THE ORANGE PILL BOOK

Arman The Parman

Why Bitcoin, Though?

Translations: Slovenian Espanol Arabic Norwegian French German Portuguese Italian Dutch

Audio by @DelioPera

0:00 / 15:06

The injustice explained

Bitcoin is not about getting rich, although the earliest in, will – It's about a *monetary revolution*. A revolution of the people (of the entire world) who are enslaved to the oppressors, the central banks, and the people that own these banks. Bitcoin will help EVERYONE, except central bankers.

It is a very powerful thing, being in control of the money. Forcing people to use it (legal tender laws), and even creating more of it at will (quantitative easing, money printing, fractional reserve lending), without cost, and spending it on

anything, including war. It is a form of theft from the people who are forced to use that money.

If you don't believe me or don't understand, consider a game of Monopoly. Imagine you and your friends are playing, and then a new player enters the game. The new player opens a fresh packet of Monopoly Money from a different set and brings it into the game. If he starts losing, imagine he opens another packet of money and brings it into the game, so he can't ever lose. This gives the new player an unfair advantage, hurts all the other players, and makes all the property more expensive – because there is more money floating around in the game which is competing to buy scarce resources.

This is quite similar to what is happening in real life. Money is being created out of nothing, prices are going up, and people who work for money and have savings are losing the purchasing power of those savings (a form of time-theft). Another blow is that wages tend to not keep up with price inflation, and people get poorer. Scarce assets go up in value, but people storing wealth in those lose a large portion to CGT (capital gains tax). They are being stolen from – a silent tax through inflation, loss of income through insufficient wage growth, and loss of assets through capital gains tax.

People were upset after the 2008 financial crisis, but didn't actually know the root cause of the problem: fiat money

Knowingly or unknowingly, economics professors (paid by governments) will hand-wave, and overcomplicate the description of what is happening, which makes it harder to understand. But if you step back from the details, look at the overall picture, this is what is happening, and it can be deduced from first principles.

This monetary system, designed to steal your time, should **outrage** you. The solution is Bitcoin, and I'll explain.

The solution

For many years, freedom-loving people have tried to resist this. They realised that using the money of their choice was the way to escape the oppression and theft. So they tried to create their own money. But doing so is punishable by the law. You must use the "master's" money.

Using gold was thought to be a solution (which was illegal from 1933). Gold is effective at resisting time-theft because it is difficult to create more gold, so being relatively scarce, storing wealth in gold gives some advantages. However, it is not a great medium of exchange across distances. It is difficult to transport and store safely, which led to it becoming centralised – stored in banks, and paper/digital promises of this gold were created for ease of spending and storage.

Thus, fiat money was created. It became law to use it. Physical-gold ownership by citizens (not banks) became outlawed (**order 6102, in 1933**). Eventually, the backing of fiat money by gold was abolished (1971, by president Nixon). Many versions of fiat came into existence as each country made it law to use their particular currency (legal tender).

"I have directed Secretary Connally to suspend, temporarily, the convertibility of the dollar into gold or other reserve assets, except in amounts and conditions determined to be in the interest of monetary stability and in the best interests of the United States." – Nixon, 1971

In a free market, one where a money is not forced on the people, they will tend to choose the money that most other people are using. This is the safest strategy for protecting wealth. You would accept as payment something that you are likely to be able to spend. ie the most saleable good. Over time, this leads to ONE money being the most dominant, as society moves away from barter. We only have multiple monies today because we are not free to choose/create our money.

Sometimes, groups of people choose a poor form of money; one that is easy to create (easy money). These people lose their wealth as more and more of their chosen money is brought into existence, and their portion of the overall pie held gets smaller and smaller. Other groups of people who choose hard money (hard, meaning hard to produce), protect their wealth from dilution, and by natural selection, only the wealth of people with the hardest money remains. This is why hard money always wins against easy money.

The cypherpunks

For decades, the **cypherpunks** were trying to fight back for our freedoms. It began with the internet, and then privacy on the internet with pgp (the first form of public/private key cryptography, which later led rise to gpg, an open-source version now freely available). This was close to being banned by the US Government, enemies of privacy, but they lost in court. Cypherpunks also attempted to create digital money in the 90s – but it needed to be centralised, necessary to oversee and prevent double-spending. This centralisation made it easy for the overlords to come in, find who was in charge, and put a stop to it – No threatening our current lucrative monetary system, thank you very much.

The cypherpunks persisted, and in secret, created Bitcoin (I suspect Satoshi Nakamoto was a group of the same cypherpunks, choosing to remain anonymous due to lessons previously learned). A magical invention, that not only created something digital and simultaneously scarce but also decentralised to the point that it can not be shut down.

There is an excellent **four-part documentary on the cypherpunks** which I highly recommend.

Perfect money?

Bitcoin has all the essential features of a perfect money, orders of magnitude better than any physical money like gold, or “competing” cryptocurrencies:

— Absolutely scarce

— Digital

— Easily transferable

— Fungible (not quite on the base layer, but good enough presently)

— Divisible

— Portable

— Recognisable and easily verifiable

— Difficult to counterfeit

— Easy to store (not requiring a 3rd party)

— Difficult to seize

— Decentralised (no leader, so no target for governments)

— Difficult to shut down the payment network

— Difficult to manipulate the total supply

— Anti-fragile (gets stronger if attacked)

— Always available

— Censorship-resistant (regarding transactions)

— Permissionless (Anyone can access without ID)

— Open-source (no secrets and anyone can contribute to improving it)

These are mostly properties of the money itself, but Bitcoin is also the payment network as well; a combination of payment processing technology AND money. If you think of the dollar, it has a payment network of VISA, Paypal, Swift, Venmo etc. But Bitcoin has its own network, the Bitcoin Network. To learn more, read the **section on Bitcoin Nodes here**.

The network of people

For a free-market money to be the dominant money, it not only has to have the best properties and be sufficiently hard to produce, it must also have a network

of people that use it. Money is technology, but it is also people – similar to the components of a language-of-meaning (money is a language-of-value by the way). English, for example, is made up of symbols, signs and rules (the "technology"), but English also lives because there is a group of people that speak it. You can't expect a language to become dominant just by making the language better, more beautiful, or easier to learn.

Then why do I think Bitcoin will overtake all other money on the planet? Because Bitcoin isn't just better than the most dominant money, it is VASTLY better – being vastly better is the only way to overtake a dominant network effect. It is also the ONLY choice available to people who want a money that can not be shut down by governments, or have their savings diluted away by some central group of people or person in charge of the monetary policy (eg The Federal Reserve with USD, or Vitalik Buterin with Ethereum).

Vitalik Buterin – created Ethereum, and awarded 70% of the supply to himself. He and a close circle, direct the monetary policy and any changes to the system, much like the controllers of the USD, The Federal Reserve.

The network is an absolute must, but it is not reasonable to expect a large network of people to use a brand new form of money (or language) instantly, even if it is vastly superior to the current dominant money. That network, to

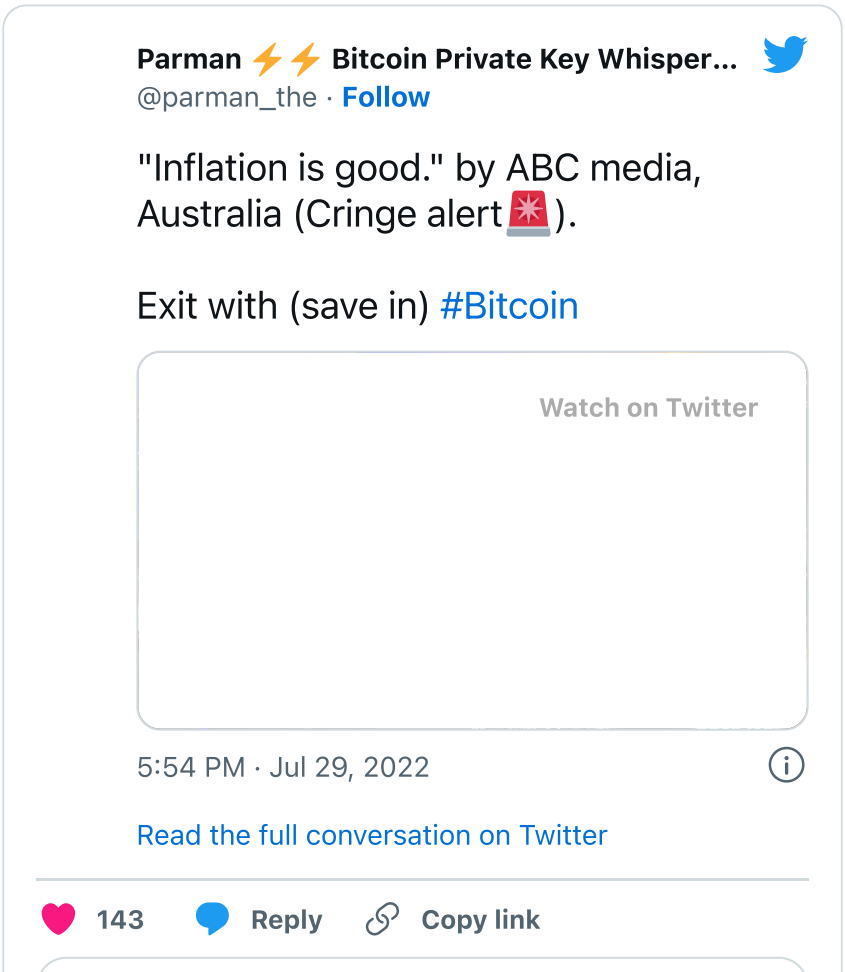
instantly adopt a new money, needs to be forced by law; it's not possible if left to the free will of people. So no matter how good Bitcoin is, even if it exceeded your wildest expectations of perfect money, in a free world, it will not be understood and adopted by everyone all at once, and therefore necessarily will be volatile in price, or attacked by the media (mouthpiece of the central banks and governments who are threatened).

Bitcoin is close enough to perfect. All that needs to happen is for people to accept it. Many people do, and once they realise how important it is, they don't forget. They teach others. And the network of people, the crucial missing component of a new perfect money, gets stronger every day.

Some people find it difficult to understand why Bitcoin Only will win and why it is inevitable. For them, I direct to **one of my earlier pieces explaining it all**.

Extra:

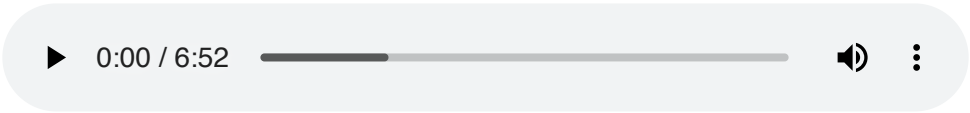
The government pays for the media. Therefore the media tells you what the government wants you to believe. Here they are telling you that inflation (stealing your purchasing power) is a good thing!



Why Bitcoin Only

German 🇩🇪 **Norwegian** 🇳🇴

Audio by **@DelioPera**



This is a reply to a comment in YouTube I wrote in a fit of insomnia at 3 am. It was surprisingly coherent and expressed *my thoughts on why altcoins should not be accumulated, and you should buy bitcoin only. I posted it to Twitter, **and reproduced it here with spelling corrections**:*

I appreciate your detail in replying. I want to start by stressing that it all comes down to scarcity. Without scarcity, cryptocurrency may as well be fiat. Good money is scarce. The biggest weakness of cryptocurrencies is that they can be created easily from nothing. All alts are like this. But Bitcoin is different. It has miraculously been born and has gained a huge lead in network effects. This can not be copied. Thus, it has gained scarcity. It is extremely decentralised, and has by far the greatest hashing power on the planet, and distribution of full nodes, which makes it not possible to tamper with the monetary policy. Bitcoin has scarcity due to network effect lead and “un-tamper-ability”.

The **Lindy effect** will only make it stronger as day after day it doesn’t die. It can’t be eradicated, just like a cancer that has spread too far.

The copies cannot compete with this. It needs the majority to not only leave Bitcoin, but mostly leave to the same choice. There are thousands of choices, so those few people that abandon Bitcoin will not all go to the same choice. In other words, defectors will disperse, not concentrate. The only way this could theoretically happen is if there is some fatal flaw with Bitcoin, AND it can’t be fixed, AND an altcoin can, AND only one altcoin can.

E.g. let’s say Bitcoin’s privacy weakness (really it’s a trade-off, not a weakness and any other coin with privacy just chooses a different trade-off) is suddenly critical and everyone is exiting. Where will they go? Monero, Zcash, DASH, some to ETH and XRP (not private btw), Cardano… Can they all be money? Money printer go brrrr much?

So how else can an Altcoin take over? Remember that people will save in the best money. An Altcoin must become fundamentally better. In the open-source world, how is that possible? It's like thinking it's possible for a better operating system to exist than the dominant open-source one today (GNU Linux). The open-source leader just gets better and better. All new ideas get absorbed.

Let's imagine another currency finds a good use case. Let's say smart contracts. First, that's like saying paper is money and valuable because contracts can be written on it. No, you need to make good money first, not find other uses for it. Aluminium has more uses than gold but it's less valuable because it is not money. It can't be money because it is not scarce. But even if smart contracts makes a cryptocurrency into good money, there are too many: ETH, Cardano, TRON, Iota, and probably others.

As soon as any becomes valuable, it will invite competition and it will be copied. There is no scarcity. For goodness sake, ETH doesn't even work yet. Its Turing completeness is not even used. Bitcoin has smart contract capability and I understand nearly everything ETH is doing program-wise can be done with Bitcoin. Let's face it, it is competing with Bitcoin as a money and is far far behind and has no credibility. What will Vitalik Buterin do with the monetary policy next?

ETH is just another fiat with a central banker. That is not a true cryptocurrency. Remember why Bitcoin was born – we are fighting central banking and trying to separate money and state, not shoot ourselves in the foot by losing focus, trying to get rich by improving on the solution we already miraculously discovered. Bitcoin is that: a miracle – and we should embrace it.

Also, you mention ROI. Bitcoin doesn't exist so you can buy it and sell it for more fiat later. It is a REPLACEMENT for fiat. You buy and NEVER sell. You spend once it achieves its true value. You don't need an exit strategy. You just save in Bitcoin. With alts, you need to time your exit and sell to a greater fool, because alts are scams, holding forever will get you rekt. Just DCA Bitcoin.

It's like picking up gold off the ground before anyone else realises it will become money. Don't pick up pebbles or seashells (alts), your pockets have limited space. Finally, the most important problem to solve is separating money and state. All other problems are tiny in comparison. We don't need to replace the legal system with smart contracts. We don't need a token for everything. We don't need to put bananas on a blockchain.

Bitcoin is an invention that solves a humanitarian problem. Altcoins take a solution (blockchain) and try to find a problem. Remember that.

A Not Too Technical Overview of This Bitcoin Thing

An overview of the Bitcoin protocol for beginners

Espanol Française Italiano Português Romanian Swedish German Armenian Catalan Chinese Taiwan Croatian Bosnian Slovenian Turkish Russian Arabic Norwegian Indonesian Greek Dutch

This article is copied from the original source at Bitcoin Reserve Journal.

Audio by @DelioPera

0:00 / 38:47

Introduction

When I was first exposed to Bitcoin, to me it was just a number on a screen that I could trade. Buy low, sell high, make money. But it is so much more than that.

I was treating a miraculous gift to humanity, seemingly with contempt. It deserves much more respect.

During the bear market of 2018, when the excitement of profits vanished, and after the hurt of them being wiped away sunk in, I decided to hold, or "HODL" as the **meme** goes. I knew I would have to be patient. I had time on my hands. So I decided to learn more about what Bitcoin was. Lucky I did! I was astonished. Since then, I have been continuously learning more, and as I learned, everything was making sense, and my conviction increased. So did my investment.

I asked myself, "Was I blindly going down a path without question?" Due diligence required that I searched very hard for weaknesses in Bitcoin. After 18 months of searching, almost daily, I have not found a satisfactory objection to not aggressively accumulate.

I will first explain what Bitcoin is and how it works. In other articles, I will go through the objections and risks that I, and others, have posed. And I will present the answers I have found to them all, and insights.

Understanding Bitcoin Is Hard, and Then It's Not

It's not easy to understand Bitcoin at first. I think it's better to explain to a newcomer WHAT Bitcoin is, not HOW. What it can do, the problems it solves, and why it's important. We shouldn't dive into HOW it works too early. There isn't a need for this. It doesn't add to the understanding and appreciation of why Bitcoin is an incredible gift to humanity.

Bitcoin is not easy to explain. There is no one paragraph that can convey all its crucial properties. Every brief explanation is misleading in *some* way.

That's partly because nothing like Bitcoin has ever existed before, so there is nothing for people to compare it to. Comparisons are automatically made to help understand concepts, but they are inaccurate and lead to wrong conclusions. It challenges many preconceived ideas about money (that are wrong) and are taken for granted. It challenges world views, and that's uncomfortable for people.

Another reason why it's difficult to explain is because it has many different and complicated parts, each with different functions – and only by understanding each part can the whole be understood. These complicated parts are easier to grasp if one has a basic understanding of various fields such as Computer

Science, Cryptography, Austrian Economics, History of Money, Social Networks, Game Theory, Human Psychology, and Evolution/Natural Selection.

A Scarce Number

Bitcoin is just a digital number. But a scarce number. How can that be? A scarce number makes no sense at first. There are 21 million of "them". Each can be broken up into tiny pieces, down to 8 decimal places. You can own an amount as little as 0.00000001 bitcoin. They are not actually "coins" as such, they are just special numbers.

Bits of it can be moved from one place to another, but these pieces ***can't exist in two places at once***. They can't be copied. That is very special.

If I have 0.5 bitcoin and send it to someone else, I no longer have that fraction of bitcoin. This is different to an email, such that if I send it, I can keep a copy. Perhaps it might help (at first) to think of a quantity of bitcoin like a uniquely identifiable email containing a number, that can only exist in one place at a time.

No digital item has ever had this property. Also note, without this property, digital money without a central coordinator is not possible.

The Blockchain

Let's increase the complexity a little. Bitcoin is not just the *number*, but also the digital "*book*", or *ledger*, where it is recorded down. The numbers (the units) are lowercase 'b', the book is uppercase 'B'. The ledger also records down what *address* the bitcoin are associated with. For now, think of these addresses like bank account numbers that "hold" bitcoin.

The Bitcoin Blockchain, or the "book", or the "ledger", contains every address's (accounts') balance, and every movement of bitcoin (the transactions) since the

beginning of Bitcoin's creation. Pause and absorb that for a moment – *Every transaction for every account, ever*. A completely transparent monetary system. Not a transparent *bank account*, but a transparent *monetary system*.

Note: addresses have no personal identification associated with them on the ledger, but ownership can be inferred from surveillance. Because of this, privacy is not the default, but can be achieved with good practices. If Bitcoin was completely private, then auditing the monetary system's integrity as a whole would not be possible.

The Blockchain is like a Bank's ledger, but it is more. It is a ledger of the entire monetary system

Every 10 minutes on average, a new "*page*" of transactions is added to the ledger, called a "*block*". Think of a physical ledger, where transactions are limited to one page every 10 minutes. There is a limit to how frequently the pages will be turned to add new transactions, and the book is continuously growing.

Because data is added in blocks, and each block is connected to the previous block (explained later), the ledger is called a "blockchain" – a chain of ever growing blocks.

Every portion of bitcoin can be traced to its original creation by examining the history of every transaction it was involved in. Everything is accounted for. Everything adds up perfectly. An accountant's dream.

The purpose of the Blockchain is not just to put new data in the right chronological order – it is to make the blocks digitally connected, so that any change to previous blocks invalidates future blocks. This makes the history of the monetary system **tamper evident**. Discussed later, mining makes the system **tamper-proof**.

Creating Bitcoins

Bitcoin started on January 3, 2009, by a person or group of people, pseudonymously called Satoshi Nakamoto. No one knows who "he" is and "he" has disappeared shortly after creating Bitcoin.

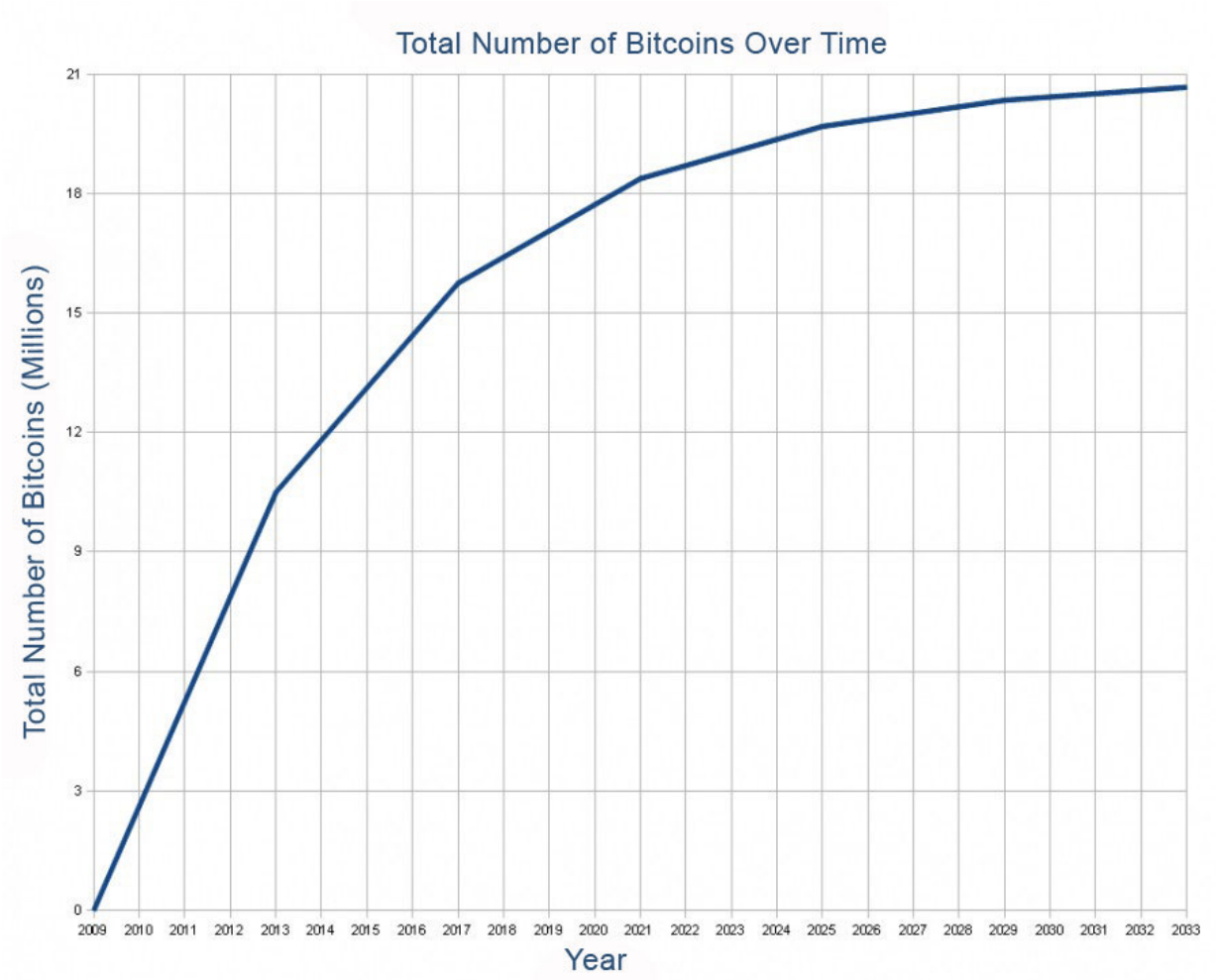
On the first page of the ledger, the first block, when Bitcoin first started, only 50 bitcoins were created. What does that mean? It means the first entry in the first block contained a transaction of 50 bitcoins – Just as you might open a new book and write down, "I have $50 dollars."

Don't be bothered too much now on the fact that they are created seemingly from nothing – this initial natural objection will be alleviated later.

For every new page added to the "book" of Bitcoin, 50 more "coins" were added. On each of the "pages", in addition to newly created coins, there also exists any movement of bitcoin from one person to another – called "transactions".

Every 210,000 pages, or "blocks", the rate of bitcoin creation halves so that on block 210,001, 25 bitcoin were being created instead of 50. Then on block 420,001, 12.5 bitcoin were being created instead of 25. Then on block 630,001, on May 12 2020, 6.25 bitcoin were being created instead of 12.5. These events are called the Bitcoin "Halvings" (or "Halvenings" – there's an ongoing debate about that terminology).

In approximately the year 2140, as fewer and fewer bitcoin are created per block, there will come a day when the smallest unit possible (0.00000001 bitcoin, called 1 Satoshi) will be created per block, and can no longer be halved. That will result in a limit of 21,000,000 bitcoin created, and no more will ever be created. Currently, there are about 18.5 million bitcoin in existence.



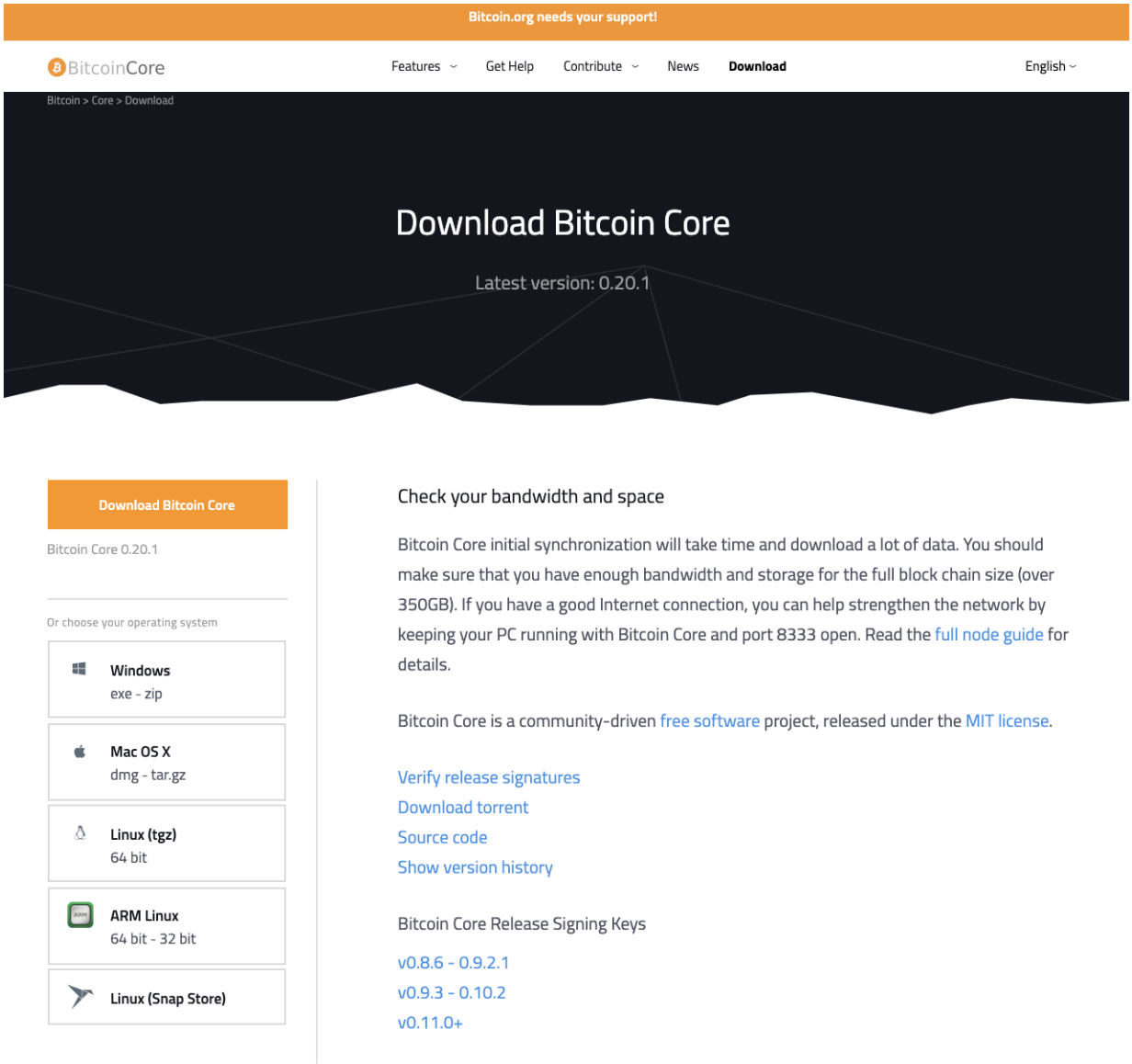
Nodes: The Blockchain Is Copied, but the Bitcoin Are Not

Importantly, although the units of bitcoin cannot be copied within the ledger, the ledger itself, Bitcoin with a capital "B", *can* be copied, and *is* copied, all the time, and that is crucial to it being resistant to attack or shutdown.

Copies of the ledger sit on thousands of computers all over the world, and they are all connected in a network and synchronised with each other. These computers are called "nodes".

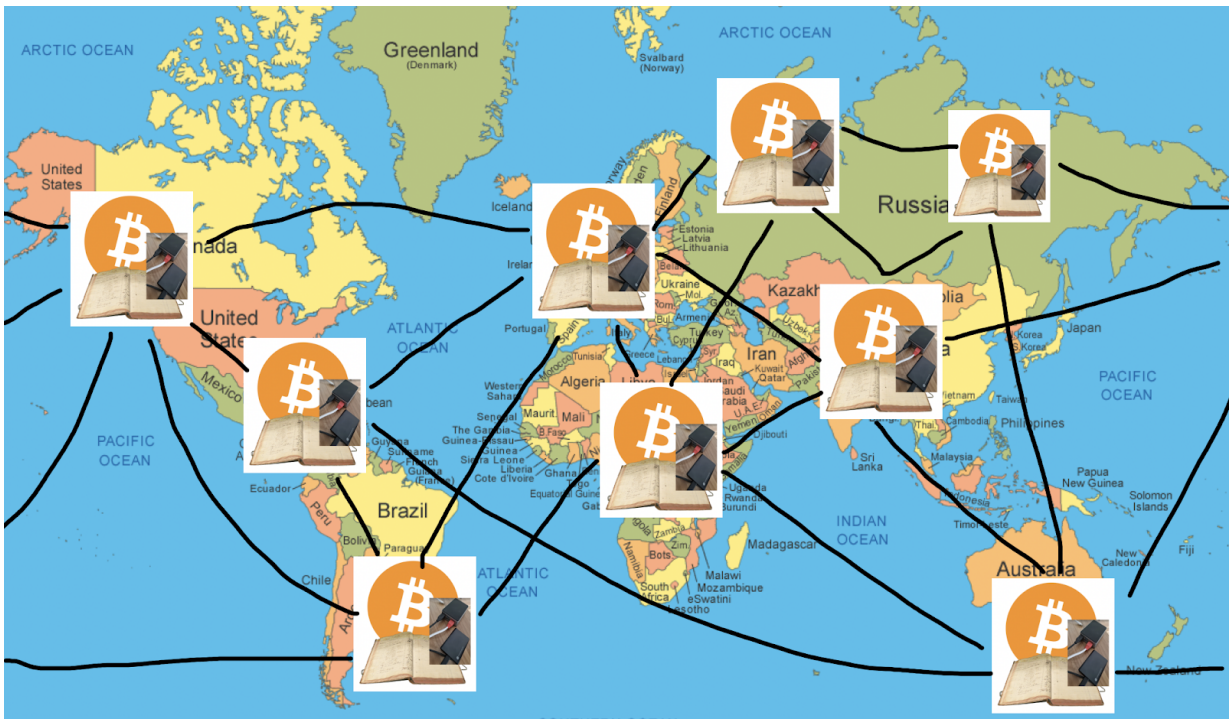
This is my personal Bitcoin Node, similar to thousands of others around the world. It is a Raspberry Pi (very cheap low powered computer), connected to an external hard drive. The device is connected to the internet via my home network.

Anyone can participate in this network of “nodes”. It is just a matter of downloading the software, called Bitcoin Core, from bitcoin.org, and connecting it to other computers via the internet that also run Bitcoin Core (the communication happens automatically).



The download page at bitcoin.org

The new downloaded program then communicates with other computers running the same software, to copy the Bitcoin Blockchain. It maintains these connections to participate as part of the network.



Once a new node is in synchrony with the others, it waits (like all the other nodes) for new blocks to be created (by miners). These get propagated through the network and all the computers update themselves. A node can switch itself off for whatever reason, and return to join the network at any time. It just has to catch up by adding the new blocks it has missed.

The blockchain's past can not be changed. It is a permanent record of all transactions, and it is distributed all over the world. It can not be eradicated. To shut down Bitcoin, every single one of these nodes needs to be found and destroyed. Because this is virtually impossible, Bitcoin is virtually impossible to stop.

Quick Review

To summarise briefly so far, the Bitcoin Blockchain contains a chain of connected blocks, each with newly created bitcoin (from "nothing"), and any movement of bitcoin ownership (transactions). New blocks are added every 10 minutes on average, and thousands of computers keep an identical up-to-date copy of the entire chain.

Storing Bitcoin: Private Keys

It is interesting to know that you can never actually "own" some bitcoin, as per the general understanding of the word "own". The bitcoin quantities are just numbers on the many identical Blockchain copies (that everyone can see), associated with a string (letters and numbers) called a Bitcoin "address".

What you have is the key. A key is like a secret "password" – it is actually a **randomly generated**, extremely large binary number (zeros and ones), that only you have access to. You can *know* a number, but you can't *own* it. So, you *know* a key, not *own* the key. But it's simple and generally accepted to say "own".

Because the number is large, and random, no two people will ever generate the same key.

An example of a Bitcoin private key (they can be twice as long):

```
11000111011 11101001001 10110110001 10011011000 01011111101
10001110101 00111110101 10000011101 00101001010 00011111101
11110111101 01001010101
```

Notice there are 12 groups of 11 digit binary numbers

This number is hard to write down for a human. So a system was developed, a protocol, in which words can be used to represent that number. Below is the set of words that is equal to the above number:

shuffle truck renew only garden modify dirt lonely citizen cabbage waste enjoy

12 words: Each word represents a protocol-defined 11-digit binary number

The private key is used to create a unique set (unique to that key) of seemingly infinite bitcoin addresses using a mathematical pre-defined formula. Below are the first several addresses for the key above:

```
bc1qazr6vda7swktarnddhyyg3krdlgspw0s5ssqs0
bc1qdv72s02rqp79n7ekeaq9hmnwmag8r0997shgcm
bc1qcqa7zrfzsaq4fvh9ygepv5xx4v9jzvasjhfely
bc1qsu3h6s36h9kfpvg4fzkgkcx0nv5h9zwcky5hsz
bc1q4gjqq5a9lgnu9qxlgcstkwdhdcp89xs398m4l7
bc1ql9rw38cyys7xn5mvy0c83gvr7pn7q6993x6v0v
bc1q9axfz39jzf9qsnj59fvhyurlv59s0xd608ae5u
bc1qa9gs4ycn77pj487megtaxztuehk7tkx9v7l3ay
bc1qt9ea768xpgg20wc0epzctjxs0ey322ey0pcaey
bc1q48hrh68rnpaq7706dtna950vzymtjl83ud9lpf
bc1qflrf30kz5kqszq9z0467uy3x2u4wnjl7hdad9a
```

If on the Bitcoin Blockchain, there is an address noted to have some bitcoin associated with it, and if you are the "owner" of the private key that made that Bitcoin address, then you have the power to remove bitcoin from that address, and send it to any other Bitcoin address you like.

If you move it to an address associated with someone else's private key, then that person controls where that bitcoin can go to next. You have effectively paid him/her. The balance in your Bitcoin address has gone down, and the balance in his/hers has gone up by the payment amount.

Another way to think of it is that the Bitcoin Blockchain is a public wall of writing that everyone can see. You have permission to make modifications to the wall if you can prove you are the key holder.

That proof comes from *using* the private key to *sign* a transaction. This is based on cryptography – you don't need to understand deeper than that to use Bitcoin. It happens in the background, and your wallet takes care of it. Wallets next...

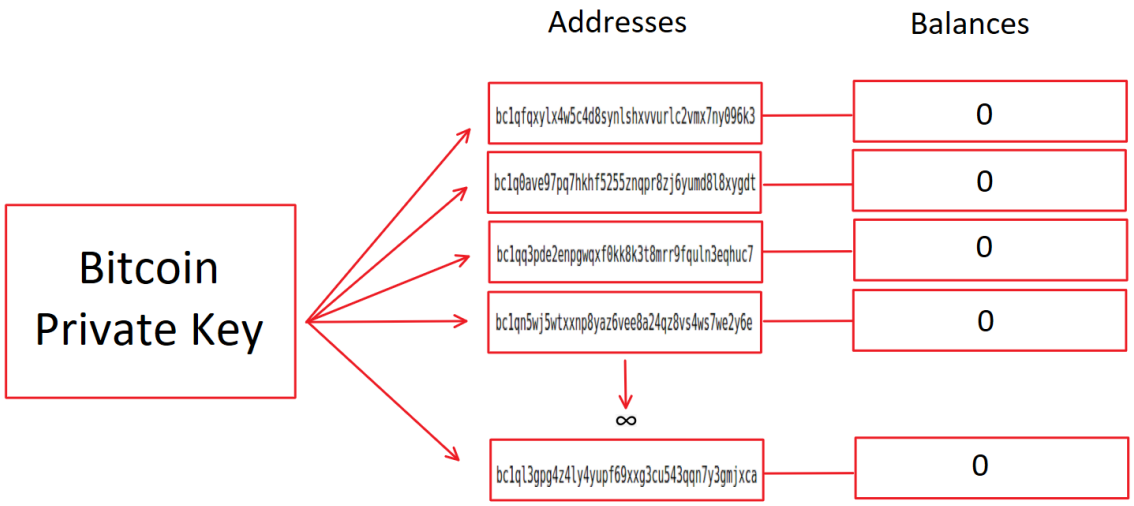
Storing Bitcoin: Wallets

A wallet is a piece of software that stores your private digital key. The wallet is not part of the Bitcoin Blockchain, it communicates with it. It is privately held software.

The wallet actually has no bitcoin in it per se. It asks the Bitcoin Network, "how much bitcoin is in my addresses?"

Remember it's the *private key* that mathematically makes limitless addresses, and controls the "spendability" of the bitcoin associated with those addresses. All the addresses are unique to the key. Because the wallet knows the private key, it can figure out the addresses. You can have many copies of a wallet on various devices, each with the same private key, and each will therefore show the same bitcoin addresses.

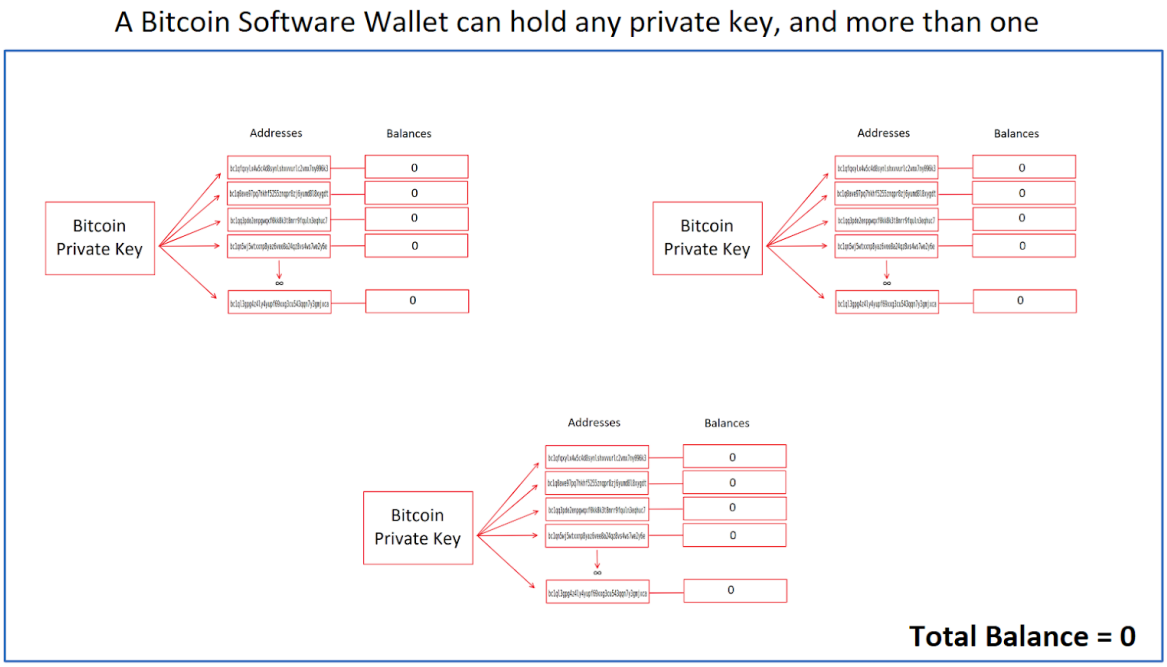
A Bitcoin Wallet:



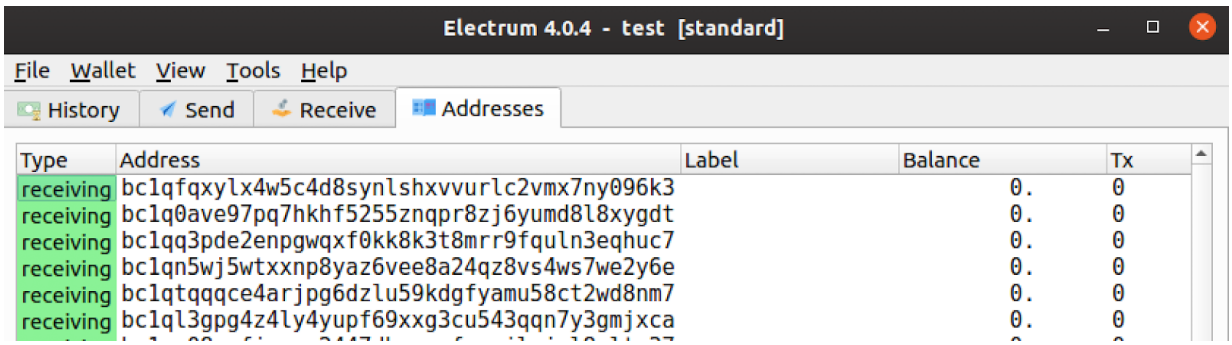
If a key is lost, the bitcoin it controls can never be spent by anyone. The bitcoin still exists on the blockchain but it cannot be spent (moved to another address) and is effectively "lost", or "unspendable".

The word "wallet" may confuse newcomers because it is used in two ways: The first usage describes software that holds your keys. The second describes all the addresses that are made by a private key.

Software (called a wallet) –> holds private key –> collection of addresses (called a wallet)



An example of a newly created wallet:



Transactions

A Bitcoin transaction can be thought of as a small package of data that states an amount of bitcoin to be moved, an origin address, a destination address, plus a signature. Sort of like a bank cheque (amount, sender, recipient, signature).

The transaction is produced by the software wallet of the sender, is signed by the private key contained in the wallet, and then the wallet sends the transaction data to a Bitcoin node. Sort of like a person writing a check, not handing it to the recipient, but directly depositing it to the recipient's bank account.

That node then checks that the transaction is valid (i.e. not cheating the rules of Bitcoin), which includes checking the signature made by the private key is

genuine. Similar to a banker checking the person writing the check has funds in the origin account, and that the signature on the check is real.

The node accepts the transaction if it is valid, and only then passes it around to other nodes. Note that a private key is used to *sign* a transaction, and it is the signature, not the private key, that gets passed around to nodes and the public blockchain.

Each node that accepts the new transaction, adds it to a waiting list called the "mempool". Each node keeps its own copy of the waiting list.

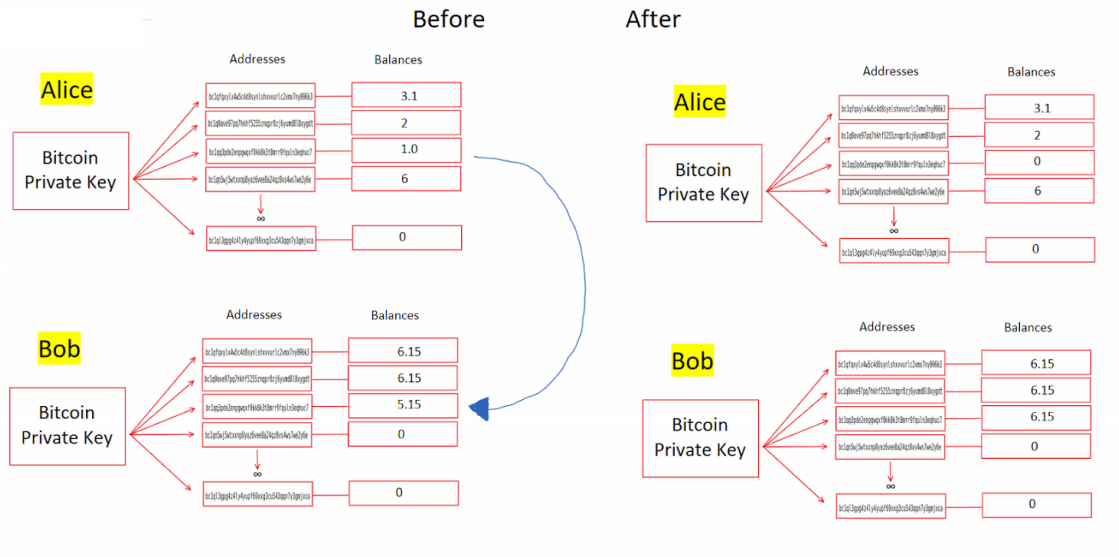
Transactions sit in the mempool, waiting for Bitcoin miners to take them, and add them to the next Bitcoin block. (Mining coming up next). A miner finalises the block, and sends it to a node, and after checking it is valid, the node passes it around to all the other nodes which also check it is valid. The block and the new transactions contained within then become part of the Blockchain.

If a wallet has an address that is expecting a payment, it checks that the relevant transaction has been added to the blockchain. The new data on the blockchain is used to update the balance reflected in the wallet.

An example will help illustrate this. Imagine Alice is paying Bob 1.0 bitcoin. I will ignore any transaction fees for simplicity. On the left half of the image below, Alice's wallet has an address (the 3rd address) with 1.0 bitcoin in it. She makes a payment of exactly that amount to Bob's 3rd Bitcoin address which has 5.15 bitcoin associated with it. Bob told Alice what his 3rd address was (i.e. provided an invoice), and Alice's wallet made a transaction that describes the origin and destination addresses, and the amount to be transferred.

She then adds a digital signature for the transaction and publishes the transaction to the Bitcoin Network (sends the transaction to a node's mempool, a miner includes the transaction in a block, the block gets sent back to a node, the new block is distributed to all the nodes). Both of their wallets update themselves based on the data on the blockchain (by asking a node via the internet).

On the right-hand side of the diagram is the status of the two wallets after the transaction is finalised. Alice's third address in her wallet has zero bitcoin. Bob's receiving address now has 6.15 bitcoin instead of 5.15 bitcoin. Bob has been paid.



Mining

You don't need to understand the inner workings of mining to understand how Bitcoin works. You probably should not consider attempting to mine bitcoin as an individual. It is generally not profitable anymore. Mining is mainly profitable for big business with access to extremely cheap (below retail price) electricity. Below is an image of a small mining "farm":

Only a basic understanding of mining is needed to understand how Bitcoin functions – In the same way that a gold accumulator doesn't need to know how gold is mined.

Mining is done block by block, and miners are all competing to mine the next block. It involves spending computing power to search for a special number, by repeated trial and error attempts. There is no "calculation" involved per se, although it is commonly described that way. It is brute force and costs electricity.

When the number is found for the next block, the miner is rewarded bitcoin within that block. Apart from including other peoples' transactions, every miner makes one transaction that effectively says "My address has 6.25 newly created bitcoin". All other transactions in the block are movements of bitcoin, not the creation of bitcoin.

This reward is how bitcoins are *regularly* created each block. Because the miner found the special number, he/she proves that computer work was done, so that when the block is passed to the nodes, they will all accept this creation of bitcoin as valid. Whoever does this first (per block), wins. Coming second is fruitless. Once there is a winner, all miners start working to win the next block.

Anyone trying to cheat will fail because they will not have the right number. The number is very difficult to find, but it is easy and quick for nodes to check that it is valid.

This computer effort is NOT WASTED energy. It is a defence mechanism. The miners spend this energy, seeking a reward in bitcoin. Any attacker, someone who wishes to tamper with the blockchain, must compete by spending more energy than the entire world mining power combined, and potentially receive NO REWARD if they fail. The more energy spent by miners, the more expensive it is to attack Bitcoin.

All the mining computer power all over the world COMBINED, is protecting the integrity of the entire Bitcoin system. It protects the blockchain, so no one can make edits against the Bitcoin rules, or steal funds.

In addition to this overall security, there is personal security. When you control bitcoin with a private key, your "control" is protected by you keeping your key safe and secret. If someone has your private key, they can steal your funds, and do so without breaking the rules of Bitcoin.

Why Can Bitcoin Be Money?

Bitcoin can be money because it has all the desirable features of a good money. It is divisible, portable, durable, recognisable, transferable (medium of exchange), measures value (unit of account), and is easily verifiable. Crucially, it is not dependent on the honesty of humans, or central coordination, and it can not be debased by creating more.

A counterargument (to be explored in a future article) is that money needs "intrinsic value" – In fact, nothing has intrinsic value. The argument would better be phrased: "It needs to have value for something other than money." – This is not true either. Money needs no alternative value. It is a language. The language of value:

Compare it to the English language: The purpose of English is to "store" and communicate MEANING. English has no "intrinsic meaning". The words themselves are just abstract symbols or noises. People don't speak English because they believe there is something intrinsic to it. They do so because the people they communicate with also speak the same language. The network of people speaking the language started small, and grew.

For free market money (not government enforced money), people speak the language of value with other humans that accept that language. In the same way that English needs no intrinsic value to be accepted as a language, money needs no intrinsic value to be accepted as a language.

Any alternative value for money is just useful for the initial stages of adoption of the language. Once it is adopted, alternative value becomes irrelevant – it could even disappear and it wouldn't matter. This is how gold grew as the language of money. Its usefulness for other purposes is nice, but irrelevant. It was its superior monetary properties and relative scarcity that grew its dominance as free-market money, not its alternative uses or alternative value.

Now, for the first time, there is something vastly better than gold. It just needs time for people to learn the language.

A candidate for money needs not only the right properties, it also needs social acceptance, and in a free market, it needs to start off as the best. Once it is in the lead for acceptance, it no longer needs to be the best. It can be *good enough* as money, and any new competitor that is only *slightly* better cannot catch up.

To illustrate with the language example, if there was a new language just like English, but a bit more beautiful sounding, we can say it is slightly better, but English will not be overtaken. English will remain dominant because it already is dominant. This is a property of networks.

Conversely, the reason Bitcoin will overtake gold is not that it is *slightly* better – but because it is *vastly* better. It is likely to overcome the dominant free-market money because it fixes gold's greatest weaknesses.

Gold's weaknesses:

- Is not easily divisible for small payments
- Is not easily portable (try taking several kilograms overseas)
- Is not digital
- Final settlement is very slow and expensive (physical delivery).
- It is expensive to store securely
- It is centralised
- It has been confiscated by governments (**Order 6102**)

To overcome many limitations, currencies backed by gold were created. This allowed people to trade value more portably, of small values, and later digitally, but it introduced new limitations – *Trusted Third Parties*. Bitcoin overcomes gold's flaws, *without* a trusted third party. This is truly amazing.

Since President Nixon's complete removal of the backing of the US dollar by gold in 1971, the dollar became money, not a currency. Easy money, not hard money. Not sound money.

We now have multiple government paper currencies backed by nothing – we can conclude that gold failed. If the world impossibly ever returns to the gold standard, the exact same thing can happen again later. We need a better solution, and there is one. But it is unlikely governments will voluntarily adopt Bitcoin (although it is possible). Instead, as the famous Austrian Economist put it, now a well-known quote in Bitcoin circles:

"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 roundaboutway introduce something they can't stop." – Friedrich Hayek in 1984

Even though it is vastly better than gold, Bitcoin won't actually be money until it is accepted by most people as money. That takes time to develop. Nearly

everyone in the world doesn't need to OWN some for it to be money, but nearly everyone in the world needs to WANT it. That is the final hurdle for Bitcoin.

Why Is Bitcoin Important?

Bitcoin is important because we don't have free-market money. Our money is created by and controlled by governments and central banks, and that control allows them to extract human time (savings) from us against our will – via money creation. This is a humanitarian disaster, and to find out more about this injustice throughout human history, I encourage you to read Robert Breedlove's incredibly well-written article, **"Masters and Slaves of Money."**

There are many other reasons Bitcoin is important, but this is by far the most. There are those that can envision (myself included) that a world with free-market money, and eradicated central banks, will be a world of peace and prosperity. That is the dream.

Free Market Money vs Barter

In a free market, there will eventually only be one money. If there are multiple monies, that is just adding friction, and is moving towards barter.
Money *solves* the problem of barter. If free-market money works, barter will eventually disappear. Note that most countries have government money, which is required by law, to use for exchange, write contracts, and pay tax. It is not free-market money, and that is why many can exist, and also why foreign exchanges are necessary for international trade.

When storing one's wealth, an individual has an incentive to store it in the money that is most accepted – not the second most accepted. This pressure eventually results in the leading money to absorb all inferior stores of wealth. But it takes time.

Summary

Hopefully, this can help you understand what Bitcoin actually is, and why it is not just a worthless token "backed by nothing" that governments can easily stop. This is a natural first impression, but as you scratch the surface, you'll realise it is something breathtaking. In future articles, I will write about peoples' typical objections (there are many), and my responses to them. I will also write about concerns that surface after understanding Bitcoin for a while – they also have excellent counter-arguments.

This article was “not too technical” by design. When you are ready for the next step in technical understanding, I strongly recommend this **superb lecture by Andreas Antonopoulos**. There is nothing else like it.

For a deeper understanding of Bitcoin overall, see the **syllabus** I have created, and various other educational articles on my **blog**.

I am also available to answer questions and can be contacted on Twitter – **@parman_the**.

Tips:

Static Lightning Address: **dandysack84@walletofsatoshi.com**

Donation

Donation

Thank you for supporting my Bitcoin work

Sats | 0 | Next

SHA256 and Bitcoin Mining Walkthrough

[Published in Bitcoin Magazine]

[French] 🇫🇷

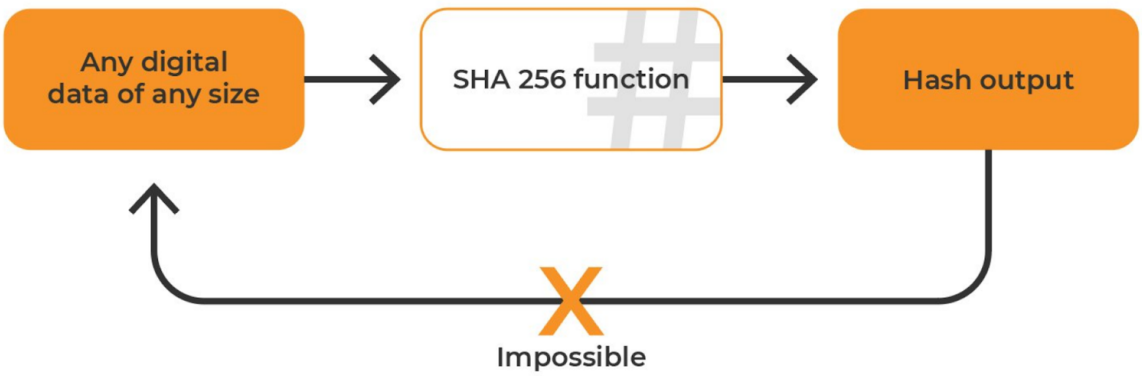
How mining works is fascinating. When I explain it to people, I enjoy seeing their face the moment their mind is blown. I'll explain it here, but just know, I'm imagining all your faces as your minds blow!

I have to start with hash functions. Without hash functions, Bitcoin would not be possible. Let me explain what they are first, not only so you can sound cool at parties, but also because it's fundamental to understanding how Bitcoin works, particularly mining, but also transactions under the hood.

You don't *need* to understand how Bitcoin works in order to benefit from it, just like how you don't need to understand how TCP/IP works to use the internet. But do go on, because it's quite interesting, and I'll make it easy to understand, promise.

HASH FUNCTIONS

Let's start with a schematic which I'll explain below...



(Image by @jirols_btc)

On the left is the INPUT, the centre is the FUNCTION, and on the right is the OUTPUT. The input can be any data, as long as it's digital. It can be of any size, provided your computer can handle it. The data is passed to the SHA256 program. The program takes the data and from it, calculates a random-looking number, but with special properties (discussed later).

The first SHA (Secure Hash Algorithm) was originally developed by the NSA and there are many different versions now (Bitcoin uses SHA256). It's a set of instructions on how to jumble up the data in a very complicated but specified way. The instructions are not a secret, and it's even possible to do it by hand, but it is very tedious.

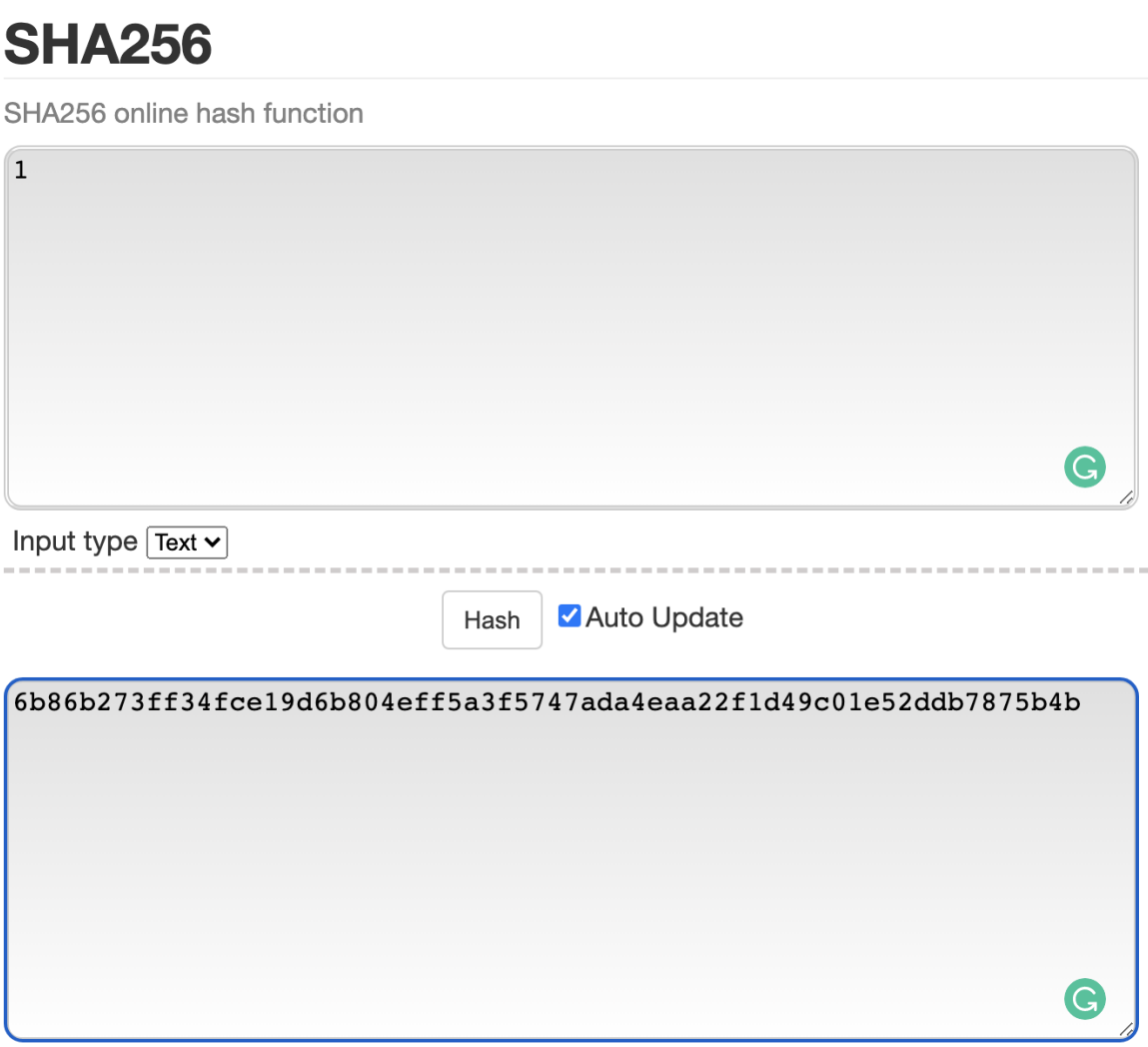
For SHA256, the output is a 256-bit number (not a coincidence).

A 256-bit number means a binary number 256 digits long. Binary means the value is represented with two symbols, either 0 or 1. Binary numbers can be converted to any other format, for example decimal numbers, which are what we are familiar with.

Although the function returns a 256 digit binary number, the value is usually expressed in hexadecimal format, 64 digits long.

Hexadecimal means that instead of 10 possible symbols like we are used to with decimal (0 to 9), we have 16 symbols (The ten we are used to, 0-9, plus the letters a, b, c, d, e, and f; which have the values 11 to 15). As an example, to represent the value of decimal 15 in hexadecimal, we just write "f" and it's the same value. There's plenty of information available online with a quick Google search if you need more elaboration.

To demonstrate SHA256 in action, I can take the number 1 and run it through an **online hash calculator**, and got this output (in hexadecimal):



The input window is the one above, the output window is the one below.

Note that all computers in the world will produce the same output, provided the input is the same and the SHA256 function is used.

The hexadecimal number output, if converted to decimal, is (notice it takes more digits to write):

48,635,463,943,209,834,798,109,814,161,294,753,926,839,975,257,569,795,305,637,098,542,720,658,922,315

And converted to binary it is:

110101110000110101100100111001111111111001101001111111001110000110011101101011100000000010011101111111101011010001111110101011101000111101011011010010011101010101000100010111100011101010010011100000000011110010100101101110111011011110000111010110110100101111010111001101011100110101110011010111001101011100110101110011010111001111

Just out of interest, here is the same value in base 64 (I'll let you Google what base 64 means):

1w1k5/5p+cM61wCd/rR+r09bSdVEXjqTgDylu28OtpY=

Note that the smallest possible value SHA256 could return is zero, but the LENGTH is still 256 bits. This is how zero is represented:

0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000

And the largest possible value is:

1111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111
1111111111

In decimal, that's:

115,792,089,237,316,195,423,570,985,008,687,907,853,269,984,665,640,564,039,457,584,007,913,129,639,935

In hexadecimal, it is:

FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

Note there are exactly 64 F's.

Zero in hexadecimal can simply be written as one single zero, but for hash output, it's 64 of them to keep to the requirement of a fixed size output:

0000000000000000000000000000000000000000000000000000000000000000

Here is a summary of some facts about the hash function that is vital to appreciate:

- The input cannot be determined from the output

- The input can be any length
- The output is always the same length
- The output will always be reproduced identically if you provide the same input.
- Any change to the input, no matter how small, will cause an unpredictable, and wildly different output
- The output is "seemingly" random, but is actually deterministic (meaning it is calculated)
- The output cannot be predicted. It can only be calculated, and this takes a measurable amount of work by a computer (and hours with pencil and paper! Don't do it.)

Now that you understand the basic concept of what a hash is, you can understand the explanation of how Bitcoin mining works.

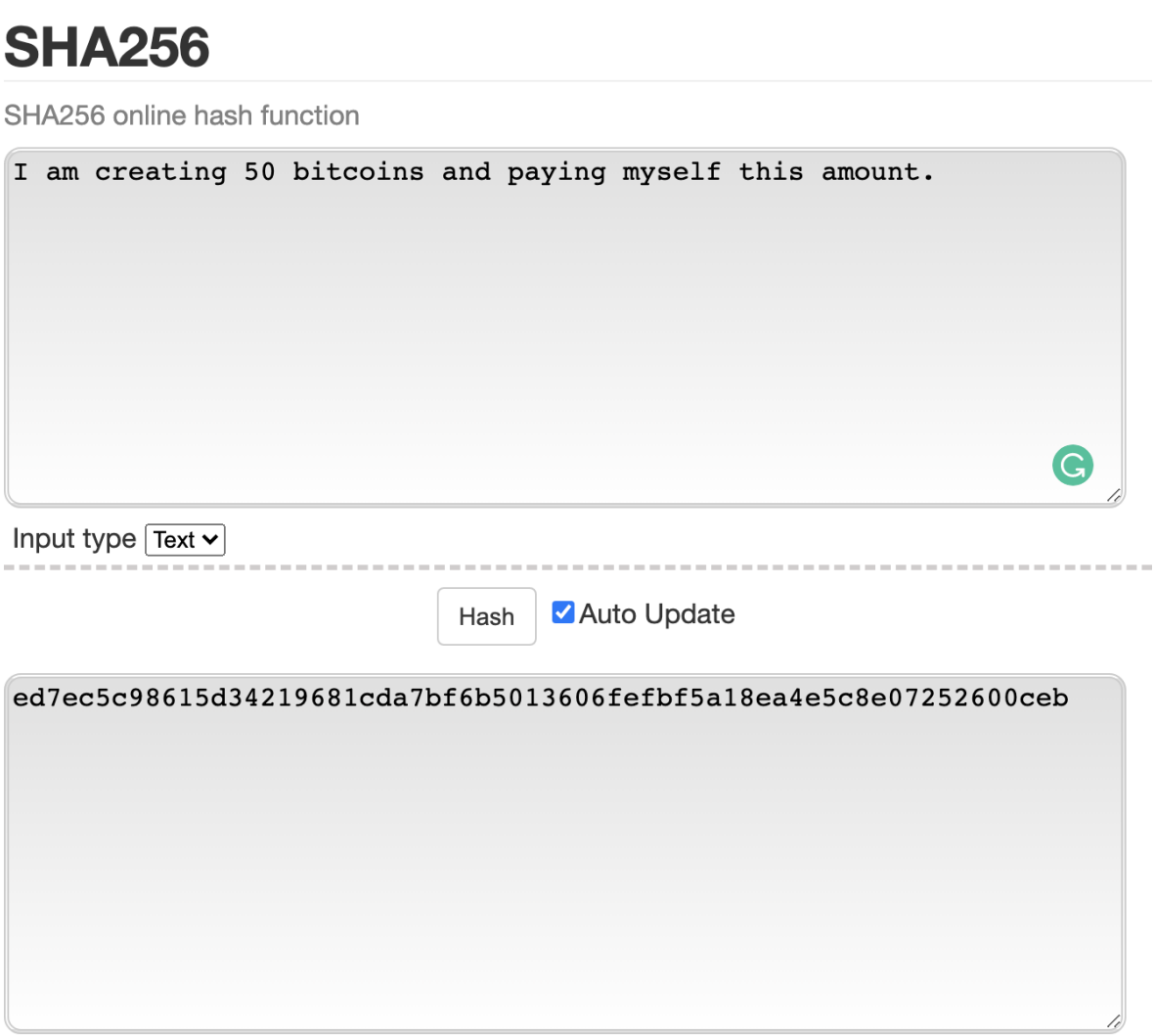
But before you move on, I recommend you go to an online hash calculator and play with it a little and test for yourself what I've said about Hash functions. **I like this one.**

Mining

I will start by demonstrating a concept of work, which is where "proof-of-work" in Bitcoin comes from.

Go to the online hash calculator and type "I am creating 50 bitcoins and paying myself this amount."

Type it exactly, case sensitive, including the full stop. You should get this output:

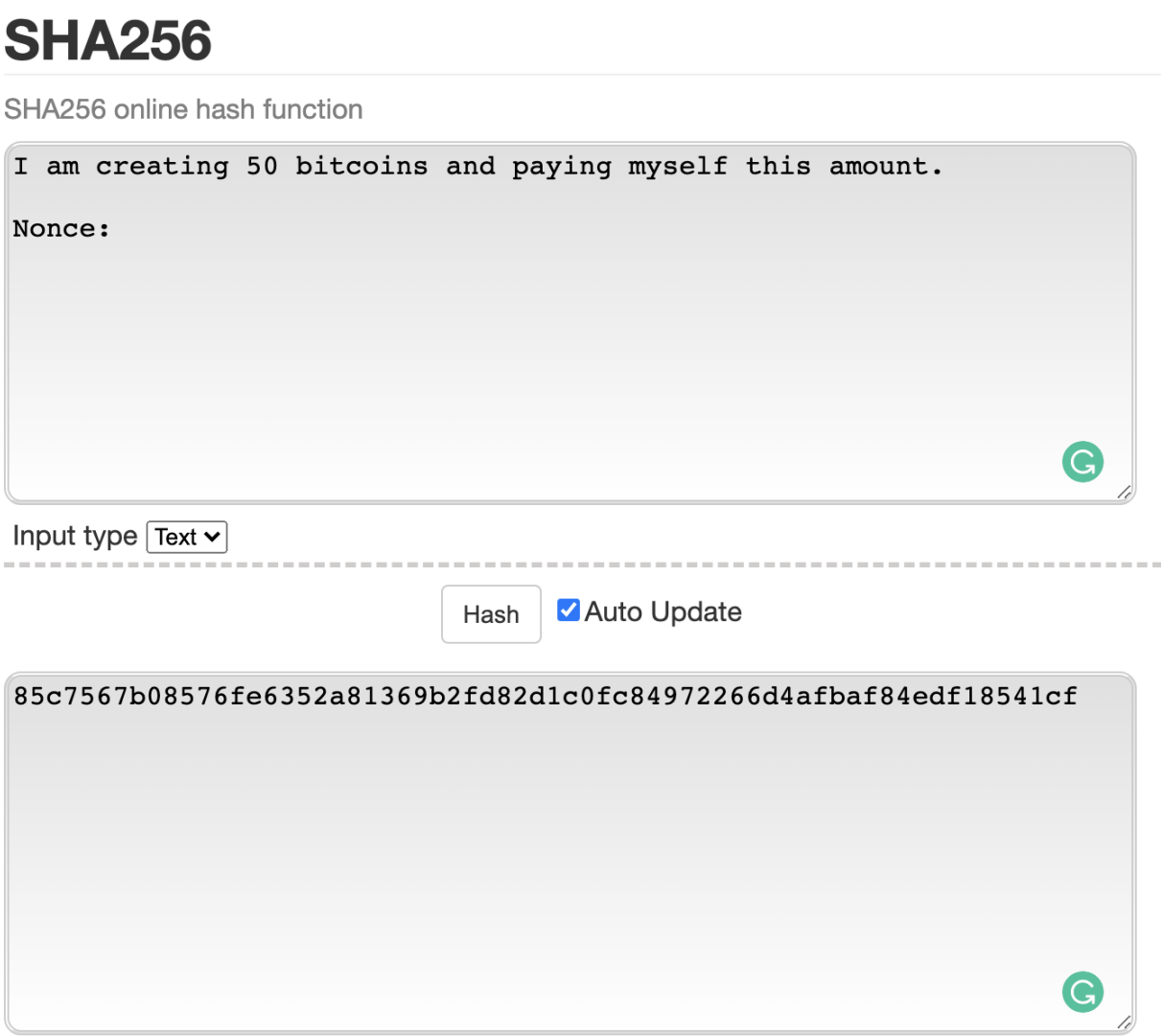


Now, let's create a rule that says for this payment message to be valid, we need the hash to start with one zero. To do that, we have to change the input somehow. But, as you've learned, it's not predictable what the output would be for a given input. What modification can we make to ensure a hash starting with zero?

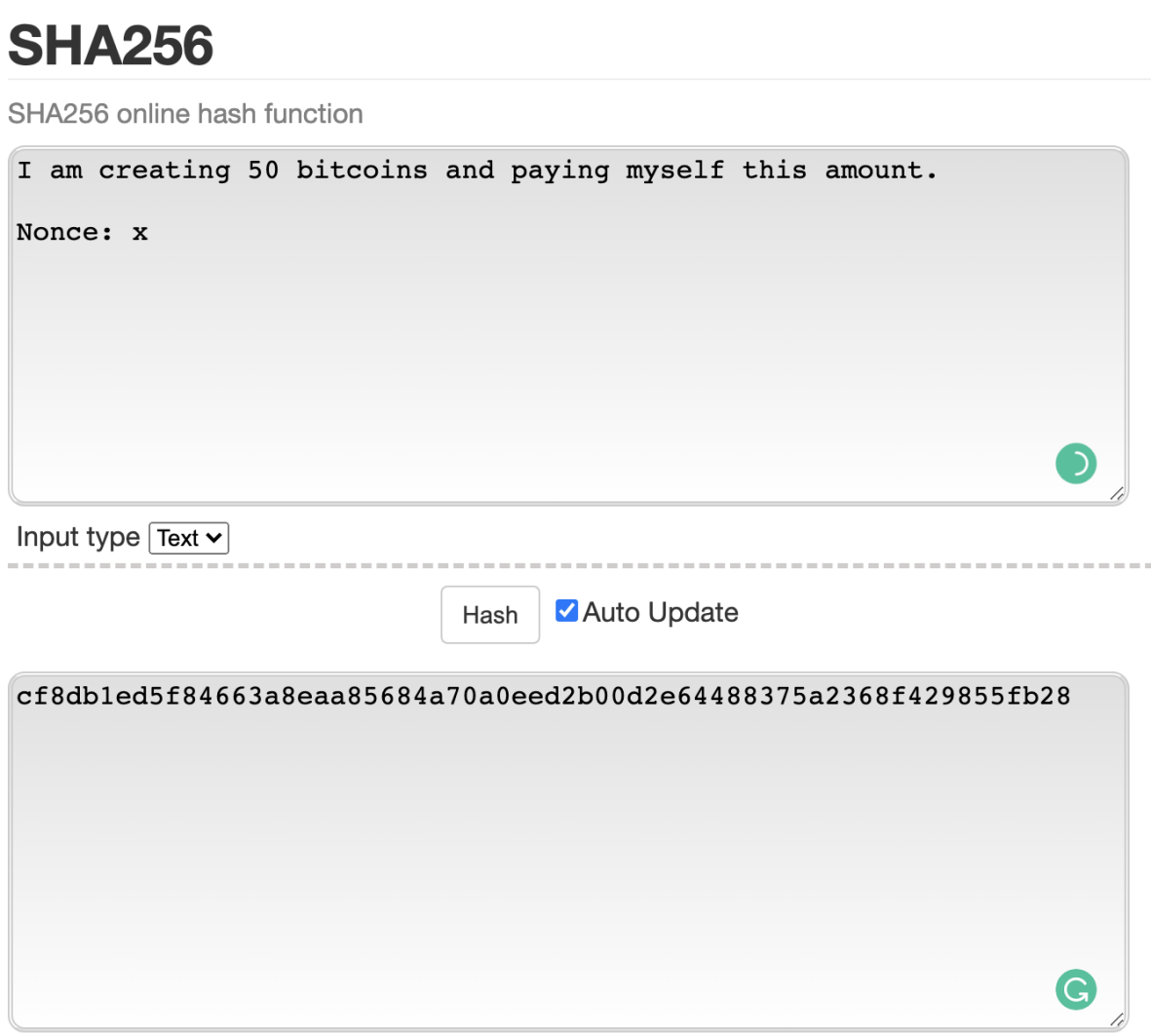
We have to add data using trial-and-error. But we also don't want to change the meaning of the input message. So, let's create a field (an allocated section) called a "nonce" which will hold a nonsense value.

The word, "Nonce", is supposed to be derived from "number only used once", but I don't see it.

Notice below how adding this extra field heading, "Nonce:", changes the hash output.



The output still doesn't start with a '0', so let's add some nonsense (I added a meaningless 'x'):

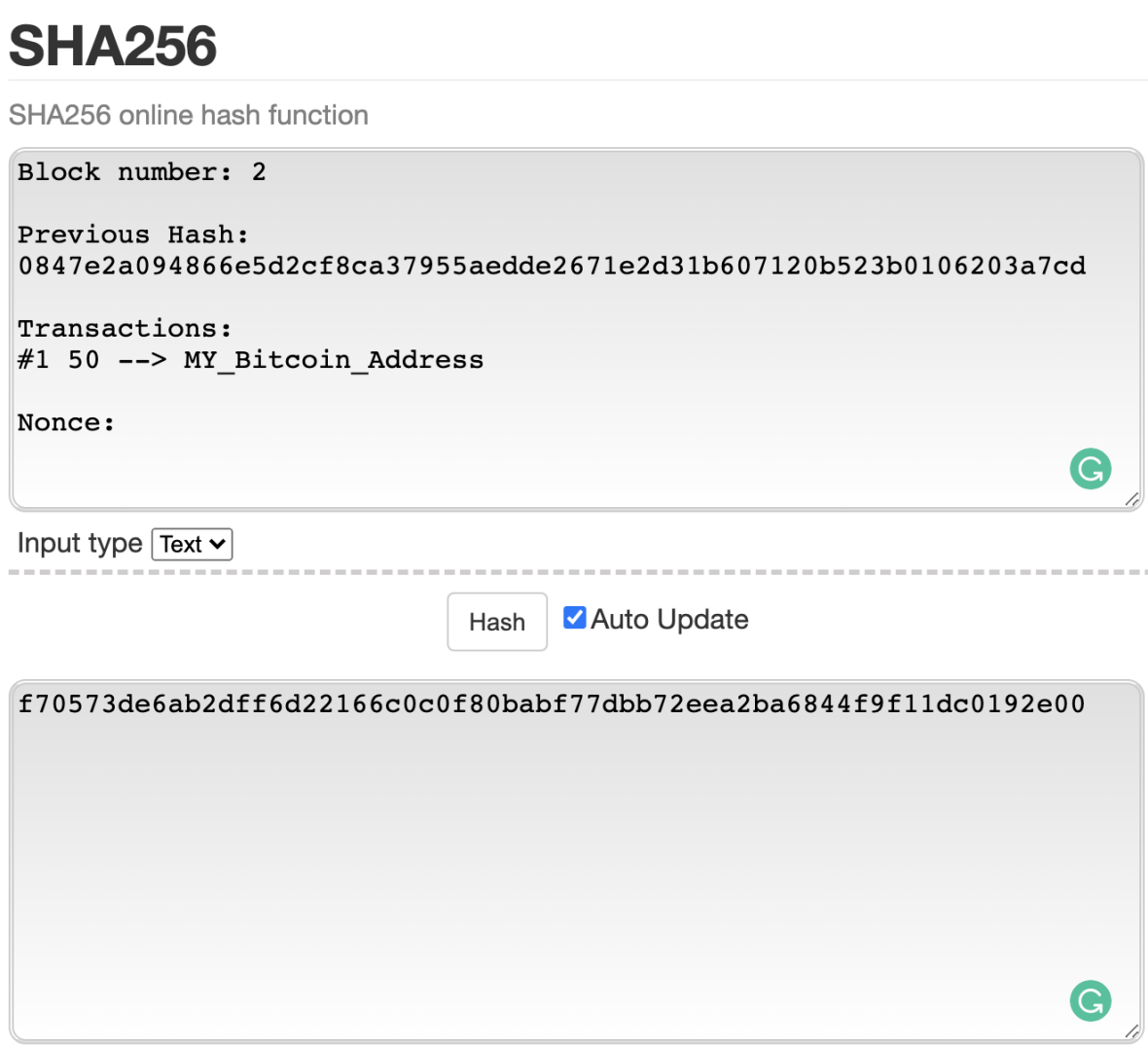


It still doesn't start with a zero. I tried some more characters until the hash started with a zero:

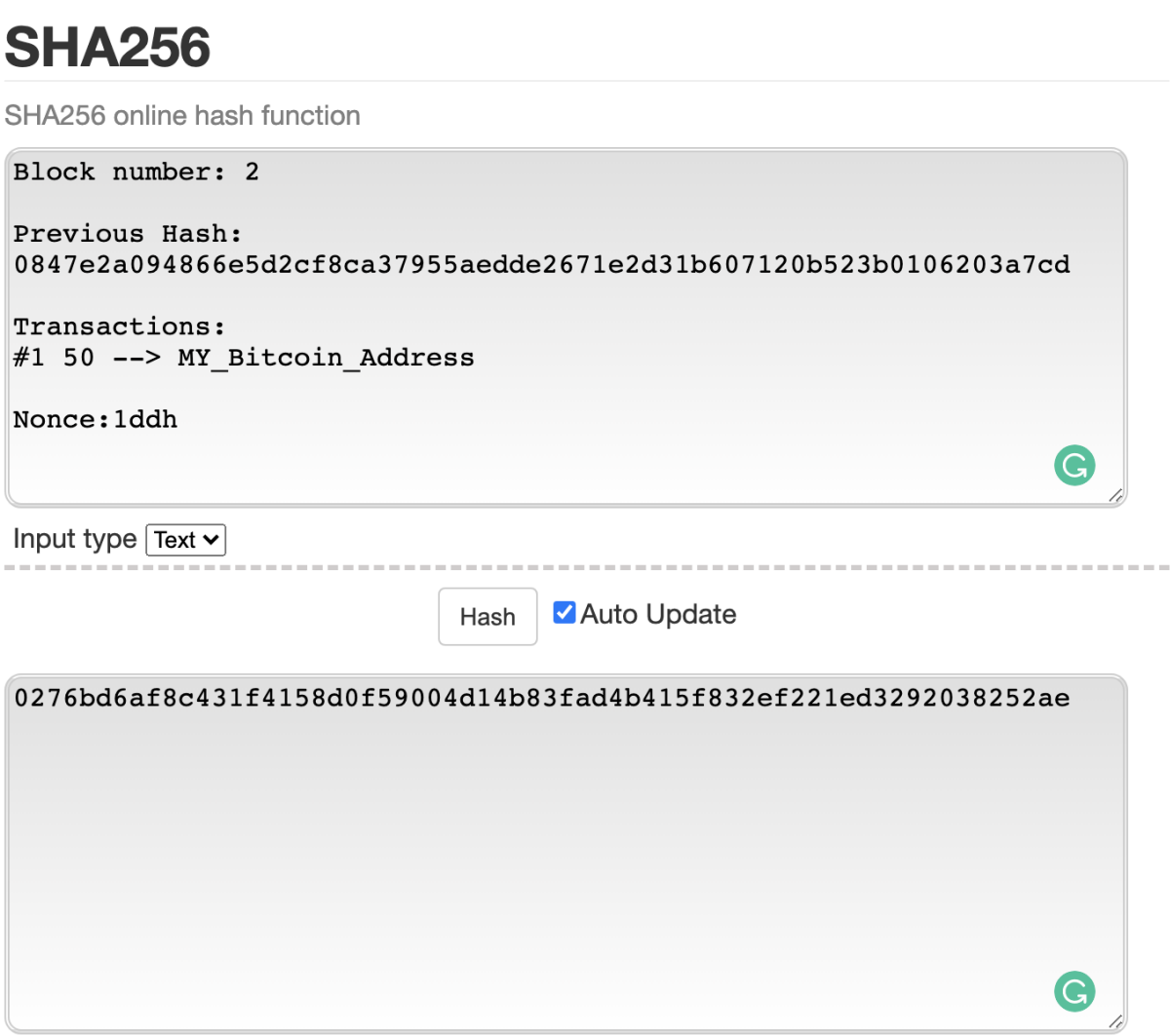
There we go. Now, according to the arbitrary rules I set, the text in the input window is a valid imaginary-Bitcoin block with a single transaction paying myself 50 bitcoins.

Note that Bitcoin blocks are essential "pages" of a ledger. Each block is numbered and creates new bitcoins, along with transactions between users. This is the record, and where bitcoins live.

Now a new rule. For the next block, the hash of the previous block must be included. I'll add a little complexity and add a few more fields to approach what the real Bitcoin block has...



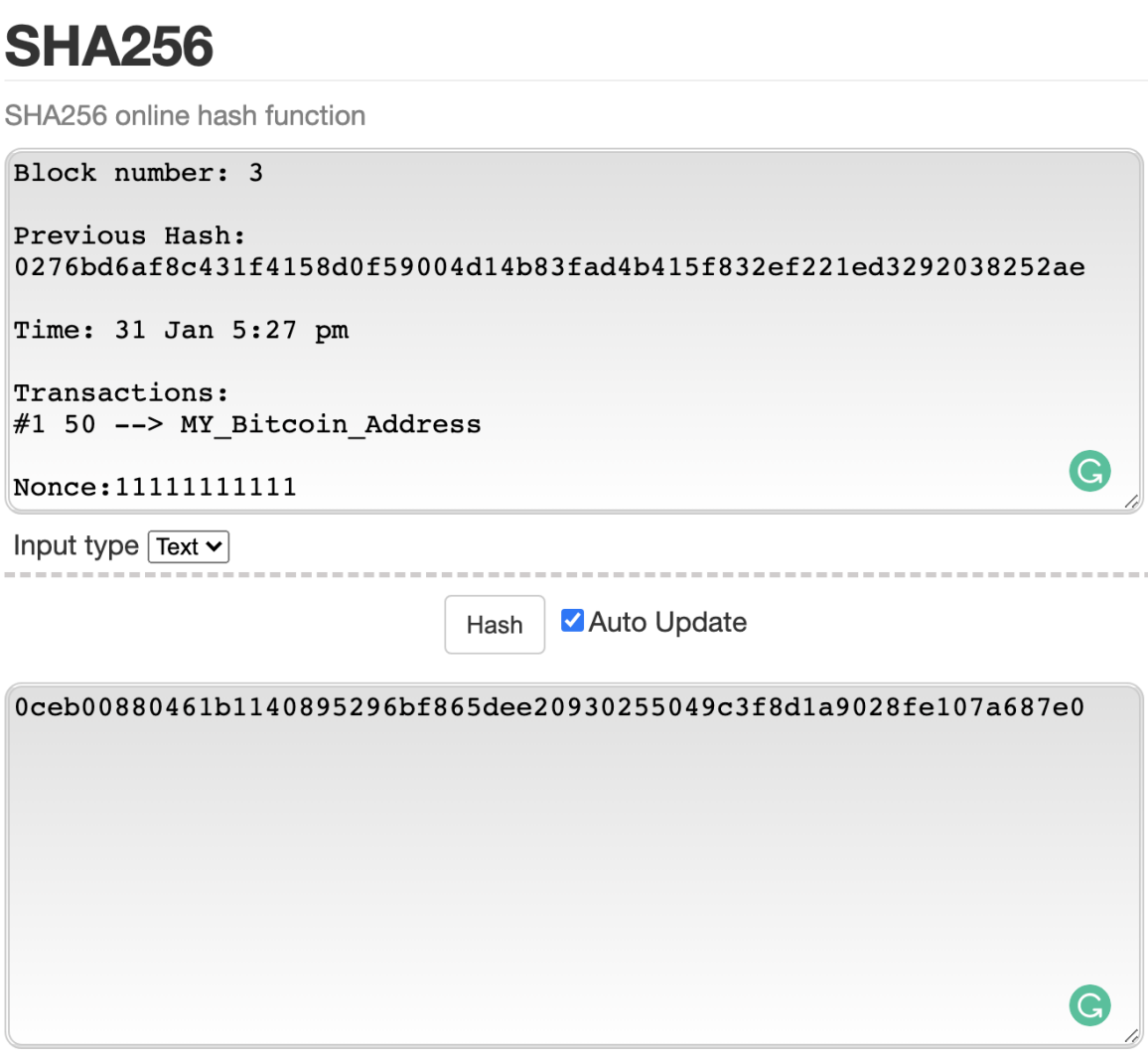
The hash starts with an ‘f’ not ‘0’, so I’ll have to try some values in the nonce field:



This time I was luckier and found a nonce after only 4 different tries. For the first block, I found one after 22 tries – there is some randomness here, but generally, it's not too difficult to find a valid hash if all we're trying to get is one zero. There are 16 possible values for the first hash digit, so I have a 1 in 16 chance that any modification I make to the input field will result in the first hash digit being '0'.

Note that Bitcoin's fields are like this, but there's more detail that I haven't added, just to illustrate a point, not necessarily to detail exactly what a Bitcoin block looks like.

I will add a time field to the next block as I need that to explain the "difficulty adjustment" next:



Above is block number 3. It includes the previous block's hash and now I've also started to include the time. The nonce I found successfully made the hash start with a zero (I just kept typing a '1' until the hash target was met).

There's enough here now that I can start explaining a few interesting concepts about the Bitcoin blockchain and mining.

Winning a block

The mining process is competitive. Whoever produces a valid block first gets to pay themselves within that block, as the block is now valid. A miner that produces the same block number a bit later (runner up) gets nothing – that block is rejected. Explaining why that is causes too much of a diversion now, so I'll explain it in the appendix.

After block 3 is found and broadcasted to everybody (all the Bitcoin nodes), all the miners stop working on block 3 and start working on block 4. The winner publishes the result, and then everyone starts working on block 5, etc.

With each block, new bitcoins are being created and collectively make up the total supply so far. If there are many miners, then statistically, blocks will be produced faster, and bitcoins will be created faster. Problem, right?

Seeking a limited supply of bitcoins with a predictable issuance over time, Satoshi Nakamoto thought of this problem and introduced a negative feedback loop to keep block production at 10-minute intervals on average. How? See if you can think of a way. Pause for a moment and ponder, and see if you can come up with the same genius solution, and read on when you give up.

NODES: I mention "valid" blocks. So what? Who's checking? The Bitcoin nodes are. A Bitcoin node ***keeps a copy of the blockchain*** *so far and follows a set of rules to check that new blocks are within the rules, and reject those that aren't. Where are the rules? In the code. A computer that downloads the Bitcoin code is a node.*

The difficulty adjustment:

The average time of new Bitcoin blocks is calculated by every node every 2016 blocks (this is why the time field is needed). This is part of the protocol and rules that the nodes follow. A formula is applied to adjust the number of zero's required for each block hash

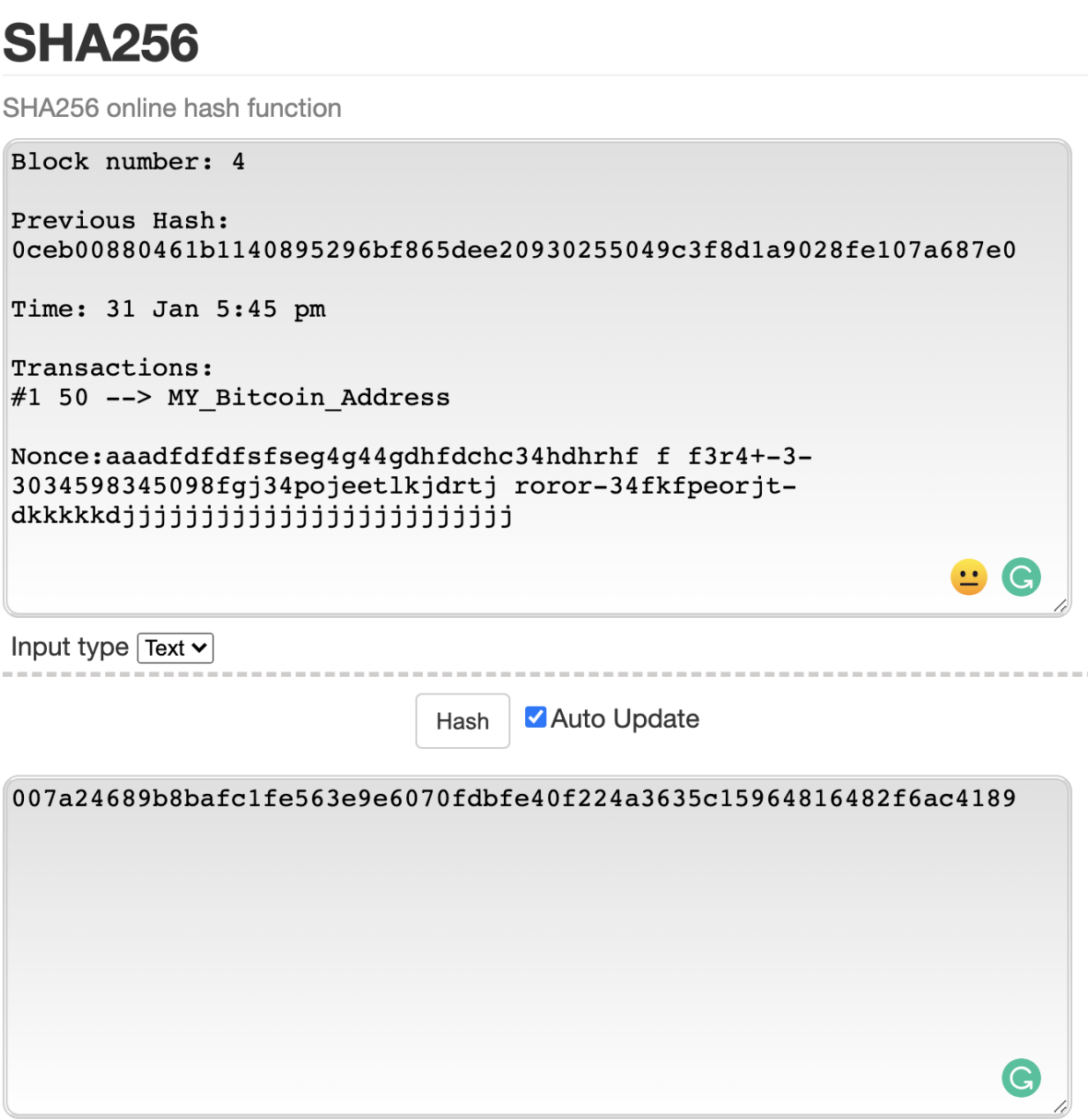
Strictly, it's not the number of zeros that is adjusted but a target value the hash has to be below, but thinking of leading zeros is simpler to explain.

If blocks are being produced too fast, then the hash target is adjusted according to pre-defined rules that all nodes follow identically (it's in their code).

Keeping it simple for my example, let's say other people are competing with me, blocks are happening too quickly, and now the 4th block needs two zeros instead of one, according to an imaginary calculation.

It's going to take me a bit longer to get two zeros, but we're imagining that there are many other people competing with me so the total time taken for *anyone* to find a block is kept to a target.

Here is the next block:



Notice the time. More than 10 minutes passed since the previous block (I just made the time up to demonstrate). The 10-minute target is statistical, it is never known exactly when the next block will be found.

I messed around on the keyboard for a minute until two zeros showed up. This was exponentially harder than finding a single zero. The chance of finding two 0's in a row is 1 in 16×16, or 1 in 256 chance.

If more people join to mine and compete for new bitcoins, then eventually 3 zeros will be required.

I just looked up the last real Bitcoin block, which contains the hash of the previous block. The hash was:

00000000000000000084d31772619ee08e21b232f755a506bc5d09f3f1a43a1

That's 19 zeros! There's a 1 in 16^{19} chance of finding such a block with each attempt. Bitcoin miners do many many attempts per second, and collectively all over the world.

The number of attempts per second is known as the "hash rate". Currently, the estimated world hash rate is just under 200 Tera hashes per second (200 trillion per second). With that many attempts per second, a block with a hash starting with 19 zeros is found around every 10 minutes.

In the future, as more miners join in, the hash rate will go up, blocks will be found faster, and Bitcoin's difficulty will adjust to require 20 zeros etc, which keeps block production around 10 minutes.

The halving:

When bitcoin first started, 50 bitcoins were produced with every block. The rules of the Bitcoin blockchain specify that after every 210,000 blocks, the reward will be cut in half. This moment is known as "the halving", and happens roughly every 4 years. The halving, combined with the difficulty adjustment keeping blocks at 10-minute intervals means that around the year 2140, the block reward will be 0.00000001, or 1 Satoshi, the smallest unit of a bitcoin, and can't be halved anymore. Mining won't stop, but the "block reward" will be zero. From this moment, no new bitcoins will be created going forward, and the number of bitcoins is mathematically calculatable and close enough to 21 million coins. This is how the total supply is known – it is programmatically set.

The miners will still be rewarded though, not from the "block reward", but from transaction fees – explained next.

How exactly is the block reward cut in half? It's in the code held by the nodes. They know to reject any new block after 210,000 where a miner pays himself over 25 bitcoins.

Transaction Fees:

So far I've only shown imaginary blocks with a single transaction, the transaction where the miner gets paid a reward. This is called the "coinbase transaction".

It's not named after the company, Conbase, I mean Coinbase. The company named itself after the coinbase transaction, not the other way around, don't get confused.

In addition to the coinbase transaction, there are transactions of people paying each other. Here's an imagined example:

SHA256

SHA256 online hash function

```
Block number: 200,001

Previous Hash:
00000000000002e3269b8a00caf315115297c626f954770e8398470d7f387e1c

Time: 22nd August 2012 8:47 pm

Transactions:
#1 27.3388022 --> The_Miner's_Bitcoin_Address
...
#132 bc1q...pns 2.3 --> bc1q97..ghei 2.1 + bc1qfg...bobs 0.1

Nonce: Craig Wright Can Go to Hell 9owefn09v34 adflkjd 92oiw
akjdakljfh0nwf0 v8d wd8yv dw8yf we8fy w9e8f dfidfdshd BSV
s5uppo4rters a7re r1etar!ds WTAF 09euf iejf
```

I didn't bother finding a real hash this time (It's actually the real hash reported in block 200,001). The Nonce I just made up for fun, but notice a message can be embedded there.

Satoshis famously included the words, "Chancellor on Brink of Second Bailout for Banks" in the first Bitcoin block (The Genesis Block), after the newspaper headline for the day.


```
00000000  f9 be b4 d9 1d 01 00 00  01 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 00 00 00 00  00 00 00 00 3b a3 ed fd  |............;...|
00000030  7a 7b 12 b2 7a c7 2c 3e  67 76 8f 61 7f c8 1b c3  |z{..z.,>gv.a....|
00000040  88 8a 51 32 3a 9f b8 aa  4b 1e 5e 4a 29 ab 5f 49  |..Q2:...K.^J)._I|
00000050  ff ff 00 1d 1d ac 2b 7c  01 01 00 00 00 01 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 00 00  00 00 00 00 00 00 ff ff  |................|
00000080  ff ff 4d 04 ff ff 00 1d  01 04 45 54 68 65 20 54  |..M.......EThe T|
00000090  69 6d 65 73 20 30 33 2f  4a 61 6e 2f 32 30 30 39  |imes 03/Jan/2009|
000000a0  20 43 68 61 6e 63 65 6c  6c 6f 72 20 6f 6e 20 62  | Chancellor on b|
000000b0  72 69 6e 6b 20 6f 66 20  73 65 63 6f 6e 64 20 62  |rink of second b|
000000c0  61 69 6c 6f 75 74 20 66  6f 72 20 62 61 6e 6b 73  |ailout for banks|
000000d0  ff ff ff ff 01 00 f2 05  2a 01 00 00 00 43 41 04  |........*....CA.|
000000e0  67 8a fd b0 fe 55 48 27  19 67 f1 a6 71 30 b7 10  |g....UH'.g..q0..|
000000f0  5c d6 a8 28 e0 39 09 a6  79 62 e0 ea 1f 61 de     |\..(.9..yb...a.|
000000ff
```

The point here is that there are 132 transactions included (not all shown). Look at transaction #132 – 2.3 bitcoins from an address is paying 2.1 bitcoins to another address and also to a second address the amount 0.1 bitcoin (I've used dots to shorten the length of the address).

So a source of 2.3 bitcoins pays a total of 2.2 bitcoin (2.2+0.1=2.2). Is there 0.1 bitcoin missing? No, the difference is claimed by the miner, as I'll explain.

The miner is allowed to pay himself 25 bitcoins as the block reward (because 210,000 blocks have passed so the reward has been halved from 50 to 25). But if you look, the coinbase transaction is 27.33880022. The extra 2.33880022 bitcoins come from other 132 transactions in the block – the inputs will all be slightly greater than the total of the outputs. So the miner gets to create these "abandoned" bitcoin as payment to himself.

The block space is limited. When Bitcoin was new, users could send transactions with no fee, and the miners would include the transaction in the block. But now, there are more users, and since getting on the next block is competitive, users include a fee in the transaction to entice the miner to choose their transaction over others'.

So when the block reward steadily goes down, halving every 4 years and eventually to zero, miners still get paid in this way.

Some have suggested that one day the reward to miners will not be enough and will cause Bitcoin to fail. This concern has been thoroughly debunked and I won't repeat it here.

Can a block be re-written?

This is extremely unlikely and it's worth understanding why. You'll then appreciate why Bitcoin transactions are immutable (unchangeable).

I explained earlier that the hash of the previous block is included in the current block. That means any editing of transactions in an old block changes the hash of the block. But that hash is recorded down in the *next* block, so the next block needs to be updated. But if you change the hash recorded in the next block, then its hash needs to change too.

Note that any time a hash is changed, you lose all these lovely zeros and will just be left with a random-looking hash – and have to do all the work again to get the zeros back. If you do that for the block you tried to edit, you then have to redo the work for the next block, and the next all the way to the most recent block. You can't simply stop at the old block, because the rules of Bitcoin are such that the longest chain of blocks is the real Bitcoin record. If you go back and edit a block 10 blocks ago, you no longer have the longest chain. You have to add 10 more blocks and then a bit more because as you were creating those 10 blocks, the real chain probably became a bit longer. You have to race to overtake the real chain. If successful, then the new version becomes the real version.

Repeating the entire world's collective hashing effort from the edited block to the latest block is the barrier to editing Bitcoin. The energy was expended to create those hashes with all those improbable zeros, and that energy expenditure must be repeated to edit Bitcoin. This is why energy used to mine Bitcoin is not "wasted"; it is there to defend Bitcoin from edits; to make the ledger immutable without needing to trust a central authority.

What happens if 2 miners find a block at the same time?

This actually happens every now and then, and it always sorts itself out as follows:

Every node will receive either one of the new nearly-simultaneous blocks first and will accept that one, and reject the one arriving later. This results in a split of the network, but it's temporary.

To illustrate, let's call one of the blocks blue and the other red (they have no colour, just bear with me)

Miners then work on the next block, but there will be a split as to which block they extend the chain from.

Let's say the winning miner found a block using the blue chain. They will send the new block to all the nodes and the longest chain will be apparent. The nodes that had accepted the red chain will then drop it, and adopt the blue chain.

All miners that were working on the red chain will stop, and will now work on the longer chain which is the blue chain. The red chain died.

Appendix

Why a runner up miner's block is invalid

Suppose block 700,000 just got mined by MINER-A. 30 seconds later, MINER-B also created a different version of block 700,000. When MINER-B broadcasts this alternative, every node is going to reject it because they have already seen and accepted the block by MINER-A. What's more, in that 30 seconds, let's say that MINER-C found block 700,001. Given that MINER-B's competing 700,000th block does not extend the current chain (which is up to 700,001), it is also rejected for that reason.

Even more interesting is that if MINER-B had been working on Block 700,001 instead of a competing version of 700,000, they would have had just as much

chance of mining a valid block than the invalid one. So as soon as any miner sees a new block, they should set their effort on the next block.

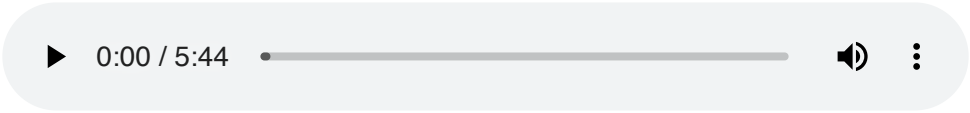
If however, Miner-B found block 700,000 1 second after MINER-A did, then it's possible that some nodes see MINER-A's block first, and some see MINER-B's block, depending on geographic locations and internet speeds. In that case, there is a temporary fork, and some miners will be working to extend one version, and some miners will be working to extend the other. As explained earlier using the "blue chain" and "red chain" descriptors, eventually one of the versions will extend further before the other and become the valid version unanimously.

Tips:

Static Lightning Address: **dandysack84@walletofsatoshi.com**

What is a blockchain and what's the point of it?

Audio by **@DelioPera**



I'd like to put out a quick demystifier about "blockchain" that you might either learn from or use to explain to others.

Blockchain is not as fancy as people are led to believe.

It's just a data structure, where new additions to the data are linked in a chain (with hashing).

The point of this is so that if any modifications are made to previous data entries, it affects the later additions of the chain, such that tampering becomes EVIDENT, and rejected by users of the blockchain.

It's better explained with an analogy.

Imagine a notebook. On page one, I write some numbers.

- Eg: 1,2,5,8,20, 12. (The average is 8).

On page two, I write the average of all the numbers on the previous page as my first number on this page.

- So I'd write 8, then I add some other numbers, eg: 2, 20, 10, 14.

The average of page 2 is 9. Importantly, the first number (8) is included in the calculation.

Then on page 3, I take the average of all the numbers on page 2, add some numbers, and put the average on the next page and so on.

A very interesting property results from doing this. If I change any number on a page that is not on the latest page, it changes the average of that page. And that

changes the average of the next and every page afterwards. Eg if there are 20 pages, and I modify the number on page 18, then page 19's average changes and so does page 20's.

As a result, any change becomes tamper-EVIDENT. It doesn't become tamper-PROOF, that's done in another way (adding proof of work, and a rule that the chain with the most work is the valid one – in practice this means "the longest chain").

For a blockchain, instead of using averages, hashes are used. You can research what they are, but the basic concept of a blockchain remains the same: All the blocks are linked, and any change in the previous block affects all the future blocks.

As you can probably tell, there is nothing magical about this on its own. It's been around for decades. Satoshi invented BITCOIN, not blockchain. He just used blockchain as one of the many essential components of generating digitally scarce money resistant to shutdown.

Other crucial components are:

- Proof of work
- Distributed nodes
- Consensus algorithm
- Public/private cryptography

That's only the tech. To be sound money, the tech needs a dominant network, which Bitcoin developed over years, free from any competition.

Earlier I mentioned proof of work makes the blockchain tamper-PROOF. Actually, something else is needed too: The algorithm. This is what's coded in a Bitcoin node, which accepts the longest chain as the valid version of the blockchain.

What happens if there is tampering and how does resistance work in Bitcoin?

If an early block is modified, an attacker then needs to modify the next block by including an updated hash of the last block. On its own, that's easy to do. Hash's are nearly instant for powerful computers. The difficulty comes from the fact that the attacker also has to RE-MINE the block.

That is because some data has been modified, and so the hash for the block will not have the required number of zeros that the earlier miner had found. The

block becomes invalid. The attacker must iterate random bits of data until the block when hashed provides a pre-required number of leading zeros. This requires work/energy/time. This is proof of work, and this is a barrier for the attacker.

What's more, he'll have to redo the work for the next block as well, all the way to the tip of the chain, and then produce more blocks to make the longest chain, to make the attacked version of the chain the valid one that all the nodes will prefer.

To conclude, I'll say there is nothing interesting about blockchain on its own, and good luck finding another monumental use case for it other than being a component necessary to create Bitcoin.

If you're interested in blockchain, not Bitcoin, and you didn't know these things, then you're not really interested in blockchain. If you did know all this, and you say blockchain is interesting and Bitcoin is not, you're either a scammer or a victim that's NGMI.

Tips:

Static Lightning Address: **dandysack84@walletofsatoshi.com**

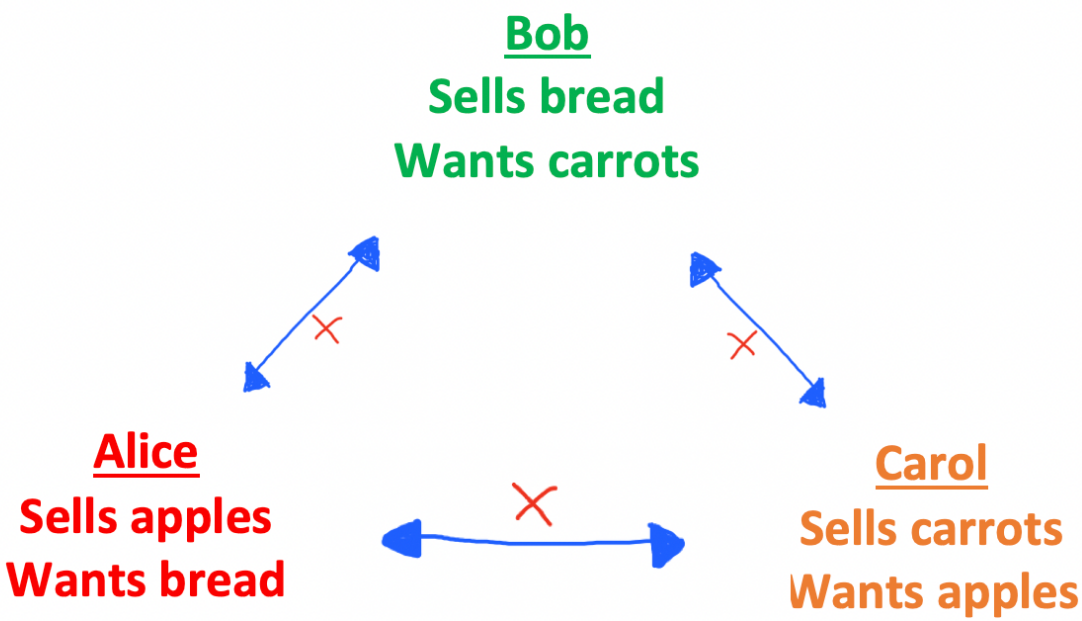
Why Money Tends Towards One (With Proof)

Money tends towards one. It's true, and I'll prove it using logic. It's a recurring argument against shitcoiners so I'm putting it down in writing once and for all.

Human society *must* have begun in a state of barter before we had money. From that starting point, in the absence of a ruler who forces tokens on people (the norm), individuals will voluntarily trade with one another with goods and services they produce (barter).

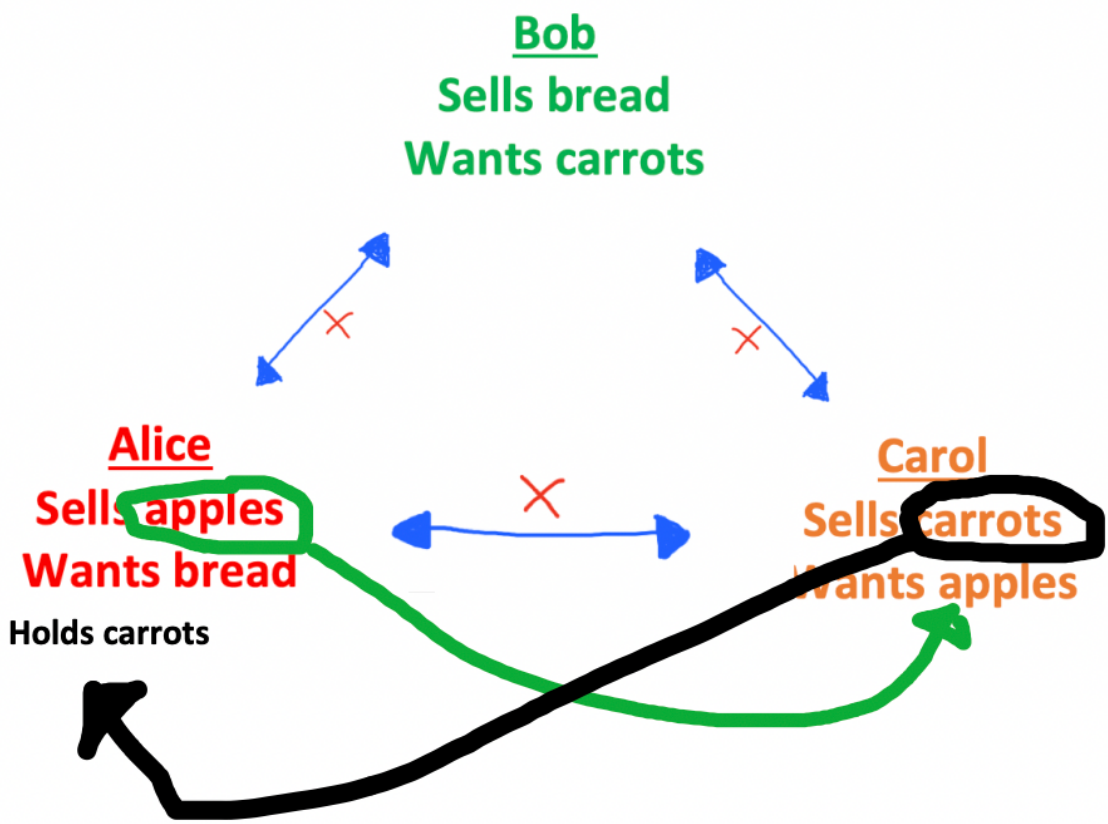
Specialisation in a particular field of production/service would increase output and prosperity, but it is risky to initiate, as not all people will accept the particular output in trade.

Specialisation would magnify a "coincidence of wants" problem (see image). Here, Alice, Bob, and Carol cannot trade with each other:

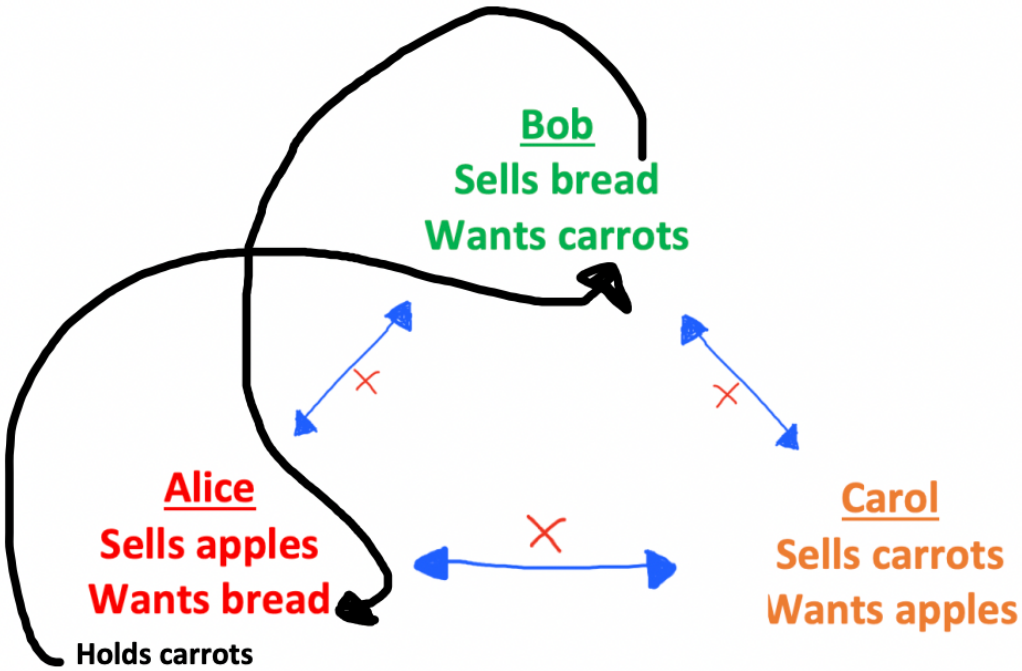


But, if one party accepts a good (eg Alice accepting carrots) that is not directly wanted/needed, to be used later as payment, then a trade may occur. This is a risk, as it is unknown for sure if that good can be used later, but the risk is

balanced with the value gained through increased trade (increased trade = increased prosperity).



Step one in indirect trade. Alice accepts carrots even though she does not want them for herself. She knows Bob wants carrots and anticipates he still will in the future.



Step 2 in indirect trade. Alice's "gamble" has paid off, as Bob retained his desire for carrots, and Alice was able to acquire apples.

No one needs to be forced into this for it to happen – It is completely voluntary, and it happens naturally because the incentives are there – Alice wants to get them apples!

When a participant in the market is uncertain of what they wish to *buy* in the future (and what might be *accepted* as payment in the future), the most suitable

good to accept will be the one that has the best properties as money – that is the one that will be least risky. The risk is calculated by a combination of assessing the good's suitability to be used in trade (scarcity, durability, divisibility, portability, recognisability etc.) and the chance of being accepted as payment (a function of the "money's" network effect, i.e. the number of merchants accepting it as payment).

> Those that choose poorly become poor. Those that choose wisely, will prosper.

Accepting goods for indirect trade will happen with many different items, but the problem of risk always remains until one universally accepted item prevails – when there is only one money, there is no risk in accepting that money, and the process of barter-to-money is complete.

When there is more than one money in society, accepting one or the other as payment always has some risk (because you don't know if it will be accepted by the merchant of your choice in the future). And so, society is said to be in a state of *partial barter* (or a society with incomplete evolution towards one with money). The incentive to choose the best money remains, and that provides the perpetual natural drive toward one money.

When money enters a barter society, specialisation of trade becomes less risky. When individuals specialise in a trade (rather than doing every task themselves), they produce more (become more efficient), and society as a whole produces more. When society produces more, society as a whole becomes "wealthier", or more prosperous. By improving the communication of value, money improves the wealth of EVERYONE in society (wealth being a product of natural prosperity to all, and your rank in society of your spending potential).

The natural state of people plonked onto the planet is what I call "baseline poverty". People initially have to fend for themselves with the resources available on the planet, and prosperity increases with free-exchange. Can they become poorer? Yes: if a ruler steps in (with violence) and enslaves the people (with good intentions or not, that's not relevant). This can take many forms, but working for pieces of paper that becomes worthless over time with no share (or reduced) of the planet's resources is WORSE than baseline poverty. I'd call it a form of slavery. This is how many people in the world live today, and don't realise.

Natural money that evolves from barter provides prosperity for society. When rulers step in and force worthless tokens on people (and *assign*s value), this can still facilitate trade and overcome barter, but it allows the ruler(s) to pillage the wealth/prosperity generated from human free-exchange. They either keep it for themselves or distribute it unevenly (to people that help keep them in power).

Ultimately the redistribution of prosperity, even if benevolent, can not be more efficient/accurate than what the free market will allow through the pricing mechanism (powered by supply and demand). Elaborating on this fully is outside the scope of this piece and I refer you to the study of Austrian Economics (well worth it!) – an excellent book to start with would be: **"Choice: Cooperation, Enterprise, and Human Action" by Robert Murphy.**

So currently, we are in a state of slavery with many rulers, many forced monies, a parallel system of free-market money that failed (gold/silver – which allowed fiat to exist in the first place), and an emerging new free-market money that will eventually dominate **(here's the logical proof)**, and eliminate the power rulers have over money.

Yes, it's Biiiiiitcoiiiiin!

Bitcoin Fundamentals – Supply and Demand, dissected

[Originally published with Amber]

Audio by [@DelioPera]

0:00 / 13:37

Often, you will hear from traders and others about the "fundamentals" of Bitcoin. That they look good or bad, or trending sideways, or some other comment. Most people don't actually know what the fundamentals are, or what that means. Some even think that *price action* is a fundamental property of any asset, which it absolutely is not.

In my view, the fundamentals of any asset is in its ability to do precisely what it is intended or designed to do, as well as in its success in doing so – intention and execution. For example, a business's fundamentals refer to the features that will enable it to grow and generate an income over time.

For a commodity, like coal, oil, coffee, wheat, sugar, gold, and Bitcoin, the fundamentals are typically in things that cause people to want to acquire it, including the dynamics around its production – i.e., its demand, and its supply; both now and in the future.

For an emergent and evolving free and open market money – like Bitcoin – the fundamentals are the things that measure the probability of it successfully becoming universal money.

There are two main components of this:

1. **The Technical Aspects**:
   - How good is Bitcoin at being money?
   - How good is Bitcoin at resisting shut off?
   - Can it scale to become a reliable medium of exchange?
   - Will it remain exchangeable and fungible?
   - Are its qualities, characteristics and its subsequent layers able to solve the world's problems with money?

- Is it **Lindy** and will it remain so?

2. **The Network of Users:**
   - How many people are committed to Bitcoin?
   - How many Bitcoin are there that will never be sold back to fiat currency; that is, sats that are waiting for **sat/cent parity** in a hyperbitcoinised world, so that they may start to be spent (this property is hard to measure; there is no chart that I know of showing this).

We know, however, that once somebody is sufficiently captured by Bitcoin – that is, once they understand it is the solution to many of the troubles of our society and civilization, more generally, and that once they see that Bitcoin is virtually inevitable over a long enough time scale – then they are highly unlikely to spend a single sat, unless in exceptional circumstances, such as an emergency.

This is a fundamental property (note: I am excluding people who simply hold some bitcoin without any particular conviction as this is not sufficient enough to be considered part of the "network" of users, in this context).

These are the fundamental properties of Bitcoin, which influence the true supply and demand of Bitcoin. Let me explain...

SUPPLY

The supply of Bitcoin comes from:

1) **New Coins**: these are Bitcoin that are mined (by miners using ASIC computers) whereby the production is programmed at a predefined rate by the Bitcoin protocol. This is an incredibly unique property of Bitcoin. It is something that humanity has never seen before, where the total supply of the asset is identifiably known upfront, in advance, and that is independent and immutable of any single person's decision.

The new coin rate currently is 6.25 Bitcoin issued in the Block reward every 10 minutes (on average). 900 new Bitcoin are being issued onto the market every day. You can think of these coins as all being sold to the market – even if you know there are some coins not being sold by some miners; it will be clear soon why this is so.

2) **Old Coins**: Added to the supply of 900 bitcoin per day, are coins sold by loyal Bitcoiners (especially the ideologically committed ones), due to certain personal circumstances. Any Bitcoin sold by a trader or a non-committed individual holding Bitcoin is *not* counted as supply. This is because the Bitcoin

they bought was never meant to be held on for too long. Their demand doesn't count, so neither does their supply.

3) **IOU Bitcoin**: This is Bitcoin bought from an exchange that does not keep a 1:1 reserve. This inflates the true supply of Bitcoin, meaning customers may be buying Bitcoin that does not really exist. Or, they are buying Bitcoin that is claimed by more than one person. This has the effect of adding excess supply to the market, thus reducing the price.

DEMAND

Demand for Bitcoin is equivalent to the supply of USD. It's worth pausing and thinking about this for a moment:

- Someone *selling* Bitcoin is supplying Bitcoin, and thus *demanding* dollars.
- Someone *buying* Bitcoin is demanding Bitcoin, and thus *supplying* dollars.

The supply of Bitcoin always equals the supply of dollars at a given moment and results in a corresponding price. If 900 bitcoin are sold in a day, and 45,000,000 USD are sold, then the average weighted price for the day would be $50,000 USD per bitcoin.

Demand for Bitcoin comes from:

1) **Bitcoiners selling dollars** (for good) to receive Bitcoin in return. Bitcoin, which is destined to be HODL'd for a very long time.

Note: Any portion of Bitcoin bought, but intended to be sold at a higher price, is not considered true Bitcoin demand. That is trading demand, which will be discussed later. Note also, that if the price is going up, and Bitcoiners as a whole are not increasing the amount of USD being 'renounced', then demand from Bitcoiners (for Bitcoin) actually falls. As the price goes up, new dollar supply must come in to maintain the higher price.

2) **Miners not selling**. A miner that produces Bitcoin is actually BUYING Bitcoin. Why?

Because they pay for that Bitcoin with equipment and electricity and other mining overheads. There is an **unforgeable costliness** that is associated with mining Bitcoin. That cost, in USD, is a supply of USD, which takes Bitcoin off the market. It is some quantity of Bitcoin (coming from the 900 per day produced) that doesn't get sold to the market – this is considered Bitcoin purchased from capital and electricity expenditure.

Yes, it is below market price, and a purist might want to consider a modifying factor to account for this. However, there is no need here; I am simply providing an overall picture of how to think about Bitcoin supply and demand. You can now see why all mined Bitcoin must be considered as part of the supply side, in order that unsold mined-Bitcoin can be included on the demand side.

3) **Traders not trading Bitcoin, but HODL'ing**. A trader who buys Bitcoin with the intention of selling at a higher price may decide to keep a portion and never sell. Particularly, when the market turns down and they instead prefer to hold on to this, (in their terms) 'bad investment'. At this point, they may begin learning what Bitcoin actually represents and suddenly become transformed into a dedicated Bitcoin HODLer.

TRADERS

Why is it that traders don't contribute to Bitcoin's supply or demand? Because, if we look across a long enough time period (longer than a typical trade) there is no net effect.

For example, if I am a trader, and I buy 6.15 bitcoin in January and sell it in February at twice the price I bought it for, then, there has been no change to the supply of bitcoin to the market over that month. I would have contributed a little to the price going up when buying, and contributed to it going back down a similar amount when I sold. However, the net effect is that I contribute only noise, or rather some volatility in the price. But, no absolute change overall.

I also took dollars out of the system, because I made a profit. How that contributes depends on who lost that money. If it was another trader, then there is no effect on Bitcoin's overall supply and demand, because those dollars were not destined to buy Bitcoin for HODLing purposes.

However, if a Bitcoiner who accumulates lost dollars, that would result in lower bitcoin demand (lower USD supply). Bitcoiners don't have to be trading to lose dollars. With the higher price, their regular purchases would have netted them fewer bitcoin, and so the demand for Bitcoin would be reduced a little.

Viewed as a whole, some traders make money while other traders lose money, and so there would be no significant dollar profit and loss to significantly impact Bitcoin supply and demand.

Withdrawing

It is worth noting that any Bitcoin bought for HODLing may not contribute 100% to demand if it is kept on exchange. It is unknown just how much fractional reserve exchanges keep; it may not necessarily be one to one, in which case there is potential for an unknown and inflated supply of Bitcoin IOUs.

Futures markets

Any person that buys a futures contract for Bitcoin, settled in cash, is not demanding Bitcoin, and not contributing to the price increase of Bitcoin over the long term. Instead, they are acting as a trader and will only produce noise in the overall price action over the particular period that they are active within the trade.

Supplementary Notes on Price

What happens when supply is equal to demand? This results in a steady price over time.

What if there is not enough supply? There is never "not enough supply", simply because price adjusts until supply is sufficient.

For example, if there is a shortage of Bitcoin at 50k, then the price will increase until people are incentivized enough to sell. There will come a point where no amount of USD will entice a single person to give up a single sat – at this point, the dollar would be considered dead and hyperbitcoinisation will have been reached. 🎉

Tips:

Static Lightning Address: **dandysack84@walletofsatoshi.com**

Won’t Governments Just Ban Bitcoin?

[Norwegian](#)

“What if the government bans Bitcoin?” has been a common concern raised by newcomers for years. It’s time we address this once and for all.

Published in Bitcoinreserve.com 26 April 2022

If you think about it, acknowledging that Bitcoin will be banned by governments is acknowledging that Bitcoin is a threat to the status quo – and to be a threat, that means it must be a credible alternative to the current monetary system. That’s a step in the right direction for someone who may have been sceptical previously.

Because Bitcoin is SO good, yes, governments are likely to see it as a threat and some may, and have, tried to ban it. I won’t ask you to believe I know what will happen. Instead, I’ll explore the possibilities and play out what *could* happen, hypothetically, and cover all options, and you can decide for yourself what’s realistic.

How might governments respond to Bitcoin?

There are 3 possibilities which I'll explore in turn.

1. Governments can try to ban Bitcoin
2. Governments may try to attack and kill Bitcoin
3. Governments may embrace Bitcoin

1. Governments can try to ban Bitcoin

A ban by government comes in two forms:

1. Isolated bans around the world
2. A coordinated ban by the majority of the world's governments

The former is easy to deal with – any government that bans Bitcoin is actually banning itself from Bitcoin. If, as expected, Bitcoin becomes the dominant money of the world, the country(ies) that ban Bitcoin will fall behind, and not benefit from sound money. The wealth of these nations will suffer, hurting them in international trade. It certainly won't hurt how Bitcoin functions and its adoption by those who seek freedom money, although it would temporarily hurt the price of Bitcoin.

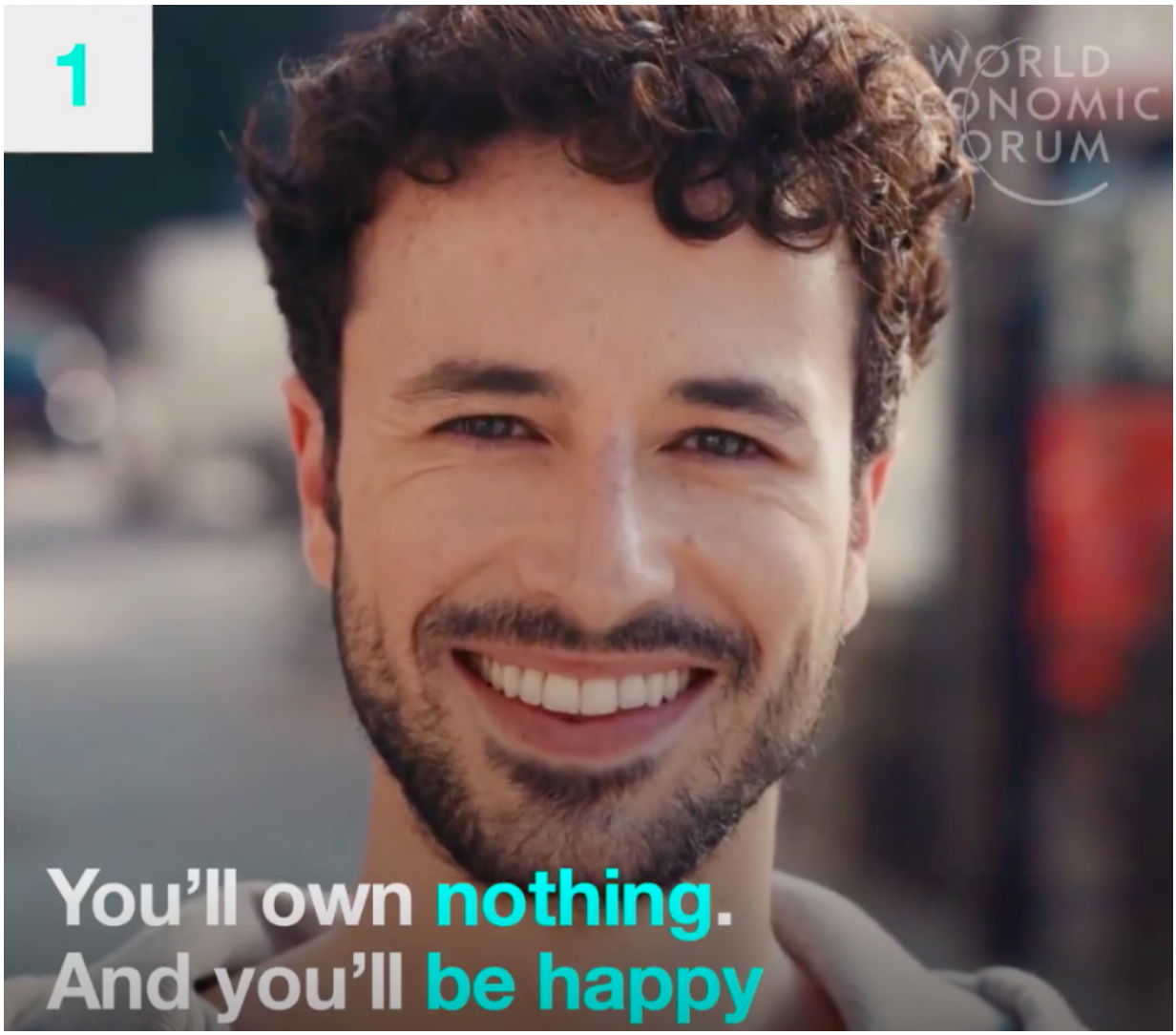
It should also be noted just how ineffective government bans are on things that are demanded by its citizens. Consider how effective the bans on alcohol, drugs, bibles, and certain movies have been.

The latter possibility (a coordinated ban) is actually something serious and worth considering more deeply. Imagine a world where most governments are coordinating in such a way that they conspire to limit the freedom of the citizens that elected them. Is this a world you would want? If we are on track for this type of coordinated authoritarianism, wouldn't we want to resist? Is there anything at all that allows us to resist such an infringement of our rights? Yes, it's Bitcoin…

The only thing that can stop worldwide coordinated authoritarianism is Bitcoin, and the only thing that can stop Bitcoin is worldwide coordinated authoritarianism.

You don't know who would win this battle with any certainty. Neither do I. But this weapon, Bitcoin, was created to fight EXACTLY this. Abandoning the only weapon we have to resist is like entering a knife-fight, and throwing away your knife because your opponent might win. Also, if we lose this battle, the rulers of

the world will own everything, and the people, us, we will own nothing. If we are destined to own nothing, what is the harm in buying bitcoin and trying to resist?



It ultimately comes down to this:
Do you want to fight for your freedom, or do you prefer the safety of being oppressed?

What happens though, if this particular coordinated attack is carried out? Does Bitcoin die? I would argue, even then, it's highly unlikely that Bitcoiners, passionate lovers of freedom, would give up. Bitcoin would move underground, the fiat conversion rate would be hurt, but a black market would develop. The fact that governments (which by then are possibly making everyone's life hell) went out of their way to ban Bitcoin, is likely to make people seek out Bitcoin. In this world, we will say, "thank God we have Bitcoin".

2. Governments may try to attack and kill Bitcoin

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

Attack the blockchain data?

Simple attacks like that just won't work because Bitcoin is truly decentralised. For example, to destroy Bitcoin, every single copy of the blockchain would need to be destroyed. The blockchain is data, and there are many copies – both public and hidden. There are thousands of copies (Bitcoin nodes) all over the world. It is simply impossible.

Attack mining?

Governments have already tried to ban mining. Recently in China (previously the largest region mining Bitcoin) banned all Bitcoin mining. Miners obeyed. But they also moved. The ASICs (single purpose powerful computers designed to mine bitcoin) were relocated or sold, and used in other parts of the world. Bitcoin didn't flinch. The network was not disturbed, and several months later, the worldwide hash rate recovered and is now at an all time high.

Governments may also cooperate to ban or coerce miners using an ESG narrative. Even if this is successful and deters big companies from mining, that allows smaller players to be profitable (a result of the Bitcoin difficulty-adjustment embedded in the protocol). Perhaps if there is extreme impairment of big players, people at home may be able to mine profitably. To be secure, there is no known "minimum worldwide hash rate" – it's quite possible for Bitcoin to be secure enough with only 10% of its current hash rate.

Governments may cooperate to incentivise miners in such a way to make mining only possible for big companies (market intervention to give selected companies an unfair advantage), and then force those companies to censor transactions. If this is actually successful, censorship of some transactions will hurt, but doesn't kill Bitcoin, and doesn't give any government control of the monetary system (The reason Bitcoin was created). Transaction censoring is also highly unlikely, because those miners not under influence will still take on the "censored" transactions and include them in the blocks they win. The users who are censored will have to wait longer to get on the blockchain, so really it's more a nuisance for them rather than censorship.

A 51% attack has been discussed as well. This is where a government, theoretically with limitless resources, accumulates 51% of the hash power of the world. Assuming this is realistic for a moment, what can they do? They certainly

would cause havoc, but would not kill Bitcoin. Their ability to censor or delay transactions is increased. Their ability to rewrite some blocks is also increased. They would also be able to engage in a DDoS attack (distributed denial of service attack), where they would mine empty blocks and re-write blocks by competitive miners that do try to include everyone's transactions. Because they have the majority of the network, and earning Bitcoin is not an incentive, they can afford to do this. This is actually a HIGHLY expensive attack, and the preparation of this attack is not something that is easy to hide – a nation accumulating that much hash power is going to be noticed. Bitcoiners are not simply going to give up. Bitcoin is antifragile. It is code, and will get stronger. It is possible that the developers could release a patch and make all the effort from this attack worthless. I don't need to speculate what that patch would be, and I won't deny that it would hurt Bitcoin to have to do this, but merely the threat that there is such a defence, deters the attack from ever being undertaken.

Attack developers?

Bitcoin is already functioning well enough, so threatening the developers will not kill it. In addition, developers are smart enough to successfully go dark, use pseudonyms, and continue to work.

Attack users?

Governments could attempt to seize bitcoin from their citizens, just like FDR's Executive Order 6102. This would be incredibly unpopular, and unlikely, but FDR did exactly that with gold. The difference with Bitcoin is subtle. In 1932, if people and companies did not hand in their gold, that component of their wealth would be excluded from the payment rails of the local and international banking system. People wouldn't be able to transact with their gold unless it was face-to-face. This was a weakness of gold which eventually led to fiat money not backed by gold.

Bitcoin users do not have this problem. If their bitcoin was excluded from the banking system (ie they were unable to electronically sell their bitcoin for fiat), that wouldn't be so damaging, because bitcoin can be sent peer to peer, instantly, ALL OVER THE WORLD. Bitcoin doesn't need the banks – it replaces the banks. So, if such an executive order came to pass, Bitcoiners would more effectively resist than gold holders in 1932.

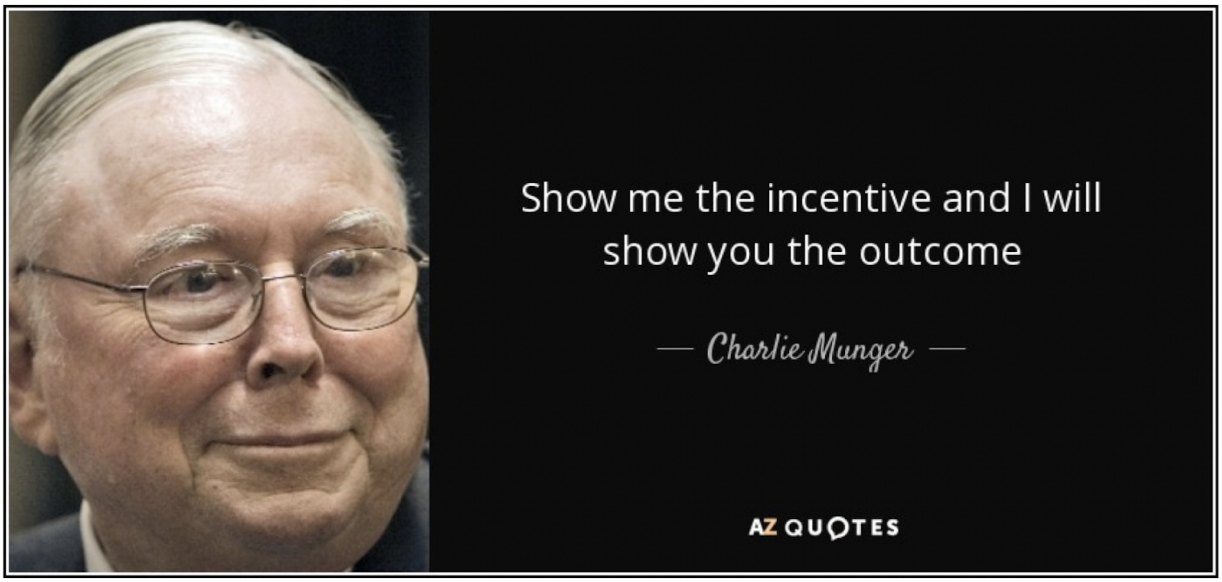
Do not forget also that if many Bitcoiners do give up their bitcoin to government, that hurts those people, not Bitcoin; Bitcoin still survives, and those that kept their bitcoin keep their wealth.

Attack custodial services?

It's quite realistic that governments may seize the bitcoin held by exchanges or major companies – "for national security", for example. Anyone who keeps their coins on the exchange would have then "donated" their bitcoin. This is particularly a risk as the price of Bitcoin continues to rise, and fiat currencies hyperinflate. This doesn't kill or hurt Bitcoin, in the same way that a bank robber successfully robbing a bank doesn't hurt the dollar.

3. Governments may embrace Bitcoin

The smartest approach; whichever nation leads the way will benefit the most. This is probably the most likely scenario if considering incentives.



The more that various nations adopt Bitcoin, the lower the chance that they will all cooperate to conduct a *coordinated* attack on Bitcoin (Bitcoin's biggest threat).

One nation has already thrown its hat into the ring, El Salvador. In 2021, President Bukele made Bitcoin legal tender in the country, alongside the dollar. While this is not the same as a nation accumulating bitcoin, the move was associated with a bitcoin accumulation strategy.

At the time of writing, three further announcements were made at the Bitcoin Miami Conference:

1. Madeira (an autonomous region of Portugal) will be welcoming Bitcoiners with tax exemptions on bitcoin payments. It initially seemed like this was a legal tender announcement, although that was not the case.

2. Prospera (a special economic zone of Honduras) is adopting Bitcoin as legal tender.
3. Senator Indira Kempis, will be introducing a bill to give Bitcoin legal tender status in Mexico.

In addition to entire nations adopting Bitcoin, other important developments to take note of are politicians that publicly support Bitcoin, or are known to own bitcoin. The more politicians that do this, the more likely it is that the nation will embrace Bitcoin, or at least, the less likely it will attack Bitcoin.

Some examples are:

- Senator Cynthia Lummis (Wyoming, USA)
- Jane Hume (Australia's minister for financial services)
- Indira Kempis (Mexican Senator)
- Pavel Nikolayevich Zavalny (Chairman of the State Duma, Russia, **accepting bitcoin payments for oil and gas**)
- Andew Yang (US presidential candidate)
- Francis Suarez (Miami Mayor)
- Pierre Poilievre (Canadian member of Parliament)

There may be nations *quietly* accumulating bitcoin as well. Given that it is competitive, it's in a nation's interest to acquire bitcoin without alerting the world, so they may continue to purchase/mine at a low cost.

Bitcoin may be acquired by nations in a few different ways:

1. Force – confiscations from exchanges, companies, and citizens.
2. Purchasing – either with reserves or printing money
3. Mining – equipment may be confiscated or purchased.

Force

The first option is the most effective way to get the most possible bitcoin quickly, and I expect some nations will do this. Note – it does not kill Bitcoin. Just because an entity maliciously acquires bitcoin, does not mean that it destroys the money.

Purchasing

I also expect purchasing in the open market to happen to some degree. Governments that do this by printing money will eventually destroy their own

currency, but in return, will have more bitcoin for the next monetary period. The people that will suffer are:

1. Those that adopt Bitcoin last
2. Those that sell their bitcoin to the government (whatever the price)
3. Those that continue to invest in fiat-based assets
4. Those that hold fiat for savings
5. Those with retirement entitlements

Mining

Mining by governments is a slow burn. It's an honest way to earn bitcoin, helps the network by making it more secure, and if done by many different nations, distributes the mining hash power, making it more difficult for one actor to get 51% of the total.

The problem with acquiring bitcoin through mining is that it is very competitive, takes time, and there are only 2 million bitcoin left to be mined. A nation that has, say 10% of the mining power of the world will earn 10% of the block reward on average. Currently, 900 bitcoin are mined per day, and so this nation would earn 90 bitcoin per day.

The 2 million bitcoin figure is a calculated and predetermined number. It's the issuance of new bitcoin over the next 100 years, but most of those 2 million bitcoin are created over the next 12 years. It's game on for those last 2 million bitcoin. It is MUCH harder to acquire 2 million bitcoin through purchasing on the open market, because MOST of the bitcoin are not for sale, at any fiat price. Many Bitcoiners are holding until the day fiat dies, including myself.

Summary

In summary, I do think governments will come for Bitcoin, either to hurt it, or to get more. Whatever they do, Bitcoin is going to be fine. **YOU** may not be though. Get your coins off exchanges and learn how to do this, to protect yourself. Ask for help or learn online. Visit my website (armantheparman.com) which is dedicated to teaching people how to hold their own coins. Don't leave them in a giant honeypot for your government to take in one swoop. Make them come after each person, one by one. Make it difficult.

Tips:

Static Lightning Address: **dandysack84@walletofsatoshi.com**

"Bitcoin is too volatile!"

[Norwegian](#)

"Bitcoin is too volatile" is not a legitimate criticism of Bitcoin. Here's why.

[Published with Bitcoinreserve.com 24th May 2022](#)

It's certainly true that the fiat price of Bitcoin, especially recently, is volatile. But, I object to the word "too" in the title.

"Bitcoin is volatile" – yes. "Bitcoin is too volatile" – no. Allow me to explain.

Bitcoin is not money yet, so expecting volatility to be low is illogical.

You will hear Bitcoiners say, "1 bitcoin = 1 bitcoin", which is an objection to the comparison of Bitcoin's value to USD's value. I'm a Bitcoiner, and I'm on the 'Bitcoin-haters' side with this specific point, although it's fun to join in with the memes – and I do. It's not meant to be taken too seriously and focusing on fighting that meme is not useful.

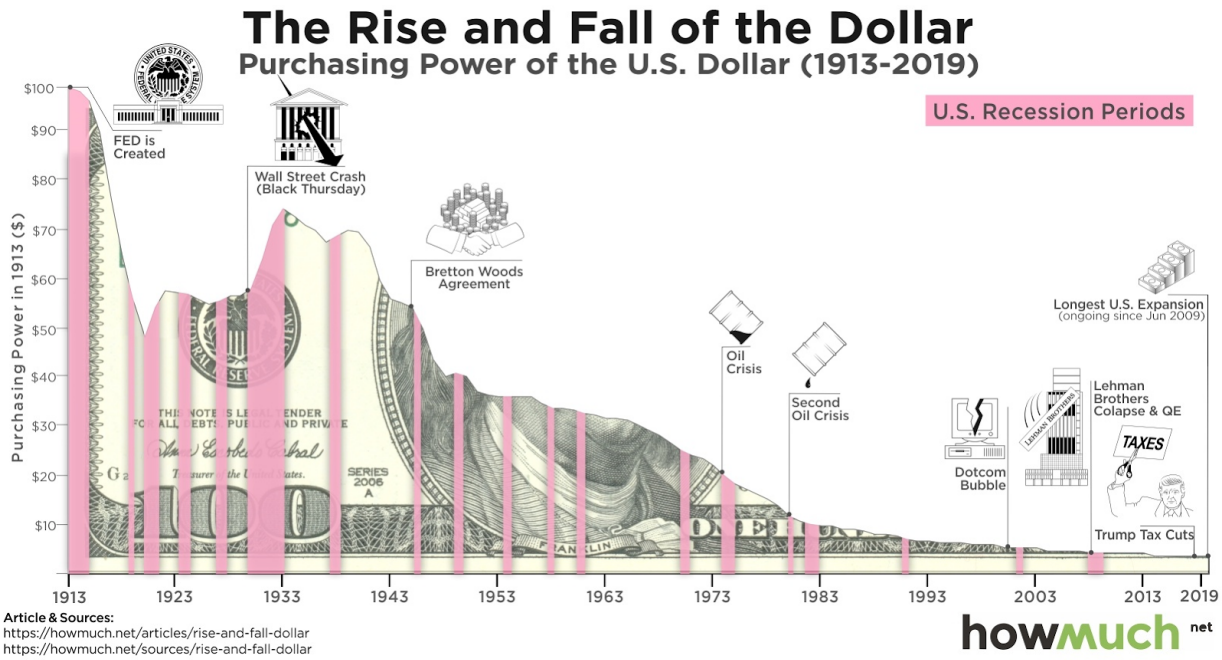
The volatility of Bitcoin is a problem particularly if you hold the position that Bitcoin is already good money. This is the crux of the issue: Is Bitcoin good money? Logically, good money not only needs to have good TECHNICAL properties (scarcity, divisibility, recognisability, portability etc), but also good

SOCIAL properties; ie, a strong network of people that use it as money to trade goods and services with each other. *(To see more on this, read Appendix A, taken from my article, **Bitcoin has no intrinsic value: Debunked**.)*

Even if a money has nearly perfected the technical properties, but has no network effect (a social property), it is still poor money. Why? Because the purpose of money is to use it in trade to overcome barter. If the people you trade with don't use the money, it's poor money, no matter how good its technical properties are.

Conversely, a money that has horrible technical properties, but is still widely used (eg USD), is poor money. One might argue it can't be poor money if many people choose to use it. That *would* be true, except that people don't *choose* to use USD, they are forced to use it. Why that is, is a whole other discussion I won't go into now, but I will say this:

USD is poor money. It is controlled by The Federal Reserve (not federal, and not a reserve; it is a privately owned institution), and they create USD out of nothing. There is no cost to producing more (they certainly don't work for it), and in doing so, they steal from: A) everyone storing their value/time/labour/energy in it or B) those who have negotiated contracts or wages in it. The purchasing power has declined by 99% since The Federal Reserve began.



If money that everyone uses is making everyone poorer, then I would argue that that is sufficient to label it as poor money. Money, by overcoming barter, makes humanity prosperous. USD is doing the opposite; it is holding humanity back.

Expecting Bitcoin to be good money right now is unreasonable.

I don't want to get caught up on good vs bad money. I mentioned it because one could argue that Bitcoin is not effective at being money now (volatility among other reasons), and therefore it is not money. But, that is dismissing the fact that Bitcoin is BECOMING money, and has all the technical properties NOW to be money – it just requires time to gain the social properties.

Bitcoin is an incredible discovery because it allows, for the first time in human history, a digital money not issued by a central authority and not controlled or changeable by any one person or group. That alone is quite remarkable, but in addition to this, it grew from grassroots sources, developed a massive decentralised network and can no longer be eradicated by forces that intend to maintain control of the world's money supply.

To not be grateful for this, and to demand that the world should be *using* Bitcoin as money now, otherwise it is useless, is intellectually dishonest or grossly ignorant. It's wrong to not allow Bitcoin to evolve into money over time. It's wrong to expect it to be money immediately.

Any money of the free market (ie not forced to be valued by government – fiat money) evolves naturally in a general process listed below (explained nicely by Vijay Boyapati's excellent piece, **The Bullish Case for Bitcoin**):

1. Collectible
2. Store of value (SoV)
3. Medium of exchange (MoE)
4. Unit of Account (UoA)

While there can be some overlap, for example, something that is stored may be exchanged, the flow is generally from steps 1 to 4. If people hold a unit for its SoV, it will inevitably be used a little as a MoE in a barter society. The MoE usage then increases the SoV properties of the unit, which increases the MoE properties, and so on, in a positive feedback loop towards monetary evolution from barter, and UoA ascendency.

Any money developing from the free market necessarily will be volatile.

When gold was discovered as money, it too was volatile! It too was risky to accept as payment because its value depended on other people accepting it as payment. That's just how free-market money starts. It takes time to develop. If only we could go back in time to the evolving stages of gold as money, and tell

our ancestors to accumulate it before anyone else knew it would be money, so that we may today reap the benefits in the present. Well, here we are today, in the middle of a new money being discovered, and people are rejecting it because it is too volatile to be used as money today – do we really need our descendants to time travel back to now, and tell us what to do?

Compare this monetary evolution of gold with fiat money. Governments started fiat money by making it backed by gold (a money of the free market). The gold backing was slowly weaned off. We can now consider USD to no longer be a currency (a unit backed by money), but to be money (poor money). Every new currency created out of thin air by a government (the Euro is a good recent example) started by pegging it to some other money. This eliminated its volatility.

But, if a new money was created out of nothing, and without any pegging, no one would know how to value it. It would be volatile, and probably close to worthless initially, as it would have to develop a network effect just like Bitcoin is doing. Bitcoin started as virtually worthless (it cost a minuscule amount of electricity to mine it initially), and has developed a network effect reflected in the steady growth of its price.

If you wanted to have an objection to Bitcoin, it would be more reasonable to say that you don't expect it to keep growing and evolving into fully adopted money, not that the process of it getting there results in price volatility!

Price volatility does not reflect the progress of Bitcoin adoption.

Bitcoin is only 13 years old, and the network of people adopting it is growing daily. The price (and its volatility) is not a good indication of this.

Some argue that as more people adopt Bitcoin, the volatility will drop. But this is not obviously true. It may be that the volatility increases strongly upwards, particularly if the measuring unit, USD, is dying/hyperinflating, and people are rushing to Bitcoin – The volatility of Bitcoin will skyrocket. But, when it is adopted (meaning when nearly everyone would accept it as payment, or work for it), there will be no other money to measure it against; it will be a unit of account (UoA).

Instead of looking at volatility to assess Bitcoin adoption, consider this:

There are two types of Bitcoin adopters.

1. Those that understand that price volatility does not matter, and see Bitcoin adoption as inevitable. They regularly accumulate bitcoin, or they bought plenty early on and are satisfied with their holdings – they rarely sell any.
2. Those that buy and sell bitcoin as they are not sure about Bitcoin's future. They use short-term price as an indicator of Bitcoin being adopted as money.

If you use both of these types of people in your assessment of Bitcoin adoption, then you will be misled.

Type 1 Bitcoiners

Focus only on type 1 to assess Bitcoin adoption, and notice that this is the foundation. By definition, people with this view are not shaken easily from it. They are well-informed and educated, and it may be argued that they are fervently ideological, but it is not blind faith that drives them – instead, it is the desire for a fair money, and not to be ruled, cheated, or stolen from by those with the monopoly on violence (the state). Bitcoin is the only thing that offers this and once you see it, you don't decide to opt for the slave master's tokens for the work you do, or opt for some altcoin whose monetary policy is heavily influenced by a nerdy computer programmer.

Let's not forget that Ethereum (a supposed "alternative" to Bitcoin) was pre-mined by 70%, meaning Vitalik and a few other founders awarded themselves 70% of the total "monetary" supply. What's more, the coin's foundation has been infiltrated by the marxist organsiation, World Economic Forum. Who knows what influence they had over the leader of this money? No one who ideologically wants a fair/ethical and open monetary system that is not under any powerful control would adopt such a thing; the only available option to them is Bitcoin.

These type 1 Bitcoiners, passionate about fairness to the benefit of all humanity (and yes, benefit to themselves too of course) educate others (as I do), and this results in more and more type 1 Bitcoiners in existence over time. Their growth ultimately leads to Bitcoin's success, in a self-fulfilling prophecy – they are the people who you can reliably sell your bitcoin too, which increases the salability of the economic unit; this is how money evolves. The more reliably that you can sell your bitcoin, the more confident you can be to accept it as payment.

Type 1 Bitcoiners are not reflected in the day-to-day price action as they are not participating significantly in the market. Their influence, however, is reflected in the general long-term trend of price (the higher lows); and that is obviously increasing. (**For more information on how Bitcoin's price works, see here**).

Type 2 Bitcoiners

Type 2 Bitcoiners (and people trading/gambling on the token) emotionally respond to the price and make it volatile. They grow in numbers, but they also run away. Their numbers and conviction over time are unknown, and contribute to the price volatility. They also outnumber type 1 Bitcoiners for now, most likely.

Another way to put it is that price represents the marginal buyer and seller's opinions, who generally are people trading bitcoin, not truly adopting it. Bitcoin is designed to be money, a savings mechanism, not a token to buy and sell for fiat profits. Although it is possible to trade it, and the vast majority of buying and selling is gambling, this does not contribute to Bitcoin adoption directly. If a person buys bitcoin with the intention of selling it at a higher price, that does not contribute to demand. Over time, that person contributes net-zero to adoption, and in the process makes the price more volatile.

It is very important to appreciate that just about all "altcoiners" are almost no different to Type 2 Bitcoiners – the only difference is their choice of cryptocurrency. If you can see from my explanation why type 2 Bitcoiners are not going to help Bitcoin adoption, then pause a moment and examine if you can see a related major weakness in altcoins. This is only one flaw of many.

How else does a free-market money evolve?

If a new economic unit came into existence, and over time, without the assistance of government or central authority, is destined to overcome all obstacles and dominate the entire world as its preferred money and unit of account – *what would that look like at the start? Would its price be volatile?*

Absolutely it would be volatile. It certainly can't be stable, it isn't money and not everyone values it to be so at the start, and not everyone will accept it as payment.

This hypothetical example describes BITCOIN. The point to debate is not its current volatility, but whether it is destined to be the world's money in the future. The volatility at the start is not an indication one way or the other if it will succeed, so please, stop mentioning it as a criticism.

Conclusion

To summarise, Bitcoin is volatile, but necessarily so because it is a free-market money that is in the early stages of adoption. It can't be any other way. Only a

money by decree (fiat) can be non-volatile to begin with, and even then it is because it is pegged by the government (with an IOU) to stable money (gold). New money arising from nowhere with no pegging is GOING to be volatile!

Appendix A – What are the Good Properties of Money?

The properties of money can be divided into two major components:

Technical Properties

Traditional:

Durable

Portable

Divisible

Fungible

Recognisable

Transferable

Hard (difficult to produce more of; vs "easy")

Inexpensive and easy to secure/store

Newly appreciated:

Digital

Borderless (can send internationally without hindrance)

Unstoppable by governments

Resistant to confiscation

Resistant to censorship

Neutral (anyone can use it without permission)

Open-source (the technology is not secret and not owned by anyone; no patents)

Antifragile and adaptable

Resistant to unwelcome changes

Social Properties

The number of people using it *(Metcalfe's Law: the value of a communications network is proportional to the square of the number of its users)*

Fair (created without a pre-mine – ie the founders did not enrich themselves)

No central control

Sufficiently distributed with a tendency to further distribute (note: even distribution is impossible to begin with)

Tips:

Static Lightning Address: **dandysack84@walletofsatoshi.com**

Bitcoin has no intrinsic value: Debunked

Norwegian Italian

A logical rebuttal to one of the most common misconceptions about Bitcoin.

Published with Bitcoinreserve.com 26 April 2022

Audio by @DelioPera

0:00 / 39:32

This is a very, very common objection to Bitcoin, and I will attempt to thoroughly debunk this criticism here.

People might mean different things when they say Bitcoin has no intrinsic value. Some may be uncomfortable that they can't touch it, and conclude that they can't trust it. Some may have an issue that it has no utility other than money, and then usually conclude from this that Bitcoin must be a Ponzi. There are intellectuals also, that cite Mises' regression theorem, and Aristotle's properties of money – they are wrong too.

In this piece, I will start by defining and dismissing the literal meaning of "intrinsic" value, then go on to address the underlying criticisms – lack of "utility", and no "backing".

I will then address the rarer concerns of Bitcoin supposedly not satisfying Mises's Regression Theorem, nor Aristotle's properties of money.

I've included an appendix that describes the properties that make good money in the modern interconnected world (spoiler alert – Bitcoin excels). There are also sections discussing how gold eventually failed as money (and why mining cost does not support its price), and another on fiat money.

Debunking the literal meaning of "intrinsic value"

We must start with some definitions so the following arguments can be meaningful.

Value: Value is something that a human appreciates as being favourable to him/her in some way. We sometimes can put a number to it (using money), to help us rank the things we value.

Intrinsic: Intrinsic, in this context, refers to a property outside of the human mind. It comes from within the object itself, and not our opinion.

Intrinsic Value: This means that something is valuable regardless of what the human thinks. The value is from the object, not our assessment of it.

Basically, intrinsic value is a nonsense term that expresses: "This is valuable to a human whether the human values it or not."

Can you see the problem? Carefully read it again if not.
A hypothetical rebuttal: One might argue (incorrectly) that water has *intrinsic value* because it sustains life. But that assumes that every human at any moment in time prefers to remain alive. Many do, but just one exception breaks the claim that water has intrinsic value. There is nothing in the universe that *every* human will *always* value, therefore *nothing* has INTRINSIC value.

Beyond Semantics

This definition of intrinsic value, and the logical proof that *nothing* has intrinsic value, should by itself be enough to debunk the criticism that "Bitcoin has no intrinsic value" – But no, that is only debating the semantics. What people really *mean* when they say "no intrinsic value", is that Bitcoin has no value

other than for its properties as money. It has no other use, or no "utility", other than money. They believe money must have some alternative use to give it "backing". I will address both in turn:

1. Utility

I feel I must also debunk the improved (yet inadequate) version of the original criticism, and state it this way: "Bitcoin has no utility".

To this, I say: "Yes, there is no utility other than for being money – and that's fine!" This is because money does not need to be anything besides money – In the same way that a TV does not also need to be an air-conditioner! Historically, money has always had utility, but that's only because pure money (Bitcoin) hadn't been invented.

Does utility really assist in an item becoming monetised?

Let's look at aluminium. It has many uses. It takes energy to produce. It has *some* good monetary properties. But it's not money and never will be. That's not to say it doesn't have value; it has *utility* value, but not monetary. Possibly the biggest monetary weakness is its abundance. The same can be said for many other useful metals or commodities.

Let's try salt. Salt *used* to be money. Its utility helped it gain monetary status, but it failed as money because of its poor monetary properties, and a superior competitor displaced it.

Now let's look at gold. Gold has excellent monetary properties (but no longer good enough, see Appendix B) and it evolved from a societal state of barter into the dominant money for humanity. It has reigned worldwide for a long time, until it failed as money and allowed the development of fiat money, which overcame some of gold's weaknesses but introduced many new problems. But gold also has many industrial uses and interesting physical properties. If you study how money evolves from barter, you'd learn that *utility* is a prerequisite to triggering the initial stages.

Briefly, monetary evolution from barter happens as follows:

Many people will value an item for its *utility*. If it is durable, then it may be stored or collected by many people in that economy. This leads to the good becoming a *store of value* (initially just the value for its utility, but during the next phase a monetary premium grows). This is really important. A durable

item begins with a store-of-value component, its utility value. Without some value to begin with, storage of the item never becomes commonplace.

Once commonly held, it is then able to be *exchanged* for other goods and services (develops as a *medium of exchange*) in order to overcome the difficulties in trade that barter poses – this allows the economy to grow. This facilitation of trade increases the store-of-value premium of the item over and above the utility-value. Then this leads to more people storing it. A positive feedback loop results, until the utility-value pales in comparison to the much larger premium-value.

The final stage of the evolution of money is when goods and services are priced in the new money (*unit of account*). This is well described (I recommend **Vijay Boyapati's, The Bullish Case For Bitcoin**), so I am not discovering anything new, just summarising. It is also worth noting that this describes a free-market money, not one that is forced on people by governments, i.e. fiat money (more on that later).

Back to gold

If you look at gold's price now of around $2000 per ounce, it's not difficult to appreciate that the vast majority of this price is composed of a monetary premium, above an unknown industrial (or utility) value. Perhaps the true industrial value is $50 or $100 per ounce? We can't precisely calculate it. But consider this – is this approximate $100 per ounce of value really "backing" gold as money? I would say "no", because a failure of gold as money would leave the investor holding a useful metal worth approximately $100 per ounce, in the red by $1900 per ounce – hardly any compensation for making a mistake in choosing the wrong money.

If it's not compensation for being wrong, then is it really a "backing"? No. What's more, if gold is abandoned by the world as money, tonnes and tonnes of yellow metal held in central banks will flood the markets and eventually be bought by industry, further reducing the price of gold. Gold would also lose much of its desire as jewellery. I'm not suggesting this is going to happen any time soon, but I do think it will happen gradually over many years as Bitcoin continues to absorb more and more of the world's desire to store value. You don't need to accept this to understand the broader argument about utility.

If you believe gold's *cost* to mine "backs" its price, that is debunked as well in Appendix D.

To summarise the point on utility

Utility can help an item become money in the early stages of its evolution, but it is no longer required after that. A commodity that is poor as money has no additional monetary value from having a high utility value. And if gold magically lost all its industrial properties (it's hypothetical, just bear with me) and kept its good monetary properties, it would still be money, no better, no worse.

So whether a money has some residual utility or none, makes no difference to its suitability and sustainability as money.

2. "Bitcoin is not backed"

Some people might mean when saying, "Bitcoin has no intrinsic value", that Bitcoin is not backed by anything. They may also believe that gold is backed by its physical properties and that the US dollar is backed by the government, the economy, the US military, or oil.

There may also be a misunderstanding of what "backed" means. It's a similar thought process to believing money's alternative "utility" supports its value – it doesn't, as explained earlier.

The following might sound startling at first:

Money is not backed by ANYTHING.

That's right. Money has no backing – it's just valuable *as money*. What does have backing, is *currency,* by definition:

Currency is a unit that is backed by money, and used as money, in place of money.

The US dollar used to be backed by the promise of gold. In this arrangement, a currency (USD), was backed by money (gold). When the dollar was a currency, it needed the "full faith and credit of the United States Government" – Faith that you'll get your gold with the piece of paper in your hand.

Once USD was no longer pegged to gold, since Nixon's "temporary" cessation of USD's convertibility to gold in 1971, USD became unbacked, and so, was transformed from currency to *money*, albeit a very poor money. "The full faith and credit" statement is now nonsense because the US already defaulted.

As I discussed earlier, gold has no *backing* either. It has a utility value (small), and a monetary value (majority). The utility value together with the monetary

value makes up the total value. Gold's utility backs its utility value, but nothing backs the monetary value apart from the fact that it is believed to be good money. If that belief disappears, there is no compensation to the gold investor apart from some utility, and hence, no backing. At best, you can say it is insignificantly backed by its utility value (although I'll disagree with the terminology).

Really? Backed by NOTHING?

It will make more sense if you think of money as a LANGUAGE, something that communicates the value of goods and services. *Money is the language of value.*

Let's compare to another language – English; *the language of meaning*.

Ultimately, English is a collection of symbols (the alphabet), sounds (speech), and rules (words, grammar), which together form English and are used to communicate *meaning*. Nothing backs the English language. There is no "intrinsic meaning" in the symbols, rules, or speech. Even if you find some intrinsic meaning through some technicality, it doesn't matter – the point is that nothing intrinsic is needed, and is not "backing" the language.

So, what gives the English language meaning, or value? The fact that it has good enough properties as a language, AND, the fact that there is a large network of people USING it. Once a large network of people use the language together, they all benefit; i.e. they all gain value from using it. If a better language comes along, they do not abandon the language and switch to another, because anyone who does so leaves the valuable network. They must take everyone with them to the new language for the incumbent language to be abandoned. The same is true for money.

If you are the only person in the world who speaks a language, no matter how good the language is, the language is useless to communicate meaning. If you are the only person in the world who uses a particular money, no matter how good the money is, the money is useless to communicate value. It is either worthless, or has utility value only – or in debunked terminology, "intrinsic value" only.

An important nuance here is that for a language of meaning, a person can adopt more than one, and so learning a new language does not mean they abandon the one they know. But for money, every unit of value can ONLY exist in one form. For example, an ounce of gold cannot be stored in Bitcoin as well as gold. One must choose, and in doing so, that unit of value abandons one for the other. This "forced" choice is a major reason why a money with sufficiently

favorable technical properties and the lead in the network participants is going to absorb the value from its competitors eventually – because monetary network participants must make a choice – people will tend to opt for the best choice when storing their wealth.

Now switch back to thinking about gold as money. Why does gold have monetary value? It's because gold was:

1. Good enough to function as money (and was the best)
2. Developed an increasingly large network of people who valued it as money, and spoke that "language" of value.

Now let's look at Bitcoin:

1. The best technical properties of money humanity has ever seen.
2. In the free market, Bitcoin is the 2nd largest network of people using it as money (2nd to gold, and excludes fiat money because that is by force, not the free market, see Appendix C).

For now, we can't call Bitcoin "good money" – it has the best technical properties of any potential money, but it does not yet have a large enough network of people using it to call it money. This is why it is premature to say "it's too volatile" or "people don't accept bitcoin, it can't function as money". The point is it WILL be money, because the technical properties are not just better than anything else, but VASTLY better. People are gradually abandoning the old network with initially small, then larger portions of their wealth. Bitcoin is evolving as money.

Academic arguments – Regression Theorem

I have heard criticism that Bitcoin does not fulfil Ludwig von Mises's Regression Theorem of money. The theory was first proposed in his 1912 book, The Theory of Money and Credit, and was used to explain away an apparent circular argument of money.

The Theorem is not supposed to be used for an isolated money such as Bitcoin, but why should money have value, generally.

Money of the free market (not fiat), as per the Austrian School of Economics, derives value from the fact that other people value it. But this creates a circular argument:

Why do other people value money? Because other people value it – You can see the circular problem.

Mises was able to explain away this criticism of money by introducing the Regression Theorem. He said that people valued money TODAY, because other people valued it YESTERDAY. And they valued money yesterday because people valued money the day before that… "regressing" all the way back to a point where someone valued money not because of someone else's value appraisal, but value for what it is, or its utility, as a commodity. Thus, the circularity of the argument for money was broken.

To come up with this insight is quite genius. But how does this apply to Bitcoin? It applies partially:

First, think about what makes Bitcoin trade at its current price. The market price of Bitcoin is an indicator of how Bitcoin is collectively valued today. This price is related to the price yesterday. Yesterday's price was related to the price the day before, etc, all the way back to the moment it was first priced – Bitcoin Pizza Day, May 22, 2010. On this day, two pizzas were purchased by poor Lazlo Hanyecz for 10,000 bitcoins, and in doing so, connected the value of Bitcoin to pizza. Pizza's value is connected to dollars, and so, Bitcoin's value was publicly connected to US dollars.

In this way, the regression theorem was partially satisfied, breaking the circular argument until we reach USD. Bitcoin's responsibility to satisfy the regression theory of money ends here, and is passed over to USD.

From Pizza Day, subsequent prices of Bitcoin were related to that price, and other people valued Bitcoin because other people valued it, a natural way that money evolves. The price increased as more people joined in to collect bitcoins, choosing it as their potential future money.

It can be argued that Bitcoin's value (not price) can go back further than Pizza day. People were mining Bitcoin using electricity, and so were choosing to endure this cost to collect bitcoins on their computers. A certain amount of electricity was required to produce bitcoins, and electricity is priced in dollars so bitcoin was loosely related to dollars even before Pizza Day (loosely, because everyone's costs are different).

Exactly what value people saw in mining bitcoins early on is actually irrelevant – what matters is that they chose to do it, at a cost. It is true that the bitcoins they mined could not fulfil any physical need, but they did fulfil a human want – whether it be curiosity, anarchist tendencies or whatever, that is most definitely

related to value. It doesn't matter that it wasn't a physical commodity; it doesn't need to be, to satisfy Mises's Regression Theorem. It was valued, and that is enough.

I have heard people on Bitcoin's side argue that Bitcoin does in fact have intrinsic value because of the network; that Bitcoin allows unconfiscatable, immutable, permissionless payments without a 3rd party – but this argument is not a good rebuttal, because all these properties are dependent on bitcoins having value. The network is useless without bitcoins being valuable, and so a circular argument exists again. The explanation I gave above is the correct one – Bitcoin satisfies the Regression Theorem to USD, and thus, the network's value.

After USD

The regression theorem as far as Bitcoin is concerned goes back to USD. Then the question remains generally for money, "why does it have value?" The answer as to why USD has value is because people valued it yesterday, regressing back to when it was pegged to gold.

Then why should gold have value? Again, we regress backwards in time to when gold was only valued for its utility, to the moments when money arose from barter.

To summarise the Regression Theorem Rebuttal:

Bitcoin regresses back to pizza (or electricity, a commodity), which regresses back to USD. USD regresses back to gold as money, which regresses finally to gold's utility. Therefore gold's commodity value breaks the circular argument for money generally.

Academic arguments – Aristotle's Properties of Money

Aristotle defined the characteristics of good money with 5 properties:

1. Durable
2. Portable
3. Divisible
4. Fungible
5. Intrinsically Valuable – *The value of money should be independent of any other object and useful with inherent value contained in the money itself.*

It *appears* that Bitcoin does not satisfy the 5th criterion. Is Bitcoin really "useful with inherent value contained in the money itself"?

There are three points to make about this.

1. Nowhere does it say HOW "inherently" useful the money needs to be. One could argue that bitcoins are useful in demonstrating a digital network of money as an intellectual exercise to cryptographers. Maybe that's not very useful, but can we say there is ZERO use? And who are we to judge what others must find useful?
2. Aristotle lived in a time when there were no computers. He had no concept of the digital. In the pre-digital era, it seems very reasonable that only a commodity can evolve into money. But if Aristotle were alive today, he'd have the benefit of seeing that digital (non physical) items can have value to people. Perhaps it is true in that era, no physical item could ever have been money without some alternative value. Perhaps it requires the invention of Bitcoin to break this rule. How can Aristotle be expected to have predicted the digital age, and the possibility of Bitcoin?
3. USD is money. It has been functioning seemingly well enough for 50 years. It has no inherent value contained within itself either. It is accepted all over the world where the US government has no authority to enforce its acceptance.

Appendix A – What are the Good Properties of Money?

The properties of money can be divided into two major components:

Technical Properties

Traditional:

Durable

Portable

Divisible

Fungible

Recognisable

Transferable

Hard (difficult to produce more of; vs "easy")

Inexpensive and easy to secure/store

Newly appreciated:

Digital

Borderless (can send internationally without hindrance)

Unstoppable by governments

Resistant to confiscation

Resistant to censorship

Neutral (anyone can use it without permission)

Open-source (the technology is not secret and not owned by anyone; no patents)

Antifragile and adaptable

Resistant to unwelcome changes

Social Properties

The number of people using it *(Metcalfe's Law: the value of a communications network is proportional to the square of the number of its users)*

Fair (created without a pre-mine – ie the founders did not enrich themselves)

No central control

Sufficiently distributed with tendency to further distribute (note: even distribution is impossible to begin with)

Appendix B – What happened to Gold and Why did it Fail?

Gold was great. Humanity flourished with gold as money, because people could save for the future with little concern that their purchasing power would evaporate. Being able to save means you can think about and plan for the future. Not being able to save means you are always thinking about satisfying your needs now, without long term thinking. Great things are built with long term thinking, not short term thinking.

The weakness of gold though is that it is difficult to transport long distances, and difficult to keep safe and store. This led to people keeping gold in banks, which, on its own, is not a problem. Banks provided a valuable service.

However, this allowed banks to issue currency backed by gold: "paper money". Paper money is an easier way to transport value. Also, the records of accounts kept by banks meant that international payments could be made without the need for the movement of gold to make payments. Banks could simply update their ledgers which stated what is owed to who.

Eventually, gold became more and more concentrated in the hands of banks and then central banks. The banks also practised what's called fractional reserve lending, which means they lend out paper money that was not backed fully by gold that they held. Central banks then took over the business of issuing currency backed by gold, and they also created more paper money than was matched by gold supplies.

People were then forced to accept paper money and were forced to hand in their gold to the government in exchange for dollars in 1933 **(See Roosevelt's Executive Order 6102)**. Gold became illegal to use as money (for the public only). It was only used to settle accounts between countries and banks.

The US printed so much money over and above its gold reserves, they began to run out of gold as other nations made more and more claims. Then in 1971, President Nixon "temporarily" suspended the convertibility of the US dollar to gold **(Nixon Shock)**.

Basically, it would no longer meet its obligations to pay gold for US dollars, effectively defaulting. The use of the US dollar was forced on the world though, due to USA's military might and deals they made with Saudi Arabia (The Petro-Dollar). Saudi Arabia, the world's greatest oil producer, agreed to only accept US dollars for oil in exchange for US protection.

To keep the USD as the world reserve currency, gold's price needed to be suppressed artificially by central bankers. This was done through the derivatives market by creating short positions. It is suggested that for every ounce of gold in existence, there exists 100 ounces worth of paper claims; just like a fractional reserve mechanism, artificially inflating the supply of gold to keep its price suppressed. This can go on forever unless people demand physical gold. Because gold is not a well-suited means of international payment and is difficult to store, the demand for holding the physical version of the gold seems not to be sufficiently high enough to break the manipulation.

The history of gold's failure is interesting and I won't say much more as I'm not an expert, but I'm just pointing out that gold failed, which is why we have government fiat money today. If gold was easy to spend across the world, without ever giving it to a bank, then it would not have become centralised.

Appendix C – Fiat money

The explanations about money in this piece relate to money of the free market. Fiat money, or government money, on the other hand, is money that citizens use initially by force. It is illegal to decline a payment made with fiat money, and taxes are required to be paid in the local government money. One must also convert all profits of assets into local fiat denomination and pay tax accordingly. This keeps the fiat money surviving longer, even though it is "easy money" (easy to produce with low or no cost).

We can not talk about money evolving when referring to fiat money. People are *made* to use it, without choice. Money of the free market tends to resolve to a single dominant money, but in the fiat system, there can be, and are, many varieties of money that exist in *relative* stability.

Interestingly, the regression theorem can apply to government money also. All government money is related to the price of something previous. A new money might be initially pegged to something else, for example, USD was pegged to gold. Once the peg or "intrinsic" value of the dollar was removed, people were valuing the dollar not just because they are forced to use it, but because "other people valued it yesterday," as I described earlier in the section about Regression Theorem.

The dollar is not really *backed* by the government, or gold, or taxes, or the military; it is unbacked, like all money. USD is a form of money that required government force for it to be *adopted in the first place*, but now it is a form of money with no real backing; simply valued because other people value it.

Appendix D – The Cost to Produce Gold is not what Supports its Value.

This thinking is actually backwards in logic. The correct way to think of it is as follows:

As an example, think of gold having been demanded because it was valuable to people for its utility, then as money. The available supply was taken. More was demanded. So more was mined. The supply was taken. Once all cheap forms of mining were consumed, more expensive ways to extract gold was embarked

upon (because it is economical, since the price is going up, due to buyer demand).

Now imagine the opposite. Miners start producing more and more gold, initially cheaply, then at greater expense, as the cheap options are exhausted. But imagine there is no demand. Will the mining of more and more, at higher and higher cost, increase the market price for gold? Of course not, that is absurd, as there is no demand as per the initial condition.

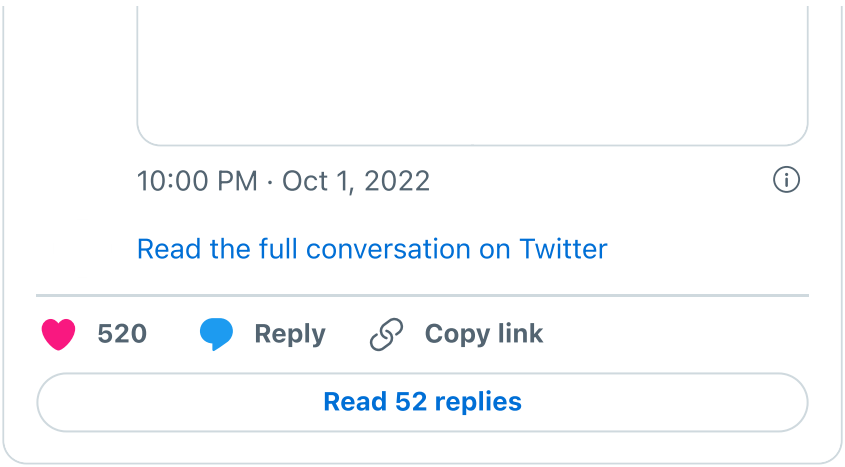
Now consider gold losing its appeal as money. Will the cost to produce gold at $1500 per ounce support the price? Of course not. That's like suggesting the price of anything, say a handmade mahogany trash can, is supported by its production cost. If nobody is willing to pay for it, production of the trash cans ceases, until such time the demand incentivises production at whatever the cost may be – and it may never happen.

So, if gold were to lose its monetary status, many tonnes of gold would be available from bank vaults, satisfying demand, and mining would become unprofitable. It would NOT support the price of suddenly abundant gold.

Conclusion

However someone might use the term "intrinsic value", I have presented an exhaustive logical rebuttal of this criticism which I believe is air-tight.

Not understanding the concepts explained within this article is no excuse to continue spreading such FUD about Bitcoin. If you don't understand the arguments or find them hard to accept on emotional grounds rather than logical, and still don't wish to adopt a money that promises freedom from authoritative control, that is entirely your prerogative, but also your loss. I hope at least you don't promote this debunked FUD to other people looking for a solution to a massive humanitarian problem – our money is broken.



Reddit reply:

Bitcoin is *becoming* money.

1. It has near-perfect technical properties (scarcity, divisibility, portability, etc)
2. It needs to develop network properties (enough people in your economy would accept it as payment)
- Bitcoin is far in the lead of any competing digital money.

THEN, it's considered money. That is its main use case. Before it becomes money, it is an emerging money, and acquiring it early gives you a massive advantage.

The invention of Bitcoin is not how it functions, but mainly...

1. It is by the people (not authority), and can't be stopped by any competing authority
2. It is digital, yet *credibly* scarce (a miracle)
3. It requires no 3rd party to ensure proper functioning and ordering of transactions (digital tokens have always needed this)
4. Ownership can be secured with a secret number (private key)

Tips:

Static Lightning Address: **dandysack84@walletofsatoshi.com**

Understanding Decentralisation in Bitcoin

[Published in Bitcoin Reserve.]

[Link to the reading by Guy Swann on Bitcoin Audible.]

Bitcoin is decentralised…but, what does that even mean?

For any cryptocurrency, exactly *what* is it that needs to be decentralised? Many elements can be decentralised – but which matter?

The meaning of decentralisation might seem obvious (it's not). The word, "decentralisation", may even obviously seem like a good thing (which is why it's thrown into the marketing spin of anything cryptocurrency related).

The literal meaning is that there is no centre.

No centre of what though? Of people? Miners? HODLers? Nodes? Exchanges? Wallets?

The answer that matters depends on the context. The context you need to have is that cryptocurrency, i.e. Bitcoin, was invented/discovered initially to allow a money *by the people* that cannot be shut down by government. In *that* context, the most important element to be decentralised is the network of **Nodes**.

- If the nodes *are not* decentralised, nothing else decentralised matters.
- If the nodes *are* decentralised, then the other things kind of matter, but not as much.

Decentralisation of **miners** is also very important, but in my view, and in the context stated, that is secondary to nodes.

How can you know which aspect of decentralisation matters, if you don't know the right PURPOSE of decentralisation (ie the stated context)?

There are 4 main purposes. The first three are node-related, and the fourth is miner-related.

1. Resist shutdown by government

The very reason Bitcoin was invented in 2008, and not sooner, was because until then, no one had come up with how to create money that the government had no capability to shut down.

This was the **cypherpunks'** aim from a long time ago, and it was the culmination of other achievements over the decades. The cypherpunks:

- advocated and developed tools to guide the internet towards more privacy and sovereignty
- invented pgp (public-private key cryptography) for private messaging
- defended (and won) against the US government outlawing pgp
- and had several failed attempts at creating digital internet money to bypass government-controlled money.

When Bitcoin was created, it was not decentralised from the beginning.
It *could* have been shut down. It was just Satoshi Nakamoto's computer and Hal Finney's (R.I.P.). But, Bitcoin was not a threat then. Why would any government know about it, or care? So it quietly grew, and more and more people joined the network, by … RUNNING NODES.

Bitcoin now has the greatest node decentralisation compared to any other cryptocurrency BY FAR. It was purposefully designed so that running a node would not be expensive, and therefore not prohibitive to those who were not wealthy. Today, the cost of running a node is about $300 to $400 plus internet data costs.

A node is literally the Bitcoin Core software which contains the rules of Bitcoin, and a copy of the blockchain (all the transactions from the beginning of Bitcoin's time). **Read here to find out in more detail what nodes are, do, and the 6 reasons to run one.**

The thing that government needs to do to wipe out Bitcoin is to destroy every single copy of the blockchain – *This* is what is decentralised. I have a copy. I have many. And many other Bitcoiners do too. And so should you. (If you're not a Bitcoiner, **here's why you should be.**)

To recap: *The nodes are decentralised*. There is more than one, and they are geographically dispersed. They cannot be wiped off the face of the planet without wiping out humanity as well.

2. Resist unilateral, unwanted rule changes by bad actors or governments

The rules of Bitcoin are encoded in the software which make a node. Anyone can suggest a change to the rules – the rules are code, but they are not *just* code, they are *agreed-on* code. If changed unilaterally, the new code is no longer part of consensus and is no longer part of Bitcoin.

Changing something with Bitcoin and remaining in consensus is tricky:

If the change is something that *doesn't break any existing rules*, then people can change that code and still play nicely with the rest of the network. Minor upgrades and improvements to the software fall under this category – for example spelling errors, nicer graphics, better structuring of data on the hard disk etc.

Sometimes the change might introduce NEW rules that are more restrictive (ie old rules are not broken). For example, there is currently an upper limit to the block size – if there was a new rule stipulating a *reduction* in the block size, this would not break the old rule: It would be called a *soft fork*, and needs to be done with care so as to not split the network in two. If done properly, those that choose not to update their software are not necessarily disadvantaged; they can continue to run the older code and remain part of the network.

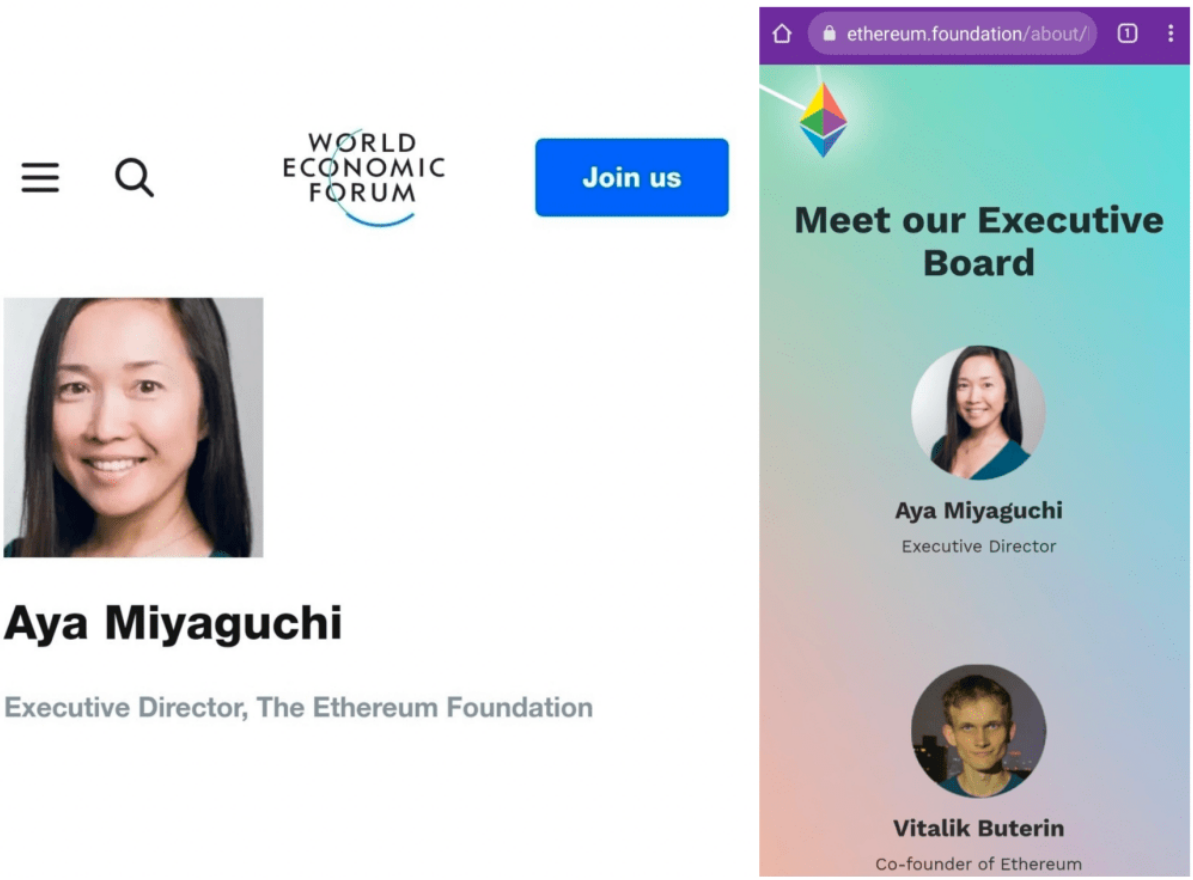
If a new rule is introduced that *breaks the current rules* (e.g. an increase in the block size, as happened in 2017 which resulted in the creation of *Bitcoin Cash* – a massive failure), then this is called a *hard fork,* and basically creates a new chain – an altcoin. Anyone is free to do this, but Bitcoiners are unlikely to unanimously agree and upgrade their nodes. The more users there are who run nodes, the more difficult it is to incorporate unilateral changes that don't split the network and create a doomed altcoin. Basically, you can't unilaterally change Bitcoin – all you'll end up with is an altcoin and a damaged ego/reputation. For an interesting history of the 2017 hard fork, there is an excellent book, "The Blocksize War: The battle over who controls Bitcoin's protocol rules", which I highly recommend.

3. Resist infiltration and coercion

Satoshi Nakomoto, the creator of Bitcoin, disappeared in 2011. Since then, Bitcoin has had no "leader" and many many people have joined in, and run Bitcoin node(s).

If Satoshi was around, the US government would have intervened by now. I'm not sure how, but one such way could have been to threaten Satoshi to encourage the development of code that would weaken Bitcoin, or help the government in some way to undermine the people who want freedom or privacy. It is unlikely that people would dare leave the main chain, away from the leadership of the creator.

This is actually the case with Ethereum. Their leader, Vitalik Buterin, has tremendous influence, and it's not clear if the directions he advocates for are coming truly from him, or if he is the puppet of say, The World Economic Forum – There are close ties between the WEF and top-level management of the Ethereum Foundation.



Having a leader (and all altcoins do), even if it is just a spiritual leader, is a weakness, and an important centralised element.

People may run their own nodes all over the world (they don't with Ethereum), but they are unlikely to form a network that all agrees to abandon the leader's wishes. So, with a leader, the decentralisation of nodes becomes almost irrelevant.

Apart from being dependent on a leader, the vast majority of altcoin owners are not looking for unstoppable-money; they are looking to buy-low and sell-high. So the question of running a node to form consensus independently to a leader isn't important to them, and you will receive blank stares when it is discussed.

Apart from lack of interest, another reason many altcoins nodes are not sufficiently decentralised (particularly Ethereum) is that it is prohibitively expensive to run a node, as the extra functionality on the base layer requires enormous computing power (and technical skill to set up and maintain). This results in the majority of "independent" nodes on large server parks, leaving them open to government and legal attacks.

4. Resist censorship and disruption of the validation mechanism

This refers to miners. Ideally, miners should be decentralised in ownership and geographic location.

If many different people mine, in many different countries, it is much more difficult to coerce a majority to the will of a nefarious actor or government. The game theory of mining resists this but it is not perfect.

While lack of mining decentralisation and coercion of the network is very undesirable, it is not a fatal threat to Bitcoin. Bitcoin is anti-fragile, meaning it can adapt and become stronger, but it may not be pleasant living through some types of attacks.

Recently, a large percentage of the mining network was lost suddenly, when China banned Bitcoin mining outright. This led to a temporary slowdown, and recovery of speed within 2 weeks, and several months later, the worldwide hashrate (mining power) surpassed the all time high. This recovery is because any loss of mining power in the absence of a proportional price drop will incentivise miners elsewhere to join and make profit.

In order to carry out censorship and network validation disturbances, an attacker would require 51% of the world's mining power – AT LEAST. The way to achieve this would be to buy or produce an enormous amount of energy and equipment (and outpace, in competition, with the rest of the world), or/and reduce the amount of equipment/energy in the possession of the rest of the

world. *In fewer words – get more, and destroy the others (physically or legally).*

If the rest of the world's *equipment* is centralised, then that would be easier. Note that *energy* is decentralised by nature already.

Mining decentralisation is probably sufficient currently. But, no matter how inadequate you may think today's level is for tomorrow's needs, over time, Bitcoin mining becomes more and more decentralised as more people enter the arena.

Extra:

It's crucial to understand that one person running 100,000 nodes does not strengthen the network, nor does it weaken it. This is because a node is not just the computers running code, but a human brain as well. It is a human that runs a node and can resist rule changes to the money he/she uses. Resisting a rule change with one computer connected to his/her wallet has the same effect as 100,000 nodes available to connect to the same wallet.

I once explored this in detail in a Tweet:

[Thoughts towards this piece were born a year prior, in this Tweet thread.]