VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

FOUNDATIONS OF BLOCKCHAIN TECHNOLOGY

BCSE324L

Dr. Malathi D.

FOUNDATIONS OF BLOCKCHAIN TECHNOLOGY

Course Objectives

- To understand building blocks of Blockchain.
- To significance of Distributed Ledger Technology and Smart Contract.
- To exploit applications of Blockchain in real world scenarios and their impacts.

Expected Outcomes

- Understand Blockchain ecosystem and its services in real world sceneries
- Apply and Analyze the requirement of Distributed Ledger Technology and Smart Contract
- Design and Demonstrate end-to-end decentralized applications
- Acquaint the protocol and assess their computational requirements

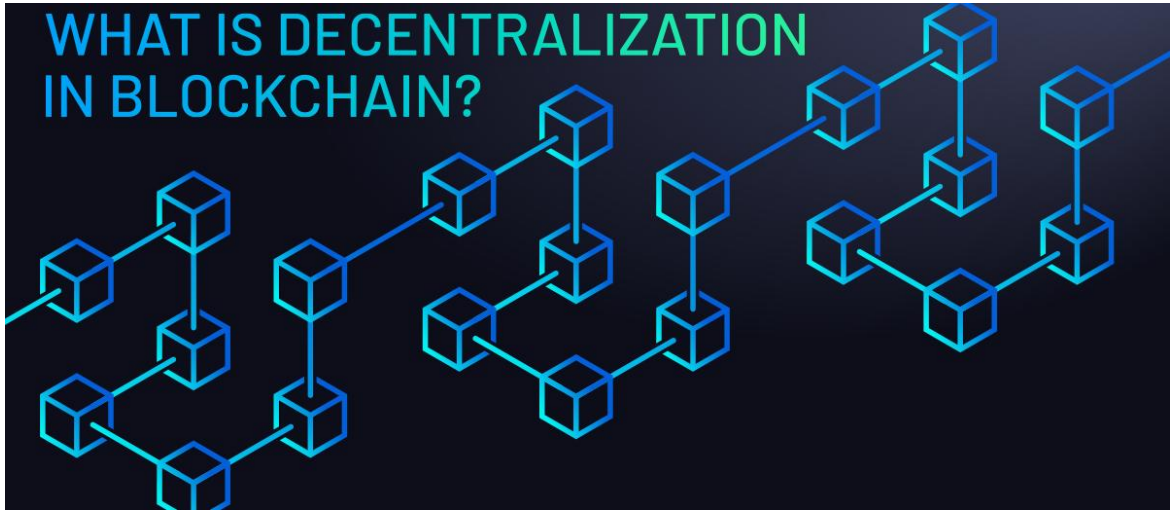
Decentralized Organization

Decentralized Organization

- Decentralization versus Distribution
- Centralized-distributed (Ce-Di) organizations
- Decentralized-distributed (De-Di) organizations
- Decentralized Autonomous Organizations
  - Aragon
  - DAOstack
  - DAOhaus
  - Colony.

Decentralization in Blockchain

- Blockchain decentralization refers to **distributing control across a network of computers** (called nodes) that work together to **maintain and validate the blockchain**.
- **Traditional centralized systems**: where a **central authority oversees transactions**. **Blockchain eliminate the need for intermediaries** by allowing **participants** to **collectively manage the system**.
- In a **decentralized blockchain**, **each node holds** a full **copy of the blockchain** and **participates in validating transactions**. This process, called a **consensus mechanism**, ensures all nodes agree on the validity of transactions, fostering trust and security within the network.



Decentralization in Blockchain

Types of Decentralization in Blockchain

- **Architectural Decentralization**
  - **physical spread of nodes across multiple locations, reducing the risk of failure** or attacks.
  - ensures the system can **continue functioning even if some nodes fail**.
- **Governance Decentralization**
  - **decision-making power is shared** among network participants through mechanisms like **voting or consensus protocols**.
  - **prevents** any single entity from **having full control** over the network's direction.
- **Data Decentralization**
  - **Data is stored** across many nodes in the network, **providing redundancy**.
  - makes the system **more secure and resistant** to censorship or **manipulation**.
- **Functional Decentralization**
  - **Different participants perform various roles** like mining, validating, executing smart contracts.
  - Spreading these functions across participants **ensures no single party controls all operations**.
- **Incentive Decentralization**
  - **Rewards or incentives are distributed** throughout the network, encouraging participants to act in the system's best interests.
  - This alignment of incentives **strengthens the network's overall security and functionality**.

Decentralization in Blockchain

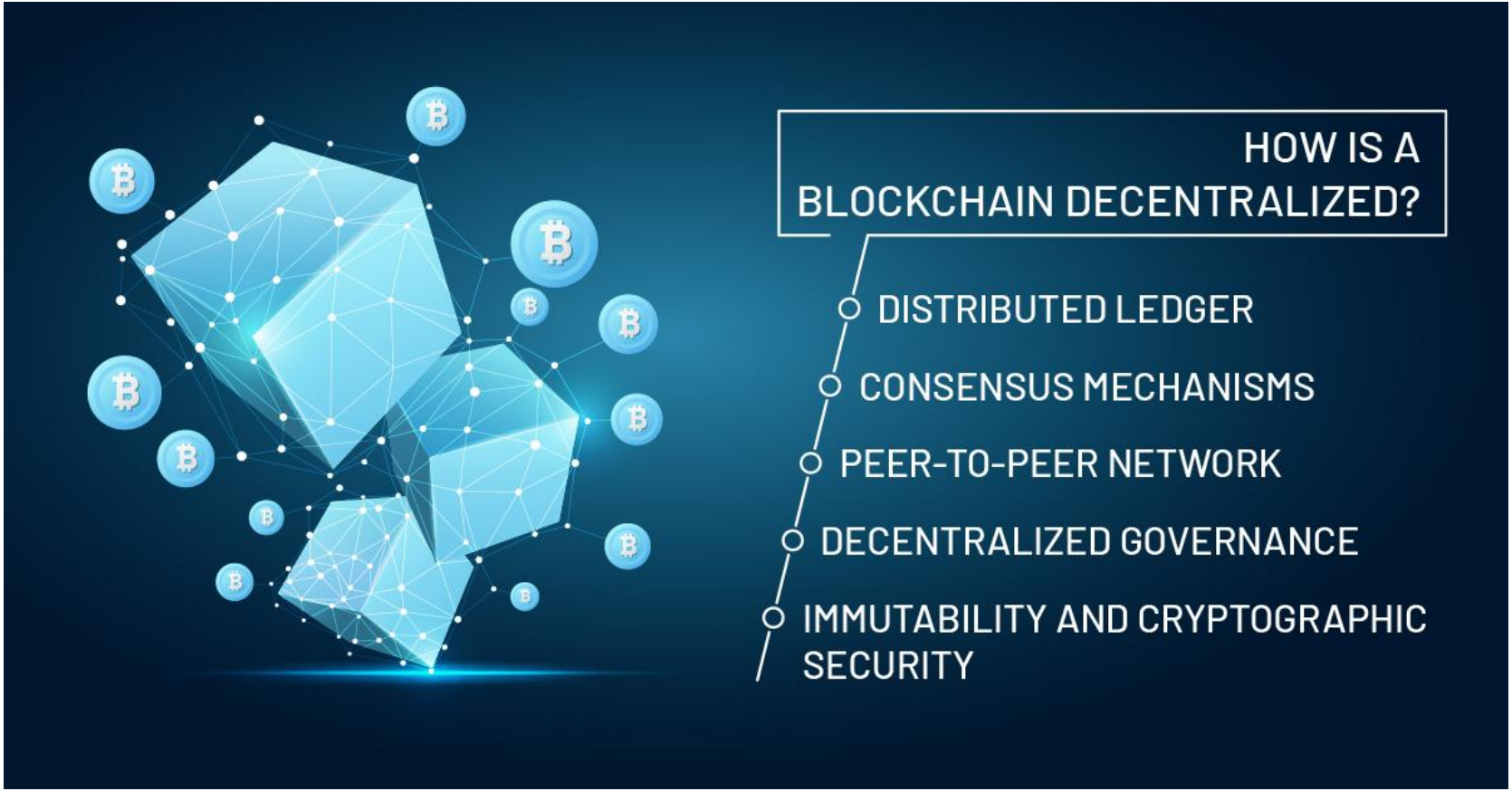
Advantages of Decentralization in Blockchain

- **Security**: **By distributing control**, decentralized networks are **harder to attack** or censor. The lack of a central authority **minimizes single points of failure**.
- **Transparency**: Blockchain's decentralized nature **allows everyone** in the network **to view transaction** history, **increasing accountability and trust**.
- **Trustlessness**: Decentralized systems **remove the need to trust central authorities**. The consensus mechanism ensures accuracy without reliance on a single entity.
- **Ownership**: Individuals can **directly control their assets and data** without relying on intermediaries.

Disadvantages of Decentralization in Blockchain

- **Scalability**: **slower transaction processing** as more nodes are involved in validating transactions.
- **Governance**: **decision-making can be slow**, leading to potential conflicts when participants disagree.
- **Security Risks**: While decentralization reduces central points of failure, **distributed networks can still be vulnerable to attacks like a 51% attack**.
- **User Experience**: **Managing private keys** & security responsibilities are difficult for non-technical users.
- **Regulatory Challenges**: complicate enforcement of regulations due to the absence of a central authority.
- **Energy Consumption**: Some consensus mechanisms, like Proof of Work, **require high energy consumption**, raising concerns about sustainability.

Decentralization in Blockchain



Decentralization in Blockchain

Blockchain decentralization is achieved through:

Distributed Ledger

- The blockchain's ledger, which **contains a record of all transactions**, is replicated and stored across multiple nodes in the network.
- **Each participating node maintains a complete copy of the blockchain**, creating a distributed ledger that is synchronized through consensus mechanisms.

Consensus Mechanisms

- utilize consensus mechanisms **to agree on the validity and order of transactions**
- Proof of Work (PoW) or Proof of Stake (PoS), involve a majority of network participants coming to a consensus on the state of the blockchain
- This consensus **ensures that all nodes have an equal say in validating transactions**, avoiding the need for a central authority.

Peer-to-Peer Network

- **operate on a peer-to-peer (P2P) network architecture**, where participants **connect directly with each other** without the need for intermediaries.
- Each node communicates with other nodes **to propagate transactions and blocks**, maintaining the integrity and consistency of the blockchain.

Decentralization in Blockchain

Decentralized Governance

- Some blockchain networks **employ decentralized governance models**, where **decisions** regarding protocol upgrades, changes, and improvements **are made through a consensus-driven process**.
- allows stakeholders in the network to **have a say in the governance of the blockchain**, reducing the centralization of power.

Cryptographic Security

- The use of cryptographic algorithms **ensures the integrity and security of data stored on the blockchain**.
- Once a block is added to the chain, it becomes extremely **difficult to alter past transactions without consensus from the majority of participants**.
- This immutability **protects the integrity of the blockchain and prevents tampering or manipulation**.

- By **combining these elements**, **blockchain decentralization** and a trustless system **is being achieved**, where **no single entity** or authority has **control over the network**. Instead, **power is distributed** among participants who **collectively maintain and secure the blockchain**.

Importance of Decentralization in Blockchain

Importance of Decentralization in Blockchain

Security: **enhances the security** of the blockchain network

- with a **distributed ledger** across multiple nodes, it becomes **challenging for malicious actors to manipulate or compromise the system**
- **no single point of failure** that can be targeted, making it **more resilient to attacks** and **ensuring the integrity** of the data stored on the blockchain

Trust and Transparency: fosters trust and transparency in blockchain networks

- Since the **ledger is distributed and replicated across multiple nodes**, anyone on the network can view the transaction history and verify its integrity
- transparency **reduces the need for trust in a central authority** and allows participants to **independently validate transactions**, ensuring the accuracy and integrity of the data

Elimination of Intermediaries

- Traditional systems often **require trusted third parties** to facilitate and validate transactions, which can **add costs, introduce delays, and increase the risk of fraud**
- With blockchain's decentralization, participants **can engage directly**, **reducing reliance on intermediaries** and **enabling peer-to-peer transactions**

Importance of Decentralization in Blockchain

Censorship Resistance: resistant to censorship and control

- As there is **no central authority** governing the network, it **becomes difficult for any single entity** or **group to exert control** over the transactions **or manipulate** the data
- This aspect is **particularly valuable in environments where censorship resistance and autonomy are desired**, such as in **financial systems or regions with political instability**

Ownership and Control

- allows individuals to have **direct ownership and control over their assets and data**
- Participants have **control over their private keys** and can **interact with** the blockchain network without relying on centralized institutions
- gives individuals **greater autonomy** and reduces the risk of their assets being subject to arbitrary restrictions or confiscation.

- Overall, decentralization in blockchain **empowers individuals, enhances security, promotes trust, and reduces reliance on intermediaries**
- making blockchain an innovative and disruptive technology with broad applications beyond just financial transactions

Impact of Decentralization in Blockchain

Impact of Decentralization in Blockchain

Disintermediation

- **removes the need for intermediaries** or central authorities in various processes
- **eliminates the associated costs, delays, and potential risks** associated with relying on intermediaries
- **enables peer-to-peer transactions and interactions**, allowing participants to transact directly with each other without the need for intermediaries like banks, clearinghouses, or brokers.

Empowerment

- Decentralization **gives individuals more control** over their data, assets, and digital interactions
- individuals can manage their own **digital identities**, **control access** to their personal information, and transact directly with others
- enhances privacy, autonomy, and self-sovereignty

Increased Transparency and Trust

- inherently transparent, as all transactions and data are **recorded on a shared ledger accessible to all**
- **combat fraud, corruption & manipulation** by providing an auditable & immutable record of activities

Enhanced Security

- improves the security and resilience of systems **by distributing control and data** across multiple nodes
- **more resistant to attacks**, hacking attempts, and single points of failure

Impact of Decentralization in Blockchain

- **even if some nodes are compromised**, the network can continue to operate without interruption, **ensuring data integrity and system availability**

Inclusive Finance Systems

- Decentralized finance (DeFi) is a rapidly growing sector within blockchain that aims to **provide inclusive financial services** to individuals who may not have access to traditional banking systems.
- DeFi **enable peer-to-peer lending, borrowing, trading, and other financial services**, eliminating the need for intermediaries and offering greater financial inclusion to underserved populations.

Democratic Decision-Making

- involves distributed governance mechanisms, allowing participants to collectively **make decisions about the network's rules, upgrades, and future development**
- ensures that stakeholders have a say in the evolution of the blockchain
- reducing the concentration of power in the hands of a few

Global Accessibility

- **accessible to anyone with an internet connection**, bypassing geographical & jurisdictional boundaries
- **enables seamless transactions and interactions across borders**, fostering interoperability between different systems and promoting international collaboration

Decentralization versus Distribution

- Blockchain networks exhibit both distribution and decentralization, but they are not the same thing.
- Understanding their differences is crucial in evaluating a blockchain's security, control, and resilience.

What is Distribution in Blockchain?

- A blockchain is **distributed** when its **ledger (database of transactions) is spread across multiple computers (nodes)** worldwide.
- This **ensures redundancy and fault tolerance** but does not necessarily mean that power is decentralized.
- **Key Features of Distribution in Blockchain**
  - **Multiple Nodes**: The blockchain ledger exists on many computers.
  - **Fault Tolerance**: If some nodes fail, the network continues to function.
  - **Geographical Spread**: Nodes are spread across different locations to increase security.
  - **Not Always Decentralized**: A network can be distributed but still controlled by a central authority (e.g., private blockchains).
- **Example of a Distributed but NOT Decentralized Blockchain**
  - Hyperledger Fabric (IBM Blockchain)
    - The ledger is distributed across multiple nodes.
    - However, a central authority (enterprise) controls who can participate.

Decentralization versus Distribution

What is Decentralization in Blockchain?

- A blockchain is decentralized when **control and decision-making are not in the hands of a single entity**. Instead, **power is spread across multiple independent participants**.
- **Key Features of Decentralization in Blockchain**
  - **No Single Authority**: No one entity controls the blockchain.
  - **Consensus-Based Decision Making**: Transactions are validated using protocols like Proof-of-Work (PoW) or Proof-of-Stake (PoS).
  - **More Security & Trust**: No reliance on a central authority to verify transactions.
  - **Censorship-Resistant**: No entity can block transactions or manipulate data.
- **Example of a Decentralized Blockchain**
  - Bitcoin (BTC) and Ethereum (ETH)
    - Thousands of nodes validate transactions.
    - No central entity has control.
    - Anyone can participate in mining or validation.

Decentralization versus Distribution

Key Differences: Decentralization vs. Distribution in Blockchain

Feature	Distributed Blockchain	Decentralized Blockchain
Control	Can be controlled by a single entity	No single entity has control
Decision-Making	Can be centralized (e.g., private blockchains)	Spread across multiple participants
Security	More secure than centralized systems but vulnerable if authority is compromised	Highly secure due to decentralization
Fault Tolerance	High (ledger is stored on many nodes)	High (many independent validators)
Example	Hyperledger (IBM)	Bitcoin, Ethereum

Can a Blockchain Be Both Distributed and Decentralized?

- Yes! The best blockchains are both distributed and decentralized:
  - **Bitcoin**: Thousands of independent nodes (distributed) with no central control (decentralized).
  - **Ethereum**: Thousands of validators (distributed) working independently (decentralized).
- However, some blockchains are distributed but NOT decentralized:
  - **Ripple (XRP)**: The ledger is distributed across multiple nodes, but Ripple Labs controls the majority of validators.
- Bitcoin and Ethereum are both decentralized and distributed, while private blockchains like Hyperledger are only distributed but centralized.

Centralized-Distributed (Ce-Di) organizations

- Centralized-distributed organizations blend elements of both centralized and distributed structures.
- In these organizations, **decision-making and control are primarily centralized**, but **operational execution or other functions are distributed across various nodes, teams, or locations**.
- This model strikes a balance between **having a central authority or leadership with the benefits of distributed execution** and autonomy in different parts of the organization.

Key Features of Ce-Di Organizations:

1. Centralized Leadership and Decision-Making

- Core strategic decisions, leadership, and high-level governance are typically **handled by a central authority or executive team**.
- This **ensures consistency in vision, strategy, and major organizational goals**.

2. Distributed Execution and Operations

- While decisions come from a central authority, **day-to-day operations, project execution, and specific functions** (like sales, R&D, or customer support) **are distributed** across teams or geographical locations.
- This is especially common in multinational corporations, franchises, or large-scale companies.

Centralized-Distributed (Ce-Di) organizations

3. Coordination and Oversight

- The **central authority maintains oversight** through reporting structures, regular communication, or performance management tools.
- **Distributed teams** or branches are held **accountable to central leadership** but are **given some degree of operational freedom**.

4. Flexibility with Accountability

- Ce-Di organizations aim to **provide local teams with enough autonomy to respond quickly to challenges**, while ensuring they **remain aligned with the overall goals and policies** set by the central leadership.

5. Scalability with Control

- The structure enables scalability by **distributing workloads, operations, or customer interaction across regions**, while **maintaining overall control** over the direction of the organization.

Centralized-Distributed (Ce-Di) organizations

Examples of Ce-Di Organizations:

- **Franchise Models**
  - In franchise businesses (e.g., McDonald's), the **central company sets guidelines**, branding, and strategy, **but franchisees operate independently** to run day-to-day activities based on the localized needs of the market.
- **Multinational Corporations**
  - Companies like Google or Amazon **maintain a centralized leadership for strategic decision-making**, but **have distributed teams or branches operating worldwide**, handling local operations and market-specific strategies.
- **Centralized IT Infrastructure with Distributed Teams**
  - In companies with centralized IT governance (cloud computing, data storage) but distributed teams, **central IT maintains control over systems and security**, while **individual teams manage their local systems or projects**.

Centralized-Distributed (Ce-Di) organizations

Benefits of Ce-Di Organizations:

- **Strategic Alignment**
  - A centralized decision-making authority ensures that **all parts of the organization are working toward the same overarching goals**.
- **Operational Flexibility**
  - Distributed teams **have the flexibility to adapt to local market conditions**, regulatory environments, or **customer needs**, providing a degree of agility.
- **Efficiency**
  - Centralized leadership **can make high-level decisions quickly**, while distributed execution **allows for efficient scaling and localized problem-solving**.
- **Risk Management**
  - Centralization helps **mitigate risks by maintaining control over critical areas** (e.g., cybersecurity, financial decisions), while distribution **allows for resilience** through redundancy in operations.

Centralized-Distributed (Ce-Di) organizations

Challenges of Ce-Di Organizations:

- **Communication Gaps**: Ensuring smooth communication between central leadership and distributed teams can be challenging, **leading to potential misunderstandings or delays**.
- **Maintaining Control**: While operations are distributed, central leadership needs to ensure that **all distributed entities remain aligned with corporate policies and goals**, which can be difficult to enforce.
- **Cultural Differences**: In multinational or geographically distributed organizations, **local teams may have different cultural approaches to work**, which can create friction with centralized management.
- **Resistance to Local Innovation**: Centralized control may **limit the ability of distributed teams to innovate or react to local conditions**, as they may be constrained by overarching policies or strategies.

Ce-Di organizations offer the stability of centralization with the operational flexibility of distribution, making them well-suited for large-scale enterprises, especially those with global operations or complex functional structures.

Decentralized-Distributed (De-Di) organizations

- Decentralized-distributed (De-Di) organizations are characterized by their **lack of a central authority** or hierarchical structure, and the **distribution of decision-making power** across various nodes or participants.
- This model is often **associated with blockchain technologies, peer-to-peer networks, and other** decentralized systems, **where autonomy, collaboration, and transparency are emphasized**.

Key features of De-Di organizations include:

- **Decentralized Governance**: Instead of relying on a single authority, **decision-making is distributed** across multiple actors. This is often **achieved through consensus mechanisms, voting systems, or smart contracts**.
- **Autonomy**: Each node or participant **operates autonomously**, contributing to the overall function of the organization **without needing constant oversight or approval from a central authority**.
- **Transparency**: Decisions, transactions, and operations are often **visible to all participants, fostering trust and accountability**.
- **Scalability**: These organizations are often **highly scalable because they don't rely on a single point of control**. The distributed nature **allows them to grow organically**, with each new participant contributing to the network.
- **Resilience**: The distributed nature of these systems makes them **more resistant to attacks, failures, or manipulation**, as there is **no single point of failure**.

Decentralized-Distributed (De-Di) organizations

Examples of De-Di organizations:

- **DAOs (Decentralized Autonomous Organizations)**: Organizations that are **governed by smart contracts** on a blockchain.
- **Peer-to-Peer Networks**: Systems like BitTorrent, where **data is shared and distributed among peers without a central server**.
- **Cryptocurrencies**: Decentralized currencies like Bitcoin and Ethereum **operate without a central authority and distribute ledger management across participants**.

Benefits of De-Di Organizations:

- **Increased Security**: By spreading decision-making and data storage, De-Di models **reduce the risks associated with centralized data breaches or attacks**.
- **Improved Efficiency**: **Automation**, especially through smart contracts, can **reduce the need for intermediaries, speeding up processes**.
- **Empowerment of Participants**: **Participants have more control and ownership over decisions and resources**.

Decentralized-Distributed (De-Di) organizations

Challenges:

- **Coordination:** Without a central authority, **achieving consensus can be complex and time-consuming**.
- **Regulatory Issues**: Governments and regulatory bodies often **struggle with how to regulate decentralized organizations**.
- **Complexity of Governance**: Developing efficient and fair governance models that **ensure accountability and prevent abuse of power remains a challenge**.

Decentralized-distributed models represent a significant shift in organizational structures, offering both new opportunities and challenges in areas like governance, security, and efficiency.

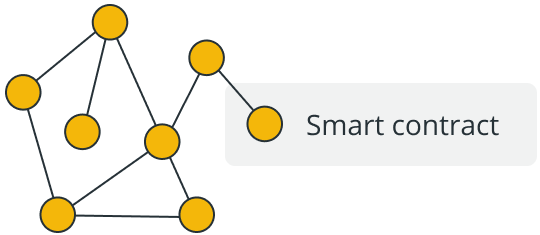
Decentralized Autonomous Organizations

- A Decentralized Autonomous Organization (DAO) is a way to **manage and organize groups without the need for a central leader** or traditional management structure.
- DAOs became possible with the rise of blockchain technology, **allowing communities to operate independently and transparently, where decisions are made collectively by the members**.
- **Example**
  - Imagine you and your friends start a fitness club, but instead of putting one person in charge, you all agree to vote on every decision.
  - If you need to decide on purchasing new equipment, everyone votes, & the majority decides.
  - This way, no single person has all the power, & everyone has an equal say.
- To make things more efficient, **instead of meeting in person, you use the internet to vote**, which further **decentralizes decision-making**.
- This system runs automatically, based on a set of agreed-upon rules. This is essentially how a DAO functions.

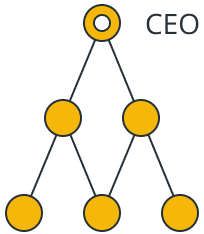
Decentralized Autonomous Organizations

DAO vs Traditional hierarchical structure

- A DAO is a modern **way to manage resources and people without relying on a central authority**, like a CEO or government.
- In traditional organizations, **leaders or boards make key decisions**.
- In a DAO, there is **no single person in charge**.
  - Instead, the **members decide together using computer code** — like a set of rules written into a computer program — that everyone in the organization agrees on.
  - These rules are often **stored on a blockchain**, a digital ledger that **tracks everything** transparently and securely.



Decentralized decision-making



Centralized decision-making

Decentralized Autonomous Organizations

How DAOs Work

- Let's take the fitness club example. Say your **club needs to buy a new treadmill**, and you must decide how to allocate the funds. Normally, a treasurer would handle the money and make purchases.
- But in a DAO, this **process is automated using smart contracts**, which are **self-executing contracts with terms directly written into the code**.
  - **Proposal**: One of the members **submits an online proposal** to buy a new treadmill, and all members can view it.
  - **Voting**: Members then **vote on the proposal**. **Voting power** may be influenced by the **level of involvement or contribution to the club**. The DAO's system automates the voting process.
  - **Execution**: If the **majority agrees**, the smart contract **automatically releases the funds and makes the purchase**. No one needs to handle the money—the code does it all.

Decentralized Autonomous Organizations

DAO vs. Traditional Organizations

- DAOs **rely on a collective decision-making process powered by smart contracts** on a blockchain.
- Traditional organizations **use a hierarchical structure where decisions are made by leaders** or managers at the top.

	Decentralized automated organization	Traditional organization
Decision-making	Collective voting	Centralized authority
Governance	Managed by smart contracts	Managed by executives or a board
Transparency	High (blockchain records)	Limited (internal reporting)
Inclusivity	Open to all members	Restricted to top management
Efficiency	Automated, minimal to no bureaucracy	Manual, often bureaucratic
Control	Decentralized, shared	Centralized, top-down
Global reach	Accessible worldwide	Often limited by geography
Adaptability	Quick, consensus-based changes	Slower, formal change processes

Decentralized Autonomous Organizations

Benefits of DAOs

- The main goal of a DAO is **to create a system where decisions are made fairly and transparently, with no single person or group having control over the rest**.
- In a DAO, **everyone has the opportunity to propose ideas and vote on important matters**, ensuring the group's direction reflects the collective will of its members.
- Key benefits of DAOs include:
  - **Inclusivity**: Every member has an **equal opportunity** to contribute and influence decisions.
  - **Decentralized control**: **Decisions are made collectively** with DAOs, **reflecting the will of all members** of the entire community.
  - **Transparency**: All decisions and transactions are recorded on a blockchain, **making everything open to review and reducing corruption**.
  - **Efficiency**: DAOs **operate through smart contracts**, which streamline processes by **removing the need for traditional administration**.
  - **Global participation**: DAOs **allow participation from people worldwide, enabling diverse perspectives**.

Decentralized Autonomous Organizations

Types of DAOs

- DAOs come in **various forms**, each designed **to address specific needs.**
- Like **managing investment, governance, services** and much more, may **have distinct committees for different responsibilities**.
  - **Investment DAOs**: **Members pool money and vote on investment opportunities**, such as buying trendy exercise equipment for your fitness club.
  - **Social DAOs**: These **focus on building a community or supporting a cause**, with members collaborating on shared goals.
  - **Service DAOs**: Members **provide services** (e.g., organizing fitness events) and **are rewarded** for their contributions.
  - **Governance DAOs**: These **allow members to vote on decisions** about how the organization is run, such as choosing new fitness classes or **setting rules**.
  - **Protocol DAOs**: These are responsible for **maintaining and updating technical protocols**, such as managing the rules for a fitness app.

Decentralized Autonomous Organizations

Challenges and Limitations of DAOs

- While DAOs offer many advantages, they also face several challenges:
  - **Scalability**: As **more members** join, **decision-making can become slower and more complicated**.
  - **Complexity**: Setting up and running a DAO **requires technical expertise**.
  - **Security risks**: DAOs are **vulnerable to hacking and coding errors**.
  - **Participation fatigue**: **Frequent voting** can lead to **decreased member engagement** over time.
  - **Legal issues:** DAOs **face uncertainty** in terms of **legal recognition and regulatory compliance**.
  - **Immaturity:** DAOs are **still new**, **with limited real-world experience** to guide best practices.

The Future of DAOs

- Although DAOs are **still in their early stages**, they **have the potential to revolutionize** how we think about governance, organizations, and decision-making.
- By eliminating the need for central authorities and ensuring transparency, DAOs may **provide a more democratic and efficient way to manage everything** from small clubs to large global projects.
- However, as with any new technology, **there are risks and challenges**, but continued development could lead to creative solutions and wider adoption.

Decentralized Autonomous Organizations

Assignment Topics

- Decentralized Autonomous Organizations:
  - Aragon
  - DAOstack
  - DAOhaus
  - Colony

Text Book and Reference Books

Text Book

- Dhillon, V., Metcalf, D., and Hooper, M, Blockchain enabled applications, 2017, 1st Edition, CA: Apress, Berkeley.

Reference Books

- Diedrich, H., Ethereum: Blockchains, digital assets, smart contracts, decentralized autonomous organizations, 2016, 1st Edition, Wildfire publishing, Sydney.
- Wattenhofer, R. P, Distributed Ledger Technology: The Science of the Blockchain (Inverted Forest Publishing), 2017, 2nd Edition, Createspace Independent Pub, Scotts Valley, California, US.