Fireblocks
Academy

Digital Assets 101:

A Beginner's Guide for Institutional Investors

Part I: Blockchain Basics

Overview

The world of digital assets is growing and changing very quickly. Your clients, customers, executive management, and board are likely all asking you about this space – and for good reason.

At the time of this writing, the crypto market now has a market cap of more than $2 trillion and the number of crypto wallets has ballooned to more than 260 million. Meanwhile, money that is “locked” in decentralized finance (“DeFi”) pools has skyrocketed to more than $80 billion in a matter of months, and there is now more than $120 billion in stablecoins. Clearly, there is retail and institutional interest in this space, but the infrastructure and operational support models for digital assets differ from traditional assets, and understanding these differences is key to being able to deliver products and services to your customers.

Our purpose here is to help create the basic building blocks of knowledge on digital assets - touching on the foundational layers of how digital assets are built and work, what the market looks like, who the players are, how the capital markets work, and how to think about the impact it can have on your business. This paper will discuss the basics of blockchain and discuss what blockchain is, how it works, and what you need to know about public and private keys. You can learn more on other topics at www.fireblocks.com/academy.

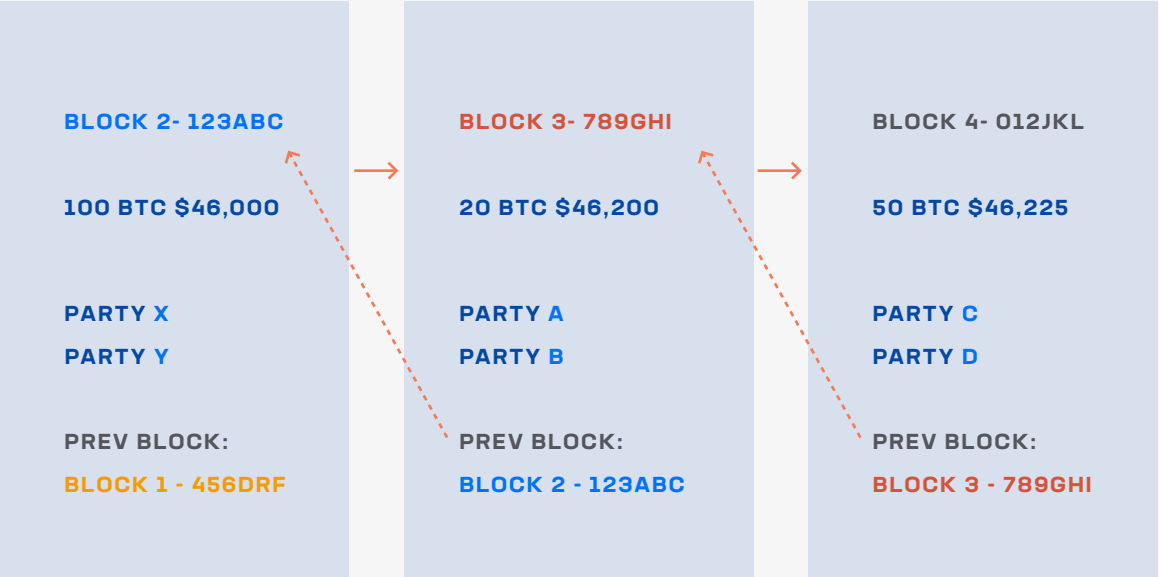
The Basics: blockchains, keys, and wallets

What is blockchain?

Blockchain technology is the foundation of the entire digital asset ecosystem and narrative – anything and everything within the digital asset ecosystem is built on a blockchain.

At a high level, a blockchain is simply a distributed (decentralized) ledger of transactions that is cryptographically secured, immutable (tamper proof), and highly resilient.

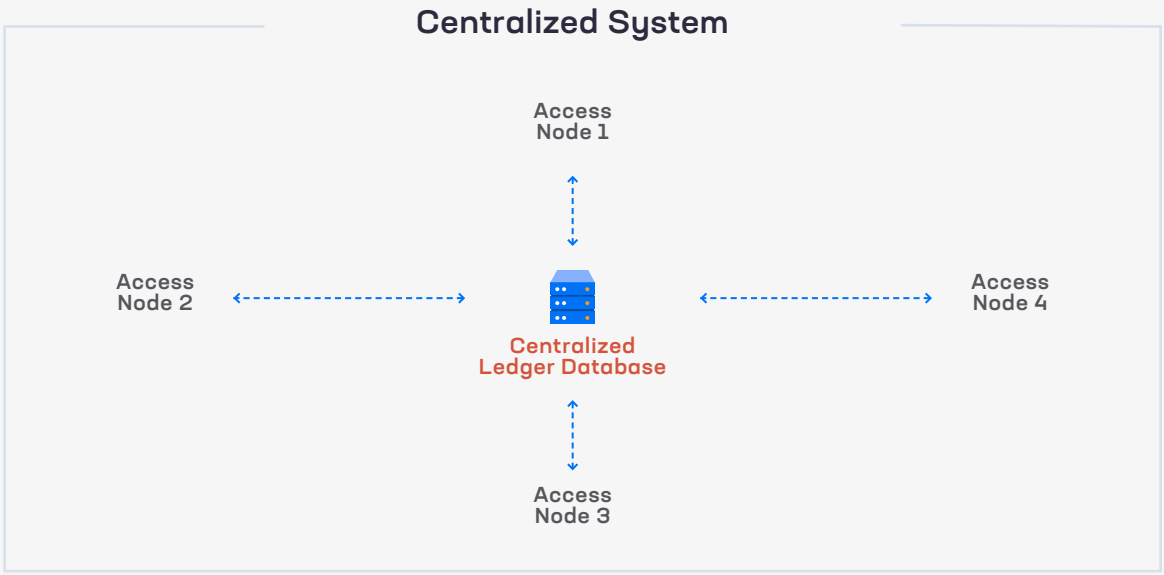
The blockchain itself is actually a linked chain of blocks of validated transaction data. Each block is a batch of validated transactions, and within that block is a link back to the previous block. This means there is a linkage (hence the chain in blockchain) back to every block and transaction that has ever been done.

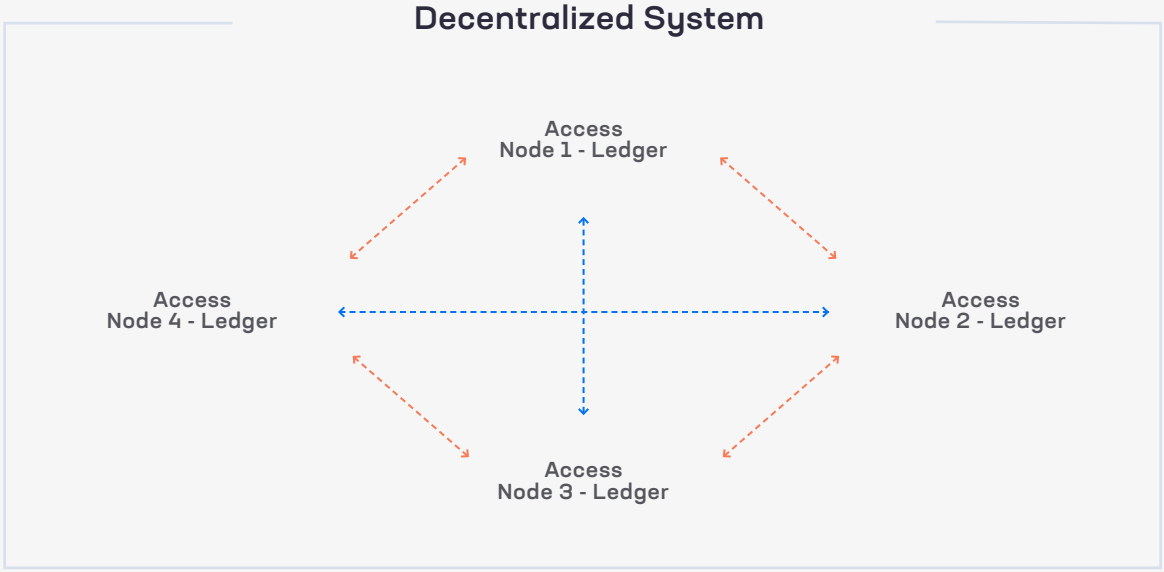


Distributed Ledger

One interesting feature of blockchains is that they are distributed and decentralized.

That means there is no one central server, set of computers, or third party that owns the only copy of the blockchain which is then accessed by the other market participants. Instead, every blockchain participant (called a node) has their own copy of the ledger.





There are two main benefits to this:

Resiliency

Because they are decentralized, there is no single point of failure, which means blockchains are typically highly resilient.

Immutable / Tamper Proof

Because blockchains are decentralized and there is no single point of failure, it is almost impossible for a malicious actor to come in and alter transaction histories (e.g. changing the transfer of $1 million of Bitcoin from ABC Corporation to Malicious Actor, LLC). If a malicious actor wanted to do this, they would need to figure out a way to change a majority of the copies of the blockchain before the next block is added (new blocks can be added every 2-10 minutes depending on which protocol you are using and transacting on). This would be extremely difficult to accomplish.

Once a transaction is added to the blockchain (e.g. Steve sends 1 Bitcoin to Dan), that transaction is now irreversible. If Steve sends that 1 Bitcoin to the wrong person and it is added to the blockchain, that 1 Bitcoin is gone forever. Obviously, this is much different than how traditional financial market transactions are currently handled.

How do transactions work?

Imagine Steve decides to buy 1 Bitcoin. This transaction is bundled up into a block, and institutions (or individuals) called miners then go solve a very difficult math logic puzzle. Whoever solves the puzzle first gets to add the block to the blockchain and gets a prize (typically payment in the form of the token they are mining or transaction fees). The other miners in the network then get together and validate that this is the next block to be added, and once consensus is reached (51% of the nodes in the blockchain network must agree that this next block should be added to the blockchain) the block is added to the blockchain and all nodes now have an updated copy of it.

Being tamper proof was discussed earlier, but to expand on this a bit further: if Malicious Actor A wanted to change the address of Steve's Bitcoin purchase to go to Malicious Actor A instead of Steve, they would need to change the address on 51% of all the ledger copies in the network before the next block is added. In a truly decentralized and scaled blockchain protocol, this is nearly impossible to accomplish.

Types of blockchains

There are essentially two types of blockchains.

Public

This is a blockchain that is open and accessible to anyone and everyone. The most popular examples of these are the Bitcoin and Ethereum blockchains.

Private

This is a blockchain that is for members only (only members of the network can access, read and mine transactions). An example of this is IBM's TradeLens.

The type of blockchain network you want to utilize will depend on your use case and other requirements (mainly privacy and liquidity). Currently, public blockchains are the most popular form of blockchain being utilized by institutions.

What are keys and why are they important?

The concept of keys comes from the cryptography side of blockchain. Without getting too technical, in order for you to transact or interact with any digital asset, you will need three basic things:

- **Private key**
- **Public key**
- **Wallet**

Public and private keys are the most important things you have when it comes to transacting with digital assets – they are the building blocks to digital asset transactions. Public and private keys are a string of characters that are randomly (and cryptographically) generated and nearly impossible to replicate. Your private key is the base, and your public key is derived from that.

Your public key is essentially the address people send transactions to – any transaction can be traced back to a public key. Your private keys allow you to initiate and authenticate transactions to access the digital assets you have stored on the blockchain in your wallet.

Your wallet contains both your public and private keys and has what's called a wallet address. In fact, your wallet address is just a cryptographically hashed version of your public key that makes it easier to send digital assets to and from it (so your wallet address and your public key are mathematically related but not identical). The wallet concept here is not much different from your traditional, physical wallet that holds things of monetary value (cash, credit cards, debit cards, etc.) that allow you to conduct transactions. A digital asset wallet is fairly similar to a physical wallet that has a lock on it.

Here is a very simplistic metaphor for how public keys, private keys, and wallets work. Think of your wallet as a treasure chest that resides on a blockchain. Your wallet address is similar to your physical mailing or email address- it is where transactions are sent to and from and your private key is the key that opens your treasure chest and allows digital assets to move around. When you purchase a digital asset, you use your private key to open up the treasure chest to allow for the exchange of the asset.

Because of the monetary value involved in institutional-level transactions, having secure private keys is extremely important. If a malicious actor were to obtain your private key, they could access your fictional treasure chest and initiate and authenticate transactions on your behalf. If you lost your private key, the assets in your treasure chest would essentially be inaccessible until you found your key. Luckily, there are many ways to securely safeguard the custody of your private keys.

When you deposit money at a bank, it's stored with the actual bank. When you are a fund manager and you buy stock, the stock or stock certificates are typically housed at a qualified custodian. With digital assets, you don't actually store or keep your assets themselves. If you own 50 Bitcoin, there is no physical place that has your bitcoin – those Bitcoin live in your treasure chest on the blockchain.

What you do possess if your private key, which gives you ownership and access to those 50 Bitcoin in your treasure chest. In the digital asset space, when custody or storage of assets is being discussed, those assets are your private keys. They are necessary for getting your assets off the blockchain and converted back into fiat currency or conducting further transactions on the blockchain.

What are wallets and storage?

There are three basic types of wallets where your private keys can be stored:

Hot

These are wallets that live on your internet browser

Warm

Similar to hot wallets but they live on software or applications and require authentication to be accessed

Cold

Also called cold storage, these wallets live on non-internet connected devices (like an unplugged USB)

Private key management

Given the importance of private keys, private key management is top of mind for any participant in the digital asset ecosystem. Private key management is essentially the custody of your private keys.

There are two basic options:

Self or Direct Custody

Your institution holds and is responsible for the safekeeping of your institution's private keys. This gives you direct control over your assets so that you have flexibility to transact however and whenever you want in conjunction with your internal policies and operational workflows.

Sub-custody

Your institution pays a third party to be responsible for the safekeeping of your private keys. This can limit your operational flexibility and put you into a closed loop with the sub-custodian, though it may offer certain conveniences.

Fireblocks

About Fireblocks

Fireblocks is an enterprise-grade platform delivering a secure infrastructure for moving, storing, and issuing digital assets. Fireblocks enables exchanges, lending desks, custodians, banks, trading desks, and hedge funds to securely scale digital asset operations through the Fireblocks Network and MPC-based Wallet Infrastructure. Fireblocks serves over 800 financial institutions, has secured the transfer of over $2 trillion in digital assets, and has a unique insurance policy that covers assets in storage & transit.

For more information, please visit www.fireblocks.com.