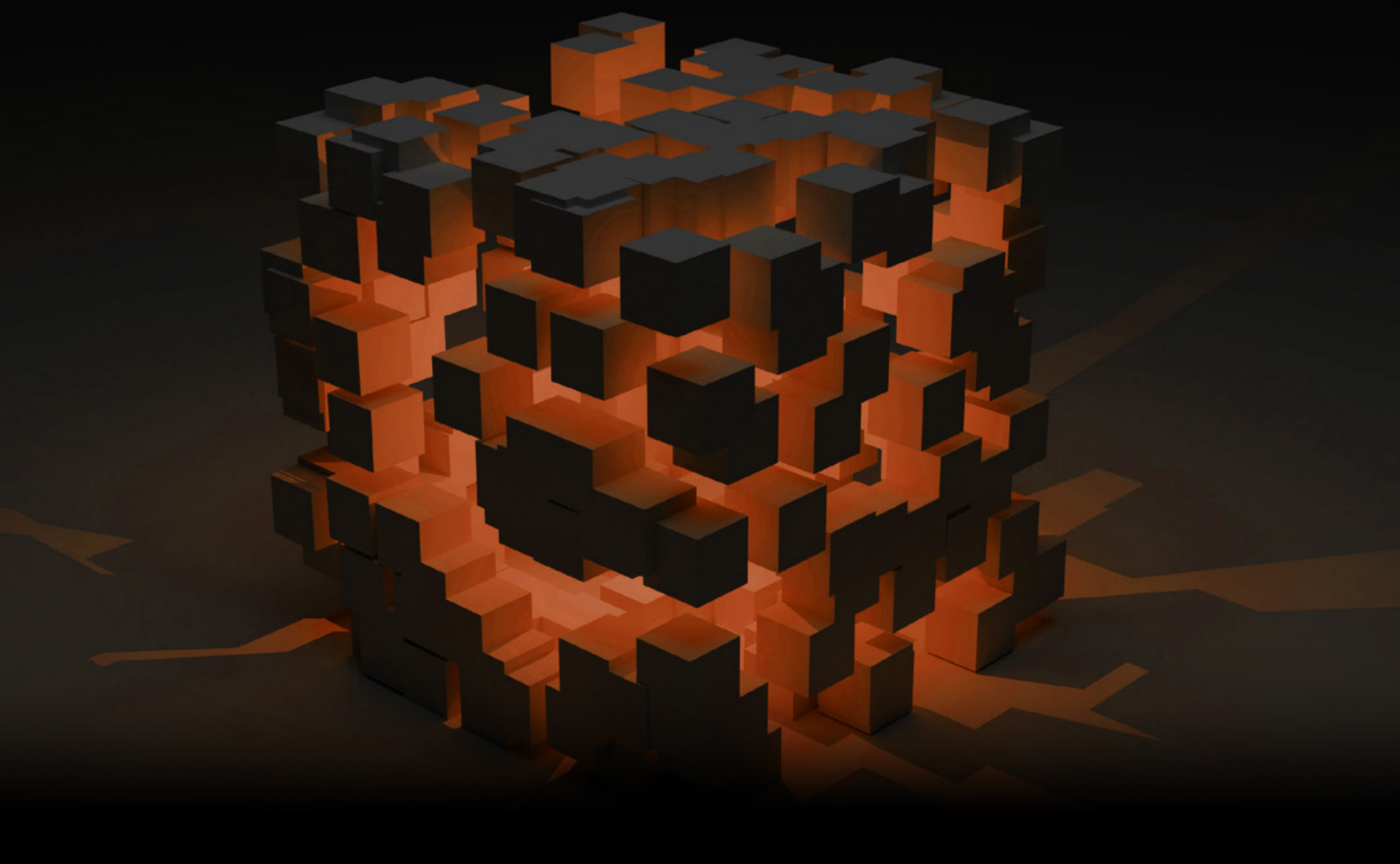
Bitcoin Reserve

Bitcoin

Everything in 21 pages



What is bitcoin?

Chances are, that's the first question on your mind

Most people have heard about bitcoin. When the price of bitcoin makes big moves, you hear or read about it in the news. Maybe you know people who own bitcoin.

Still, few people have even a basic understanding of what it is and how it works. Understanding its main concepts and principles, however, is highly recommended, and might prove to be incredibly important in the future. Your future.

That's why Bitcoin Reserve has created this concise overview for anyone who takes an interest in the subject. After reading through it, you'll know why bitcoin was created, how it works, what makes it unique, why you personally need it, and how you can safely store and buy it.

So, what is bitcoin?

The short and easy answer is: "Decentralized digital money". But, what does that really mean? Just those three words open the door to more questions. What is decentralization? Why does it matter? Is it possible?

Understanding bitcoin means first and foremost understanding what money really is. Not many people know exactly what money is, how it came about and how it works. Similarly, few people know that what we call money nowadays is fundamentally different from what it was half a century ago.

At the same time, almost every aspect of your life is influenced by money in some shape or form. Therefore, in the next section, we'll first give a short overview of the history of money before elaborating on how bitcoin fits in.

Who created bitcoin?

Believe it or not, nobody knows who created bitcoin - the creator(s) used the pseudonym "Satoshi Nakamoto" when releasing the white paper in 2008 and launching the software in 2009. Some people have made claims of being Satoshi, but none of these claims have turned out to be true. Satoshi was involved with the project for a small amount of time before disappearing only a few years after releasing it to the world. To this day, nobody knows who it is.

This is a notable event and might seem unsettling because of the 'secret' of who Satoshi is, but really, there are no secrets in bitcoin itself. The entire protocol is based on what's called "open source code". As Satoshi Nakamoto said, "*Being open source means anyone can independently review the code. If it was closed source, nobody could verify the security. I think it's essential for a program of this nature to be open source.*"

While the creator of bitcoin is a mystery, bitcoin itself has no mysteries since it's an open and transparent monetary network which can be carefully looked at and used by anyone. As a result of this, bitcoin is the most reviewed code out of all software that has ever existed.

A short history of money

Once human societies had grown beyond small isolated communities, there was a gerneral need for a medium that allowed people to store and exchange value. The long history of this process of natural selection teaches us which qualities are crucial for something to become money.

What is money?

In order to understand bitcoin, we must first understand what money even is. Simply put, in order for something to be "money", it must have three characteristics:

1. Store of value

Stating the obvious, in order for something to be money, people must assign value to it.

2. Medium of exchange

Because people assign value to a form of money, they're willing to exchange it for other goods and services which are valuable to them.

3. Unit of account

Money serves as a tool to indicate how much value a certain good or service has.

Human interaction

For as long as there have been human beings on our planet, people have always worked to keep themselves alive and create circumstances that allowed them to make life worthwhile and even enjoyable. Hunter-gatherers collected what food they could find in nature and made simple tools that enabled them to kill animals, prepare food, build simple shelters and make clothes.

At a certain point in history, people started to specialize. This meant more and more people spent the majority of their time perfecting a certain type of skill such as farming, creating tools, building houses, etc. This specialization meant that people had to trade amongst themselves. Someone who made tools also needed to eat, so they would trade some of the things they made for food. This is called bartering.

The issue with bartering was that there had to be a coincidence of desires and value. The blacksmith could only trade a sword for food if the farmer he wanted to trade with needed a sword. If not, the blacksmith had a problem. Even if the farmer wanted a sword, but could only offer something in return that either had more value or less value than the sword, both people would have a problem.

People required something that could function as a medium to bridge that gap. Because everyone worked hard to create something that other people wanted or needed, they would only sell their product or service for something that more or less represented the same amount of energy and resources spent to make the object they were trying to acquire. This, in turn, would allow them to use that exchange medium for something of comparable value they needed. That's why one of the important functions of money is called "medium of exchange".

The earliest forms of money were objects that were made for ritual and often religious purposes. These artefacts were made of scarce materials and usually required a lot of labour to create. Because people within a certain culture valued these collectibles equally, they became exchangeable.

Daggers, axes and seashells are examples of some of such early artefacts. Because of their ceremonial significance in palaeolithic societies, they were desirable across the population of large geographic areas, meaning they could easily be exchanged for other goods. That's how they fulfilled the role of money, bridging the gap between differing needs, desires and value of tradable goods.

Throughout history, many objects and materials have played the role of money. From glass beads and seashells, to cattle and silver and gold. They all had in common certain important characteristics. Besides the medium of exchange function, another significant role of items or materials used as money was their ability to store value.

Money had to allow people to transport the value it represented over space, taking it with them. For example, when they travelled. These monetary objects also had to allow people to store value over time. It had to enable them to save up the value for a time when they would need it more.

Important characteristics all forms of money had in common

Scarce
Because monetary goods functioned as a proxy for the effort or energy people expended to make tradable goods and services, they had to be scarce. Materials and goods that were readily available everywhere or could be produced in bulk with little effort were unsuitable as money.

Verifiable
Because of the importance of scarcity, anyone engaging in trade had to be able to quickly and easily verify the authenticity of the monetary good used for exchange.

Divisible
As discussed earlier, a lack of coincidence of value among tradable goods was a problem in barter transactions. Therefore, a monetary good had to be divisible into smaller units in order to facilitate these trades.

Transportable
Scaling societies and their economies beyond the boundaries of a small region or settlement through trade required monetary goods to be transportable. A piece of land or a house might be a store of value, but they're not suitable as money because they can't be taken to another town to be traded for something else.

Fungible
Monetary goods had to be interchangeable. The more homogenous the quality of different units of a good was, the higher their suitability to be used as money.

Natural selection

Over the centuries, a process of natural selection took place that caused practically every nation on earth to eventually converge on gold as the most suitable monetary good. Gold's scarcity, corrosion resistance and other characteristics made it win the race of monetary evolution based on the above-mentioned criteria.

Although monarchs and nation states eventually monopolized money by issuing coins, the use of gold itself as money wasn't so much mandated by central authorities, as it had already acquired its monetary function before it was turned into sovereign coins.

Because gold is heavy, and its divisibility isn't endless, paper gold certificates came into use. These were first issued by goldsmiths and later by (central) banks. These banknotes represented and were redeemable for a certain quantity of gold, stored in the vaults of banks.

War financed with the hidden tax of inflation

At the beginning of World War I (1914), most countries were on a gold standard. Central banks held reserves in gold which formed the backing of the paper money that was used in day-to-day commerce. Shortly after the war broke out, most of the countries going to war abandoned the gold standard. Their war effort required more money than they had in reserves or could raise through direct taxation of their population.

Paper money allowed governments to print more than they actually had in gold, which was held in their central bank vaults. Printing money was of course much easier than taxing citizens. This inflation of the money supply not only financed the colossal cost of the war, but at the same time diluted the store of value of anyone not holding a significant portion of their wealth in hard assets that the governments couldn't print, such as gold or real estate.

On the one hand, the population sacrificed hundreds of thousands of their young men to fight a pointless war. On the other hand, those that weren't sent to the trenches were impoverished by the hidden mechanism that funded that same war.

The second world war dwarfed the first in almost every aspect. While first world war battles had taken place predominantly on concentrated battlefields, the second world war devastated large parts of Europe, North Africa and the Asian Pacific regions. Towards the end of the war, in 1944, the ministers of finance of the allied nations convened in Bretton Woods (New Hampshire, USA) for a two-week conference on the future of the global monetary and financial system.

They eventually agreed upon a system by which the US dollar became the global reserve currency. It was backed by the US Federal Reserve's gold reserves, which at that moment accounted for 70% of the global stockpile. The other nations held dollars in their national reserves that could at any time be exchanged for gold from the US Federal Reserve.

The currencies of the other nations were pegged to the value of the dollar within a 1% volatility range. This meant that with the US dollar as a proxy, all major currencies were indirectly pegged to gold as a scarce monetary asset. This to a large extent prevented uncontrolled money printing and the resulting monetary inflation.

This system was in place until 1971. Several countries, notably France, increasingly exchanged large quantities of their dollar reserves for physical gold. Combined with the enormous cost of the Vietnam War, this brought President Richard Nixon to suspension of the gold exchange window. It was announced as a "temporary" measure, but after 1971, dollar redeemability for gold never returned.

From sound money to fiat money

The significance of the decision to remove money's scarce anchor (gold) is difficult to overstate. Breaking the age-old link between money and a scarce asset that required human effort (energy) to produce, meant governments could print unlimited quantities of money to finance their deficits - money everyone else had to work for. As had been the case during and after WWI, this mechanism wasn't understood by the majority of the population.

Since 1971, money has no longer been a good that requires energy to produce, since governments can simply print the money with no scarce supply of gold backing it. From that point, all currencies were effectively turned into "fiat" currencies, meaning they are only used as money because of government decree.

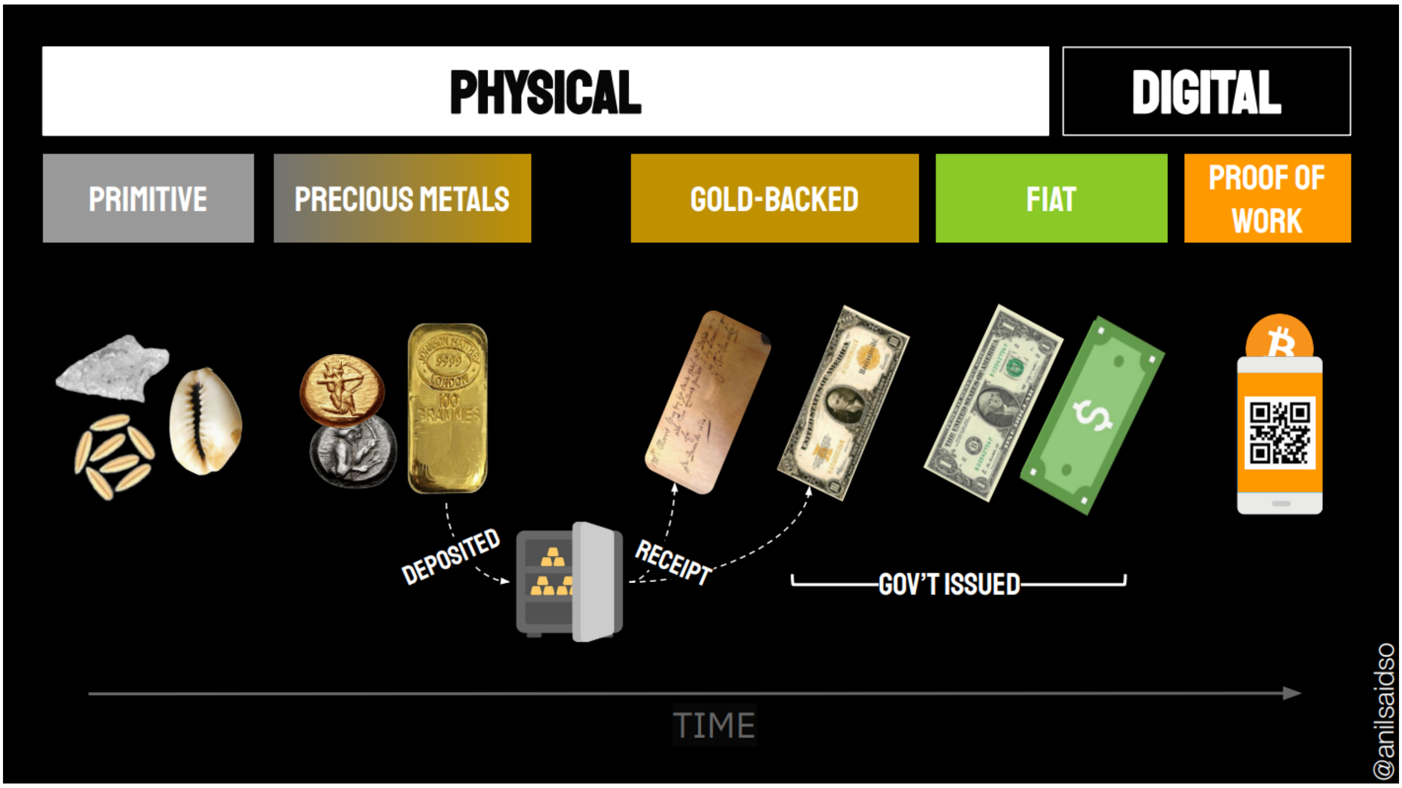
What people nowadays call money has lost all backing that it might have had in the past, whether that backing was based on hard assets, investments or labour. The yardstick of scarcity that has been the basis for human socio-economic interactions and progress for thousands of years, can now be changed arbitrarily by a single central authority.

Money is created when governments issue debt in the form of sovereign bonds. Central banks add these to their balance sheet in exchange for money they print. This money is brought into circulation by government spending and credit issuance by commercial banks. That's why, in effect, all fiat currencies are debt, and the only thing keeping them from collapsing is the collective confidence that these debts will be paid back in the future.

Unbridled money printing and credit expansion have caused a host of social and economic problems. They create asset bubbles in stock and real estate markets, which go through corrective crashes roughly every 7 years. The ones closest to the source of freshly printed money benefit immensely from these cycles. However, the lower echelons of society that don't own hard assets and live from pay cheque to pay cheque are hit the hardest by the inflation and the economic boom and bust cycles that the fiat system generates.

One of the most striking examples many will probably remember, is the Global Financial Crisis that started unfolding in 2008. The years leading up to this event were characterized by an enormous build-up of debt and risk in the commercial banking system.

When that erupted, the ensuing worldwide domino effect of financial institutions on the verge of collapse should have led to a purge that punished the organizations that had taken on excessive risk and debt. Instead, many of them received bailouts from governments. In response to the economic downturn, central banks lowered interest rates and printed unprecedented amounts of money in an effort to dampen the blow. As so often in history, once again, the average Joe paid for all of this through inflation and increased government debts. **It's no coincidence that this is exactly the moment Satoshi Nakamoto introduced bitcoin to the world.**



Why bitcoin was created

"The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve."
- Satoshi Nakamoto

Removing the need for trust

Because fiat money is debt based, the post-1971 fiat currency system requires trust at all levels. This means that the confidence that debts will be paid off in the future is a hard condition for the system to continue operating. But, it doesn't end there.

As fiat money lacks a scarce anchor, people need to trust commercial and central banks not to debase the currency by creating more of it without any backing. And because of the central role these organizations play in the system, we also need to trust they won't limit people's access to their funds and their freedom to use them for transactions.

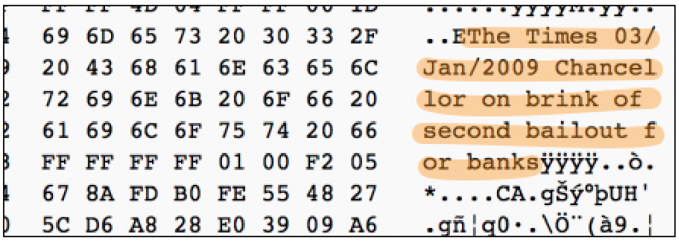
As we have seen, this trust has been breached countless times, with the 2008/09 Global Financial Crisis being one of the ugliest examples. Satoshi Nakamoto set out to create a digital form of money that didn't require trusting third parties for transacting and that couldn't be debased by a central authority issuing more currency units.

Nakamoto's motivation becomes perfectly clear when we look at the first block of the bitcoin blockchain, called the Genesis block (the next section will explain in more detail how bitcoin works). He created that block himself when he launched bitcoin in 2009. The first block contains a direct reference to banks receiving bailouts in the aftermath of the financial crisis: "*The Times 03/Jan/2009 Chancellor on the brink of second bailout for banks*".

Earlier attempts to create peer-to-peer (P2P) digital cash suffered from at least one of two shortcomings:

- They relied on a central authority that managed the ledger of who owns what.
- The currency units of the system could be copied.

The first problem meant the controlling entity became the de facto central bank that users need to trust. The second was the so called "double-spending problem". If digital money can be copied in the same fashion as e-books or music and video files, the tokens can be spent more than once. Satoshi Nakamoto combined existing technologies, particularly cryptography, to solve both of these seemingly unsolvable issues.




THE TIMES

£1.50

Eat Out from £5

More than 900 great restaurants, including four Gordon Ramsay favourites from £15

Israel prepares to send tanks and troops into Gaza

Michael Sheen
Frost, Nixon and me

Working mums
So that's how she does it

Detox in style
The best spas on the planet

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Salman Rushdie
I won't marry again

Bitcoin Reserve

bitcoinreserve.com

How bitcoin works

"Bitcoin is the first software network capable of storing all the monetary energy in the world with no loss of power over time and negligible transmission loss. Assuming broad adoption, that would make it the most valuable invention of the modern era. Few understand this."
- Michael Saylor, CEO & Founder of MicroStrategy

Solving the seemingly unsolvable

To solve the earlier mentioned issues of centralization and possible double spends, Satoshi invented a solution based on a decentralized network of nodes and published a white paper in which he laid out the concept. Nodes are computers that are in constant contact with each other. This by itself is nothing new. The internet itself has a similar infrastructure of interconnected nodes. All bitcoin nodes, however, store a copy of the blockchain, which is a log of the history of every bitcoin transaction.

Nodes can participate in a process called mining. This means they have to input random values in an algorithm (the one used for bitcoin mining is called SHA-256), in an attempt to get a specific output.

The miner who finds that required value first, has the right to create the next block. You could see each block as a page in the bitcoin bookkeeping or ledger. To this new block, the miner adds transactions that users have submitted since the creation of the previous block(s).

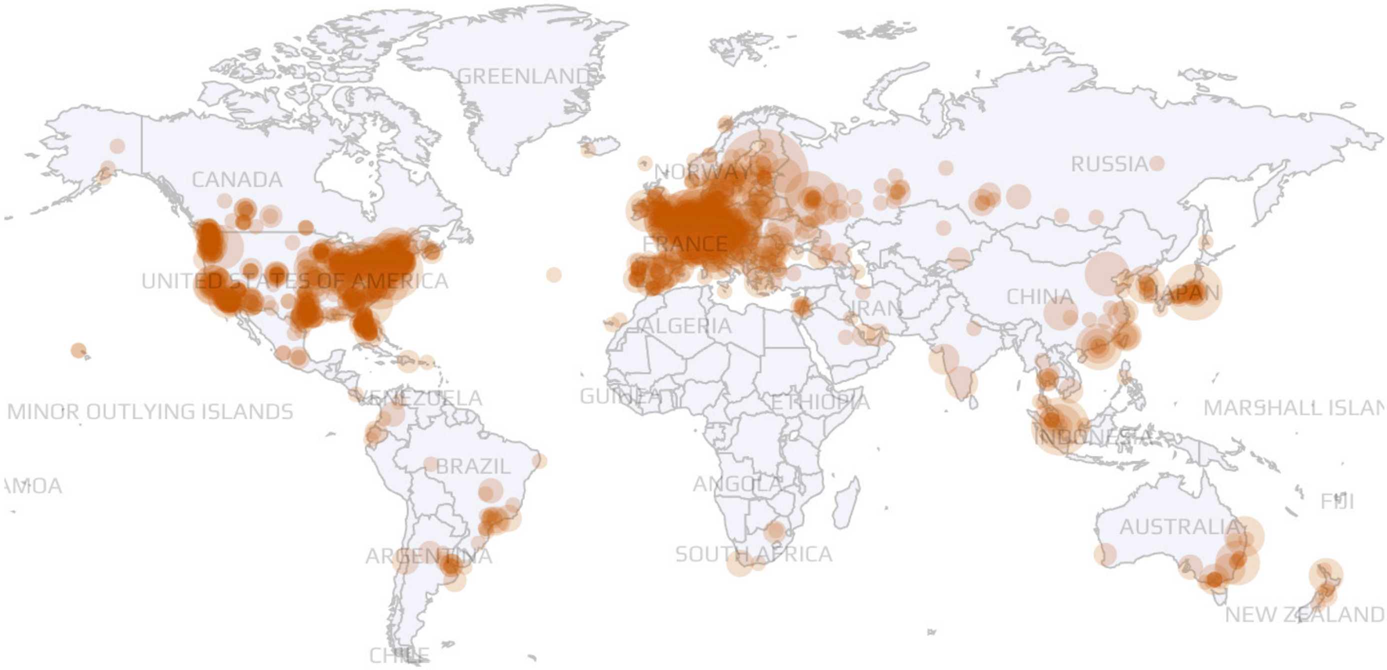
After creating the block, the miner broadcasts it to the rest of the network. Each block includes a cryptographic summary of the previous block called a hash. These hashes are what links each block to the previous one, creating a chronological chain of all transactions.

Independent, decentralized verification

As indicated above, each node stores its own copy of bitcoin's entire history. As soon as a new block is broadcasted to the network, all nodes use their own copy of the blockchain to check the cryptographic validity of the new block. If that is the case, it means three things:

- The block is linked to the previous block, which means users can verify the full history of the blockchain.
- The miner carried out the required amount of work to find the target value which gives him the right to create the block.
- The transactions that were added to the block are valid, meaning they were signed with a cryptographic signature that proves the persons sending the transactions are the owners of those funds.

For the work they carry out, miners receive a reward. This consists of new bitcoins that are created with each new block, and a small fee they receive from users for processing individual transactions. Miners selling newly mined coins to cover their operating costs is the only way new bitcoins appear on the market.



Visualization of the global spread of bitcoin nodes by bitnodes.io

Although this might be a difficult concept to grasp at first, this ingenious mechanism, also called "Nakamoto consensus" or "Proof of Work" achieves decentralization and at the same time prevents double spends. Two elements that, until the invention of bitcoin, were impossible to reconcile in one digital cash system. Every participant in the network can independently verify transactions without the need to trust a central authority, and cryptography prevents users from spending coins they don't own.

One of the most crucial elements of the bitcoin protocol, called the "difficulty adjustment", is an algorithm built into the protocol, which ensures that on average, blocks are found every 10 minutes. If more miners join the network, the average time required to find a new block will go down.

Adjustment of the difficulty of the work they carry out to match changes in the combined computing power of all miners, called the "hash rate", prevents the creation of more (or less) coins than the predetermined supply schedule.

Contrary to physical mining of precious metals such as gold, adding more miners to bitcoin doesn't lead to a higher supply and therefore a decrease in the price. It only adds more security to the network.

One final element that is important to understand, is the fact that the block reward gets cut in half every four years (technically, every 210,000 blocks). This reduction in the mining reward, called the "halving", is preprogrammed into the bitcoin software that everyone runs.

When bitcoin was just launched, miners received 50 newly created bitcoin for each block they found. So, while miners are currently rewarded with 6.25 bitcoin every 10 minutes, when the next reward "halving" takes place in 2024, this will drop to 3.125 BTC per block.

These 4-year halvings will keep taking place until the year 2140. This step function means that over time, bitcoin becomes more and more scarce and that only 21 million bitcoin will ever be mined.

Currently, around 90% of all bitcoins (19 million) have already been mined. Contrary to fiat currencies such as the US dollar or the Euro, it is deflationary in nature. This makes bitcoin more scarce than precious metals such as gold and silver.

In this day and age, having an understanding of the core concepts of why bitcoin was created and how it works is crucial for everyone. Without it, many people overlook its revolutionary nature and dismiss it as a speculative Ponzi scheme.

In the next section, we will give you an overview of the unique qualities bitcoin derives from the way it is designed and the way it functions.

What makes bitcoin unique?

Separation of money and state

The main takeaways from the previous sections are that bitcoin is decentralized digital money - with no central bank - that has a scarce supply of 21 million coins that can ever exist, which can be sent from peer-to-peer without the use of an intermediary.

Let's break all that down and start with a simple analogy:

Like any other product or service, if one single entity has total control over the market, as a result of the lack of competition, the consumer/user will have a low quality product which will not last through time. Imagine if there was only one company that made cars. The vehicles would be expensive and poorly made, and the lone car company would likely offer horrible customer service. Why? Without any competitor to take away the company's business, they would have no incentive to provide a better product to their customers..

So, how does this relate to bitcoin? For a large part of human history, central banks and governments have quite literally had a monopoly on money. Bitcoin changes this paradigm, and it is humanity's first real-world competitor to this monopoly.

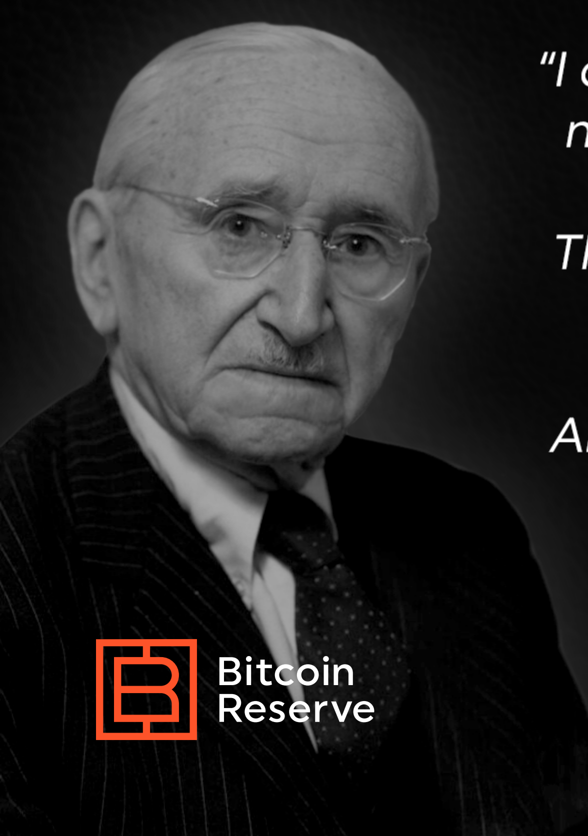
After the Middle Ages, the invention of the printing press led to the individual being able to search for truth without the need to trust the church. Although at the time, very few could envision it, this eventually led to the **separation of church and state**.

This drastically changed the way society functioned and caused unprecedented progress in almost every thinkable area. The achievements in art, music, architecture, literature and science from the era we now call the Renaissance have retained their value until this day.

Similarly, the invention of bitcoin brings about a **separation of money and state**. Although it might be hard to imagine right now, this paradigm shift will allow everyone to know what their share of the total global money supply is, without anyone being able to change the denominator of that share.

The printing press freed the individual from religious oppression. The internet revolutionized access to information and communication. Bitcoin will free people from financial slavery and will enable everyone to accumulate, store and transfer value, without the need to ask permission from or trust a government or financial institution.

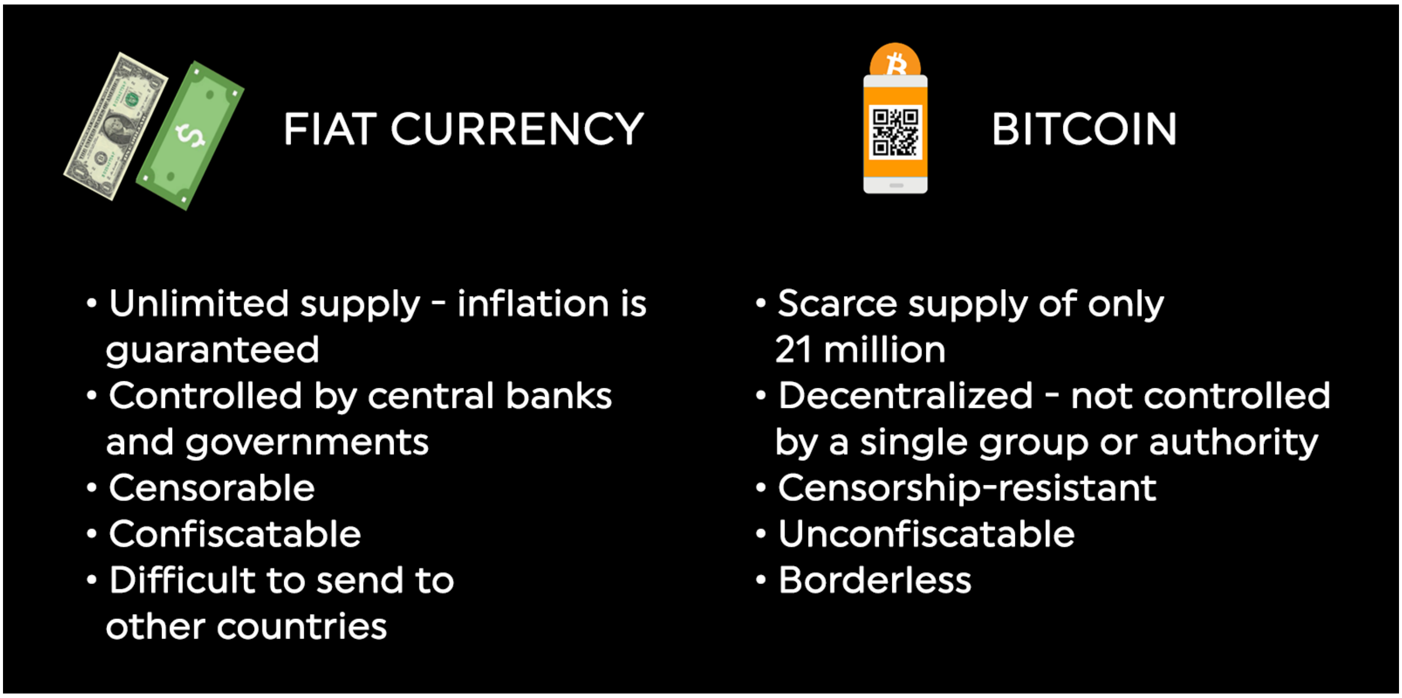
The 1974 Nobel Prize in Economic Sciences laureate Friedrich von Hayek understood this is a condition for human progress. Satoshi Nakamoto invented the tool that makes it possible.



"I don't believe we shall ever have a good money again before we take the thing out of the hands of government. That is, we can't take them violently out of the hands of government.

All we can do is by some sly roundabout way introduce something that they can't stop."

- Friedrich von Hayek



Money is a form of technology, which serves the purpose of storing and exchanging value. Human beings are constantly creating and improving technology, and with that, money will inevitably be improved over time as well, just as it has evolved throughout history. Let's have a closer look at the different properties that make bitcoin unique.

Bitcoin is scarce money

If a currency is easy to produce and bring into the market, it will almost certainly be produced in great quantity. Fiat currencies are extremely easy to produce, and in today's world, creating money is even easier than printing. It's simply a matter of adding digits in a database.

Governments have two options for generating revenue:

1. Taxation
2. Inflation

From the state's perspective, taxation is the more difficult option of the two because citizens will feel the direct financial burden of paying for government programs and therefore are more likely to oppose them. As a result, the state has more of an incentive to simply have money created through the central bank. This causes inflation, which harms citizens since their hard-earned money will now buy less than it did before.

Because of its infinite supply, fiat currency gives governments the unique ability to fund what they want in the present moment, while delaying the consequences (inflation) to the future.

Given that a high quality money is one that is scarce, gold has been the predominant form of money throughout history. This is because it is hard to produce (hence the commonly used term "hard money").

At first sight, it may be easy to feel that gold is safer than bitcoin because it has a baseline demand for industrial use, and therefore could never theoretically "go to zero". However, this notion completely ignores the true reason why gold became valuable in the first place.

Gold did not become valuable because of its industrial uses. If that were the case, then why not aluminum? Why not the other 94 metals on the periodic table? In reality, gold became "gold" because of its scarcity.

It is one of the most scarce, as well as one of the most recognizable metals in the world. Why is gold scarce? Again, because it is hard to produce, having an annual production rate of only about 1-2% per year.

Additionally, with any other commodity in demand, as the value of that commodity increases, the supply can then be increased, which ultimately causes the price to decrease.

As a result, the price of bitcoin is exponentially rising. Why? Because the supply is literally "programmed" to decrease, while its demand is increasing. As Satoshi stated, "*When someone tries to buy all the world's supply of a scarce asset, the more they buy the higher the price goes. At some point, it gets too expensive for them to buy any more.*"

Bitcoin as a superior store of value

Bitcoin solves the problem of "where do I store my value?", because unlike fiat currency, it is a form of money which provides an incentive to be saved. We live in a world that is on a fiat standard. Inflation is an issue which affects every single man and woman on Earth. It destroys your ability to save money and plan for the future. As a result, inflation forces us to do one of two things:

1. Do nothing, stay in fiat currency and lose purchasing power.
2. Invest and hope the returns are higher than the rate of inflation.

Bitcoin fixes this problem by giving everyone the ability to store value in a sound form of money, instead of real estate, equities, bonds, etc.

To give a perspective on just how scarce bitcoin is, if you take the total supply (21 million) and divide that by the world population (8.2 billion), this equates to only 0.002 BTC per person. It's so scarce that not even every millionaire on Earth will be able to own 1 whole bitcoin. This may seem problematic in the future, but we'll touch upon bitcoin's divisibility later on.

Never before has humanity had a form of money, or any other asset in general, which is verifiably finite. In essence, bitcoin can be described as the most advanced form of savings technology that mankind has ever possessed.

Bitcoin is decentralized money

"*I've developed a new open source P2P e-cash system called bitcoin. It's completely decentralized, with no central server or trusted parties, because everything is based on crypto proof instead of trust.*"
— Satoshi Nakamoto

Central banks can realistically be described as small groups of people who attempt to find the "perfect formula" to set the money supply and interest rates for millions of people. This is a system which is doomed to fail from the start, and history is our proof.

Central banks have their own representatives who publicly speak about their respective fiat currencies. They appear on TV, magazines, meetings with government officials and more. Bitcoin is drastically different. Bitcoin is software. It has no CEO, no official organization, and no designated representatives.

As you read earlier in the "How Bitcoin Works" section, bitcoin is controlled by its users all around the world. Developers improve the software, however, they can't force the protocol itself to be changed since all users can choose what version of the software they run. In order for everyone to stay compatible with each other, everyone needs to use software that complies with the same rules - there must be consensus. Therefore, all users and developers have an incentive to protect this consensus.

"*The nature of bitcoin is such that once version 0.1 was released, the core design was set in stone for the rest of its lifetime.*"
— Satoshi Nakamoto

So, instead of a centralized entity deciding on what the monetary policy will be, bitcoin's monetary policy has already been decided. It was set in stone once it was released in 2009. Central banks can change their monetary policy every quarter, while bitcoin's monetary policy is set to remain unchanged for the next millennia.

Tens of thousands of computers all spread across the globe, "enforce" the rules of the monetary policy. As mentioned earlier, these computers are known as "nodes". Effectively, the purpose of running a node is to:

- Verify transactions.
- Audit bitcoin's total supply.
- Keep a record of transactions that have taken place on the bitcoin blockchain.
- Ensure that no coins are double-spent and no bitcoin is counterfeited.

In order to kill bitcoin, you would have to go to each and every single node on Earth and destroy them. Estimates show that there are anywhere from 15,000 to 100,000 nodes which currently exist.

Imagine there were tens of thousands of computers all over the world constantly auditing the Federal Reserve or the ECB. This is the level of improvement that bitcoin brings to the standard of money.

In September 2021, China banned bitcoin mining. Until then, a large part of bitcoin mining operations were located there. The ban caused a temporary drop in the hash rate (computing power) of the network.

After the subsequent difficulty adjustment, mining became more profitable for miners in other countries. This meant that within months, the bitcoin hashrate had climbed back to previous levels. Bitcoin's network never skipped a single block.

All this goes to show that both the network nodes and mining operations are sufficiently decentralized to withstand a physical attack by a single nation state or even a group of nations.

Bitcoin is censorship-resistant money

"*Governments are good at cutting off the heads of centrally controlled networks like Napster, but pure P2P networks like Gnutella and Tor seem to be holding their own.*"
— Satoshi Nakamoto

Bitcoin is a peer-to-peer network: It cannot be controlled or stopped by any person, organization, or government. Why? Because as you read earlier, there is no central point of failure which can be taken down.

Bitcoin restores financial sovereignty to the user in the sense that the user can hold their own funds, as well as send them directly to a recipient without the use of a middleman, such as a bank or payment provider.

You need permission to use your bank. Every time you make a payment, you are indirectly asking your bank to give you permission to spend your own money. By eliminating the need for banks and payment providers, this means that a bitcoin holder's funds cannot be censored in any way by an outside party.

It has often been said that not having your bank account shut off or censored is a first world privilege, and there is indeed truth to that statement. Looking in the past, there are many examples which show the importance of having a form of money which can't be censored.

You don't need permission to use bitcoin. It gives people who live under tyrannical regimes the ability to receive aid, it allows people to not have to worry about banks freezing their funds, and most notably grants financial inclusion for the approximate 1.7 billion people who do not have access to bank accounts.

Bitcoin cannot be confiscated

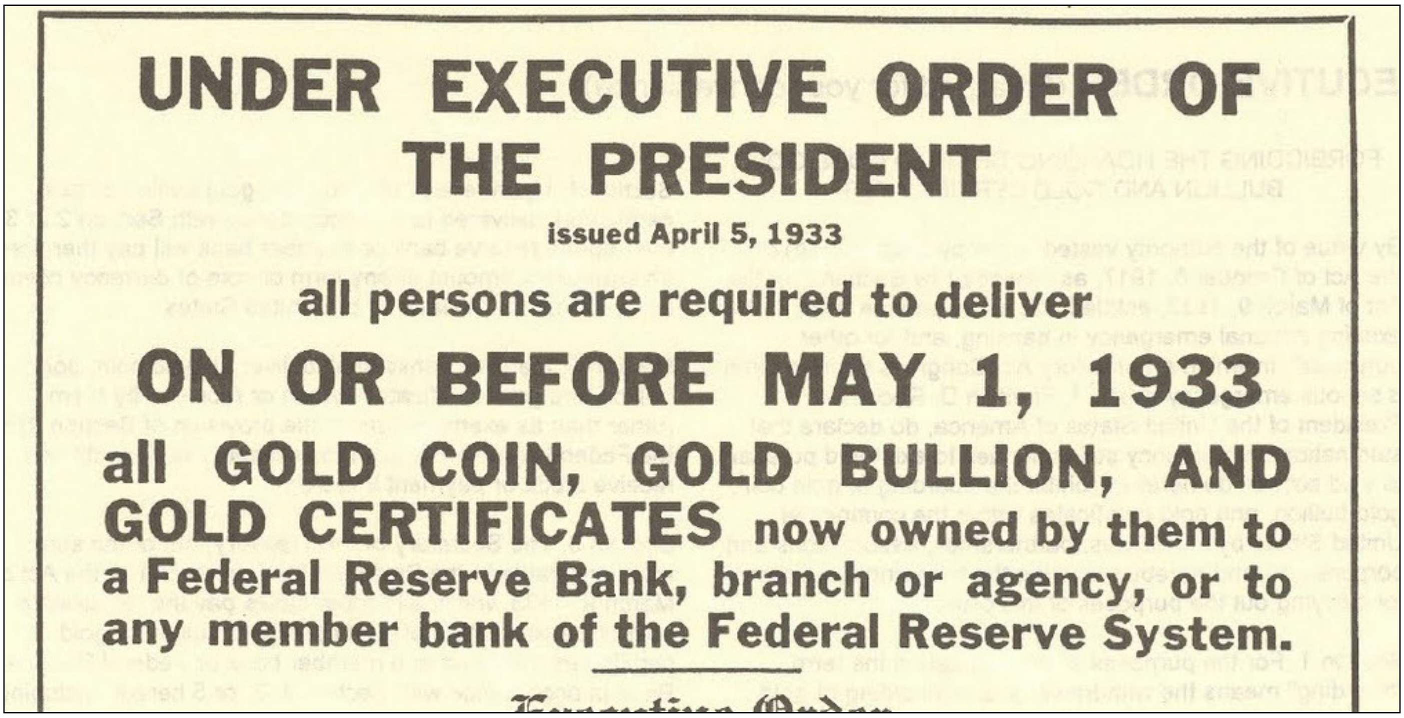
Not only does bitcoin provide the strongest form of money that humanity has ever had, it also provides the strongest form of private property rights that we have today.

Some have had concerns over the fact that bitcoin isn't physical, and therefore it doesn't seem "real". However, the fact that bitcoin is not physical in nature is actually a major benefit, instead of a curse. Take real estate for example, your property can be claimed by the state in order to have a new construction project done in the area.

Another physical form of wealth, gold, which by many is still seen as hedge against inflation, can still be confiscated. This has happened many times in history, most notably in 1933 in the US, under Executive Order 6102.

As with gold and real estate, any physical property can be confiscated using violence or the threat of violence. With bitcoin, no government, thief or hacker can take your wealth as long as they don't have your private keys - they are what you need in order to spend your bitcoin. Your private keys are typically a 12 or 24 word phrase that is written down or even memorized. This is essentially the "password" for your bitcoin.

The security of your bitcoin ultimately depends on you. You are responsible for how safe your bitcoin is, nobody else. The "How do I store my bitcoin" section will explain more about how you can keep your funds secure.



UNDER EXECUTIVE ORDER OF THE PRESIDENT

issued April 5, 1933

all persons are required to deliver

ON OR BEFORE MAY 1, 1933

all GOLD COIN, GOLD BULLION, AND GOLD CERTIFICATES now owned by them to a Federal Reserve Bank, branch or agency, or to any member bank of the Federal Reserve System.

Bitcoin is borderless money

Money has been extremely difficult to transfer across different countries. Wealth in general is difficult to transport. Traditional forms of wealth that were mentioned earlier, such as fine art, gold, real estate, equities, fine wine, are all very inconvenient to move, and real estate is of course not even possible to move.

Sending larger quantities of gold would require armored trucks, security guards, and a lot of money in order to make the transfer happen. Sending fiat currency across different countries often requires extortionate fees, long delays, and inconvenient paperwork. In contrast, you could send billions of dollars worth of bitcoin to anyone, anywhere on earth, for a fraction of the fee that you'd pay when doing a bank transfer. Bitcoin is the most portable form of money that has ever existed.

Let's take it a step further: imagine that you needed to flee to a different country in order to keep you and your family safe. What can you take with you? You can't take any real estate, or any major form of physical wealth for that matter, because of difficulty to transport. You won't be able to transfer money out of your bank account because of capital controls. Until bitcoin was created, refugees would practically lose everything they had when fleeing to a safer place. Thanks to bitcoin, refugees can still hang onto their wealth no matter where they are going. There is a very compelling humanitarian case for bitcoin adoption.

Bitcoin is extremely divisible money

As you know by now, bitcoin has a hard cap of 21 million coins that will ever exist. However, it is extremely divisible - you can own just a fraction of a bitcoin. In fact, bitcoin is divisible up to eight decimal points - the smallest unit being 0.00000001 - these smallest units of bitcoin are known as "satoshis".

1 satoshi = 0.00000001 BTC ("BTC" is an acronym for "bitcoin"). Second layer solutions that are built on top of the bitcoin protocol, such as the Lightning Network, even make using fractions of satoshis (milisatoshis or msat) possible.

SATOSHI	BITCOIN
1	0.00000001
10	0.00000010
100	0.00000100
1,000	0.00001000
10,000	0.00010000
100,000	0.00100000
1,000,000	0.01000000
10,000,000	0.10000000
100,000,000	1.00000000

Common misconceptions

"If you don't believe it or don't get it, I don't have the time to try to convince you, sorry."
- Satoshi Nakamoto

Often misunderstood

As you have probably found out by now, there is a lot more to bitcoin than meets the eye. Learning about bitcoin is something that requires personal effort. Good resources are abundantly available, but you're in charge of the learning process. This publication is meant to give anyone who takes a sincere interest in the subject a solid foundation.

Having read this far, you have a more detailed understanding of what bitcoin entails than 99% of people out there. Unfortunately, among them are a lot of politicians, journalists and other public figures with large audiences. Many of them love criticizing bitcoin by throwing around sound bites without having done profound research themselves.

It shouldn't come as a surprise that some of the dominant power structures in the world stand to lose a lot of control and revenue as bitcoin continues to give power back to the individual. This is an additional incentive for a lot of influential people to push negative narratives on bitcoin. These usually boil down to a few categories which we will discuss point by point in this section.

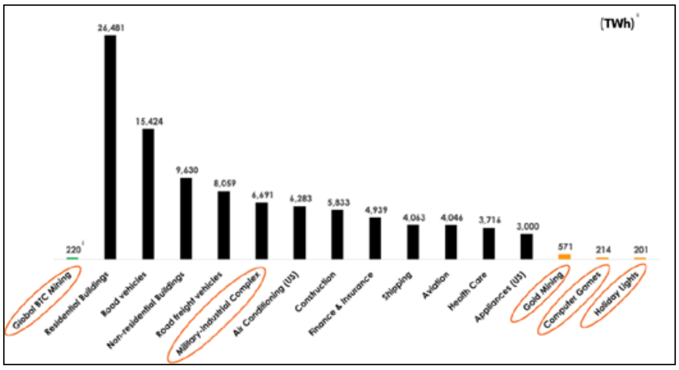
"Bitcoin is bad for the environment"

With headlines like "Bitcoin mining is disastrous for the environment – it is time for governments to intervene", and "Bitcoin consumes more electricity than Argentina", this narrative has reached the minds of many. However, the reality is that this is antithetical to the true impact that bitcoin mining has on the Earth. How?

The first thing to note is that bitcoin mining actually doesn't consume nearly as much energy as most would think. Let's compare bitcoin's energy use with other industries.

Computer games and holiday lights use about the same amount of energy per year that bitcoin uses, but you don't see any outraged news headlines about that. Additionally, the gold industry (which some believe bitcoin is currently demonetizing) uses 160% more energy, and the military-industrial complex uses almost 3,000% more than bitcoin.

The amount of energy that the world produces every year is 154,750 TWh. Out of that, bitcoin uses as much as 220 TWh, which equates to only 0.14% of total global energy production, a negligible amount.

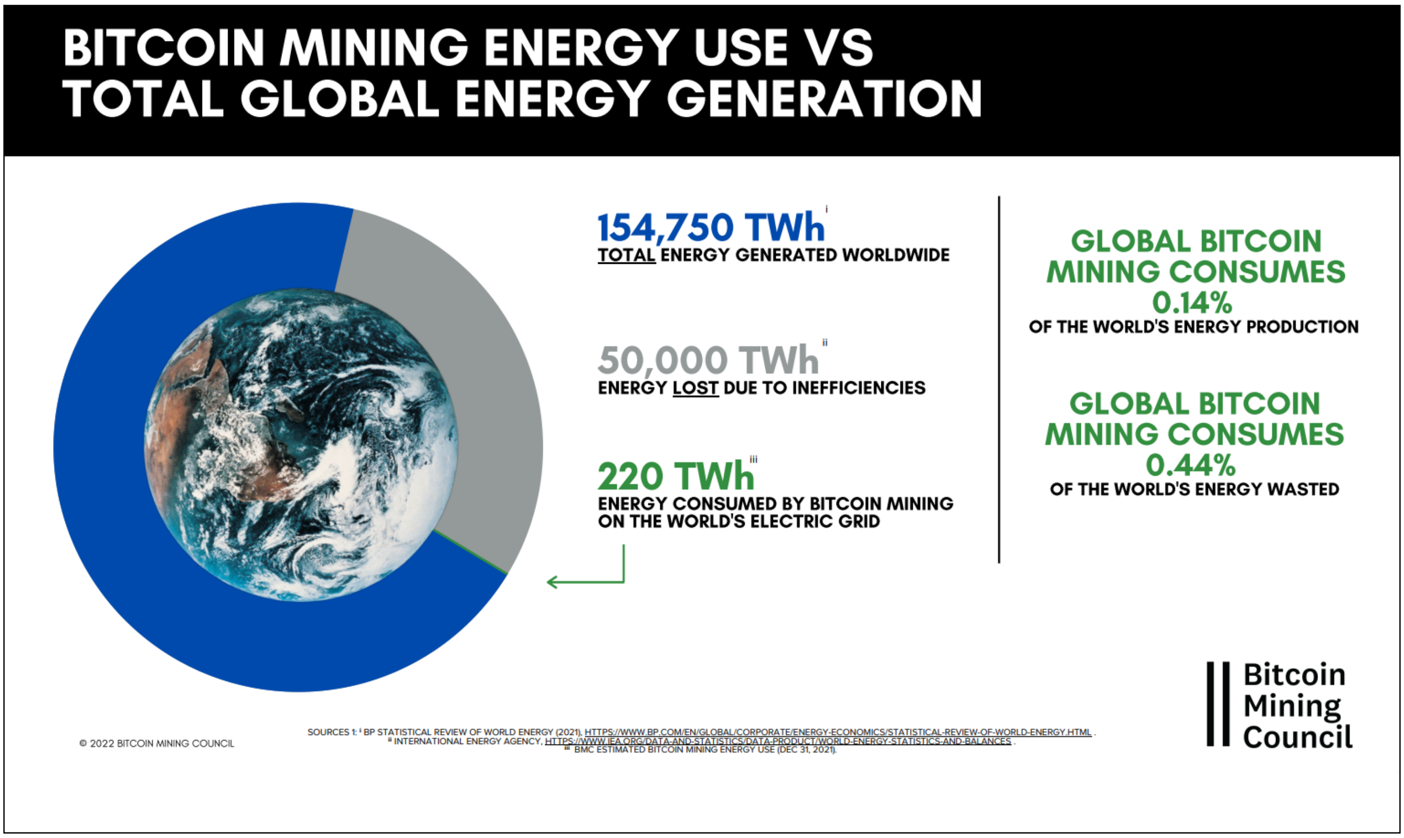


Source: Bitcoin Mining Council

An important thing to also keep in mind is the fact that bitcoin consumes 0.44% of the world's wasted energy. Under this metric, the amount of wasted energy is 227x larger than the amount that bitcoin uses today. So, how does this relate? Because bitcoin miners are largely using energy that would've otherwise been wasted, such as from stranded oil & gas wells, hydroelectric power, and solar power.

For example, let's take oil & gas wells. The majority of oil production sites produce associated gasses as a by-product of the production process. For safety and economic reasons, these gasses are usually burned off by flaring.

This flaring can contribute to up to 90% of an oil site's emissions, and bitcoin mining offers a solution to this. Companies like Great American Mining, Upstream Data, and Giga Energy are able to take the wasted methane from flaring and use the energy for mining bitcoin. Not only does this reduce methane leakage into the atmosphere by approximately 99%, it also provides a financial incentive for oil & gas companies to do so in the first place, since they have a new source of generating revenue.



Globally, the total figure for flaring is 150 billion cubic meters of methane, which results in 1536 TWh wasted. This is enough energy to power bitcoin about 7x over what it's currently using.

The logical path forward is for bitcoin to continue using increasing amounts of energy, and that's a positive factor, not a negative one. Bitcoin will continue to use more energy that would have otherwise been wasted or what some fear would have been desctructive to the environment..

Aside from bitcoin helping the oil & gas industry to prevent emissions, it is largely beneficial for the renewable energy industry as well. Conservatively speaking, 58% of global bitcoin mining uses renewable energy.

This is a higher sustainable energy mix than any country has today. Bitcoin mining acts as a "buyer of last resort" for the energy that solar and hydroelectric power plants produce - this helps to stabilize the grid and assist the growth of the renewable energy industry.

Although bitcoin is often criticized for its large use of energy, the data shows us that it is of utmost importance to understand where the energy itself is coming from. Bitcoin's impact on the environment, as well as the energy industry, is a positive one, despite what central banks and uninformed media outlets claim.

The last point to keep in mind is that bitcoin's energy use is by no means a waste. Many other products and services we have today use large amounts of energy, yet we don't question these because we need them in order to have a good standard of living. Providing sound money for 8.2 billion people, helping them escape the dangers of inflation and financial censorship, is incontrovertibly a worthwhile cause.

"Bitcoin is too volatile for a currency"

You may be wondering how bitcoin can be used as a currency if its price is constantly fluctuating, and understandably so. One of the most important concepts to keep in mind is that there's no way bitcoin can go from being created in 2009 to becoming the world reserve currency without having any volatility along the way.

The logical path for bitcoin's adoption is:

1. **Store of value:** People see the value in bitcoin's monetary properties, and they want to hold it in order to possess a scarce asset that can't be inflated like fiat currency.
2. **Medium of exchange:** As more people continue to buy bitcoin, its liquidity increases - more people will be willing to accept it. Bitcoin becomes easier to spend as more of the population sees value in it.
3. **Unit of account:** Now that bitcoin has become a store of value, and then a medium of exchange, goods and services will eventually be priced in bitcoin. Once this happens, prices will be much more stable than they are today, because bitcoin's monetary policy is stable and predictable, unlike the monetary policy of central banks.

The word "volatility" can have a negative connotation. However, volatility can go both ways. Gold is a lot less volatile. But, over the last 10 years, gold has not been a viable store of value and hedge against inflation. The cummulative US Consumer Price Index (CPI) for January 2012 - January 2022 is around 20%. Appreciation of the gold price over that same period was 15% while experiencing a -35% bear market that lasted roughly until 2018.

Over that same period of time, the bitcoin price expressed in US dollars appreciated by one million percent. One good way to filter out the noise caused by bitcoin's price swings is to focus on its yearly lows, as shown above. Bitcoin's logarithmic chart also shows a long term upward trend.

Volatility is only frightening if you're thinking of selling it in the short term. Bitcoin is not something you would want to use for planning to buy property in a few months, or for any other kind of purchase that you would need to make in the near term.

Currently, bitcoin is primarily a savings technology that allows us to store value for the long term and opt out of the central banking system.

Every 4 years the supply of newly mined bitcoin gets cut in half. It's logical to expect bitcoin's volatility will stabilize as it becomes more scarce, while at the same time, it becomes more widespread with more of the world's population holding it.

Central bankers often criticize bitcoin for its volatility. However, this logic is only thinking in terms of days, weeks, and months. Again, bitcoin is savings technology, and that means holding onto it for years, decades, and generations.

"Bitcoin can be replaced by another cryptocurrency"

"Shouldn't I diversify?" or "Shouldn't I own more than one?" are questions that may have crossed your mind. You may be wondering if bitcoin can simply be replaced by another cryptocurrency. Let's examine this.

Bitcoin has the most dominant network effect

One concept which is crucial to understand is that naturally, people will want to transact in one currency that everyone agrees has value, and will therefore exchange real world items for it in return.

One of the most respected thought leaders in Austrian economics, Ludwig von Mises, describes this concept brilliantly in his book, The Theory of Money & Credit when he said, "*Thus there would be an inevitable tendency for the less marketable of the series of good used as a media of exchange to be one by one rejected until at last only a single commodity remained, which was universally employed as a medium of exchange; in a word, money.*"

Human beings naturally don't want to transact in thousands of different currencies because it's inefficient and confusing to do so. Does it make sense for Bob to pay Alice in X-coin, then for Alice to convert X-coin to Y-coin in order to pay Steve, then in order for Steve to pay Patrick, he needs to convert his Y-coin into Z-coin? Obviously not. Therefore, diversifying in investments may be a good idea, but when it comes to an actual form of money, the case is much different as a result of the network effect.

Bitcoin has the strongest network effect and significantly outcompetes any altcoin. Network effects are paramount when it comes to technology. A great example of this would be the backbone of the internet, which is called "TCP/IP" (Transmission Control Protocol / Internet Protocol). According to computerhistory.org, similar to bitcoin vs. altcoins, there was competition among what would be the prevailing protocol everything else would be built on top of for the internet:

"*Protocol Wars:*

Everyone agreed on the goal: develop a global computer network. They didn't agree on how. By the early 1980s, several different protocols competed.

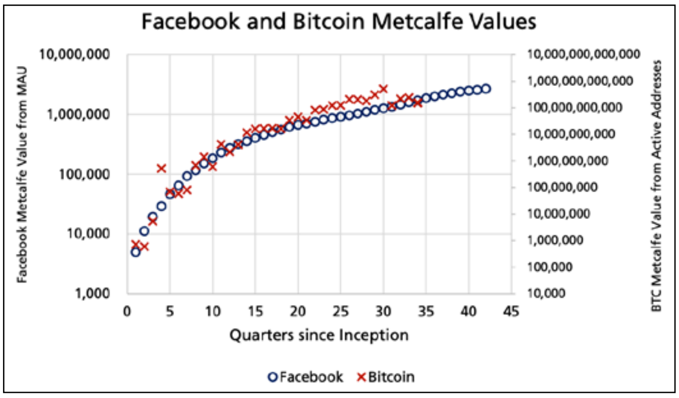
OSI (Open Systems Interconnect), backed by European telephone monopolies and most governments, was favored. Other strong competitors included two corporate networks, IBM's SNA and DEC's DECNET. The dark horse contender was the Internet (TCP/IP), defined only by a self-governing community dependent on volunteers.

The Internet community was nimble—able to develop in months what took the OSI committee-based process years—but it scared off some potential adopters because nobody seemed 'in charge.'"

Isn't that interesting? A "self-governing community dependent on volunteers", and "nobody seemed in charge"... sounds a lot like bitcoin, doesn't it? Aside from that, even the inventor of Gmail, Paul Buchheit stated that, "*bitcoin may be the TCP/IP of money*".

Metcalfe's law essentially states that the more users a network has, the more valuable the network is. The law itself was observed by Robert Metcalfe, who was the co-inventor of Ethernet. With this in mind, Timothy Peterson (CFA, CAIA) wrote a report titled, "Bitcoin Spreads Like a Virus" in which he uses Facebook's adoption in comparison:

"*Facebook is ideally suited for comparison to Bitcoin. The lengths of each data series are nearly the same (about ten years). Both were fairly innovative, though not entirely original (Digicash preceded Bitcoin, MySpace preceded Facebook.) Both faced bans in China, a large potential marketplace. Both received widespread publicity about their adoption.*"



Relating to altcoins, Michael Saylor, CEO of MicroStrategy also commented on the idea of bitcoin being overtaken by a competitor: "*There's never been an example of a $100 billion dollar monster digital network that was vanquished once it got to that dominant position*"

When you look at the institutional and political adoption of bitcoin, you see that the network effect is undeniable. Corporations such as MicroStrategy, Tesla, Block, MassMutual, and Stone Ridge Holdings Group own bitcoin.

Billionaires such as Paul Tudor Jones, Bill Miller, and Ricardo Salinas Pliego own bitcoin. Many politicians all around the world have embraced bitcoin, from Mexican senators to US congressmen. Even an entire country has adopted it; El Salvador being the first nation in the world to make bitcoin legal tender.

Bitcoin is the most secure

As pointed out earlier, bitcoin is extremely decentralized - having anywhere from 15,000 to 100,000 different nodes distributed all over the world. No other cryptocurrency is even close to having this kind of security. Additionally, no other cryptocurrency has the amount of hash rate that bitcoin possesses.

Hash rate is defined as "the measuring unit of the processing power of the bitcoin network". Having a strong hash rate is crucial to bitcoin's security because this ensures that it cannot be 51% attacked - this is essentially when over 50% of the mining power is controlled by one single entity, which would then have the ability to double spend and block transactions.

Some real world examples of blockcahins that experienced 51% attacks include Bitcoin Cash, Ethereum Classic, Vertcoin, and Bitcoin Gold. So, how does bitcoin's hash rate compare with other cryptocurrencies? The chart below indicates that the difference is not even close, to the point where you can barely even see the hash rate of the other cryptocurrencies which aim to compete against bitcoin.

"Bitcoin is mainly used for criminal activity"

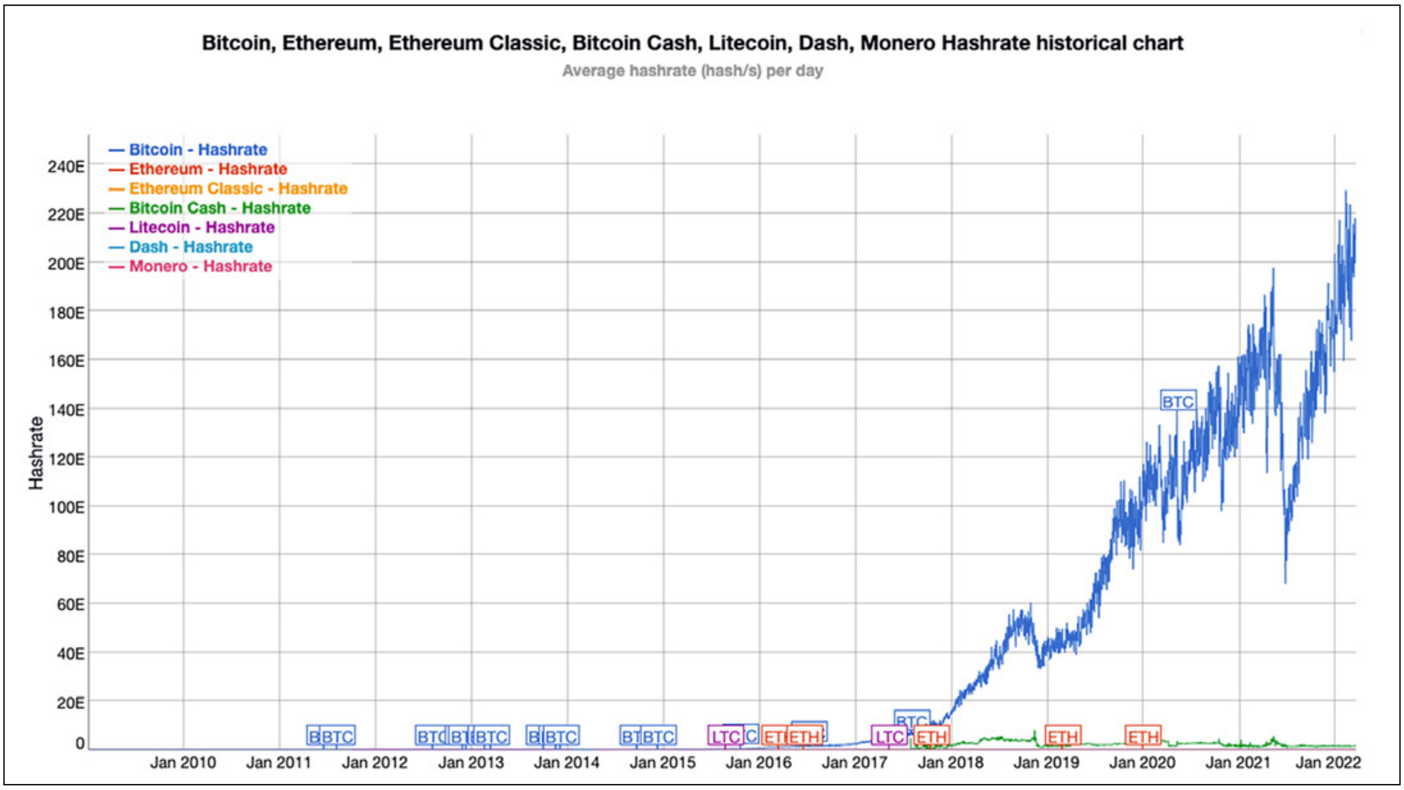
In terms of criminal activity, the true culprit here is actually the traditional banking system. So, comparing bitcoin and banks, we can look at a report published by Chainalysis, a blockchain analytics company which is specialized in forensic blockchain research. The company has government contracts with the FBI, DEA, ICE, SEC, CFTC, FinCEN, IRS, the US Air Force and even the United Nations Office on Drugs & Crime.

According to Chainalysis, the overwhelming majority of cryptocurrency is actually not used for criminal activity. In a report the company released, they indicate that in 2019, criminal activity represented only 2.1% of all cryptocurrency transaction volume. In 2020, the criminal share of all cryptocurrency activity decreased to only 0.34%.

Furthermore, according to a 2020 report published by SWIFT, "*cases of laundering through cryptocurrencies remain relatively small compared to the volumes of cash laundered through traditional methods*".

For example, between 2006 and 2010, HSBC was found to have laundered at least $881 million on behalf of Mexican cartels. Another example is The Danske Bank money laundering scandal in 2017-2018, when it became known that around €200 billion of suspicious transactions were conducted with Russian mafia money between 2007 and 2015. Bank fines since 2008 are up to approximately $321 billion.

The moral of the story here is, yes, central bankers will shout from the rooftops about how bitcoin is "used for criminal activity" - but the data clearly suggests otherwise.



"The government can ban bitcoin"

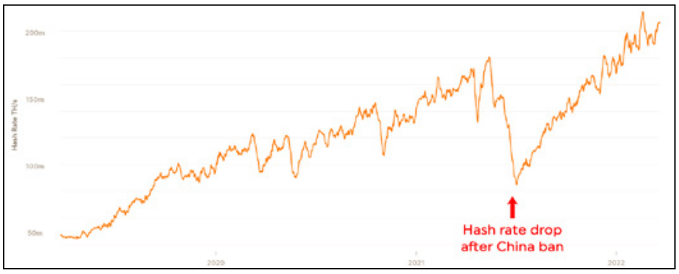
So, governments have the ability to create money out of thin air through the central banking system...why wouldn't they just ban bitcoin since it can take away this kind of power?

A government can certainly attempt to ban bitcoin, but as you read earlier, they are not able to confiscate bitcoin, nor do they have the ability to censor it. If a government were to ban bitcoin, since it is a peer-to-peer network, this of course wouldn't stop it from existing. It would only result in that country's citizens being economically subdued, while other more free jurisdictions benefit from embracing this industry.

A profound example of this is the earlier mentioned bitcoin mining ban that China imposed in 2021. Almost two-thirds of the world's bitcoin mining infrastructure was located in China before the ban, and now there is basically none.

One of the most powerful governments on Earth banned bitcoin, and what happened? Shortly after the ban took place, bitcoin's hash rate decreased by about 60%, yet the network continued to operate without any interruptions whatsoever.

Most Chinese bitcoin miners simply shipped their equipment to jurisdictions which were more welcoming to the industry. A lot of Chinese mining infrastructure eventually ended up in the United States, especially in the state of Texas.



Two things happened:

1. China severely limited its future economic growth by banning bitcoin.

2. The US gained economic power by welcoming bitcoin.

The Federal Reserve may not like bitcoin, but that doesn't mean local politicians feel the same way. Politicians are people too, and if the right incentives are in place, then they will make decisions accordingly. When politicians embrace bitcoin, they see an increase in tourism, economic growth, and tax revenue.

Since El Salvador made bitcoin legal tender, it has experienced a 30% increase in tourism, 13% more exports compared to the year before, and double digit GDP growth for the first time in the country's history.

A final point to consider is, if the concern is about "the government" banning bitcoin, which government are you referring to? All governments are different and, in many ways, they compete against each other. Some embrace innovation, while others prevent it. Bitcoin financially rewards the jurisdictions where it is welcomed.

Bitcoin's incentive structure and the game theory behind it don't just play out when we're talking about miners, individual investors or corporations. It also holds true for competition among nation states.

If one government bans bitcoin, this only provides more of an incentive for others to embrace it, creating a positive feedback loop for even more jurisdictions to adopt it.

As the saying goes: "No one wants to be the first and no one wants to be the last". The fact that the first countries have already made bitcoin legal tender should tell you enough.

So, what's next?

We've given you a short overview of why bitcoin was created, how it works, what makes it unique, and what some common misconceptions are. The level of knowledge you have gained by reading up to this point, in itself, is enough for many to realize they want to learn more. Bitcoin is here to stay, so congratulations on taking the first steps to discover what it is and why it's important!

Is all of this relevant for you?

For many, quickly rising inflation figures used to be something that happened to people in other countries. However, they have now become a reality almost everywhere. Politicians and the media first said it would be transitory, blaming Covid-19. The latest culprit they are pointing at is the war in Ukraine, and we can be pretty certain there will be a next crisis that'll get blamed for rising inflation.

What they fail to mention, however, is that 80% of all US dollars in existence were created out of thin air in just the last 2 years. The same goes for most of the other fiat currencies. Trillions of dollars and euros have been pumped into the economy as "stimulus". It's pretty straightforward arithmetic to figure out that you can't dilute the money supply like that without creating inflation.

Inflation isn't the only thing. Recent events in Canada, Russia and Ukraine show that the fiat money you have in your bank account can get frozen in a matter of days. If even nation states' foreign currency reserves can get frozen, having access to unstoppable, unconfiscatable, censorship resistant money is no longer a luxury for anyone.

From here, it's up to you to decide whether you want to learn more and whether you want to buy bitcoin. If you decide to do so, there are two important questions left: **How do I safely store bitcoin, and where to buy it?**

The importance of self-custody

Owning bitcoin means having the private keys that enable you to send it to another address. There are essentially three different ways:

Centralized exchanges

After what you've read, this name alone should make you suspicious. There's a huge variety of cryptocurrency exchanges where you can buy bitcoin. This usually involves installing an app on your phone, creating an account, getting your account verified and sending money to it that you then exchange for bitcoin. If you leave your bitcoin on the exchange, it means they hold the private keys to your coins.

By choosing this option, which admittedly is the easiest thing to do, you only retain exposure to bitcoin's price action, forfeiting all other unique qualities of bitcoin discussed earlier. You replace the need to trust a bank with the need to trust the exchange.

Disadvantages of using a centralized exchange:

- The exchange can freeze or close your account.
- Similar to banks, the exchange can hold less than 100% of account holders' bitcoin in reserves (fractional reserve banking).
- The exchange can go bankrupt.
- The exchange can get hacked. This has happened many times in the past. Bitcoin itself cannot be hacked though.
- The founders or employees of the exchange can disappear, taking the funds. This has also happened in the past.
- Your bank can blacklist the exchange, making it impossible to get your funds out.
- Most exchanges are trading platforms, meaning their user interface can be very complex for new users.

This is why there's a well known saying among bitcoiners: "Not your keys, not your coins".

Hot wallets

A hot wallet is a smartphone app or a program that you install on your desktop computer which allows you to store, send and receive bitcoin. Contrary to a centralized exchange, using such a wallet allows you to take control of your bitcoin by managing the private keys for you.

When you install and set up the wallet, you will be asked to write down 12 or 24 words and store them in a safe location. This is called the "seed phrase". This is what gives access to your funds. Even if you lose your phone or computer, you can use this seed phrase to install a wallet app on another device and restore access to your bitcoin.

The most important disadvantage of this method is that your phone or computer are connected to the internet. That's why this is called a "hot wallet". Although it is unlikely, hackers could potentially install malicious software without you knowing it, which specifically looks for the seed phrase. If they get their hands on it, they can send your funds to another address and there will be nothing you can do to reverse that.

Using a hot wallet is excellent for getting familiar with how bitcoin works, but only with small sums of money.

Our recommendation for a hot wallet is Blockstream Green * (can be used in combination with Jade hardware wallet, see next section).

Cold storage

The best way to prevent the risk of a malicious actor such as a hacker getting their hands on your seed phrase is to use a so-called "hardware wallet". This is a small device that contains a secure chip where your private keys are stored. This device itself isn't connected to the internet.

When you send bitcoin, you approve the transaction on that device. It uses the private keys stored on the secure chip to sign the transaction and sends it back to the app on your phone or computer. From there, the signed transaction gets sent to the bitcoin network.

When setting up or restoring a hardware wallet, you only enter the 12 or 24 word seed phrase on the hardware device, not on your computer or phone. This method has the best balance between security and ease of use.

The only other thing to consider is how you store the seed phrase itself, because you can also lose or damage a hardware wallet. Writing the seed phrase down on paper and putting it in a fireproof safe is an option, but many bitcoiners choose to engrave or stamp the words on a piece of stainless steel. With a melting point above 1500° C., such a back-up will even survive a house fire.

Our recommendation for a hardware wallet is Blockstream Jade *

Why open an account with Bitcoin Reserve?

We help serious beginners and investors take part in the bitcoin revolution. Our goal is to make the bitcoin buying experience as easy as possible for you.

You can buy any amount of bitcoin with Bitcoin Reserve - starting from €10, all the way up to large purchases for high-net-worth individuals, companies and family offices.

For clients looking to purchase €10,000 or more per quarter, Bitcoin Reserve offers a unique experience:

- **1-on-1 personal guidance with real people on the phone**
- **24/7 service through private, end-to-end encrypted chat groups with our team**
- **Fast onboarding**
- **Low fees**
- **No slippage, regardless of order size**
- **Minimal data gathering**
- **Unparalleled support throughout the process**

Bitcoin Reserve is non-custodial, which means we never hold your coins. Instead, we enable you to receive them directly in your wallet. This is the only way to guarantee you actually own your bitcoin and enjoy its unconfiscatable and censorship-resistant qualities.

Click the button below to learn why our white glove service is what you've been looking for:

LEARN MORE

* Although the recommended app and hardware wallet, as well as the company behind them, have a good reputation, and we use these products ourselves, we cannot assume any liability for vulnerabilities that could get discovered and exploited in the future.