

1. Welcome to Crypto

TL;DR:

Welcome to Crypto aims to educate about cryptocurrency and blockchain technology through over 489 articles in 31 languages. The guide introduces key concepts like cryptocurrencies, blockchain, trading, investing, and earning passive income. It also covers privacy and security tips. Dive into the world of digital currencies and explore a wealth of knowledge to kick-start your journey.

What's a cryptocurrency?

A cryptocurrency is just like a digital form of cash. You can use it to pay friends for your share of the bar tab, buy that new pair of socks you've been eyeing up , or book flights and hotels for your next holiday. Because cryptocurrency is digital, it can also be sent to friends and family anywhere in the world.

Just like PayPal or bank transfers, right?

Well, not really. It's way more interesting!

You see, 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!

To use cryptocurrency, you don't need to sign up for a website with an email address and password. You can download a wide variety of apps onto your smartphone to begin sending and receiving within minutes.



Why do they call it cryptocurrency?

The name **cryptocurrency** is a combination of *cryptology* and *currency*. With **cryptology**, we use advanced math to secure our funds, making sure that nobody else can spend them.

There's no need to understand all this – applications you use will do all the heavy lifting. You won't even know what's going on under the hood.

If you're interested in that kind of thing, though, we've got a few articles for you:

- What is Public-Key Cryptography?
- History of Cryptography
- Symmetric vs. Asymmetric Encryption
- What is a Digital Signature?

So, this magical internet money isn't owned by anyone and uses cryptography to secure the system. But you've already got apps for paying people – why should you care?

It's Permissionless

No one can stop you from using cryptocurrency. Centralized payment services, on the other hand, can freeze accounts or prevent transactions from being made.

Censorship-resistant

Because of the way the network is designed, it's virtually impossible for hackers or other attackers to shut it down.

A cheap and fast payment method

When you make a transaction to someone at the other side of the world, your money can be with them within seconds – at a fraction of the cost of an international wire transfer.

What about that Bitcoin thing your friend or family member keeps talking about? That's the original cryptocurrency, and, to date, the most popular.



Who invented Bitcoin?

Amazingly, nobody knows who invented Bitcoin. We only know them by their screen name - **Satoshi Nakamoto**. Satoshi could be a single person, a group of programmers, or if you believe some of the weirder theories, a time-traveling alien or secret government team.

Satoshi published a 9-page document in 2008, detailing how the Bitcoin system worked. Months later, in 2009, the software itself was released.

Bitcoin provided the foundation for many other cryptocurrencies. Some were based on the same software, while others took a very different approach. Ok, but what's the difference between all the cryptocurrencies?

To even make a list of all the different cryptocurrencies would take us weeks. Some are faster than others, some are more private, some are more secure, and some are more programmable.

There's a common saying in the cryptocurrency space: **Do Your Own Research** (or DYOR). We're not saying that to be rude, we promise. It just means that you shouldn't take information from a single source as the truth.

Before investing your money into a particular project, make sure you do your due diligence.

Cryptocurrencies aren't all the same!

If you're interested in learning about some of the different coins and tokens, we've compiled a list of guides on Binance Academy:

- What Is Bitcoin? (the king of cryptocurrencies)
- What Is Ethereum? (the distributed computer)
- What Is BNB? (the original exchange coin)
- A Beginner's Guide to Monero (for the privacy aficionados)

In the next section, we're going to talk about the technology that the vast majority of digital currencies are based on, known as blockchain.



What is blockchain?

Don't be spooked by the technobabble that people use to describe "blockchain." A blockchain is just a database. It isn't a particularly sophisticated one, either - you could create it in a spreadsheet with minimal effort.

There are some peculiarities with these databases. The first is that blockchains are *append-only*. That means that you can only *add* information - you can't just click on a cell and delete stuff that you've already added, or change it in any way.

The second is that each entry (called a *block*) in the database is cryptographically linked to the last entry. In plain English, each new entry must contain a sort of digital fingerprint (hash) of the last one.

And that's it! Since each fingerprint points back to the last one, you end up with a chain of blocks. Or - as the cool kids like to call it - a blockchain.

A blockchain is *immutable*: if you change a block, it changes the fingerprint. And since that fingerprint is included in the next block, the next block is changed too. And since that block's fingerprint... well, you get the idea. You end up with a domino effect where any change becomes evident. You can't alter any information without everyone noticing.

Is that it?

Underwhelmed? That's fair. The innovation here isn't some cumbersome alternative to Google Sheets. It's that everyone can download blocks from other people on the network to build identical copies of the blockchain on their computers. That's what the software we mentioned earlier does.

Suppose that you and your friends Alice, Bob, Carol, and Dan are running the software. You might say "I want to send five coins to Bob." So you send that instruction to everyone else, but the coins aren't sent to Bob immediately.

Carol might decide at the same time to send Alice five coins. She also sends her instruction out to the network. At any time, a participant can gather up the pending instructions to create a block.

If anyone can make a block, what stops them from cheating?



It probably seems very attractive to you to create a block that says “Bob pays me a million coins.” Or to start buying Lamborghinis and fur coats from Carol by making transactions with funds you don’t own.

Well, that’s not how it works. Because of some cryptography, game theory, and something called a **consensus algorithm**, the system prevents you from spending funds you shouldn’t be able to spend.

Free blockchain knowledge!

- What Is a Blockchain **Consensus Algorithm**
- What Is Proof of Work (PoW)?
- **Double Spending** Explained
- Game Theory and Cryptocurrencies
- Byzantine Fault Tolerance Explained

Did you know all that already, and just want to learn how to trade or invest? Let’s get onto that next.

Trading

As you might have heard, blockchain and cryptocurrencies are already used in a **lot of different areas**. Undoubtedly, one of the biggest current use cases is speculation.

Trading generally implies a shorter-term approach to generating profit. Traders may jump in and out of positions all the time. But how do they know when to get in and out?

One of the most common ways to make sense of the cryptocurrency market is through an approach called **technical analysis** (TA). Technical analysts look at price history, charts, and other types of market data to find bets that have a good chance of returning a profit.

You must be dying to get started right away. And technically, you could. It’s that easy! But, like most things worth pursuing, trading is hard! It would take us a long time to talk about all that you need to keep in mind.



Learn the special craft of chart mastery!

We have some articles to get you started:

- What Is Technical Analysis (TA)?
- A Beginner's Guide to Candlestick Charts

Luckily, we've also created an extensive guide for new crypto traders! It contains pretty much everything (and probably more) that you need to know about trading crypto:

- A Complete Guide to Cryptocurrency Trading for Beginners

Once you can quote that article after being woken up at five in the morning, you could move on to other related topics:

- A Beginners Guide to Understanding Risk Management
- A Beginner's Guide to Cryptocurrency Trading Strategies
- 5 Essential Indicators Used in Technical Analysis
- 12 Popular Candlestick Patterns Used in Technical Analysis
- 7 Common Mistakes in Technical Analysis (TA)

Investing

Investors look for long-term bets based on the fundamentals of an investment. For example, how much profit a company is making. While cryptocurrencies are a new and unique type of assets, they can also be viewed through a similar lens.

Many Bitcoin investors follow the “**HODL**” philosophy. This means that they believe so deeply in the success of Bitcoin that they don't intend to sell for a long time. But don't take their word for it! Read our **extensive Bitcoin guide** and decide for yourself.

After going through that, you may decide that you want to become a Bitcoin HODLER. Well, you could become one in a matter of minutes. Just go to the **Buy Crypto** page and follow the instructions.

The onboarding process is smooth and quick. You don't have to jump in with large amounts, either. You could start with as little as 15 dollars! So, what is some mind candy that you should be looking into related to crypto investing?



Crypto Investing 101

If you want to invest in cryptocurrencies, these articles will help you get started:

- What is Fundamental Analysis (FA)?
- Asset Allocation and Diversification Explained
- Dollar-Cost Averaging (DCA) Explained

Passive income

So far, we've talked about trading and investing. These methods generally require a lot of time, which not everyone has. If you're one of those busy but efficient people, we have some other options for you.

As Warren Buffett, one of the most successful investors of all time, said: "If you don't find a way to make money while you sleep, you will work until you die."

Good news, the world of cryptocurrency offers many opportunities to **earn passive income**. You can basically use your crypto holdings to make more crypto!

Why isn't everyone doing this? Well, they probably don't know. But now you do!

One of the ways to earn passive income is by securely lending your holdings to other people. In exchange for the opportunity to borrow your funds, they'll pay interest to you.

Besides, you may have heard about Bitcoin **mining**. It generally involves a lot of loud and expensive machines churning away for Bitcoin rewards. However, there are other ways to secure a cryptocurrency network. One of these is through a process called staking. And spoiler alert, it doesn't involve meat.

What is staking?

In simple terms, staking means getting rewards for locking up coins. So, if you invest in a coin that supports staking, you could build up a larger holding over time. Read more about in these articles:

- What Is Staking?
- Proof of Stake Explained



Privacy and Security

We're a cryptocurrency website, but we also privacy and security topics – and you should, too!

The digital age brought with it some serious innovation. Your fridge can text you when you forget to close the door, you can summon your car from a smartphone app, and it looks like you'll soon be receiving mail by drone.

Unfortunately, there's also been innovation in ways to steal your sensitive data – something we unknowingly produce A LOT of. Do you know the best way to deal with ransomware? Or the steps you can take to stop websites from finding out where you're browsing from?

Protect yourself with knowledge

Here are some articles that make good starting points:

- What Is the TOR Network?
- Device Fingerprinting: How Exposed Are You?
- What Is Phishing?
- What Is End-to-End Encryption (E2EE)?

Well, that about brings us up to speed!

Hopefully you can leave this guide with a better understanding of cryptocurrency and how it works. On Binance Academy, you'll find a huge variety of articles, ranging from beginner's guides to overviews of more advanced topics.

Critical Thinking Questions

1. How does the decentralized nature of cryptocurrencies like Bitcoin challenge traditional financial institutions and what implications could this have for financial inclusion and economic equality?
2. Considering the security features of blockchain technology, such as immutability and cryptographic links between blocks, how might these features be leveraged to enhance transparency and trust in other areas, such as voting systems or supply chain management?



3. The concept of “permissionless” transactions in cryptocurrency means that anyone can participate without the need for approval from a central authority. What are the potential benefits and risks of this feature in the context of global financial systems?

4. The term “censorship-resistant” is used to describe cryptocurrencies’ ability to prevent unauthorized control or suppression of transactions. How could this characteristic impact individuals’ freedom and privacy, and what ethical considerations arise from this capability?

5. Cryptocurrencies and blockchain technology introduce new concepts such as “staking” and “proof of work.” How do these mechanisms differ from traditional financial practices, and what potential do they hold for creating innovative economic models or disrupting existing ones?

Glossary

- Algorithm (noun): A set of rules or processes followed in calculations or problem-solving operations, often by a computer.
- Asymmetric Encryption (noun): A type of encryption where different keys are used for encryption and decryption.
- Blockchain (noun): A digital database containing information (such as records of financial transactions) that can be simultaneously used and shared within a large decentralized, publicly accessible network.
- Candlestick Chart (noun): A style of financial chart used to describe price movements of a security, derivative, or currency.
- Censorship-resistant (adjective): Designed to resist control or suppression, ensuring open access and freedom of communication.
- Consensus Algorithm (noun): A procedure through which all the peers of a blockchain network reach a common agreement about the present state of the distributed ledger.
- Cryptography (noun): The practice of securing information by transforming it into an unreadable format, only accessible to those possessing a secret key.
- Cryptocurrency (noun): A digital or virtual form of money that uses cryptography for security and operates independently of a central authority.



- Decentralized (adjective): Distributed or spread out across multiple locations or individuals, not controlled by a central authority.
- Double Spending (noun): The risk that a digital currency can be spent twice, due to the ease of duplicating digital information.
- Encryption (noun): The process of converting data into a code to prevent unauthorized access.
- Immutable (adjective): Unchangeable; in the context of blockchain, it refers to the property that data, once written, cannot be altered or deleted.
- Mining (noun): The process of using computer power to solve complex mathematical problems to validate transactions and add them to the blockchain, often rewarded with cryptocurrency.
- Peer-to-Peer (adjective): A decentralized network where each party has equal capabilities and can initiate a communication session, as opposed to a client-server model.
- Public-Key Cryptography (noun): A cryptographic system that uses pairs of keys; one public and one private. The public key is shared openly, while the private key is kept secret.
- Staking (noun): The process of participating in the validation of transactions on a blockchain by locking up cryptocurrency holdings, typically rewarded with additional cryptocurrency.
- Symmetric Encryption (noun): A type of encryption where the same key is used for both encryption and decryption.
- Technical Analysis (noun): A trading discipline employed to evaluate investments and identify trading opportunities by analyzing statistical trends from trading activity.
- Transaction (noun): An instance of buying or selling something; in cryptocurrency, it refers to the transfer of digital currency between accounts.
- Wallet (noun): A digital tool (software or hardware) used to store and manage cryptocurrencies, allowing users to send, receive, and track their digital currency balances.

