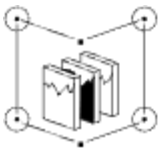

Digital Assets Academy[23]

Lecture 06 — What is Decentralization and why is it key to Digital Assets?

Transcript

Decentralization occurs when individuals or nodes work collectively in a distributed manner to achieve an objective without reliance on a centralized intermediary. In the case of a blockchain, maintaining decentralization while processing transactions, adding to the ledger, and extending the blockchain is a core attribute that can offer advantages over traditional centralized systems.

Centralized networks are controlled by a central authority, such as a corporation, government, or central bank.

Decentralized networks are usually controlled by the community or the users themselves.

Decentralization can offer benefits in security, resilience, and scalability.

In this Digital Asset Academy, we looked at the three main categories of digital assets: (1) Cryptocurrencies, (2) Tokenized Money, and (3) Tokenized Assets.

As explained in our introduction lecture, digital assets leverage blockchain technology to transmit information on a peer-to-peer network and store it in a decentralized ledger.

We differentiate between public and private blockchains. Public blockchains utilize open infrastructure to arrive at a consensus among nodes and are developed using open-source methodologies. Private blockchains may restrict who can participate in consensus, which nodes can access data, and who can transact. Depending on their design, private blockchain records may be edited, overridden, or even deleted by the operator of the network.

Today, most digital assets are utilizing “public blockchains” and are either fully decentralized or aspire to be. For instance, the two largest cryptocurrencies by market capitalization, Bitcoin and Ethereum, are developed in a completely open-source process and operate as decentralized public blockchains.

Public blockchains offer transparency and accessibility, while private blockchains may be able to offer additional privacy, speed, or control at the expense of decentralization. Whether an application is best suited for a decentralized public blockchain or a centralized private blockchain depends on the use case and needs of its users.

So why do most digital assets use public blockchains and leverage decentralization?

To answer that, we can look at the evolution of the Internet. An illustrative analogy is the rivalry in the 2000s between Wikipedia and its centralized competitors like Encarta. If you compared

the two products in the early 2000s, Encarta was a far better product, it had better topic coverage and much higher accuracy. But Wikipedia improved at a much faster rate because it had an active, global community of volunteer contributors who were attracted to its decentralized, community-governed ethos. By 2005, Wikipedia was the most popular reference site on the internet. Encarta, on the other hand, was shut down in 2009. Global, permissionless decentralization dramatically scaled both the number of contributors and the scrutiny of the content, ultimately leading to the high levels of accuracy. Similarly, anyone can view and contribute to the open-source software that powers Bitcoin and Ethereum, dramatically increasing the likelihood that bugs are identified, particularly given the significant amount of money and resources committed.

During the first era of the internet — from the 1980s through the early 2000s — internet services were built on open protocols that were controlled by the internet community. The internet was largely decentralized and centralized platforms like AOL remained relatively small. Applications with decentralization properties like IRC, BitTorrent, and WordPress were extremely common.

During the second era of the internet, from the mid-2000s to the present, for-profit tech companies — most notably Google, Apple, Facebook, and Amazon — built software and services that rapidly outpaced the capabilities of more decentralized and open protocols. The internet as a result became largely centralized, and digital private property wasn't possible. Advertising became one of the main forms of economic incentive and monetization.

We are in the process of entering the third phase of the Internet: Web3, where decentralization is again possible with the emergence of networks that (1) use consensus mechanisms such as blockchains to maintain and update data and transactions and (2) use cryptocurrencies (coins/tokens) to incentivize consensus participants, such as miners and validators, and other network participants.

In the early days of the Internet, working groups and non-profits relied solely on the alignment of interests of the community. The same has been true for much of open-source software over the years, which can sometimes result in misaligned incentives, diverging project goals, or wasteful resource allocation. But blockchain-based networks can offer a solution to this tragedy of the commons by providing economic incentives to developers, maintainers, and other network participants in the form of tokens.

Why can decentralization be useful?

Governments and corporations keep ledgers and databases to confirm authority, ownership, status, or transactions. For instance, your bank manages a bank ledger to know how much money you have in your bank account and how much is owed to the bank by its debtors, such as mortgage borrowers. Or the government, they keep a database of citizenship and manage your right to travel. These entities have near total control over the ledgers and users must trust them to operate them effectively, efficiently, and fairly.

A public blockchain is a digital, decentralized, distributed ledger that confirms ownership, identity, status, and transaction history without relying on centralized authorities or single institutions. Regarding Bitcoin, Satoshi Nakamoto wrote "the problem with conventional currency is all the trust that's required to make it work." Public blockchains like Bitcoin and Ethereum achieve data integrity and database state change – that's the concept of altering records and changing the "final state" of the database – using mathematics, computer science, and cryptography rather than trusting a centralized institution.

This achievement allows for trust-minimized money, cryptocurrencies, and for decentralized applications such as those that power tokenized money or tokenized assets. The public blockchain's decentralization allows these assets and use cases to be transparent, unalterable, verifiable, and secure. Together, these features help public blockchains achieve "credible neutrality," an important concept that public blockchains achieve or aspire to.

This is not to say that all centralized organizations are bad or that all institutions and corporations should be decentralized, but rather that blockchain technology offers an alternative. It can enable us to build more efficient, transparent, and robust networks with the right incentive structures.

There are trade-offs that need to be considered. For instance, in a fully decentralized system, the lack of a central governing authority means that there is no one to hold accountable if something goes wrong. Decentralization can also lead to slower transaction speeds or higher costs to transact. However, decentralization can offer the following advantages:

Fault Tolerance: Decentralized systems are less likely to fail accidentally because they rely on many separate components. They are not linked to a single point of failure.

Attack Resistance: Decentralized systems are more expensive to attack and destroy or manipulate because they lack sensitive central points that can be attacked at much lower cost than the economic size of the surrounding system.

Collusion Resistance: It is much harder for participants in decentralized systems to collude to act in ways that benefit them at the expense of other participants.

Centralized platforms have been dominant for so long that many people have forgotten there could be a better way to build internet services. Blockchain technology offers an innovative and powerful way to develop community-owned networks. It can help level the playing field for third-party developers, creators, and businesses.

We saw the value of decentralized systems in the first era of the Internet. Hopefully, we'll get to see it again in the next.

In Summary:

Decentralization can have scalability and safety benefits.

A public permissionless blockchain is a digital, decentralized, distributed ledger that doesn't rely on single centralized authorities or institutions.

Most of the biggest cryptocurrencies use decentralized public blockchains.

Tokens can provide economic incentives, allowing for a potentially better Internet, where more decentralization is possible. We call this Web3.

There are trade-offs that need to be considered, such as the lack of a central governing authority that can be held accountable.

Decentralization can potentially provide three main advantages, depending on the size and structure of the network. These include: Fault Tolerance, Attack Resistance, and Collusion Resistance.