BITCOIN IN 1₿ MINUTES

Everything you always wanted to know about Bitcoin

Brought to you by Relai

WHAT IS BITCOIN?

Bitcoin, the world's most successful cryptocurrency, is making headlines around the globe. Many want to profit from its success, others are indifferent or even skeptical.

The digital currency has sparked countless discussions about money, investing, and technology. Some see Bitcoin as a sheer speculation vehicle or denounce it as a bubble, while others talk of innovation, monetary revolution, or even redemption from the current monetary system.

Various countries, including China, see Bitcoin as a threat and have declared war on the cryptocurrency. Other governments, such as that of El Salvador, have introduced Bitcoin as an official means of payment in the hope of economic growth.

But what is Bitcoin? Is it money? Digital gold? A fad for computer scientists and speculators?
Or something else entirely? In the following paragraphs, we will get to the bottom of these questions and take a closer look at the digital currency to better understand the philosophy and functionality behind Bitcoin. To accomplish this, it is important to start at the very beginning: with the story of Bitcoin's origins.

THE STORY OF BITCOIN

Bitcoin‘s beginnings date back to the early nineties. In 1992, a group of computer scientists in California started an email list to exchange ideas with like-minded people about cryptography, mathematics, politics, and philosophy. They called themselves ‚Cypherpunks‘ - a play on words from cyberpunk (person in sci-fi literature who is skeptical of society - and rightly so) and cipher (to encrypt).

The Cypherpunks

The Cypherpunks soon grew into a motley crew. Despite their different backgrounds, they were united by the conviction that the Internet would become one of the most contested arenas for human freedom soon.
To protect themselves against the threat of control, surveillance, and censorship of the Internet and preserve a free and open Internet, the Cypherpunks used a powerful weapon: Cryptography, the encryption of information.

In their 1993 manifesto, they stated: “Cypherpunks write [computer] code. We know that someone has to write software to defend privacy, and [...] we‘re going to write it.

But cryptography alone would not be enough for a free Internet. Because, and the Cypherpunks were convinced of this, the Internet cannot be truly free if it does not have its own money. Money that is independent of states, central banks, and companies; a cryptocurrency as fair and decentralized as the Internet itself.

Monetary Experiments

But the creation of independent, digital money presented the Cypherpunks with technical challenges. As early as 1990, cryptologist David Chaum had created eCash, the first cryptocurrency, which was not decentralized but ensured anonymity thanks to cryptography. However, eCash was not able to assert itself against other online payment systems in the long term. The company behind the project had to file for bankruptcy after 8 years of service and eCash disappeared.

Other attempts followed, of which E-Gold stood out. E-Gold was a gold-backed cryptocurrency that was open to everyone. Founded during the dot-com era in 1996, the company struck a chord with its peers, processing over two billion dollars worth of transactions per year at its peak.

But E-gold was controlled by a central institution and thus vulnerable to attacks. Legal problems soon followed, and the U.S. government took legal action against E-Gold. In 2008, E-Gold was found guilty by a U.S. court of money laundering and violations of the Patriot Act. All assets were frozen, and E-Gold had to cease operations.

These failed attempts have demonstrated two facts to the Cypherpunks. First, both eCash and E-gold had been backed by collateral. This collateral had proven to be a weak spot, as it could be seized by states. Therefore, a free cryptocurrency should have no central points of attack such as a registered company, a bank account, or a centralized server location. And second, both, governments and regulators have no interest in state-independent digital money.

For the Cypherpunks the basic question, for which no solution had yet been found, remained: How can an independent digital money work without a central party to keep the books and ensure that money is not spent twice? After all, if it were possible to solve the problem of double-spending without relying on a central party, it might be possible to create free digital money that is native to the Internet.

A mystical Act of Creation

For these reasons, the Cypherpunks began to discuss designs for a cryptocurrency without a central party and collateral. Two of the most important concepts were b-money (1998) and BitGold (2005). These theoretical ideas, which were never implemented in practice, were already very similar to Bitcoin in their design. A public/private key pair was envisaged for encryption and a Proof-of-Work was to be provided for the creation of additional digital coins, as is also the case with Bitcoin. In his Whitepaper, the inventor of Bitcoin also confirmed that he was aware of b-money and BitGold.

However, because b-money and BitGold relied on a voting system for consensus (the agreement on who owns which monetary units at present), they were vulnerable to malicious attacks that could manipulate such elections and thus distort ownership.

For this last problem, which still stood in the way of the creation of new Internet money, a solution was presented on Friday, October 31, 2008. On that day, the Bitcoin Whitepaper, in which Satoshi Nakamoto explains his concept for a decentralized payment network, was emailed to the Cypherpunks. Two months later, on January 3, 2009, the Bitcoin network went live.

The initial reactions to the new network were muted. A few enthusiasts began to test the network and report errors. In the beginning, however, it was mainly Satoshi Nakamoto himself who kept the network running. But slowly the news of the new Internet money spread to computer and tech forums and interest in the network grew. After a year, the Bitcoin network already counted some users. Bitcoin itself, however, had no value yet.

Who is Satoshi Nakamoto?

The Bitcoin Whitepaper, as well as the e-mail communication of the Bitcoin inventor, were both signed with the name Satoshi Nakamoto. However, the true identity of the Bitcoin inventor remains unknown to this day, as his name appears to be an alias. To address like-minded people and later the Bitcoin developer community, Nakamoto used at least three different e-mail addresses, which he thoroughly encrypted to conceal the sender’s true identity.

Various people have already claimed to be Satoshi Nakamoto. But until today, every one of them has failed to prove it. Because the ultimate proof, namely the sending of Bitcoin from one of the wallet addresses that most probably belong to Satoshi, has not yet been provided by anyone.

Moreover, the group of those who have communicated „personally“ with Satoshi Nakamoto via the Internet is very small. Satoshi Nakamoto wrote his last message to the Bitcoin community on December 12, 2010, but this was by no means a farewell message - Satoshi simply stopped communicating after that.

His withdrawal, however, was only to the broader community. Nakamoto continued to gather a small group of core programmers around him and informed them about the further development of the Bitcoin network. But in April 2011, he sent a final message to this group as well. Just as mysteriously as Nakamoto appeared in 2008, he disappeared again three years later.

Bitcoin‘s “Pizza Day”

But how did Bitcoin get value in the first place? In the beginning, Bitcoin could be mined and sent back and forth between members of the network, but the digital units had no value. Also, the group of those who knew Bitcoin, let alone could send and receive it, was still very small.

This changed on May 22, 2010, when an unusual request appeared on the Internet forum bitcointalk.org. A 28-year-old man named Laszlo Hanyecz from Florida offered 10,000 Bitcoin to the person who would order two pizzas to his home. A Californian student took him up on the offer and had two large pizzas worth $41 delivered to his home. In return, Hanyecz sent him the 10,000 Bitcoin.

Since that day, May 22 has been celebrated annually by Bitcoiners as Bitcoin „Pizza Day“. The day became popular because it illustrates three things:

- Bitcoin have value

- Bitcoin are suitable as a means of exchange and payment

- Bitcoin as a currency is disinflationary.

The number of additional Bitcoin brought into circulation is steadily decreasing, which can lead to an increase in value.

The two pizzas have gone down in the history books as the most expensive in the world. Calculating their cost with the Bitcoin price from December 2021, an incredible 460 million US dollars were paid for them. That is a lot of money. But the recipient of the 10,000 Bitcoin has already spent them, too. In an interview, he stated that he had sold the Bitcoin not long after to pay for a road trip - at today‘s Bitcoin price probably the most expensive road trip in human history as well.

The Bitcoin „Pizza Day“ also impressively illustrates why ‚hodling‘ - derived from ‚to hold‘ - is so popular among Bitcoiners. ‘Hodling’ means keeping one‘s Bitcoin over extended periods with the intent of (possibly) never selling them. After all, who wants to spend their Bitcoin today when they could be worth double, triple, or even ten times as much in the years to come?

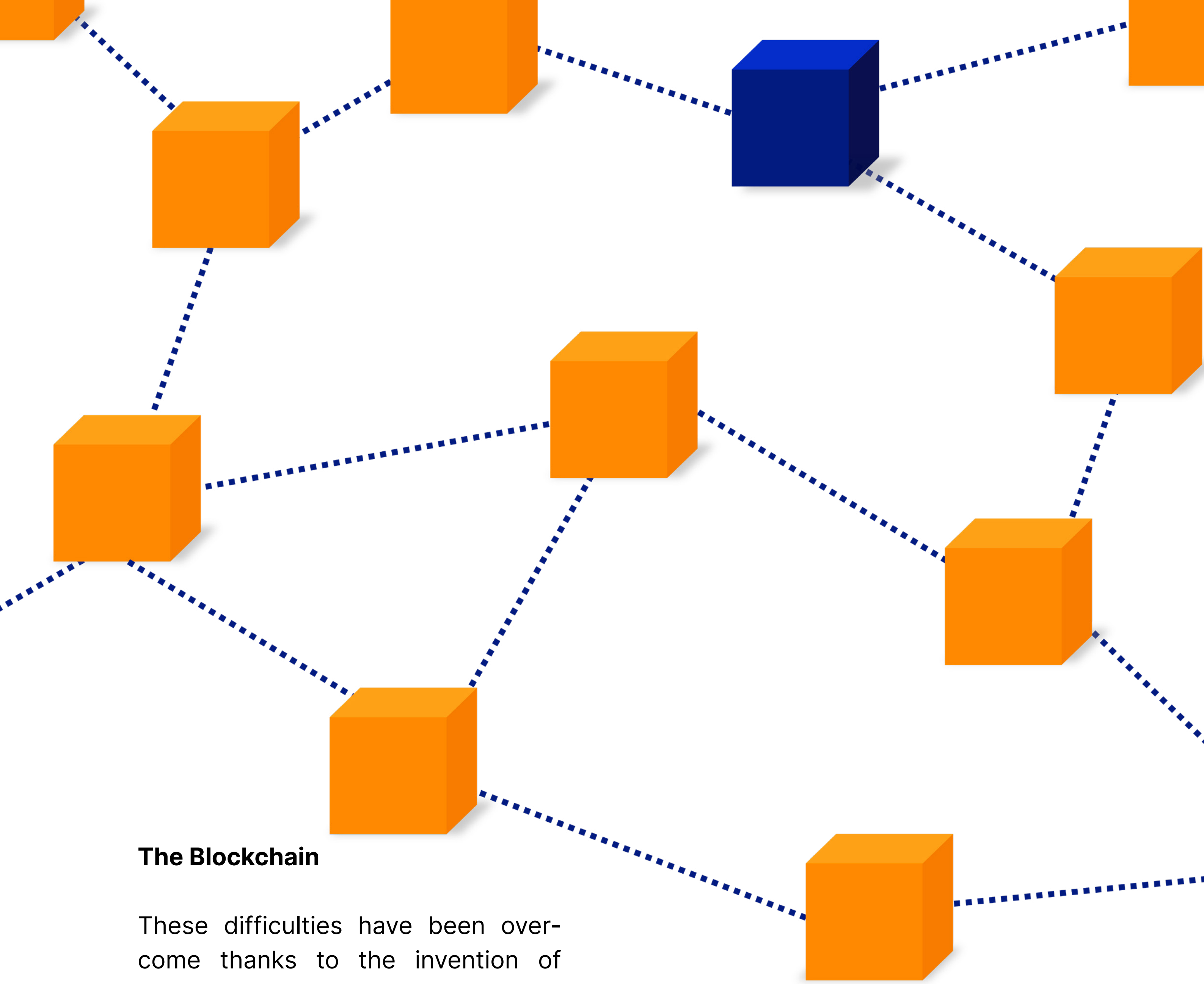
HOW DOES BITCOIN WORK?

After learning about the history of Bitcoin, we will now dive into its way of operation. The goal is to understand how the Bitcoin network works, what problems it solves, and what its practical benefits are.

The intention behind Bitcoin is to be a decentralized network. No network participant should be able to rule the network alone - the decision-making power and supervision are distributed among all participants. This is important because no individual, no government, and no company can change the network independently, but changes are only possible collectively.

Bitcoin works in such a way that every network participant has an identical copy of the most up-to-date ownership ledger at all times – as a result, everyone always knows who currently owns which Bitcoin. Thus, no one can claim that they own more Bitcoin than they do, because every network participant can check this claim against its ledger copy and prove it false.

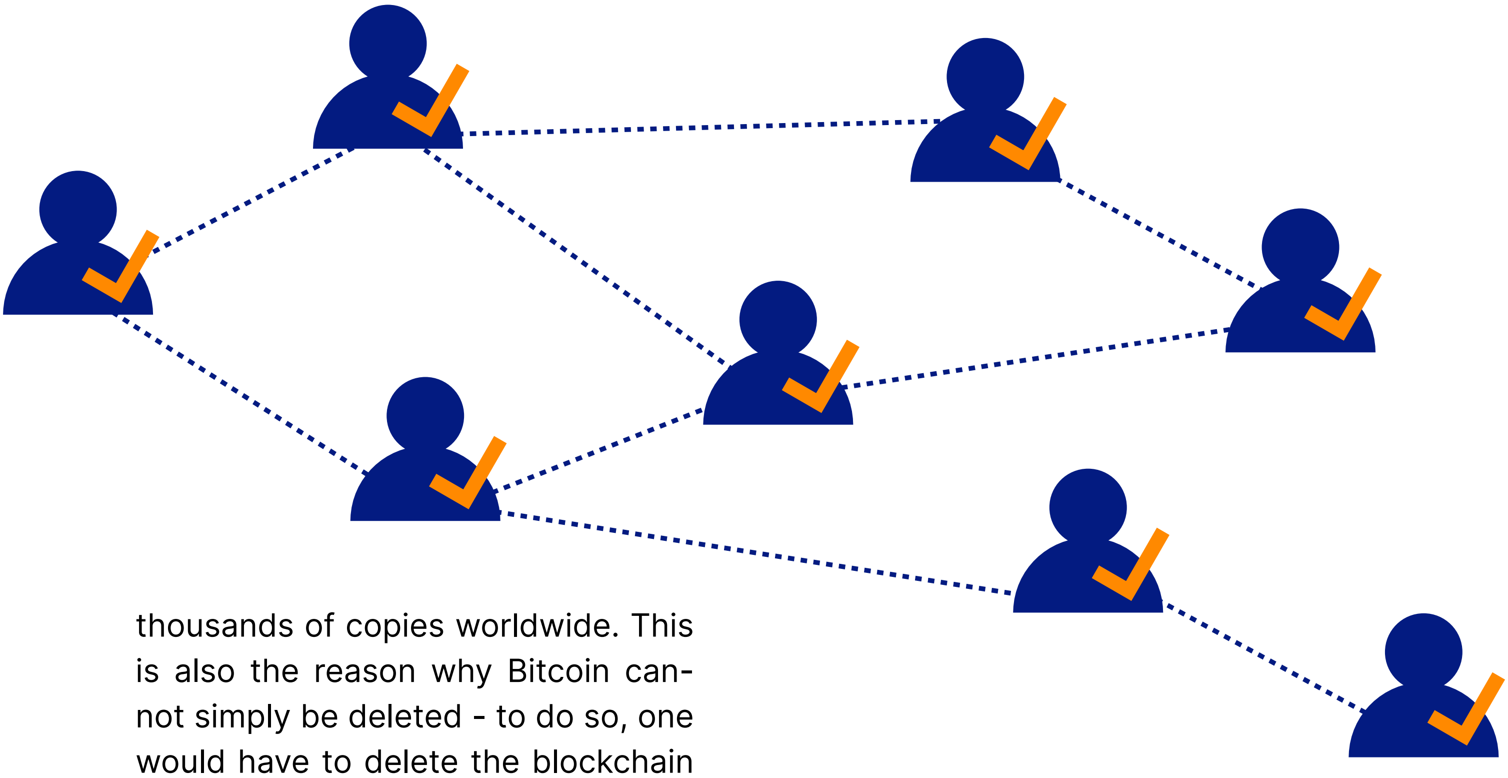
Before Bitcoin was launched, decentralized networks faced two major challenges. First, how can be ensured that all participants receive the latest updates on changes in ownership - that is, the information about which Bitcoin have been transferred and to whom. And second, how can participants verify with absolute certainty that the information they receive is correct.



The Blockchain

These difficulties have been overcome thanks to the invention of the blockchain. A blockchain stores information and data in chronological order. In the case of Bitcoin, all transactions since the creation of Bitcoin are stored in chronological order in tens of thousands of blocks, which together form the Bitcoin blockchain. Any network participant wanting to know who owns which Bitcoin can trace the transaction history on the Bitcoin blockchain and determine exactly who owns how many Bitcoin at present. Thus, if someone wants to send a Bitcoin, anyone can check whether this Bitcoin truly belongs to the person in question.

Up to this point, this mechanism is nothing new since banks use a similar process. If a customer wants to spend one Swiss Franc, the bank looks up the transaction history to see whether the Franc still belongs to the customer or whether it has already been spent (sent to someone else). The unique characteristic of a blockchain, however, is that this information is not stored on a central bank server, but on the computers of all network participants (so-called full nodes) and thus exists in tens of



thousands of copies worldwide. This is also the reason why Bitcoin cannot simply be deleted - to do so, one would have to delete the blockchain copy from all participating computers worldwide at the same time.

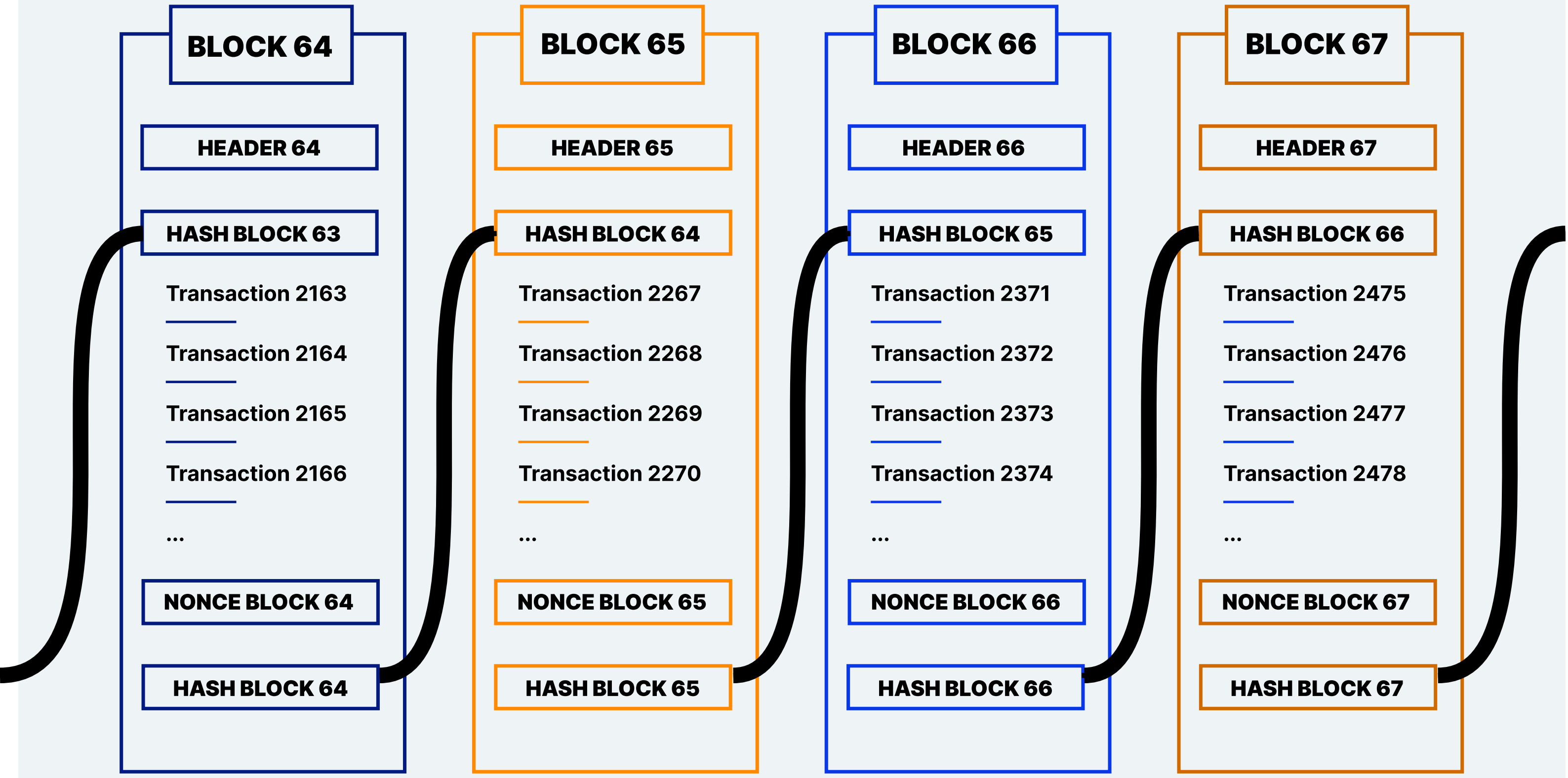
However, the challenge blockchains face is that every network participant must be able to determine with absolute certainty that its copy of the blockchain is correct and that no erroneous or fraudulent transaction enters their copy of the ledger. Since new blocks with new transactions are being added to the blockchain every 10 minutes, the blockchain is constantly growing and must be updated continuously on all participating computers worldwide.

These newly attached blocks must be verifiable by everyone. The verification is done using unchangeable rules that are defined in the computer code of the Bitcoin network. These rules define exactly which transactions are allowed and which are not. Every user who downloads the copy of the blockchain can therefore verify whether all transactions comply with the given rules. If a transaction violates the rules, i.e. if it is incorrect or fraudulent, it is rejected by the network participants (full nodes) and not included in the blockchain.

Proof-of-Work (PoW) Mining

In addition, the Bitcoin network has a mechanism to limit the appending of new blocks. If new transactions and blocks could be added to the blockchain by anyone, the network would end up in chaos, as the blockchain would not be able to update itself worldwide to the same state quickly enough.

To prevent this, Bitcoin works with a Proof-of-Work mechanism. For someone to earn the right to add a new block to the blockchain, they must provide proof of work. A simple illustration of this process is a group of people searching for needles in a haystack. Whoever finds a needle first is allowed to add a new block



The Header, the result of the previous block's hash function, all transactions of the current block, and a Nonce (random number) are put into a mathematical function. The Nonce is changed until the result of the hash function has enough preceding zeros. This process is called mining.

to the blockchain. In addition, the finder is rewarded with new Bitcoin units as well as the transaction fees contained in this block. As soon as the block has been attached, this process starts again.

In reality, miners are executing a mathematical hash function (SHA-256 hash algorithm) in the search for specific numbers. The hash number of the previous block, the transactions of the current block, and a random number (nonce) are hashed together. The random number is changed until the hash function spits out a result with a minimum number of leading zeros. For example, block #700000, created on September 11, 2021, had the valid hash number: 0000000000000000000590fc0f3eba193a278534220b2b37e 9849e1a770ca959.

The search for this number, also called mining, has two main functions: First, it links the blocks together in a mathematical-cryptographic way so that everyone can easily verify the correct order. At the same time, the Proof-of-Work mechanism makes it close to impossible to change this order. Second, this mechanism delays the addition of new blocks so that, on average, a new block is added to the blockchain only every 10 minutes. Thus, all network participants worldwide are given enough time to update to the same, latest state of the blockchain.

In summary, miners keep the Bitcoin network running. Thanks to them, new transactions are being processed and added to the blockchain. The full nodes keep copies of the ledger, make sure that the rules are complied with, and ensure that no fraudulent transactions enter the blockchain.

21 million Bitcoin

Although more blocks are constantly being added to the Bitcoin blockchain and miners are rewarded for this work with new Bitcoin, the total number of Bitcoin is limited to 21 million Bitcoin. There will never be more than 21 million Bitcoin. But these 21 million coins were not in circulation from the beginning. Rather, they are released by the Bitcoin code according to a strict issuance schedule.

When Bitcoin was launched, the code released 50 new Bitcoin to miners approximately every 10 minutes. Four years after launch, the number of Bitcoin released per ten minutes has halved. This process is called 'halving' and describes the fact that the block reward for miners decreases by half every 4 years. Currently, there is already 19 million Bitcoin in circulation. The remaining Bitcoin will be mined until the year 2140. After that, miners will only be compensated via transaction fees.

The strictly limited quantity of Bitcoin units is one of the fundamental properties of cryptocurrency and makes Bitcoin an extremely scarce commodity. This absolute digital scarcity is also an important prerequisite for Bitcoin's function as a store of value over long periods and is the reason why Bitcoin is often called digital gold or gold 2.0.

The result: Digital property

Examining all the features of the Bitcoin network in combination, one can see the importance of this invention. For the first time in history, there exists a digital good that is only available in a strictly limited number. Bitcoin cannot be copied or duplicated.

Thanks to this achievement, Bitcoin is often referred to as digital property. Because just as every piece of land on this earth is unique and exists only once, each Bitcoin unit is also unique and exists only once in the digital space.

And these Bitcoin units can be truly owned. Only the person in possession of the corresponding private key, which is a combination of numbers and letters consisting of 64 characters, can move the associated Bitcoin. In other words, without this private key, Bitcoin cannot be stolen, confiscated, or blocked. This allows the owner to have absolute control over their financial resources, regardless of whether they are a millionaire, a political refugee, or a persecuted creditor. For the first time since the invention of the computer, it is possible to truly own digital assets.

WHY BITCOIN?

But why all this hype around Bitcoin? The possibility of truly owning a digital asset may be revolutionary. But why would anyone want to own Bitcoin in the first place?

The Best of Both Worlds

In past centuries, precious metals and later cash in the form of coins and banknotes were used as means of payment. These had the advantage that they could be stored and spent independently of third parties. The saying “cash is printed freedom” sums this up very well. However, the disadvantage of precious metals and cash is that they are difficult to use in the digital Internet space. At the latest since the advent of online shopping, debit and credit cards have therefore become established among the general population.

But now that most people are using digital money in bank accounts instead of cash, the counterparty risks they face are increasing. If, for example, a financial institution declares insolvency, the clients’ savings might be lost. Or, as happened in Cyprus in 2013, if cash withdrawals are severely limited, capital controls are put in place, and forced expropriation on savings accounts is happening, then people are no longer in control of their money. Or, as currently is the case in many western countries, if banking clients are not allowed to send money to relatives because they live in Cuba or Iran, they are reliant on a third party to approve all their transactions.

With the switch from paper-based to digital money, stored in bank accounts, we are ultimately no longer in control of our own money. Until now, however, this downside has been the price we had to pay to participate in a digitized life.

Bitcoin offers a solution to this dilemma. As digital money, it is ideally suited for use in the digital space. At the same time, Bitcoin can be stored as digital property without having to rely on third parties (banks) for safekeeping. So, Bitcoin owners can store their coins – in form of the private keys - under the mattress or wherever they think it is safest.

Perfect Timing

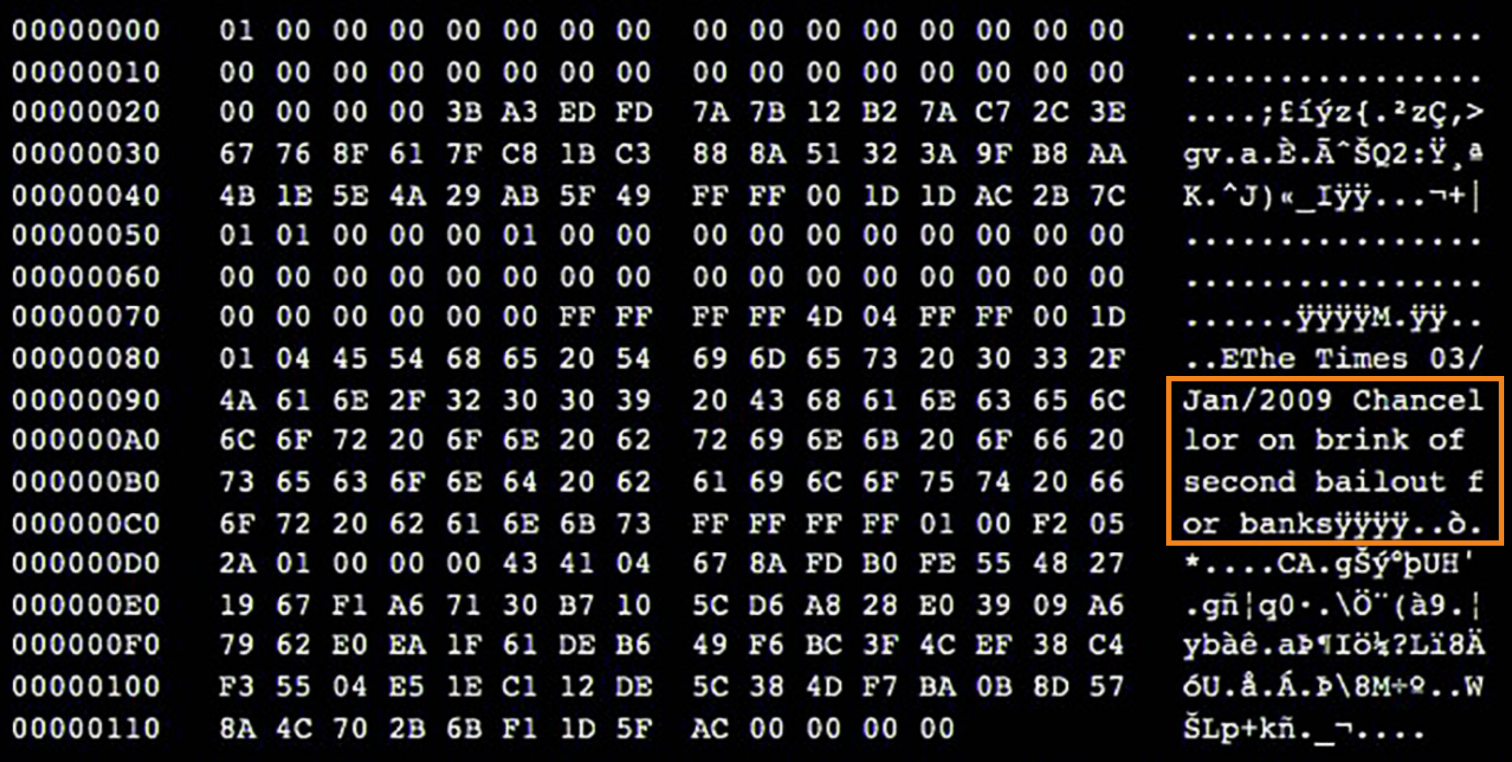
Bitcoin was created amid the global financial crisis of 2008/09. On the first block of the Bitcoin blockchain - also called the Genesis block - Satoshi Nakamoto left a strong message. He quoted a headline published in The Times newspaper saying, “Chancellor on brink of second bailout for banks.”

With this act, Satoshi expressed the state-critical philosophy of the Cypherpunks. In the financial crisis of 2008, the central banks put vast amounts of new money into circulation to save the banks. In the end, however, the savers paid for it, as their savings lost value through dilution by the money glut. This fact once again confirmed the Cypherpunks in their distrust of the state and central banks and reinforced their conviction that state-independent money was urgently needed.

The same procedure, only on a larger scale, has been repeated since the outbreak of the Covid-19 pandemic. In 2020 alone, the U.S. money supply was expanded by 50 percent, and in

Bitcoin Genesis Block

Raw Hex Version



```
00000000   01 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000010   00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000020   00 00 00 00 3B A3 ED FD   7A 7B 12 B2 7A C7 2C 3E   ....;£íýz{.²zÇ,>
00000030   67 76 8F 61 7F C8 1B C3   88 8A 51 32 3A 9F B8 AA   gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040   4B 1E 5E 4A 29 AB 5F 49   FF FF 00 1D 1D AC 2B 7C   K.^J)«_Iÿÿ...¬+|
00000050   01 01 00 00 00 01 00 00   00 00 00 00 00 00 00 00   ................
00000060   00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000070   00 00 00 00 00 00 FF FF   FF FF 4D 04 FF FF 00 1D   ......ÿÿÿÿM.ÿÿ..
00000080   01 04 45 54 68 65 20 54   69 6D 65 73 20 30 33 2F   ..EThe Times 03/
00000090   4A 61 6E 2F 32 30 30 39   20 43 68 61 6E 63 65 6C   Jan/2009 Chancel
000000A0   6C 6F 72 20 6F 6E 20 62   72 69 6E 6B 20 6F 66 20   lor on brink of 
000000B0   73 65 63 6F 6E 64 20 62   61 69 6C 6F 75 74 20 66   second bailout f
000000C0   6F 72 20 62 61 6E 6B 73   FF FF FF FF 01 00 F2 05   or banksÿÿÿÿ..ò.
000000D0   2A 01 00 00 00 43 41 04   67 8A FD B0 FE 55 48 27   *....CA.gŠý°þUH'
000000E0   19 67 F1 A6 71 30 B7 10   5C D6 A8 28 E0 39 09 A6   .gñ¦q0·.\Ö¨(à9.¦
000000F0   79 62 E0 EA 1F 61 DE B6   49 F6 BC 3F 4C EF 38 C4   ybàê.aÞ¶Iö¼?Lï8Ä
00000100   F3 55 04 E5 1E C1 12 DE   5C 38 4D F7 BA 0B 8D 57   óU.å.Á.Þ\8M÷º..W
00000110   8A 4C 70 2B 6B F1 1D 5F   AC 00 00 00 00            ŠLp+kñ._¬....
```

other countries - including Switzerland - the digital printing press is running constantly. A direct consequence of this is record low-interest rates - even negative interest rates in Switzerland - and strong asset inflation.

Hedging against Currency Devaluation

Bitcoin was therefore launched at the best possible time. Seldom has the money issue been more relevant and the question marks bigger than today. With its limited supply of 21 million, Bitcoin provides a pleasant contrast to the endlessly growing balance sheets of central banks. Its limited supply offers protection against the dilution of one‘s capital, as has been observed with all currencies worldwide over the past decades.

Due to its specific setup, Bitcoin is designed to ensure the preservation of purchasing power over long periods. Since Bitcoin is scarce, it should be even better at this task than gold, which has a net inflow of 1-2% every year. In addition, the costs of storing and transporting Bitcoin are also significantly lower compared to gold, which also allows for better value preservation over time.

Property Protection

Another issue that Bitcoin mitigates is the protection of property. While gold or cash usually must be stored securely at great expense to protect them from theft, Bitcoin can be stored and transported at virtually zero cost. Even substantial amounts can be taken anywhere in the world with a code consisting of twelve or twenty-four words. Once memorized and physically destroyed, this code cannot be stolen by anyone, making the Bitcoin behind the code secure and allowing its owner to take them with him to the grave if desired.

BUY BITCOIN

There are two ways to get hold of Bitcoin. Either you earn Bitcoin as a miner, or you buy Bitcoin from another person. Since mining with home devices has become virtually impossible nowadays, the only way left for newcomers is to buy Bitcoin.

Crypto Exchanges & Brokers

The easiest way to buy Bitcoin is through a crypto exchange or a broker. These work similarly to stock trading platforms. After opening a personal account, Swiss francs, Euros, or US dollars can be transferred via bank transfer or credit card. Once the money has arrived in the personal account at the trading exchange, Bitcoin can be bought 24/7 with a few clicks at the current market price. In Europe, it is possible to buy Bitcoin without registration, verification, or depositing money first with the popular Bitcoin-only investment app Relai.

Peer-to-peer

As an alternative to crypto exchanges, Bitcoin can also be purchased directly from other market participants via peer-to-peer platforms without involving an exchange. This allows for greater anonymity, as no personal data must be revealed in the process.

Bitcoin ATMs

There is also the possibility to withdraw Bitcoin via ATMs. These are already available in many countries, including Switzerland, Germany, and Austria. At Bitcoin ATMs, Bitcoin can be withdrawn anonymously with cash or credit card. Neither an account nor an existing crypto wallet is necessary.

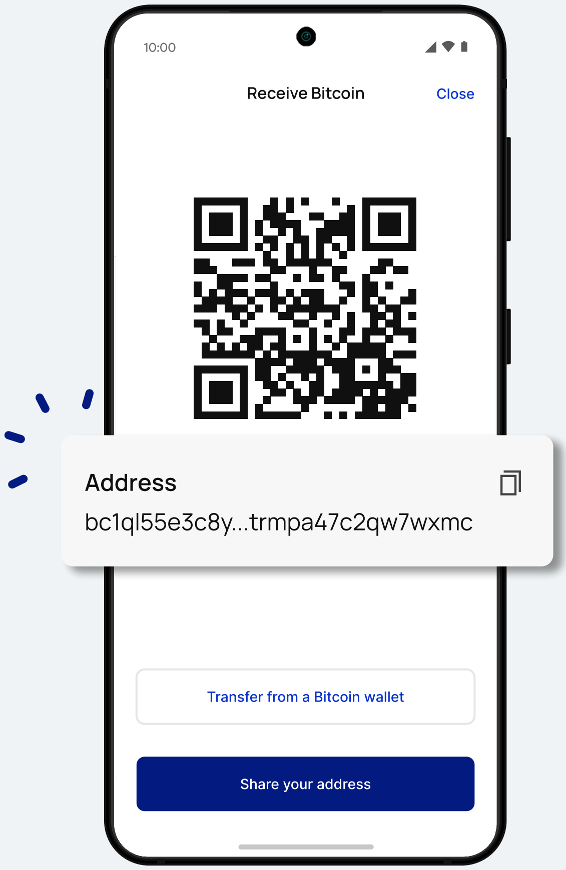
Store Bitcoin securely

Once Bitcoin have been acquired, the question of their safe handling and storage arises. Bitcoin and cryptocurrencies are governed by the principle: „not your keys, not your coins“. To truly own your Bitcoin, you must be in possession of the corresponding private keys. This somewhat technical expression means that you only really have control over your Bitcoin if you store them in a personal digital wallet to which you have the private keys.

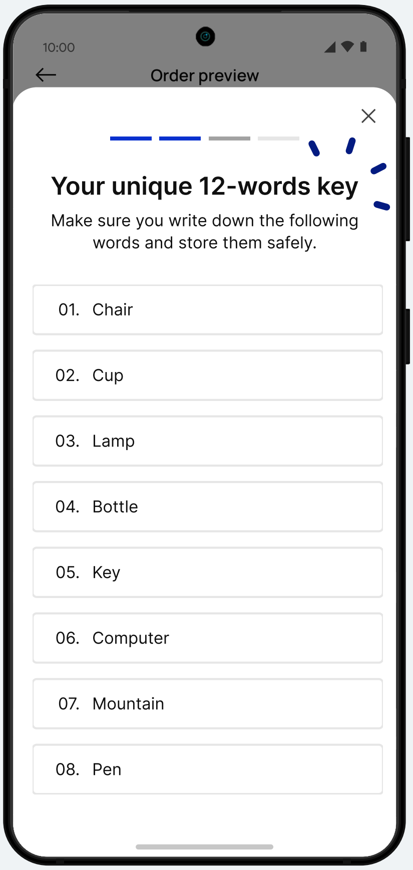
As long as the Bitcoin are deposited on a crypto exchange, they are under the control of the exchange. If the exchange is hacked, goes bankrupt, or is fraudulent, the Bitcoin could be lost forever.

Self-Custody

Unlike a bank account, Bitcoin gives you the option to store your monetary units in a personal wallet. This allows you to be your own bank and has the advantage that you have absolute control over your Bitcoin. In return, this also comes with responsibilities. The private key, which often comes in the form of twelve or twenty-four words, must be stored and kept safe by the owner of the respective Bitcoin himself. Incorrect or negligent handling can lead to the irrevocable loss of Bitcoin.



Address
bc1ql55e3c8y...trmpa47c2qw7wxmc



Your unique 12-words key

Make sure you write down the following words and store them safely.

01. Chair
02. Cup
03. Lamp
04. Bottle
05. Key
06. Computer
07. Mountain
08. Pen

Wallets: Digital wallets

Digital wallets help to securely store Bitcoin, or more precisely, private keys. The Bitcoin themselves are always stored on the blockchain and cannot be transferred to a wallet. Only the access keys to the Bitcoin can be stored in a wallet.

So, wallets were created to store the private keys safely and in a simple way. Besides, they enable sending and receiving Bitcoin with just a few clicks. Thus, wallets are a useful tool for handling Bitcoin.

Software Wallet

The most common wallets are software wallets. Software wallets can be set up as desktop applications or as smartphone apps. During setup, the private keys to the wallet are listed in the form of twelve or twenty-four words (seed phrase). These words are synonymous with the Bitcoin in that wallet. Whoever knows these words has control over the coins. Therefore, the words must be written down analogously, preferably on paper, in secret and kept safe. Should the computer or smartphone ever be lost or get stolen, the wallet can be restored at any time with these words.

Software wallets have the advantage that they can be set up quickly and are easy to use. However, since software wallets are computer programs installed on a device and connected directly to the Internet, there is always a risk of hacker attacks.

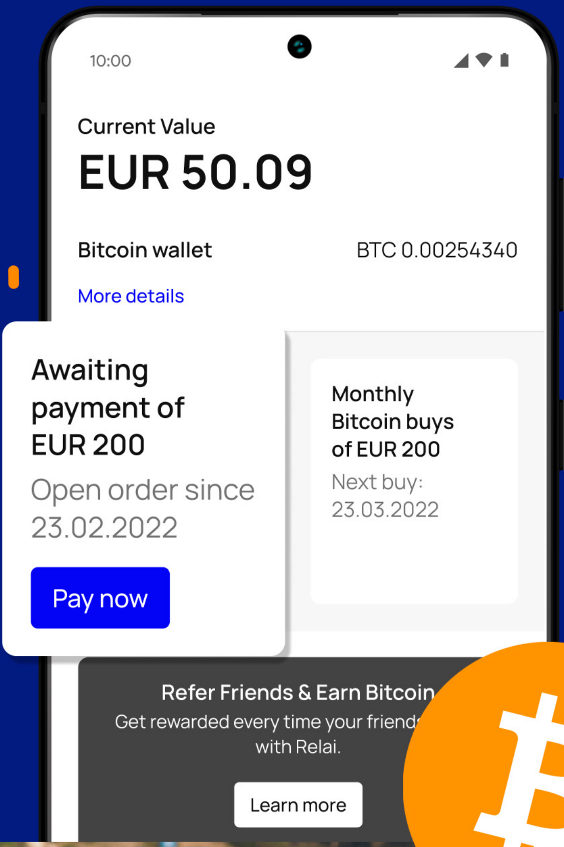
Hardware Wallet

If you value security, you should use a hardware wallet instead. These small devices store the access codes for the Bitcoin on a USB stick-like device that is only connected to the computer when needed. The device is designed in such a way that even a computer infected with malicious software cannot access the codes.

When setting up a hardware wallet, twelve or twenty-four words (seed phrase) are generated, which have to be written down analogously and kept safe. If the hardware wallet is ever lost, it can be restored with the help of the words. Examples of hardware wallets are BitBox and Trezor.

Made in Switzerland

EUROPE'S EASIEST BITCOIN APP


10:00

Current Value

EUR 50.09

Bitcoin wallet BTC 0.00254340

More details

Awaiting payment of EUR 200

Open order since 23.02.2022

Pay now

Monthly Bitcoin buys of EUR 200

Next buy: 23.03.2022

Refer Friends & Earn Bitcoin

Get rewarded every time your friends with Relai.

Learn more

Received Bitcoin BTC 0.00254340

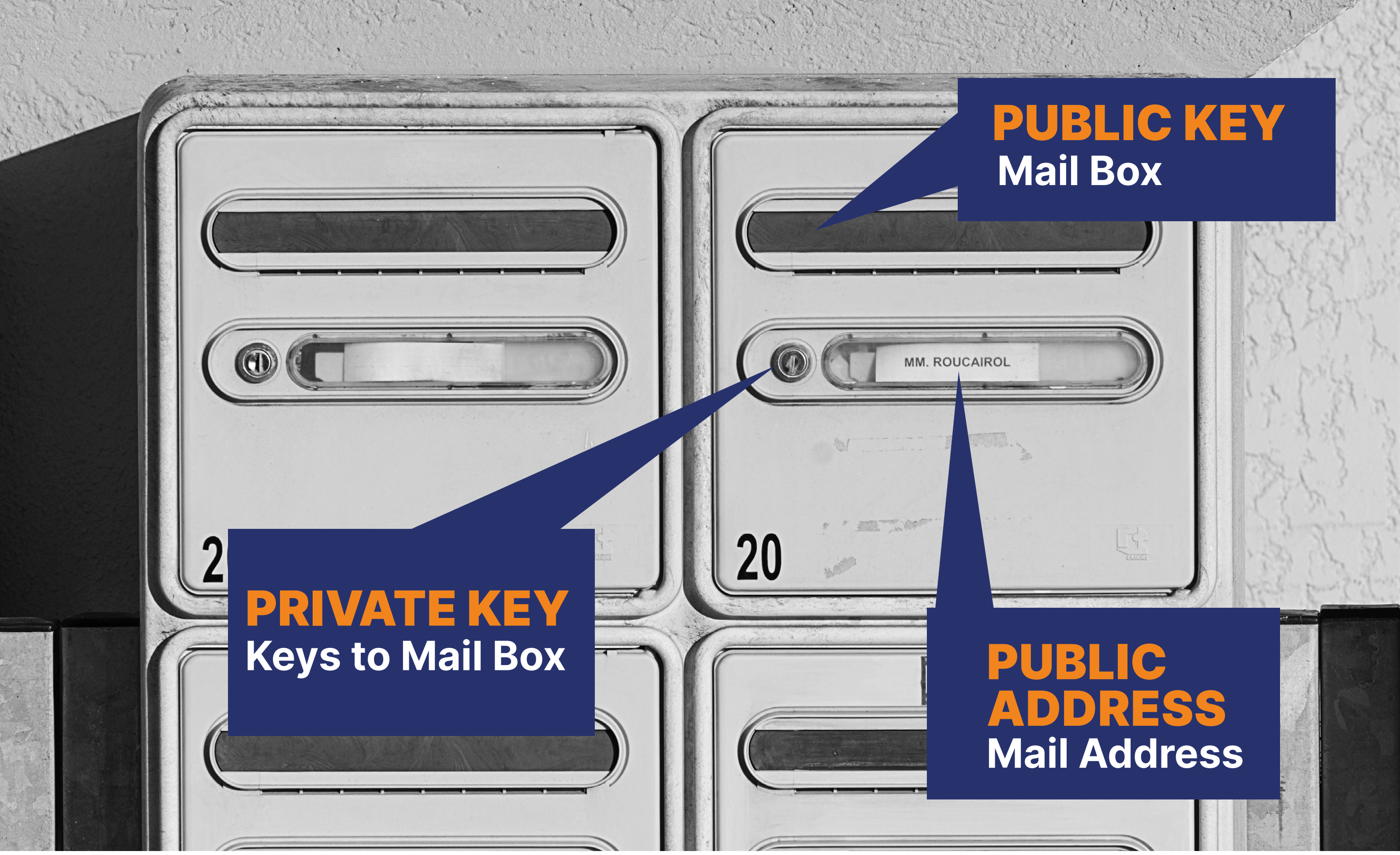
24.09.2021 CHF 50.65

Relai

Download on the App Store

GET IT ON Google Play

Buy bitcoin in 1 minute from as little as 10 EUR/CHF without verification.



Send and receive Bitcoin

Sending and receiving Bitcoin is very easy. Each Bitcoin wallet has its public address generated from the so-called public key. This serves as the receiving address, similar to an IBAN. Anyone who has this address can send Bitcoin to the corresponding wallet. The address is often displayed as a QR code, which further simplifies handling.

If you want to send Bitcoin to someone, you can either enter the recipient's Bitcoin address in your wallet under ‚send' or scan the corresponding QR code. The transaction fees incurred are automatically deducted from the sender's wallet. The amount of the transaction fees varies depending on the load of the network and can be looked up here.

It takes an average of 10 minutes for the transfer to reach the recipient. However, it can also take longer, depending on the number of transaction fees that you are willing to pay.

Pay with Bitcoin

When Bitcoin was created, it was hoped that Bitcoin could one day be used to pay for everyday goods. And in theory, this is possible today. Some government tax departments, non-profit organizations, and a growing number of companies accept Bitcoin as a means of payment. But since transactions via the Bitcoin network can cost several francs and take at least 10 minutes, this only makes sense for larger amounts. To send Bitcoin cheaply and quickly, an alternative solution is needed.

Lightning network - faster and cheaper

Therefore, an additional layer was built on top of the Bitcoin network. This network, called Lightning, allows paying with Bitcoin in seconds at a minimal cost. In countries like El Salvador, the Lightning network is already in active and successful use.

Paying for everyday goods with Bitcoin will therefore largely take place via the Lightning network in the future. Developments in this area are running at full speed. Twitter, for example, recently introduced a ‚tip' function that uses the Lightning network. Furthermore, the app Strike offers worldwide payments in various currencies at zero cost via the Lightning network. It is, therefore, to be expected that in the future only larger amounts will be settled directly via the Bitcoin network, while all other transactions will run via the Lightning network.

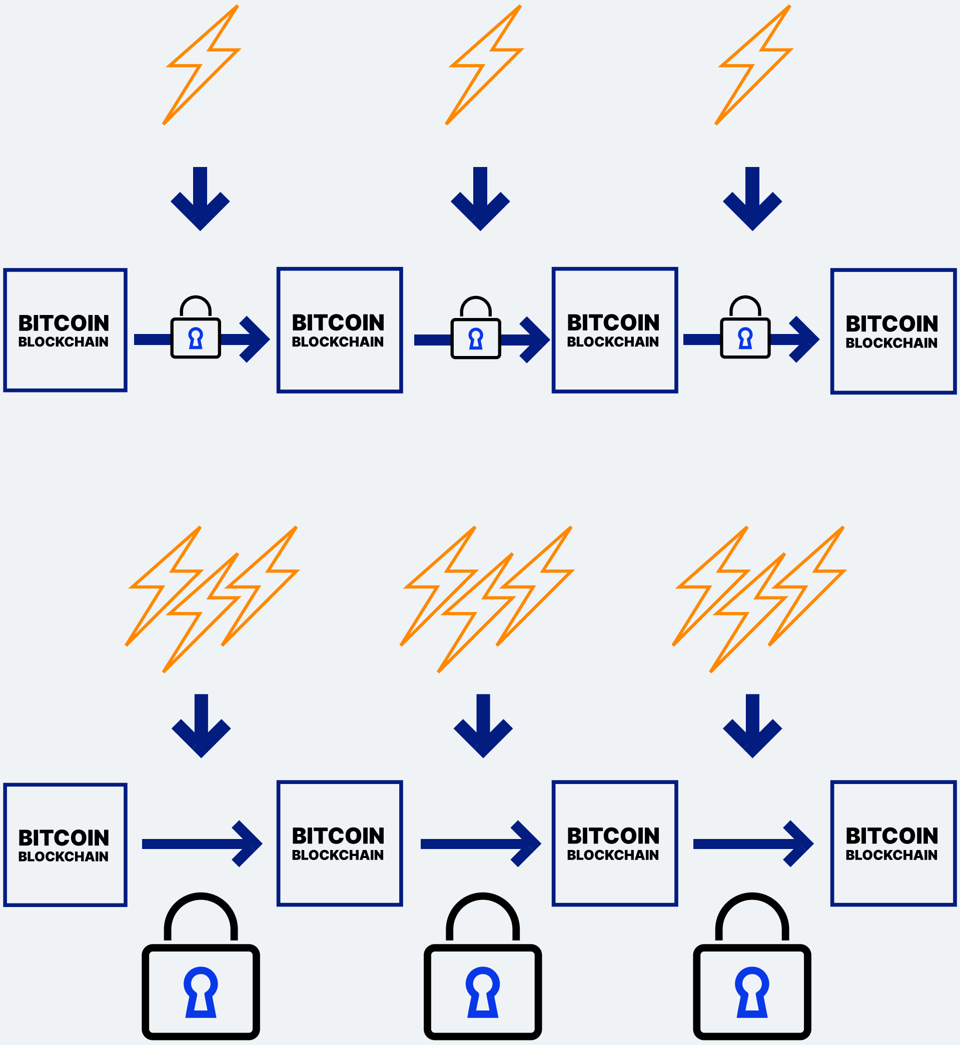
Since primarily smaller amounts are sent through the Lightning network, Satoshis, or short Sats, are used as the unit of account instead of Bitcoin. 1 Bitcoin is equal to 100,000,000 Satoshis. To use the Lightning Network, a Lightning wallet must be set up.

A LOOK INTO THE FUTURE

In its more than ten years of existence, Bitcoin has gone through many highs and lows. The cryptocurrency was declared dead or fell into oblivion among the general public several times after heavy price losses. However, Bitcoin has spread inexorably around the globe over the last decade.

Bitcoin and Energy

One of the first concerns that are oftentimes raised regarding the development of Bitcoin is the energy consumption of the Bitcoin network. Bitcoin mining already consumes a significant amount of electricity worldwide. And this consumption is likely to increase in the future as more people get into Bitcoin mining.



The less energy in the form of computing power is used to build the Bitcoin blockchain, the easier it is to alter it later on.

The more energy in the form of computing power is used to create the Bitcoin Blockchain, the harder it is to alter it later on.

When talking about Bitcoin and Energy, it is important to understand that the amount of energy flowing into the Bitcoin network is critical to the security of the network. The more energy that flows into the network, the more secure it is. This is because, for the Bitcoin blockchain to be altered, the same amount of computing power - and therefore energy - that was invested to create the blockchain in the first place must be expended again. However, with millions of computers worldwide providing computing power to the Bitcoin network, it is nearly impossible for an individual, organization, or a state to ever muster enough computing power to make even the smallest changes to the blockchain. Therefore, hashpower and the associated energy consumption is an important security feature of the Bitcoin network.

Furthermore, Bitcoin mining computers have the advantage that they can be located anywhere in the world. Since miners need the cheapest possible electricity to be profitable, they often locate in places where there are a lot of surpluses, and therefore cheap, energy. In the longer term, this is likely to be in places where there is a lot of renewable energy, as this produces the cheapest electricity.

According to the Bitcoin Mining Council, Bitcoin miners currently use about 56% renewable energy and the trend is increasing. Many Bitcoin experts believe that Bitcoin mining will be powered by up to 100% renewable energy in the future.

Until that is the case, however, Bitcoin‘s energy consumption boils down to the question of whether secure and unforgeable money and store of value are worth this expenditure of energy - or not.

El Salvador - Bitcoin as the National Currency

A few years ago, visionaries already thought it possible that Bitcoin would one day be recognized as legal tender by nation-states. In the summer of 2021, the time had come: El Salvador was the first country in the world to introduce Bitcoin as legal tender. In stores, restaurants, and at service providers of all kinds, payment can not only be made with US dollars but also with Bitcoin. For this purpose, citizens were provided with a customized Bitcoin wallet, which enables payments via the Lightning network in a matter of seconds and at a minimal cost.

Other countries such as Ukraine, Brazil, and Panama are currently discussing similar draft laws. Should other countries follow El Salvador‘s example, this would on the one hand further increase the demand for Bitcoin and even more importantly underpin Bitcoin’s credibility as ‚money‘. The acceptance of Bitcoin as a legal tender in more and more countries, therefore, represents a decisive phase in the global adaptation process of Bitcoin.

Laws and regulations

These developments have led to nation-states, central banks, and companies having to deal intensively with cryptocurrencies. Various states, including Switzerland, have issued regulations and guidelines regarding cryptocurrencies. This step is welcomed by many market participants, as it creates legal certainty for both crypto projects and the investors involved.

Regulations are also on the horizon in the USA, which has so far taken a laissez-faire approach. The exact form these new regulation laws in the US will take is being closely monitored by the global crypto community, as they will have a major impact on the entire crypto sector.

Other cryptocurrencies

Bitcoin is by far not the only cryptocurrency nowadays. There are now over 16,000 different cryptocurrencies and assets. These coins and tokens have different characteristics and functionalities and have not all been designed as ‚currencies' or money. Some are more like stocks, in that their value reflects the success of a crypto project. Others are required to make use of a particular service. And still others - so-called meme tokens - are primarily fun currencies.

To avoid losses, it is, therefore, advisable to take a closer look at the respective currency and the project behind it before making any investment.

Central Bank Digital Currencies (CBDC)

Cryptocurrencies are in transition from an unregulated Wild-West phase to a regulated crypto finance world. This development has not left central banks unscathed, and ideas have been raised that central banks should issue their own cryptocurrencies. These „Central Bank Digital Currencies," or CBDCs, would, proponents say, combine the stability of a state currency with the benefits of a blockchain-based currency. In short, they would create digital cash, so to speak.

However, depending on its design, a CBDC can take on fundamentally different forms.

Various countries have launched pilot tests with different types of CBDCs, and CBDCs have already been launched in a few countries. However, it is eagerly awaited whether and in what shape and form economically strong currency areas such as the USA, EU, or China will launch their CBDCs.

Money Competition

Our society has become so accustomed to state currencies in recent decades that other types of money were hardly imaginable for many until recently. But not so long ago, it was part of everyday life to have different types of money circulate in parallel. There were banknotes from various banks, coins made of different metals, and other monetary values that could be used as means of payment.

With Bitcoin, non-state currencies are now available again as an alternative to state currencies. Until now, the majority of governments have tolerated Bitcoin. To some extent, this might be thanks to its decentralized nature, which makes Bitcoin difficult to attack. For citizens, this means that a digital alternative to state money is now available alongside gold and silver. The effects of this additional monetary competition will be exciting to observe in the future.

BITCOIN, WHAT NOW?

If you‘re asking yourself what you should do with all this information, let me make a suggestion. Entering the world of Bitcoin costs nothing, neither time nor money. But you will get to know a technology that is about to change our world and the future.

Therefore: Create an account on a crypto exchange or download a wallet on your smartphone and buy Bitcoin for 50 CHF. Or have a colleague send you some Bitcoin to your wallet. But get your hands on Bitcoin at least once.

Because should Bitcoin make the breakthrough and become as ubiquitous as the Internet, you will not only know about it theoretically but will also have used Bitcoin yourself. Sometimes this makes all the difference, as this gives you a look and feel for the technology, which puts you ahead of a majority of the people.

ABOUT

THE AUTHOR

Daniel Jungen is an economist and financial journalist with expertise in crypto assets. Daniel is co-founder of InsightDeFi, a research boutique specializing in all things crypto.

Together with his partners at InsightDeFi, they publish a bi-weekly newsletter (German) about Bitcoin, DeFi, and Crypto.

RELAI

Founded in Switzerland by Julian Liniger and Adem Bilican after they struggled to find a safe, hassle-free space for buying bitcoin, Relai is making bitcoin saving and investment accessible for everyone. The bitcoin-only app is designed to be simple and intuitive, enabling anyone in Europe to buy and sell bitcoin within minutes, with no need for registration, verification, or deposits. Independently audited, and with over 35 million CHF of bitcoin invested through its platform, Relai is giving consumers the chance to unlock new means of saving and investing.

Learn more at Relai.app.

Dieses Büchlein ist auch auf Deutsch erhältlich.