



Lecture 01 — Introducing the Basics – What are Digital Assets?

Transcript

Welcome to our Digital Asset Academy. We hope to offer you a bite-sized learning program that can help you understand the basics of digital assets, including Bitcoin, Ethereum, Stablecoins, and much more.

Over the course of eight weeks, you will receive a weekly video lecture, a list of resources, and the opportunity to engage with us on digital assets.

Let's get started by defining some key terms:

Crypto. Before the advent of cryptocurrencies, the term “crypto” was most used as shorthand for cryptography, the study of techniques for secure communication. However, since the launch of Bitcoin in 2009, crypto became shorthand to refer to the budding and fast-growing industry of cryptocurrency companies, markets, and applications.

Digital assets in the context of crypto are any assets issued, represented, and transferred on a blockchain.

Blockchains are the technology solutions that enable digital assets. We differentiate between public and private blockchains, but much more on that later. What you need to know: a public blockchain is a method of securely recording information on a peer-to-peer network. It's a shared public database, replicated across computer systems in which new entries can be added but existing entries cannot be altered or reversed.

Blockchain entries, called blocks, are generated via specific consensus protocols that are different for each blockchain. Each block contains information about the previous block, reinforcing the order of entries, or transactions, as the network progresses.

Every time a user initiates a transfer of digital assets, these transactions are recorded on the blockchain ledger. Digital assets are transferred to and from blockchain addresses or accounts. Each address has a public and private key associated with it, which you can think of like a computer-generated email address and password. A public key can be shared publicly and is used to receive digital assets, while a private key must be kept secret and is used to sign the messages that send digital assets from your wallet.

A wallet is a tool that stores public and private keys and enables the user to use those keys to sign off on transactions.

A custodial wallet is controlled by a trusted third party, such as an exchange or a custodian, and users generally have access to their wallet through a third-party web interface. These providers store the private keys for the end user.

A non-custodial wallet gives users complete control over their keys, without relying on any trusted third party.

You can also purchase a hardware wallet, a device that can look like a small USB drive and allows you to store your digital assets—it's often considered the most secure and private solution to store your crypto, as long as you take the appropriate measures. You can even retrieve your digital assets if you lose your wallet, you just cannot lose your private keys or your recovery phrases.

Let's take a look at how we can break down the digital asset ecosystem to better understand the different types of blockchains. For digital assets we usually draw a comparison to today's financial ecosystem and how it translates to a new tokenized financial ecosystem.

We can break down digital assets into three main categories:

Category one: cryptocurrencies. Cryptocurrency refers to digital assets native to a blockchain that can have multiple value propositions including their function as infrastructure, payment, and/or utility tokens.

Crucially, cryptocurrencies do not reference off-chain data to derive their value, that is, they are native to the public blockchain.

Category two: tokenized money. Tokenized money includes stablecoins, Central Bank Digital Currencies or CBDCs, and tokenized deposits, designed to leverage blockchain technology to fully digitize fiat currencies and make them more efficient in terms of settlement, programmability, and transparency.

Stablecoin prices are most often backed by fiat currencies. We will provide more details in our Stablecoins lecture. CBDCs are a tokenized money form that represents legal tender fiat currency and is backed by central banks.

Category three: token assets. The third category, tokenized assets, includes security tokens, tokenized funds, and Non-Fungible Tokens, NFTs, that allow the digitization of traditional assets, as well as the protection and proof of ownership of virtual items and intellectual property. Crucially, tokenized assets involve the creation of a blockchain token that references an asset that lives off the blockchain. For example, real estate exists in the physical world – it is not natively digital. The record of ownership, such as a property deed, exists in paper form

today. “Tokenizing real estate” thus involves replacing the physical paper property deed with a blockchain token.

We will offer more details in our “DeFi, Tokenization, and NFTs” lecture.

It’s okay to be confused by digital assets. They can often be overwhelming and complex. Think about it this way, every day people use the Internet without fully understanding every protocol and network layer. Similarly, we believe blockchain technology will become an invisible part of our lives. So don’t worry and take your time learning about this new space. Let’s try to understand the basic architecture of digital assets.

Layer 1: The protocol that fulfills the basic functions of a blockchain architecture such as code execution, data availability, consensus, and transaction settlement.

Most Layer 1 are “public blockchains” like Bitcoin or Ethereum. Public blockchains utilize open infrastructure to arrive at consensus among nodes and are developed using open-source methodologies. Private blockchains, on the other hand, may restrict who can participate in consensus, which nodes can access data, and who can transact.

Layer 2: Scaling solutions that sit on top of the main blockchain, Layer 1. While they can all work differently, their main function is to make transactions faster and cheaper by aggregating data and transactions.

For example, Bitcoin’s Lightning Network allows users to send many cheap payments quickly while minimizing the need to settle on the Layer 1 blockchain. This concept of “aggregate settlement” or “delayed settlement” is a common way that Layer 2 networks can help address concerns around transaction time, fees, or energy consumption.

Applications may be supported directly on Layer 1 or seek more scalability on a Layer 2 network.

The Application Layer hosts services for users to view, trade, and utilize digital assets in on-chain exchanges, games, or DeFi.

In essence, these layers together make the blockchain a complete solution, ranging from data management at the back end to enabling user-facing applications at the front end.

In the following lectures, we’ll explore some of the fundamental concepts and the three digital asset categories in more detail.

In Summary:

Blockchains are the underlying technology solutions that enable digital assets.

We differentiate three main digital asset categories: Cryptocurrencies, Tokenized Money, and Tokenized Assets

Digital assets are stored and recorded on a blockchain ledger.

A ledger entry has a public and private key associated with it. The keys that give you access to it are stored in a wallet.

Always protect your private key by using a custodial or a non-custodial wallet.

We identify different blockchain layers that allow a blockchain to scale and offer different functional applications and use cases for digital assets.