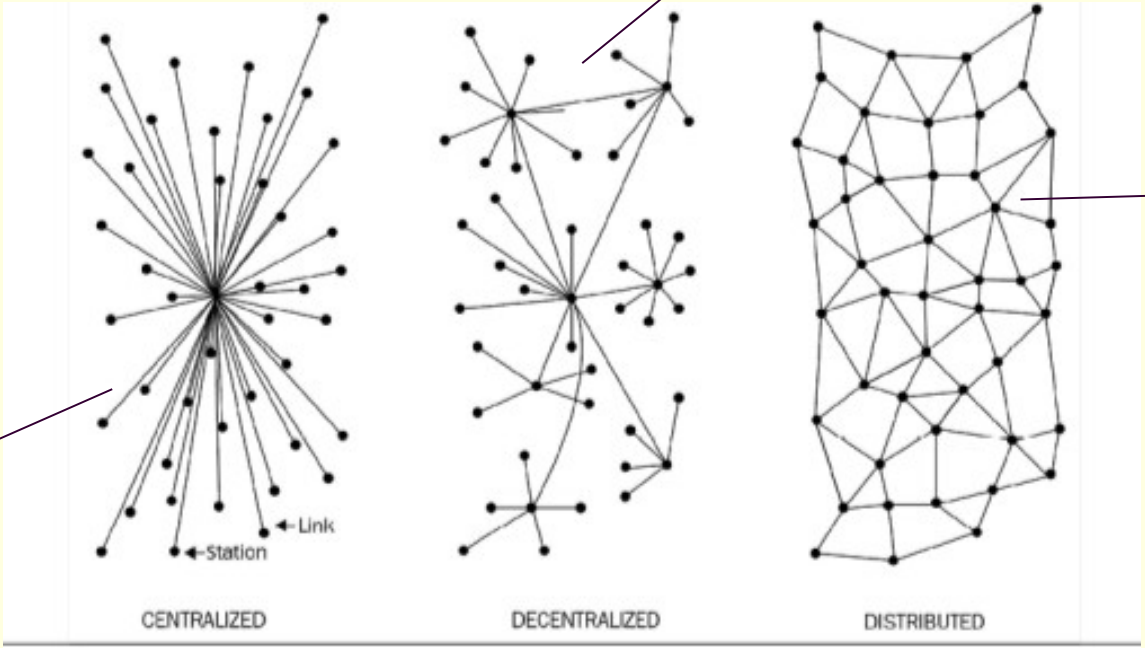


Figure 2.1: Different types of networks/systems

computation may not happen in parallel and data is replicated across multiple nodes that users view as a single, coherent System

still a central authority that governs the entire system

majority of online service providers, including Google, Amazon, eBay, and Apple's App Store, use this model to deliver services

Decentralization

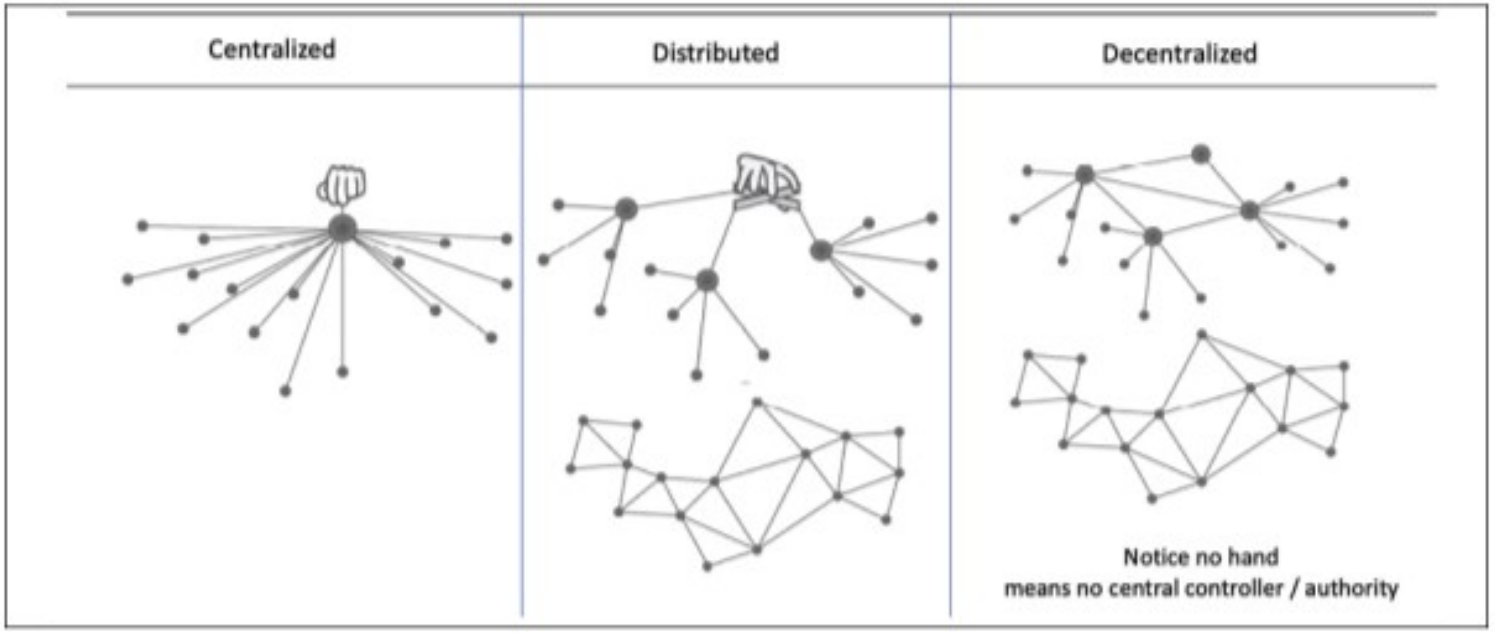


Figure 2.2: Different types of networks/systems depicting decentralization from a modern perspective

Decentralization

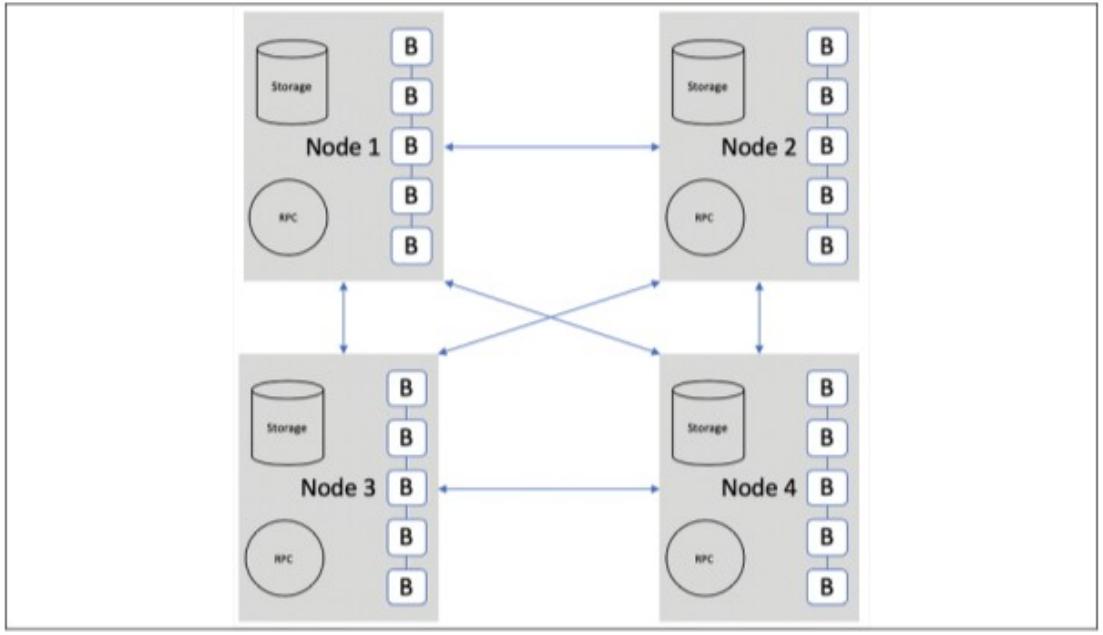


Figure 2.4: A blockchain-based decentralized system (notice the direct P2P connections and the exact replicas of blocks)

Decentralization

Feature	Centralized	Decentralized
Ownership	Service provider	All users
Architecture	Client/server	Distributed, different topologies
Security	Basic	More secure
High availability	No	Yes
Fault tolerance	Basic, single point of failure	Highly tolerant, as service is replicated
Collusion resistance	Basic, because it's under the control of a group or even single individual	Highly resistant, as consensus algorithms ensure defense against adversaries

Decentralization

Feature	Centralized	Decentralized
Application architecture	Single application	Application replicated across all nodes
Trust	Consumers have to trust the service provider	No mutual trust required
Cost for consumer	Higher	Lower

Methods of decentralization

- Two methods - disintermediation and competition
- Disintermediation - the intermediary (that is, the bank) is no longer required
  - used not only in finance but in many other industries as well, such as health, law, and the public sector

Methods of decentralization

- Contest-driven decentralization - different service providers compete with each other in order to be selected for the provision of services by the system
  - ensures that an intermediary or service provider is not monopolizing the service
  - will not result in full decentralization, but it allows smart contracts to make a free choice based on the criteria just mentioned

Routes to decentralization

Case of a Money transfer system

1. What is being decentralized?
2. What level of decentralization is required?
3. What blockchain is used?
4. What security mechanism is used?

1. Money transfer system
2. Disintermediation
3. Bitcoin
4. Atomicity (ensure that transactions execute successfully in full or do not execute at all)

Blockchain and full ecosystem decentralization

- Storage
  - stored directly in a blockchain which achieves decentralization but is not suitable for large data
  - better alternative for storing data is to use distributed hash tables (DHTs)
  - BitTorrent is the most scalable and fastest network

Blockchain and full ecosystem decentralization

- There are other alternatives for data storage, such as Ethereum Swarm, Storj, and MaidSafe
- Ethereum has its own decentralized and distributed ecosystem that uses Swarm for storage and the Whisper protocol for communication
- BigChainDB is another storage layer decentralization project aimed at providing a scalable, fast, and linearly scalable decentralized database

Blockchain and full ecosystem decentralization

- Communication
  - based on the unconditional trust of a central authority (the service provider) where users are not in control of their data
  - Even user passwords are stored on trusted third-party systems
  - need to provide control to individual users in such a way that access to their data is guaranteed and is not dependent on a single third party

Blockchain and full ecosystem decentralization

- Communication
  - alternative to ISP is to use mesh networks
  - provides a decentralized alternative where nodes can talk directly to each other without a central hub such as an ISP
- Computing power and decentralization
  - achieved by a blockchain technology such as Ethereum, where smart contracts with embedded business logic can run on the blockchain network

Questions

1. Illustrate the blockchain based decentralized system.
2. Explain how Proof of Stake can achieve consensus among peers.
3. Illustrate and explain how blockchain works using a neat diagram.
4. Explain the benefits, features and limitations of blockchain.
5. Explain consensus mechanisms used in blockchain. List out any six consensus algorithms used in the context of blockchain.
6. Define blockchain. Explain how decentralization of computing or processing power is achieved by a blockchain.
7. Explain the fundamental concepts of blockchain technology

Link to additional resources

Bitcoin Script: An Introduction For Beginners (komodoplatform.com)

Ethereum Transactions Information | Etherscan

Ethereum Blocks #0 | Etherscan

Blockchain.com Explorer | BCH | ETH | BCH