Blockchain

What is a Blockchain?

Blockchain is a distributed decentralised database governed by a protocol that allows for peer-to-peer transactions and uses network-wide consensus. It is also known as a "distributed ledger". As we learned in the first module, depending on the structure of a network, a blockchain can be centralized or decentralized distributed. If control is not in the hands of a financial organization, then the blockchain network is decentralized distributed.

This type of blockchain contains a series of interconnected blocks that store data. Blocks are records that form a blockchain. In the world of cryptocurrencies, blocks are like ledger pages and the entire book of records is the blockchain. A block is a file that stores immutable data related to the network. Blocks hold all records of valid cryptocurrency transactions.

It was first designed to timestamp digital documents so that they could not be tampered with. The goal of blockchain is to eliminate the need for a central server and to tackle duplicate entries. Duplicate entries cause problems with double-spending. This occurs when a blockchain network is disrupted and cryptocurrency is essentially stolen. The thief sends a copy of the currency transaction to make it look legitimate, or deletes the transaction altogether. Although it's uncommon, double spending can occur.

A blockchain is commonly used to securely transmit assets such as money, contracts, and other information without the need for a third-party intermediary such as a bank or government.

What a Blockchain is NOT

Before we move ahead, it's best to clear up some common misconceptions! The following is what a blockchain is not:

Blockchain is not Bitcoin

Bitcoin is just one cryptocurrency application of blockchain. Blockchain technology has a vast range of applications, for example, it can enable the secure sharing of medical data, create NFT marketplaces, track music royalties , allow cross-border payments, and more.

Blockchain is 100% Secure

Overall, blockchain system security depends on the other applications running on the blockchain.

Data Stored on a Blockchain is 100% Accurate

Blockchain cannot assess whether or not an external input stored on a blockchain is accurate; this applies to all off-chain assets and data digitally represented on a blockchain. Essentially, it is like a digital order book, it can display the information recorded but cannot ensure its accuracy.

Documentation

When researching blockchain technology and cryptocurrencies, you are likely to encounter whitepapers, yellowpapers and pitch decks. Let's have a look at what each of these are.

Whitepaper

A whitepaper is a marketing document that is intended to raise awareness of a service or technology among potential buyers. The whitepaper should clearly set out: the problem, the solution, how the token works to provide the solution, the team, the deployment plan, and its economics. A whitepaper can be considered as a proposal.

Yellowpaper

A yellowpaper is a more technical version of a whitepaper. It offers the technology's scientific details in a very concise manner. If you consider a whitepaper to be a proposal, the yellow paper might be considered the second component, which contains all of the detailed details.

Litepaper

A litepaper is a condensed version of the whitepaper. It is intended to give a brief overview of what a project entails to be digested in a shorter time.

Pitch Deck

A pitch deck is a presentation deck that is used to present an idea or business to an audience, usually investors. One of the most important aspects of an effective pitch deck is to organize it according to the audience and forum it will be presented to. This document usually has a heavier focus on visual materials, such as mockups.

Blockchain Architecture

Blocks, miners, and nodes are the three primary elements of blockchain.

Blocks

A blockchain is a chain of blocks that contain information. The Genesis block is the first link in the chain. Each new block in the chain is connected to the one before it.

The data which is stored inside a block depends on the type of blockchain. For example, a Bitcoin block comprises information about the sender, receiver, and the number of bitcoins to be transferred.

A hash is also a part of a block. It can be thought of as a unique fingerprint for each block. It uniquely identifies a block and all of its contents. As a result, any change within the block will modify the hash once a block is created.

The hash is needed to identify changes to intersections. If a block's fingerprint changes, it is no longer the same block. Hence, all blocks contain hashes of previous blocks.

Remember, each block contains:

1. Data
2. Hash
3. Hash of the previous block

This composition is what makes a blockchain secure against malicious attacks. Imagine a scenario where a hacker can alter the data in the second block. As a result, the hash of the block changes as well. However, the third block still retains the second block's hash. Now, the third block and all

subsequent blocks are invalid since the last block's hash is incorrect. Therefore, changing a single block can quickly make the subsequent blocks invalid.

Also, The blockchain is constantly being verified by a network of users, making it difficult to hack. For blockchains that use proof of work, 51% of attacks are due to the attacker gaining control of more than 50% of the hashing power.

Miners

The process of each new block allowing the series of transactions to continue is known as mining.

Every block in a blockchain has a unique nonce and hash. A nonce is an abbreviation for "number only used once," which is a number added to a hashed or encrypted block in a blockchain that meets difficulty constraints when hashed again. The nonce is the number that blockchain miners solve to obtain cryptocurrency. It also refers to the hash of the previous block in the chain. This setup is what makes mining a block difficult, particularly on big chains.

Making a change to any block earlier in the chain necessitates re-mining not only the affected block but all subsequent blocks as well. This is why manipulating blockchain technology is so tough. However, consider it "safety in math" because identifying “golden nonces” takes a long time and many computational resources.

A golden nonce provides a hash value lower than the target difficulty, which means it satisfies the requirement of the next block.

When a block is mined, all nodes in the network acknowledge the change, and the miner is compensated for their efforts.

Nodes

Decentralisation is an essential component of blockchain technology. The chain cannot be owned by a single computer on the chain. Any type of electronic equipment that saves copies of the blockchain and keeps the network running is referred to as a node.

The primary function of a blockchain node is to check the legitimacy of each subsequent batch of network transactions, known as blocks. Each node's device has a unique identification that allows it to be recognised by other nodes in the network. The nodes connecting to the chain form a distributed ledger.

The Three Types of Blockchain Architecture

There are only three types of blockchain structures that exist:

Public blockchain architecture

A public blockchain architecture means that the data and access to the system are available to anyone who is willing to participate (e.g. Bitcoin, Ethereum, and Litecoin blockchain systems are public).

Private blockchain architecture

As opposed to public blockchain architecture, the private system is controlled only by users from a specific organisation or authorised users who have an invitation for participation. The most common examples of private blockchains are Ripple (XRP) and Hyperledger.

Consortium blockchain architecture

This blockchain structure can consist of a few organisations. In a consortium, procedures are set up and controlled by the preliminary assigned users. Two examples of consortium blockchains are Energy Web Foundation and IBM Food Trust.

Consensus Protocols

Before moving on to consensus protocols, let's look at a statistic regarding consensus procedures: If a hacker gains access to 51% or more of the blockchain network, they could potentially manipulate the governance structure. When this happens, the platform is considered hacked. The 51% attack problem is solved in a variety of ways by various sorts of consensus mechanisms that we will examine in more detail below.

Consensus procedures allow all the nodes in the network to verify transactions. In distributed systems, there is no perfect consensus protocol. The consensus protocol needs to make a trade-off among consistency, availability and partition fault tolerance.

Next, we are going to take a look at the different consensus mechanisms below, proof of work, proof of stake, and proof of space.

Proof of Work

Proof of Work was one of the first consensus protocols utilised in the blockchain. It operates by computing hash values and validating transactions until the hash value contains a certain amount of trailing zeros. PoW requires the people who own the computers in the network to solve a complex mathematical problem to be able to add a block to the chain. Solving the problem is known as mining, and 'miners' are usually rewarded for their work in cryptocurrency.

However, mining is a difficult task. The mathematical challenge can only be solved through trial and error, with a 1 in 5.9 trillion chance of succeeding. It necessitates a significant amount of computational power, which consumes a considerable quantity of energy. This means that the benefits of mining must surpass the cost of the computers and the electricity used to power them because a single computer would take years to solve the mathematical problem.

Furthermore, as a network grows, it becomes increasingly difficult to turn a profit.

Bitcoin and Litecoin are two prominent cryptocurrencies using PoW.

PoW Overview

- Proof of Work is a consensus algorithm designed for permissionless public ledgers.
- A linear structure is used to represent the blocks. A set of transactions is represented by each block.
- The cryptographic puzzle of finding a random integer that leads to hashes with a certain amount of leading zeros is what bitcoin mining is all about.
- The public and private keys issued to each user are used to validate and sign each transaction.

Proof of Stake

Later blockchain networks incorporated "Proof of Stake" validation consensus algorithms, in which members must have a stake in the blockchain – typically by owning some of the cryptocurrency – to

be eligible to select, verify, and validate transactions. Because no mining is required, this saves a significant amount of computational power. With a PoS model, a validator is chosen and a block is assigned. A blockchain validator is someone who is responsible for verifying transactions on a blockchain. Once transactions are verified, they are added to the distributed ledger. To validate a block, the miner must set aside a portion of their cryptocurrency. If the miner is successful in validating the transaction, they will receive the stake they offered initially, plus specific transaction fees.

PoS is also seen as less risky in terms of the potential for miners to attack the network, as it structures compensation in a way that makes an attack less advantageous for the miner.

PoS Overview

- Validators are chosen based on their economic stake in the network.
- The goal is to minimise the centralisation of mining centres and provide all miners with a chance to validate blocks.
- There is no computational challenge to solve; hence it is environmentally friendly.
- Mining does not require any special hardware.

Proof of Space

Proof of Space, often known as PoSpace, is a network consensus system that works in a similar way to Proof of Work. PoSpace validates transactions using disk storage rather than computing resources.

PoSpace uses up disk space and rewards miners who have the largest disk space allotted to a block. This data structure is used to solve the pebbling game and is implemented using hard-to-pebble graphs. The term "pebbling" refers to the act of storing the hash values of the parents.

Plots are generated at random to represent all possible solutions to the problem. These plots are saved on disks and solved using a method known as Shabal's algorithm. The structure of the algorithm is a context for Shabal computations: It contains the intermediate values and some data from the last block entered.

The miners compare their answers once they've been computed, and the solution with the best time and space complexity is rewarded with the next block.

PoSpace Overview

- PoSpace is very similar to PoW, except that storage is used to earn cryptocurrency instead of computation.
- Blockchain enthusiasts view proof of space as a greener alternative due to the general-purpose nature of storage and the lower energy cost required by storage. However, this method has still been criticised for increasing the demand for storage.
- This consensus protocol again favours the miners with the maximum amount of space. It is resource biased, and therefore, miners with less amount of space cannot participate actively. This is a problem that goes against the concept of decentralisation.

How Blockchain Transaction Works?

There are several steps a transaction must go through before it is added to the blockchain, but the execution is relatively straightforward:

1. A transaction request is entered into the system. Cryptocurrency, contracts, records, or other information could be involved in the transaction.
2. The requested transaction is broadcasted via nodes to a peer-to-peer network.
3. The transaction and the user's status are validated by the network of nodes using algorithms.
4. The new block is then added to the old blockchain once the transaction is completed.

Why Do We Need Blockchain?

Blockchain is a fascinating and extremely useful technology. Here are some of the reasons why blockchain technology has gained so much popularity:

Efficiency

In the financial industry, blockchain technology can play a critical role by enabling faster transactions. In addition, it eliminates the need for a lengthy verification, settlement, and clearing process because all parties have access to a single version of data from the share ledger.

DeFi leverages emerging blockchain technologies to enable cross-border, permissionless transactions in digital assets, resulting in much faster global transactions.

In contrast, global payments via CeFi are much slower, as payments must pass through a chain of intermediaries before reaching the recipient.

Reliability

The identities of the interested parties are certified and verified using blockchain. This eliminates the possibility of duplicate records while also lowering rates and speeding up transactions.

In contrast, KYC (Know Your Customer) and AML (Anti-Money Laundering) checks in traditional financial institutions can take substantially longer and delay transactions.

Top Blockchain Use Cases

Blockchain use cases continue to expand. Here are two commercial applications:

Smart Contracts

The primary purpose of computer programs known as "smart contracts" is to automate the implementation of contract provisions when the circumstances call for it. The computer code uses the "when/if/then" command to ensure that all parties receive the rewards or penalties that the contract demands. Many sectors now employ smart contracts for a range of functions that were previously governed by paper contracts.

Cybersecurity

Because of their durability, openness, and distributed nature, blockchains are incredibly safe. There is no centralised database or central entity to attack with blockchain storage. Furthermore, it is complicated for criminals to access information contained in blockchains because they are decentralised, including privately-held blockchains, and the data saved in each block is unchangeable.

Blockchain Limitations

Although the blockchain offers numerous advantages, it does have certain limitations. The main drawback is that when the network becomes too crowded, the blockchain can slow down. It's also more challenging to grow due to its consensus-based work approach.

Another downside is that data in the blockchain is immutable; once a block has been recorded, it cannot be changed. Some may see it as an imitation that necessitates self-maintenance, implying that users must maintain their wallets or risk losing access.

On the other hand, immutability also offers advantages, such as greater efficiency. Blockchain immutability not only benefits auditing. It also provides new capabilities for analytics, queries, and general business processes. This capability helps an organization save time and money when it comes to auditing specific application data, tracking major errors, backing up and restoring a database to retrieve information, etc.

Blockchain technology is also still in its infancy and, unfortunately, lacks interoperability with other blockchains. However, several solutions are on the horizon to develop a solution to this issue.

Join us for the next module where we cover the evolution of money and the bitcoin protocol, here.