Crypto and blockchain

NFT's Zero To Hero

Contents

Quick definitions: *Blockchain* is the technology that enables the existence of cryptocurrency (among other things). *Bitcoin* is the name of the best-known cryptocurrency, the one for which blockchain technology was invented. A *cryptocurrency* is a medium of exchange, such as the US dollar, but is digital and uses encryption techniques to control the creation of monetary units and to verify the transfer of funds.

1   Blockchain

1.1   What is it

A blockchain is a distributed database (ledger or records) that is shared among the nodes of a computer network. As a database, a blockchain stores information electronically in digital format.

Think of a blockchain as a new, digital form of record-keeping.

1.2   Purpose

The goal of blockchain is to allow digital information to be recorded and distributed, but not edited. In this way, a blockchain is a foundation for immutable ledgers, or records of transactions that cannot be altered, deleted, or destroyed. Therefore, blockchains are also known as distributed ledger technology (DLT).

1.3   Distributed ledger technology

Distributed ledger technology (DLT) allows record-keeping across multiple computers, known as "nodes." Any user of the blockchain can be a node, but it takes a lot of computer power to operate. Nodes verify, approve, and store data within the ledger. This is different from traditional record-keeping methods which store data in a central place, such as a computer server.

A blockchain organizes information added to the ledger into blocks, or groups of data. Each block can only hold a certain amount of information, so new blocks are continually added to the ledger, forming a chain.

Each block has its own unique identifier, a cryptographic "hash." The hash not only protects the information within the block from anyone without the required code but also protects the block's place along the chain by identifying the block that came before it.

Once information is added to the blockchain and encrypted with a hash, it's permanent and unchangeable. Each node has its own record of the full timeline of data along with the blockchain, going back to its start. If someone tampered with or hacked into one computer and manipulated the data for their own gain,
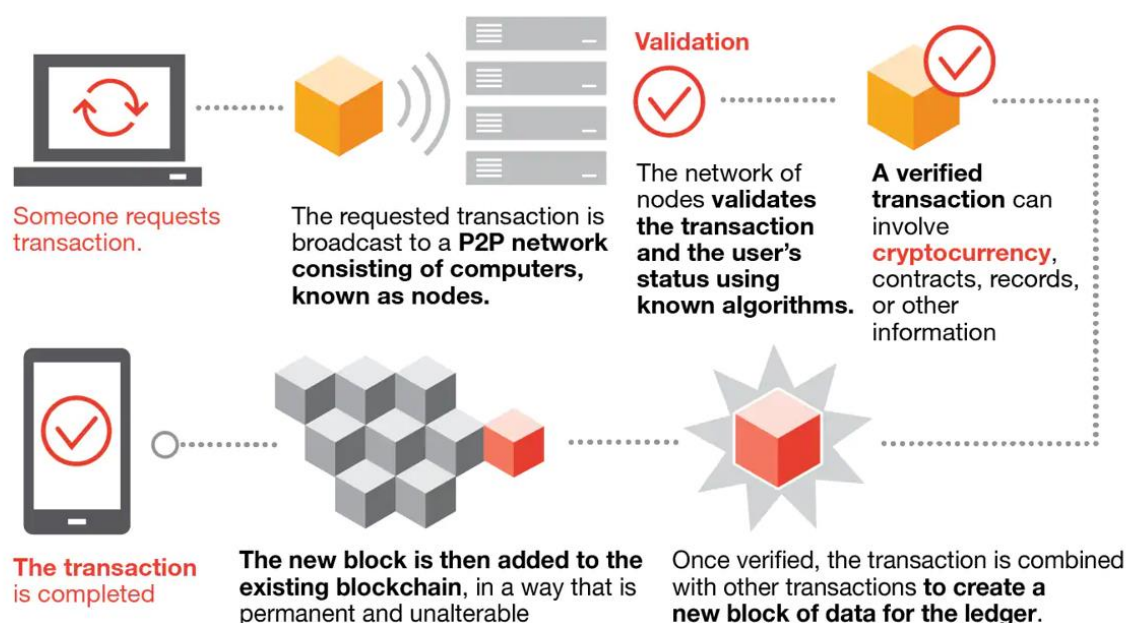
it wouldn't alter the information stored by other nodes. The altered record can be easily distinguished and corrected since it doesn't match the majority.

1.4   How does blockchain work

Here's an example of how blockchain is used to verify and record Bitcoin transactions.

1. A consumer buys Bitcoin.
2. The transaction data is sent across Bitcoin's decentralized network of nodes.
3. Nodes validate the transaction.
4. After approval, the transaction is grouped with other transactions to form a block, which is added to an ever-growing chain of transactions.
5. The completed block is encrypted, and the transaction record is permanent; it cannot be removed or altered on the blockchain.

Bitcoin's blockchain is public, which means anyone who owns Bitcoin can view the transaction record. While it can be difficult to trace the identity behind an account, the record shows which accounts are transacting on the blockchain. Public blockchains also allow any user with the required computer power to participate in approving and recording transactions onto the blockchain as a node.

Someone requests transaction.

The requested transaction is broadcast to a **P2P network** consisting of computers, known as nodes.

Validation

The network of nodes **validates the transaction and the user's status using known algorithms.**

A verified transaction can involve **cryptocurrency**, contracts, records, or other information

The transaction is completed

The new block is then added to the existing blockchain, in a way that is permanent and unalterable

Once verified, the transaction is combined with other transactions **to create a new block of data for the ledger.**

2 Crypto

2.1 What is it

cryptocurrencies are electronic peer-to-peer (directly exchanged) currencies. They don't physically exist. You can't pick up a bitcoin and hold it in your hand or pull one out of your wallet.

2.2 Tokens

Individual units of cryptocurrencies can be referred to as coins or *tokens*, depending on how they are used. Some are intended to be units of exchange for goods and services, others are stores of value, and some are mostly designed to help run computer networks that carry out more complex financial transactions.

2.3 Mining

One common way cryptocurrencies are verified is through a process known as *mining*, which is used by Bitcoin. Mining can be an energy-intensive process in which computers solve complex puzzles in order to verify the authenticity of transactions on the network. As a reward, the owners of those computers can receive newly created cryptocurrency. Other cryptocurrencies use different methods to create and distribute tokens, and many have a significantly lighter environmental impact.

For most people, the easiest way to get cryptocurrency is to buy it, either from an exchange or another user.

2.4 Benefits of Cryptocurrency

With cryptocurrency, the transaction cost is low to nothing at all—unlike, for example, the fee for transferring money from a digital wallet to a bank account. You can make transactions at any time of the day or night, and there are no limits on purchases and withdrawals. And anyone is free to use cryptocurrency, unlike setting up a bank account, which requires documentation and other paperwork.

International cryptocurrency transactions are faster than wire transfers too. Wire transfers take about half a day for the money to be moved from one place to another. With cryptocurrencies, transactions take only a matter of minutes or even seconds.

To summarize traditional online payment gateways are owned by organizations. They hold your money for you, and you need to ask them to transfer it on your behalf when you want to spend it.

In cryptocurrencies, there isn't an organization. You, your friends, and thousands of others can act as your own banks by running free software. Your computer connects with other people's computers, meaning you communicate directly – no middlemen required!

3   Crypto wallet

Crypto wallets keep your private keys – the passwords that give you access to your cryptocurrencies – safe and accessible, allowing you to send and receive cryptocurrencies.

3.1   Public vs. private keys—what's the difference?

Crypto wallets generally use two types of keys: public keys and private keys.

Public keys operate in a similar way to your bank account number. A public key is a long string of random numbers that can be shared with a third party, such as a cryptocurrency exchange, without compromising the security of your wallet. This key allows you to receive cryptocurrency in transactions— oftentimes by using a wallet address, which is essentially a compressed version of the wallet's public key.

Private keys, on the other hand, should always be kept private. A private key allows you to access the actual cryptocurrency on the blockchain. So, if someone has access to your private keys, it's as good as having access to the crypto in your wallet.

3.2   Types of crypto wallets

- Paper wallets: Keys are written on a physical medium like paper and stored in a safe place. This, of course, makes using your crypto harder, because as digital money it can only be used on the internet.
- Hardware wallets: Keys are stored in a thumb-drive device that is kept in a safe place and only connected to a computer when you want to use your crypto. The idea is to try to balance security and convenience.
- Online wallets: Keys are stored in an app or other software – look for one that is protected by two-step encryption. This makes sending, receiving, and using your crypto as easy as using an online bank account, payment system, or brokerage.

4   Tokens

The blockchain terms; token and cryptocurrency are often used interchangeably, as these are both digital assets on blockchains. The biggest difference between a cryptocurrency and a token is that cryptocurrencies are the native asset of a blockchain like BTC, RBTC, or ETH, whereas tokens are built on an existing blockchain, using *smart contracts* (a self-executing contract with the terms of the agreement between buyer and seller being directly written into lines of code). Most commonly, these are EIP-20 tokens.

The main difference between tokens and coins is the *gas fees*:

- Fees (or gas) for transactions are cheaper when transferring the cryptocurrency, and more expensive when transferring tokens.
- Fees (or gas) are always paid for in the cryptocurrency, and therefore when transferring tokens, you will still need some cryptocurrency in the same account.

4.1   Gas fees

Gas is the lifeblood of any blockchain network. It is a monetary fee that compensates miners/validators of a blockchain in exchange for their computational effort of mining blocks. So, basically, it's what the fees to the blockchain miners/validators paid with each transaction. They are Gas fees are paid in Ethereum's native currency, ether (ETH).

4.2   Types of tokens

There can be tokens for any kind of service or product in the crypto space. Payment tokens, for example, are coins like Bitcoin or Litecoin (LTC), used to pay for transactions in the digital world.

Utility tokens give holders access to products and services that are blockchain-based.

Security tokens are traditional assets like stocks and shares represented by digital tokens on the blockchain.

The most distinct types of tokens are fungible and nonfungible tokens.

Fungible tokens - Fungible tokens represent assets of equal value. For example, Cardano's native token, ADA, is a fungible token, as each ADA is worth the same amount as the next. Similarly, stablecoins, such as those pegged to a national currency, would be considered fungible tokens. Fungible tokens are often used similarly to fiat currency, or pegged to the price of a particular asset, such as an ounce of gold.

Non-fungible tokens (NFT) - Not every asset is of equal value, even if it is of the same type. Non-fungible tokens, often called NFTs, ensure that each token is unique, with its own characteristics. Take a piece of artwork for example. Superficially, a painting is the same type of object or asset as any other painting. However, we know that a Van Gogh is intrinsically more valuable than an amateur piece of art, and these important unique characteristics can be coded into an NFT to reflect these differences.

Fungible vs. nonfungible tokens

	Fungible tokens	Nonfungible tokens
Main features	Divisible	Indivisible
	Non-unique	Unique
	Interchangeable	Irreplaceable
Real-world purposes	Payment system	Intellectual property
	Store of value	Academic title
		Artwork
		Music composition
		Gaming
		Utility
		Assets like stocks, shares
		Access to a service i.e., a subscription
Technology used	Own blockchain	Built on another blockchain
Example of tokens	Bitcoin; Litecoin; ERC-20	ERC-721
Content stored	Value	Data

cointelegraph.com

Examples of Fungible & Non-Fungible Tokens

Fungible		Non-Fungible	
Dollar		Cryptokitties	
Bitcoin		Art	
Ethereum		House/Property	

5 Crypto-related vocab

1. **Blockchain:** Blockchain is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system. The most popular blockchain is Ethereum.

2. **NFT minting:** The process of making a digital work an NFT by registering it on a blockchain like Ethereum.

3. **Chain**: the sequence of blocks in the blockchain.

4. **Blocks (in the blockchain)**: Groups of data.

5. **Tokens:** Individual units of cryptocurrencies can be referred to as coins or *tokens*, depending on how they are used.

6. **immutable ledgers:** Records of transactions that cannot be altered, deleted, or destroyed.

7. **Distributed ledger technology (DLT):** A digital system for recording the transaction of assets in which the transactions and their details are recorded in multiple places at the same time.

8. **Nodes:** A place where things such as lines or systems join

9. **Ledger**: log.

10. **Cryptography**: a method of protecting information and communications using codes, so that only those for whom the information is intended can read and process it.

11. **Hash**: the function that transforms data into encrypted numbers.

12. **Decentralized:** Doesn't have a controlling authority (bank).

13. **Peer-to-peer:** the direct exchange of some asset, such as a digital currency, between individual parties without the involvement of a central authority.

14. **Mining:** The process of verifying transactions on a digital ledger for a blockchain using machines with extensive computing power.

15. **Digital wallet (e-wallet):** Software-based system that securely stores users' payment information and passwords for numerous payment methods and websites

16. **Wire transfers:** bank transfers.

17. **Crypto wallet:** a device or software that stores your crypto keys, and transactions and gives access to your cryptocurrencies.

18. **Crypto key:** Keys that are issued when purchasing a cryptocurrency and are two: public and private.

19. **Public key:** A key that you can safely share with others, allowing you to send or receive funds.

20. **Private key:** a password that unlocks the virtual vault that holds your money.

21. **Thumb-drive**: USB flash drives are for storage, supplementary back-ups, and transferring of computer files.

22. **Native assets:** Have their own blockchains.

23. **Digital Asset:** An asset that is created, traded, and stored in a digital format.

24. **Smart contracts**: programs stored on a blockchain that run when predetermined conditions are met.

25. **EIP-20 tokens:** Standard tokens used for creating and issuing smart contracts on the Ethereum blockchain.

26. **Gas fees:** payments made by users to compensate for the energy required to process and validate transactions on the Ethereum blockchain.

27. **Gas limit:** The maximum amount of gas (or energy) that you're willing to spend on a particular transaction.

28. **Fungible tokens:** An asset on a blockchain that has the same value as any other asset of the same type, like cryptocurrencies.

29. **Non-Fungible tokens:** Very specific items such as a work or land of art that has its own value.