Consensus Mechanisms and Types of Blockchain

Chapter – 3

Fall 2025

Middle Tennessee State University

Summary of Key Steps in Blockchain

- 1. Transaction
- 2. Verification
- 3. Block Formation
- 4. **Consensus**
- 5. Chaining

Why Do We Need Consensus?

- Centralized systems rely on a single authority such as a bank or government
  - One party decides what is valid
  - Everyone agrees to trust that party
- Blockchains have no central authority
  - Many participants maintain copies of the ledger
  - They must agree on one version of the truth
- Without consensus the system would collapse
  - A user could spend the same coin twice
  - Fraudulent transactions could enter the ledger
  - Different nodes might record different histories
- Consensus ensures fairness and honesty
  - All nodes follow the same rules
  - Agreement happens even without trust between participants

Consensus Mechanisms/Algorithms/Protocols

Some examples:

1. Proof of Work (PoW)
2. Proof of Stake (PoS)
3. Proof of Authority (PoA)
4. Delegated Proof of Stake (DPoS)

How Consensus Works in Practice (Example)

1. A transaction is created and broadcast to the network
   - Example: Alice sends 5 coins to Bob
   - The transaction enters the mempool (waiting area)

2. Nodes verify the transaction
   - Check balance of Alice's account
   - Check digital signature for validity
   - Reject if rules are not met

How Consensus Works in Practice (Example) (Contd...)

3. A single node proposes a new block
   - Miner in Proof of Work
   - Validator in Proof of Stake
   - Block includes verified transactions

4. Other nodes check the block again
   - Validate each transaction inside
   - Confirm block hash or validator signature
   - Accept only if correct

5. Once accepted, block is added permanently

Evolution of Consensus Algorithms (Consensus Protocols/Mechanisms)

- 2009 – Bitcoin introduces Proof of Work
  - First practical decentralized ledger
  - Solved double-spending problem

- 2012 – Peercoin introduces Proof of Stake
  - Energy efficient alternative
  - Validators replace miners as block proposers

- 2015 – Ethereum launches using Proof of Work
  - Extended blockchain beyond currency into smart contracts and DApps
  - Became the foundation for DeFi, NFTs, and thousands of projects

Evolution of Consensus Algorithms (Consensus Protocols/Mechanisms) – (Contd...)

- 2022 – Ethereum transitions to Proof of Stake (The Merge)
  - Validators replace miners, requiring 32 ETH to stake
  - Reduced energy consumption by more than 99 percent
  - Created the base for Ethereum's future scaling (sharding, rollups)

- 2022 and beyond – New models and ongoing innovation
  - Delegated Proof of Stake (EOS)
  - Proof of Authority (VeChain, enterprise blockchains)
  - BFT and hybrid models in private and consortium chains
  - DAG-based systems and quantum-resistant approaches

Announcement/Reminder

- **Next week** (**Oct 1, 3, 6**) – **Paper Presentation (5% of total grade)**
  - *1 unique paper on **any** topic related to **Blockchain** by a group (a pair of students).*
  - *Groups should consist of 2 students.*
  - *Group can be a combination of undergraduate and graduate students.*
  - *Papers available in Google Scholar, IEEE Xplore, ACM, Springer, etc.*
  - *Use university Wi-Fi to access papers for free.*
  - *Papers only from 2022 and later.*
  - *Paper length – more than 2 pages each.*
  - *Each member of the group is expected to contribute equally to the group's efforts.*

  - The **deadline** for completing the information in the following table (table in Google Doc) including the submission of PowerPoint file on D2L is on **Tuesday, Sept 30, 11:59 PM**.
  - Only one submission per group in D2L is required.
  - The presentation will start on **Wednesday, Oct 1** during lecture hours.
  - The presentation will be in ascending order. First team in the table will present first and so on.
  - **Example: Wednesday, Oct 1** – **Group 1, Group 2, Group 3, Group 4, Group 5** and so on.
  - Google Doc Link for Group Formation and Paper Selection:
  - https://docs.google.com/document/d/1mzNrHneG8OBcse8dmv98Rz7gYjX-4OIlbsXCl2aTivQ/edit?usp=sharing
  - Make sure there is **no collision in paper selection**.
  - Presentation strictly NOT more than 10 minutes for each team.
  - The presentation should focus on problem motivation, the problem being solved, other existing related studies, the current solution, system architecture and implementation, results, and finally the conclusion. Do not forget to add references, and you may include screenshots of diagrams with proper citations.

1. Proof of Work (PoW) Consensus

- Oldest and widely-used consensus mechanism
- Known for its role in Bitcoin and Litecoin
- Relies on miners (nodes) solving complex cryptographic puzzles to validate transactions and create new blocks
- The one who does it first receives the right to propose or add the next block
- “Winner” gets rewarded with newly minted crypto

1. Proof of Work (PoW) Consensus (Contd...)

Strength:

- High security due to computational work required
- Decentralized and open to anyone with computing power
  - ASIC (Application-Specific Integrated Circuits) machines are used these days

Weaknesses:

- High energy consumption
  - In 2021, Cambridge researchers estimated Bitcoin mining used ~91 TWh annually, almost the same as Pakistan's yearly electricity consumption
- Vulnerable to 51% attacks if a single entity controls majority hashpower
  - If one entity controls more than half of the total computing power, it could rewrite blockchain history
  - In 2019, Ethereum Classic suffered a 51% attack, where an attacker reorganized the chain and double-spent coins

1. Proof of Work (PoW) Consensus (Contd…)

- So, what is ‘mining’ in Proof of Work?
  - Miners keep changing a special number called a nonce (number used once)
  - Goal: make the block’s hash start with enough zeros (meet the difficulty target)
    - Rule: `Block hash ≤ target difficulty value`
      - A hash is just a big number (256-bit numbers) written in hexadecimal (base-16)
      - The difficulty target says: “*Your block hash must be less than this value*”
      - Smaller numbers in hex start with more zeros at the front
        - 0000abc123… (very small number)
        - 1234def456… (much larger number)
      - The smaller the target, the harder it is to find a valid hash
      - If the target is very low, the only valid hashes will look like they have lots of zeros in the front
  - Refer here for demo: https://andersbrownworth.com/blockchain/block
  - Takes millions of guesses (brute-force) before finding the right one
  - Easy for everyone else to validate the winner’s hash once it’s found
  - Prevents fake blocks and keeps the network secure
    - Everyone is guessing nonces, but the chance to win is proportional to your computing power
  - Winner gets block reward + transaction fees

2. Proof of Stake (PoS) Consensus

- Energy-efficient consensus mechanism
- Validators are chosen based on the amount of cryptocurrency they hold
- Validators are willing to “stake” as collateral

2. Proof of Stake (PoS) Consensus – (Contd...)

Strength:

- Energy-efficient and environmentally friendly
- Incentivizes holding and investing in the native cryptocurrency

Weaknesses:

- Possible centralization as wealthier participants have more influence
- Limited security if a large amount of coins is staked by malicious actors

2. Proof of Stake (PoS) Consensus – (Contd…)

- Validators are not solving “puzzles” to be a winner

- Instead, one validator is randomly chosen to propose a block

  - Selection uses Verifiable Random Function (VRF) to ensure fairness and unpredictability
  - Every validator runs the VRF locally
    - Each validator combines their private key, a random seed, and their stake weight
    - A random number (output) and a cryptographic proof (like a certificate) that the output was honestly generated

  - When a validator claims: *“I was selected to propose the next block”* they must also broadcast the proof
    - Other nodes verify the proof with the validator’s public key
    - This confirms:
      - The randomness was generated correctly (no cheating)
      - The validator truly had the stake weight they claimed
    - Prevents someone from faking their selection

2. Proof of Stake (PoS) Consensus – (Contd…)

- Larger stakes increase the probability of being selected, but outcome is still random
  - If Alice stakes 64 ETH and Bob stakes 32 ETH, Alice is twice as likely to be chosen. But it's still random. Bob can still win

- So, if selection is random, why does larger stake even matter???
  - Ensures fairness
  - Discourages attack
    - Who will lose more stake if the blockchain network is attacked?

3. Proof of Authority (PoA) Consensus

- Commonly used in private blockchains
- A trusted, pre-approved set of nodes or authorities validate transactions
- Prioritizes identity and reputation over computational power (PoW) and stake-based ownership (PoS)
- Validators, also known as authorities, are predetermined
- Validators are responsible for validating transactions and creating new blocks in the blockchain
- Commonly used in test networks or development environments to ensure fast and reliable testing of blockchain applications
- E.g., in VeChain, validators are businesses with verified identities
  - Supply chain blockchains, where only approved companies can validate

3. Proof of Authority (PoA) Consensus – (Contd...)

Strength:

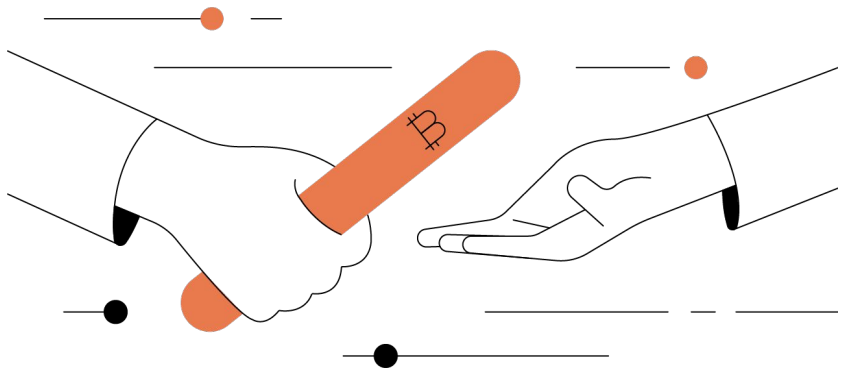
- Reduced energy consumption
- Faster consensus and efficient
  - Since there are fewer validators, blocks are created quickly without competition

Weaknesses:

- Centralization
- Trust in Validators
  - Assumes validators will act honestly because their reputation is at stake

4. Delegated Proof of Stake (DPoS) Consensus

- Token/Stake holders vote for their preferred delegates
- Delegates with the highest number of votes become active block producers
- Delegates of one block might not be the delegates of the next
- Delegates are rewarded for their role in maintaining the network's security and functionality. Similarly, token holders earn voting and staking rewards
- More democratic
- E.g., Cardano, EOS, TRON use DPoS



4. Delegated Proof of Stake (DPoS) Consensus – (Contd...)

Strength:

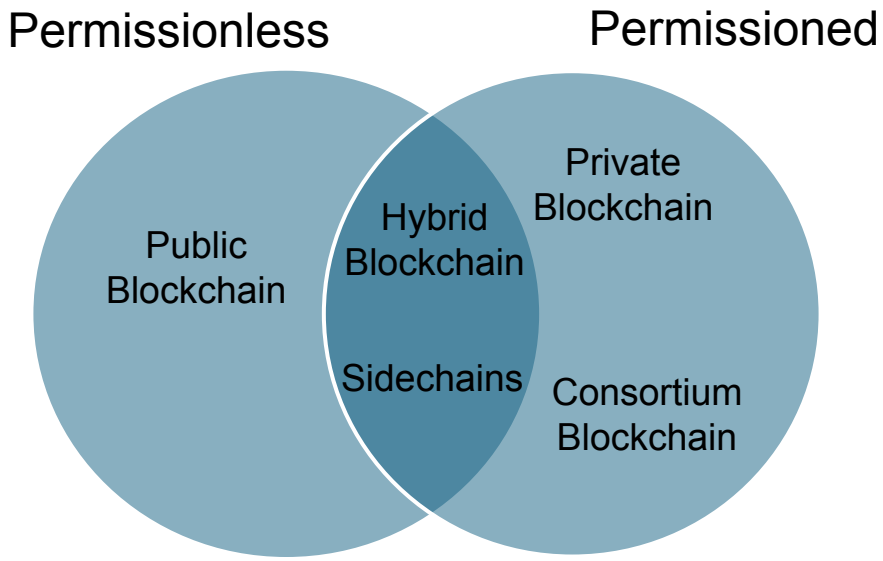
- Decentralization with community participation
- Quick consensus due to limited number of validators/nodes
- Energy efficient

Weaknesses:

- Potential centralization due to limited number of delegates
- Voting manipulation by large token holders

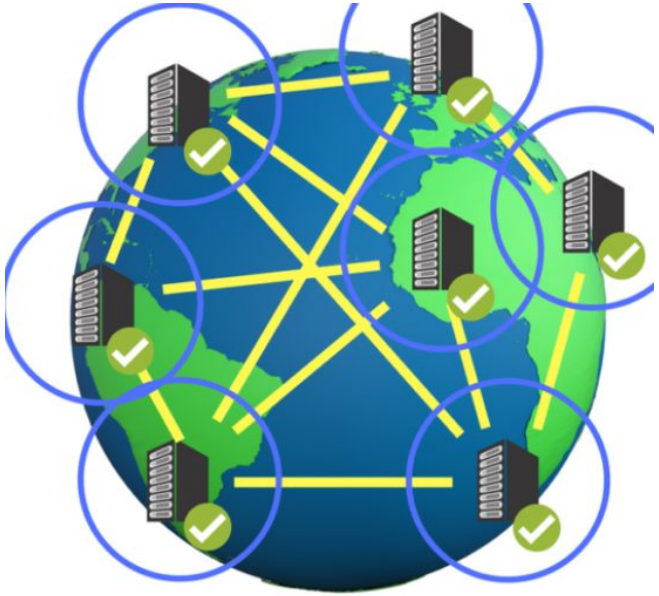
Types of Blockchains

- Public Blockchain
- Private Blockchain
- Consortium Blockchain
- Hybrid Blockchain
- Sidechains



Public Blockchain

- Open and permissionless
- No central authority
- Transactions are transparent and immutable
- E.g., Bitcoin (BTC), Ethereum (ETH), Ripple (XRP), Litecoin (LTC), Cardano (ADA), Polkadot (DOT), etc.



Public Blockchain (Contd...)

Strength:

- Decentralization
- Censorship resistance – ability to resist censorship
- High security through cryptographic consensus
- Global participation and inclusivity
- Proven track record of durability and reliability (e.g., Bitcoin and Ethereum)

Weakness:

- Scalability challenges (e.g., Bitcoin's block creation time – 10 minutes)
- Energy-intensive (e.g., Proof of Work)
- Limited privacy for transactions

Private Blockchain

- Permissioned blockchain
- Restricted access
- Controlled by one authority (although nodes are decentralized)
- Typically used in enterprise settings
- E.g., Hyperledger Fabric, Corda, Quorum, IBM Blockchain Platform, Celo, etc.

Private Blockchain (Contd...)

Strengths:

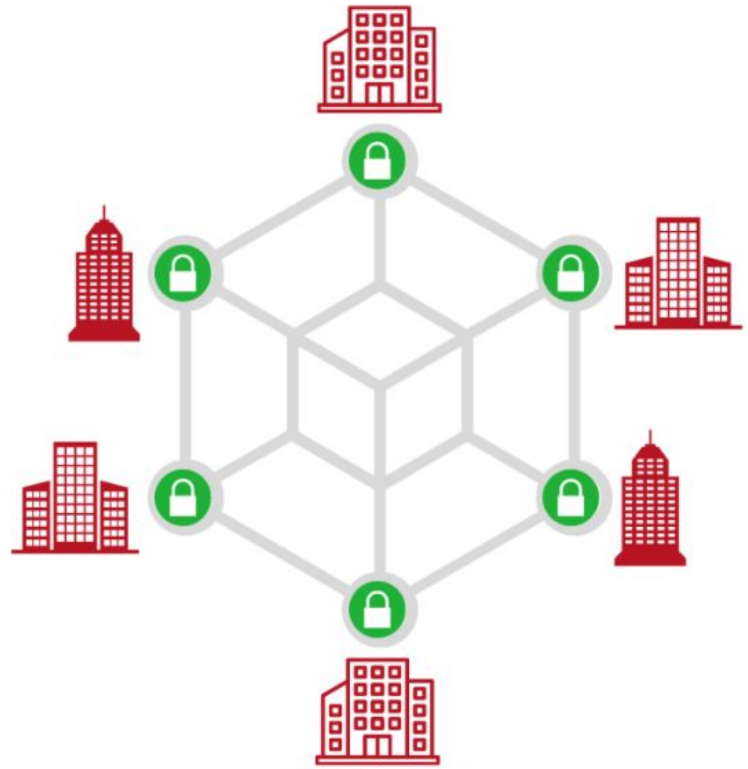
- Enhanced privacy and control
- Faster transaction processing
- Reduced resource consumption
- Suitable for business use cases

Weakness:

- Reduced decentralization and trust requirements
- Limited transparency and potential centralization
- Requires trust in validators
- Not as censorship-resistant as public blockchains

Consortium Blockchain

- Also known as Federated Blockchain
- Consortium - an association, typically of several business companies
- Permissioned blockchain
- Governed by multiple organizations
- Only organization members with access can be on the network
- E.g., R3 Corda Consortium, Enterprise Ethereum Alliance, Komgo Consortium, etc.



Consortium Blockchain (Contd...)

Strengths:

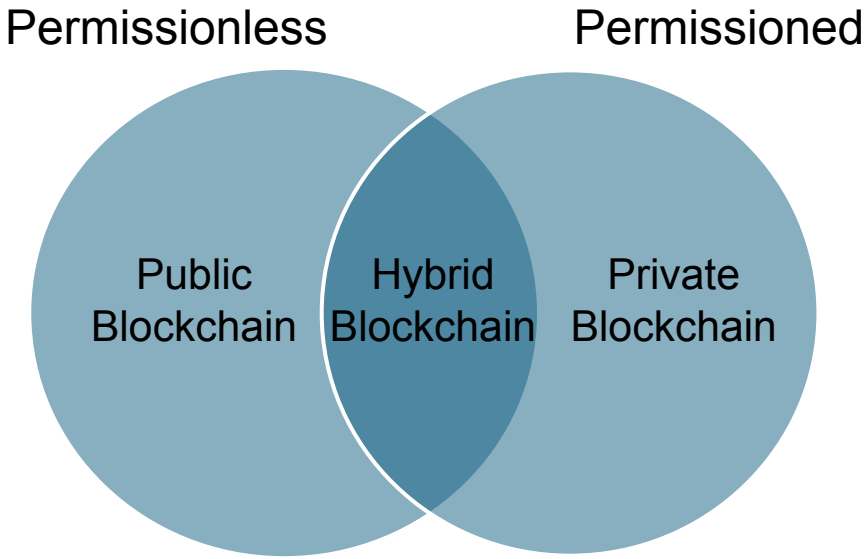
- Enhanced trust among participants
- Greater scalability and efficiency
- Improved privacy compared to public blockchains
- Collaboration among known entities

Weakness:

- Centralization among consortium members
- Less open than public blockchains
- Governance complexity and potential conflicts
- Limited participation outside the consortium

Hybrid Blockchain

- Combines features of both public and private (or consortium) blockchains
- Some parts of the data/transactions are open and transparent (like a public chain), while others remain private and permissioned (like a private chain)
- To balance transparency and control
- Same chain blends both models for different use cases
- For e.g., A hospital system might run a private blockchain to manage patient medical records but connect it to a public blockchain to publish proof-of-existence hashes for auditability
- E.g., Dragonchain, Ardor, Syscoin, Polkadot



Hybrid Blockchain (Contd...)

Strengths:

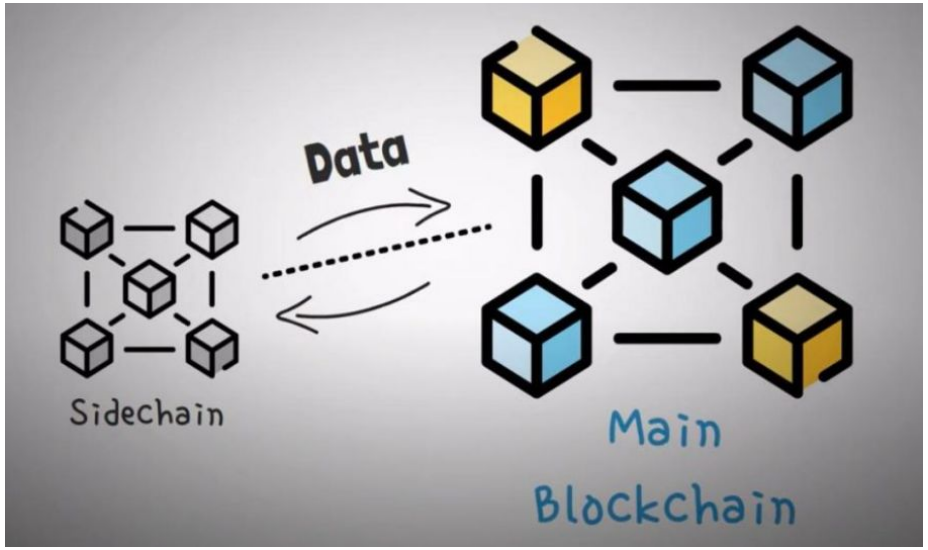
- Balance between transparency and privacy
- Customizable for various use cases
- Interoperability between public and private chains
- Flexibility to adapt to changing needs

Weakness:

- Complexity in managing both sides
- Potential security challenges at the hybrid boundary
- Governance and coordination complexities
- Trade-offs between decentralization and control

Sidechains

- Separate blockchain that runs in parallel to a main chain
- Connected to the main chain through a bridge
- Transactions or assets can be transferred from the main chain to the sidechain for faster, cheaper, or experimental operations, then moved back
- To offload traffic or test new features without risking the security of the main chain
- For e.g., Ethereum's Polygon (Matic Network) and Plasma chains allow faster and cheaper transactions while pegged to Ethereum's mainnet
- Similarly, Bitcoin has sidechains like Liquid for faster settlement
- A sidechain is a supporting chain, not a mix. It works alongside a main chain
- E.g., Raiden Network, Plasma, Avalanche C-Chain, Matic Network, etc.



Sidechains (Contd...)

Strengths:

- Allows for experimentation without affecting the main chain
- Potential for innovative design

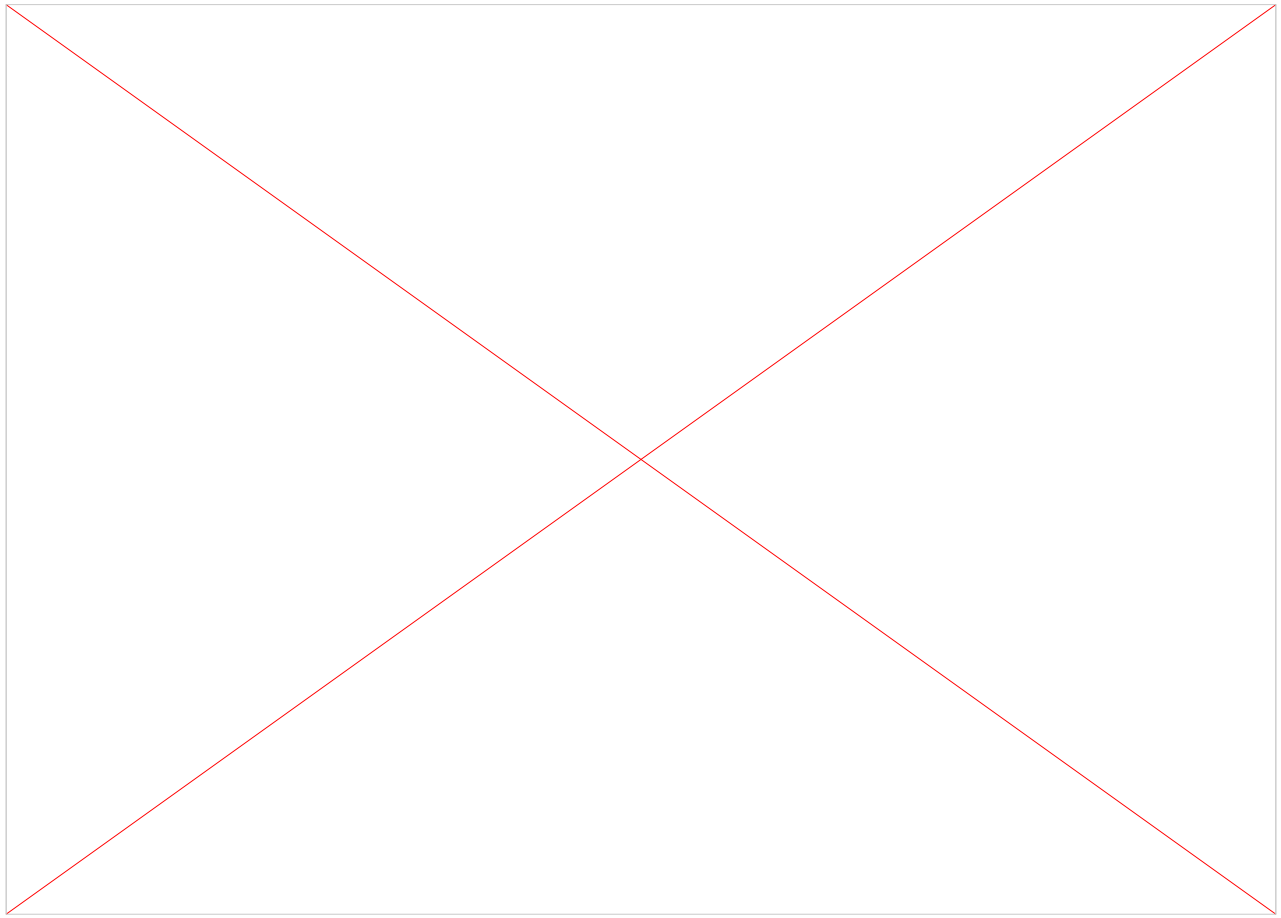
Weakness:

- Security concerns in bridging and cross-chain transactions
- Governance and coordination challenges
- Requires careful design and management
- May introduce complexity to the overall network

What type of Blockchain to choose?

Choose the blockchain type based on:

- ✔ Use case and objectives
- ✔ Trust and privacy requirements
- ✔ Governance and scalability needs



Comparison between major types of Blockchains

Features	*Public Blockchain*	*Private Blockchain*	*Consortium Blockchain*
Control	No central authority	By a single group/organization	More than one group/organization
Decentralization	Complete	Less	More than *Private*
Access	Anyone	Limited	Limited
Transaction Speed	Slower	Fast	Fast
Immutability	Impossible to tamper	Could be tampered	Could be tampered
Secure	More	Very less	Less
Scalability	Less	Highly scalable	Highly scalable
Use Cases	Cryptocurrency, Smart Contracts, DApps	Enterprise solutions	Collaborative projects
Examples	Ethereum, Bitcoin	Hyperledger Fabric, Corda	R3 Corda Consortium

End of Chapter-3