Introduction to Blockchain Technologies

Unit 2

Decentralization

Methods of Decentralization – Routes to Decentralization – Smart Contract – Decentralized Organization – Platforms for Decentralization – Consensus Algorithms

Decentralization and its Methods

What is decentralization

- Decentralization is the idea that power doesn't sit in one place.
- In decentralized systems, control is distributed across a network.
- In blockchain, decentralization means that no single entity has the power to alter the ledger or control the network.

Importance of Decentralization

- Too much power is too few hands leads to abuse- whether it is banks, tech giants, or governments.
- By spreading power across a network, blockchain makes it harder to abuse power. Blockchain makes systems more resilient, transparent and ultimately, more democratic.
- In a decentralized blockchain, the rules are clear, and no one- not even the developers can change them on a whim.

Methods of Decentralization

1. **Technology-Based Decentralization**
    - In this method, the technology does all the work, where no kind of compromise is possible.
    - Blockchain's architecture- cryptographic algorithms, distributed ledgers, peer-to-peer networking- ensures that no single point of failure exists.

- If one node goes down, another node takes its place.
- Technology-based protocol uses protocol that runs like clockwork, so long as the network is alive.

2. **Governance-based Decentralization**
    - In governance-based decentralization, it is not about distributing power in the system- rather it is about distributing decision-making.
    - In governance-based decentralization, everyone has a stake in the system. All shareholders can decide how the network evolves.
    - This can happen on-chain, where votes are coded into the blockchain itself, or off-chain, where decisions are hashed out by the community.

3. **Hybrid Approaches**
    - Hybrid approaches are middle ground approaches that recognize that pure decentralization isn't always practical- or even desirable.
    - Hybrid models start out centralized but plan to decentralize over time, or they keep some centralized elements to ensure that things don't spiral out of control.
    - For example, in Ethereum, it started out with a clear leadership structure, but it has gradually moved towards a more decentralized model.
    - Hybrid models are about balancing the ideal with the practical- decentralization but with a safety net.

Routes to Decentralization

Blockchain projects can take different routes on their way to decentralization. Some paths and strategies include:

1. **Gradual Decentralization**
    - Most projects start on this path- centralized leadership with a plan to hand over control as the project matures.
    - It starts with a core team that makes big decisions, then gradually decentralizing that control to the community through governance mechanisms like token voting or decentralized autonomous organizations (DAOs).

Example-When Ethereum was first launched, it was managed by its creator- Vitalik Buterin. But over time, Ethereum has evolved into a project where the community has a real say in its direction. It is not fully decentralized yet, but it is on the road, with mechanisms like the Ethereum Improvement Proposal (EIP) process giving the community more control.

2. Forks and Splits

- When gradual decentralization doesn't work, some projects take the more radical route-splitting off entirely.
- This happens when there is a fundamental disagreement in the community about the direction of the project.
- It could be about technical issues, governance or philosophy.
- Whatever be the cause, the solution is the same: a fork in the road where each side goes their own way.
- Sometimes both parties of a fork go on to create something great, while at other times, there is one side that flourishes, while the other side fades into obscurity.
- Forks are risky, but they are also a way to force innovation and maintain decentralization, when a project original vision starts to get blurry.

Examples

- **Bitcoin**'s story is all about forks- the split between Bitcoin and Bitcoin cash is a classic example of how decentralization can lead to divergent paths.
- Bitcoin stuck with the stuck with its original version, while Bitcoin Cash pursued larger block sizes for faster transactions.

- Another example is the **Ethereum Classic** saga- after the DAO hack, Ethereum decided to roll back its blockchain. This was a move that didn't sit well with everyone.
- As a result, the hard fork created Ethereum Classic, a project that stuck with the original, unaltered blockchain.

Smart Contracts

What

- A smart contract is a self-executing agreement coded directly into the blockchain.
- Once certain conditions are met, it automatically does what it is programmed to do- whether it is transferring money, changing ownership, or executing any other agreed-upon action.
- The key is that there is no middleman. There is only code running on the blockchain, doing exactly what it is supposed to do.
- And since it is on a blockchain, it is immutable- once it is deployed there is no going back.

How They Work on Platforms like Ethereum

- Platforms like Ethereum are where smart contracts are primarily written.
- Ethereum has a Turing-complete blockchain, which can run any computation expressible by an algorithm.
- This means that smart contracts aren't just static agreements, they're dynamic programmable tools that can handle complex transactions and processes automatically.

Use Cases of Smart Contracts in Various Industries

1. Finance- Smart contracts are the backbone of DeFi. They automate everything from loans to trading. There is no need for any banker's approval, its just you, the code and your collateral.
2. Real Estate- A smart contract could handle the entire transaction of buying a house, from automating payments, transferring ownership and recording everything on the blockchain.
3. Supply Chain: Supply chains are becoming more transparent thanks to smart contracts. This can be in the form of contracts that release payment only when goods are delivered and verified. This will prevent shady deals and delays. The contract enforces itself, keeping everyone honest and efficient.
4. Insurance- Normally, insurance claims are notoriously slow and bureaucratic. Smart contracts can automatically trigger payouts based on pre-set conditions. There is no need to haggle with an insurance adjuster- the contract just does its job

5. Intellectual Property- Smart contracts are also changing the game for artists and creators. Musicians for example, can use smart contracts to get paid instantly whenever their song is streamed. There are no middlemen or delays- just money flowing straight from the listener to the artist.

Decentralized Autonomous Organizations (DAOs)

What

- A DAO is essentially a company without the company.
- It is an organization that is governed entirely by smart contracts and the people who hold its tokens.
- There is no central authority, no management structure, just a set of rules encoded on the organization that dictate how the organization operates.
- Decisions are made collectively by the community through votes, with each token representing a vote.
- The more tokens you hold, the more influence you have.
- DAOs are transparent, democratic, and runs autonomously.
- Once the code is deployed, the DAO operates on its own, executing decisions based on the outcome of votes, all without needing human intervention.

Structure and Operation of DAOs

- The structure of a DAO is flat—no bosses, no departments, no bureaucracy. Everything is laid out in smart contracts, which handle the nuts and bolts of operations.
- If one wants to start a new project or change the rules-submit a proposal to the DAO.
- The community votes on it, and if it passes, the smart contracts execute the decision automatically.
- DAOs typically have treasuries funded by their members or through investments, and these funds are used to finance projects, pay contributors, or reward participants. But every spending decision is put to a vote, ensuring that no single person can drain the coffers or steer the organization in the wrong direction.

Notable DA and their Influence

- **MakerDAO-**It's the decentralized organization behind the DAI stablecoin, a cryptocurrency pegged to the US dollar. MakerDAO operates without a central authority, with decisions made by its community of token holders. They vote on everything from monetary policy to system upgrades, effectively running what is essentially a decentralized central bank.
- Another example is **Uniswap**, a decentralized exchange that lets users trade cryptocurrencies without a middleman. Uniswap is governed by a DAO, where token holders vote on changes to the protocol, fee structures, and new features..
- "**The DAO",** raised $150 million in a 2016 crowdfunding campaign. It was designed to be a venture capital fund run entirely by its investors, with no general partners or management team. Unfortunately, The DAO was hacked due to a flaw in its smart contract, leading to a loss of funds and a controversial hard fork in the Ethereum blockchain.

Impact of DAOs

- It reshapes the concept of what an organization can be
- It takes the core idea of decentralization and applies it to corporate governance.
- The model has huge implications for the future of work, finance and governance.
- DAOs offer a glimpse of a world where organizations are more transparent, more democratic and more aligned with the interests of their members.
- They also come with challenges- security risks, slow decision making processes, the potential for factionalism.

Platforms for Decentralization

There are numerous platforms where decentralization is offered, but each has its own quirks, strengths and flaws. Some of the most notable platforms are:

1. **Ethereum**
    - One of the first decentralized platforms
    - Launched in 2015, the brainchild of Vitalik Buterin
    - Ethereum is more than just a cryptocurrency, it is a platform for building dApps.

- It is the platform that made blockchain a household term.

Strengths

- First in the market advantage
- It is the platform that introduced the world to smart contracts and decentralized apps, and it has a massive developer community behind it.
- It has led to innovation in DeFi, DAOs, NFTs etc.
- Most new applications start out on Ethereum

Weaknesses

- Biggest weakness is scalability.
- As more and more people use the platform, it has struggled to keep up
- Transactions can be slow, and fees can skyrocket during peak times.
- Ethereum 2.0 promises to fix this with PoS and sharding, but those upgrades are still in progress.

2. EOS

- Relatively new- launched in 2018
- EOS was designed to solve some of Ethereum's biggest problems- namely scalability and transaction speed.
- EOS has a very user-friendly experience, zero transaction fees, and the ability to process millions of transactions per second.
- However, EOS uses Delegated Proof of Stake consensus mechanism, which has raised questions about how decentralized it actually is.
- It is a platform that promises to make blockchain accessible to the masses but at the potential cost of trust decentralization.

Strengths

- Biggest strength- speed
- Designed to be fast, scalable and user friendly
- Can handle a high volume of transactions

Weaknesses

- Platform not as decentralized as it sounds
- Only 21 people are responsible for validating transactions- power is in the hands of a few.

3. Cardano

- Founded by Charles Hoskinson, Cardano is all about using peer-reviewed research and evidence-based methods to build a more secure, scalable and sustainable blockchain.
- Cardano is notable for its layered architecture, and focus on solving the big issues that have plagued its predecessors.

Strengths

- Biggest strength is in its methodical approach
- All aspects of Cardano are built on a foundation of rigorous academic research
- Gives it a solid technical base and a clear roadmap for future development
- Has a layered architecture that separates the settlement layer from the computation layer, which should make it scalable and secure over the long term.

Weaknesses

- Progress is very slow due to careful, academic approach
- Takes a long time to roll out features
- Cardano is still catching up to Ethereum in terms of real-world adoption and developer activity.