THE SIMPLEST  BOOK EVER WRITTEN

Keysa Luna

* to orange-pill: (verb) / tu' ȯr-inj-'pil/
: the act of explaining bitcoin in such a way that a pre-coiner gets it, and becomes a bitcoiner!

1 bitcoin = 100,000,000 satoshis

The Simplest Bitcoin Book Ever Written

Cover and interior design by Keysa Luna

Cover photo by Vallota from Pixabay.com

Independently Published

TABLE OF CONTENTS

for all our children

with thanks to Satoshi and the cypherpunks

I love the simple life,
I love nature, I love being barefoot,
I love profound conversation that sparks creativity,
connection and inspiration.
I love freedom.

And, I love bitcoin.

Love is a big word, bitcoin is worthy of big love.

It's existence is a point of bright light in this most
challenged time in human existence.

I wrote this book in the hopes of making bitcoin, and the
reasons we need it, more accessible to more seekers.

This book is a starting point, into what I, and many others,
have discovered is a phenomenally endless, life-changing
and beautiful rabbit hole!

May you be orange-pilled, may you be free,
and may you be well enriched by the journey!

- **Note:** Everything presented in this little book is up for debate, discussion, updates and corrections!

- As with everything in life, there are numerous viewpoints on bitcoin, it's future and every other aspect of it.

- Lively commentary is streamed 24/7 on Twitter, that bounces between confusing and clarifying! And yet, an invaluable resource (until a better, decentralized platform gains wide adoption) for interacting with people who have been very deep down the rabbit hole, for a very long time…

- This entire ecosystem is an emergent, grassroots, messy, fascinating unfolding! It is by far the largest global experiment ever undertaken, with people of every race, religion, class and persuasion engaging permissionlessly together, to discover a new way forward.

- If you are inspired by such a movement, you will very likely find yourself falling down the rabbit hole with the rest of us!

- Here's to open minds and open hearts along the way…

- Remember: Don't Trust, Verify

- And always DYOR - Do Your Own Research!

I've developed a new open source P2P e-cash system called Bitcoin. It's completely decentralized, with no central server or trusted parties, because everything is based on crypto proof instead of trust. Give it a try, or take a look at the screenshots and design paper:

Download Bitcoin v0.1 at http://www.bitcoin.org

~ Satoshi Nakamoto 2009-02-11 22:27:00 UTC
Posted on metzdowd.com, an early cryptography mailing list

WHY WE NEED bitcoin

WE NEED bitcoin BECAUSE MONEY IS BROKEN

> *The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts.*
>
> ~ Satoshi Nakamoto 2009-02-11

- The fiat money system is broken (always has been).
- It is not sustainable (never has been).
- There is no way to fix it (never will be).

THE (NOT) GOLD STANDARD

- Most people still believe that money is backed by gold.
- It is not.
- It has not been backed by gold since 1971, when President Nixon unilaterally took the world off the gold standard (the Nixon Shock).
- See **wtfhappenedin1971.com** to get a clear picture of the damage this did.

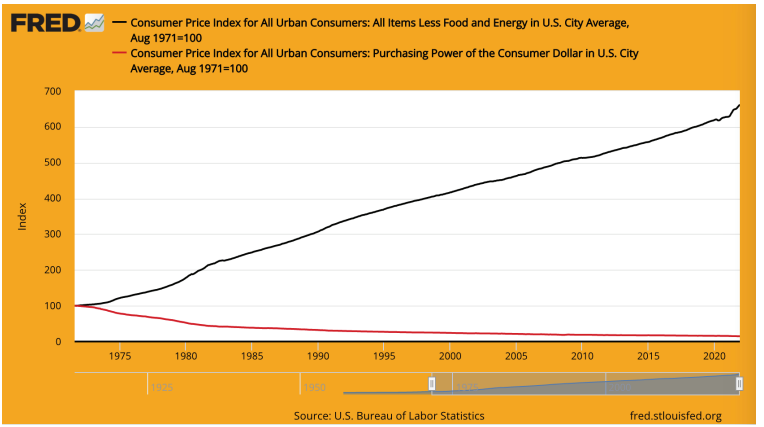


Chart showing CPI inflation (black line) vs the purchasing power of the dollar (red line) since 1971.

- **Fun Fact:** The WEF was formed in 1971.

FIAT: (noun) /'fi:.æt/
: an authoritative or arbitrary order : DECREE
: an authoritative determination : DICTATE
: a command or act of will that creates something without or as if without further effort

~ merriam-webster.com/dictionary

FIAT : from Latin fieri «to be made, come into being»

- Fiat is money that has value only because the government says it does.
- Therefore people (have to) believe it does.
- **Even if they don't believe fiat has value, by law they are forced to use it and to accept it as payment for goods and services.**
- **Fiat money is printed/created out of thin air.**
- These days 3% of all dollars are printed as cash.
- The other 97% is created by banks entering numbers into a computer (not kidding!), when they issue loans.

It costs only a few cents for the Bureau of Engraving and Printing to produce a $100 bill…

~ American Economist, Barry Eichengreen

> ***Scott Pelley of NBC '60 Minutes'**: Fair to say you simply flooded the system with money?*
>
> ***Fed Chair Jerome Powell**: Yes. We did.*
>
> *That's another way to think about it. We did.*
>
> ***Pelley**: Where does it come from?*
>
> *Do you just print it?*
>
> ***Powell**: We print it digitally. So as a central bank, we have the ability to create money digitally. And we do that by buying Treasury Bills or bonds for other government guaranteed securities. And that actually increases the money supply. We also print actual currency and we distribute that through the Federal Reserve banks.*

~ CNBC '60 Minutes' Interview, May 17, 2020
Two months after the onset of the C*vid-19 lockdown

> There's really no limit to what we can do with these lending programs that we have.
>
> ~ Fed Chair Jerome Powell

> Yes, there is an infinite amount of cash in the Federal Reserve. We will do whatever we need to do to make sure there's enough cash in the banking system.
>
> ~ Neel Kashkari , Pres of the Minneapolis Fed

> The 'we' here is five people voting on changes to monetary policy within the Federal Reserve system during FOMC meetings. 5 out of 330,000,000. That's all it takes to change US monetary policy.
>
> ~ @MartyBent, Founder of TFTC.io

FROM THE HORSE'S MOUTH OF OLDE

The bank hath benefit of interest on all monies that it creates out of nothing.

~ William Paterson, 1694,
Founder of the Bank of England

All of the perplexities, confusion, and distress in America arises, not from the defects of the Constitution or Confederation, not from the want of honor or virtue, so much as from downright ignorance of the nature of coin, credit, and circulation.

~ John Adams
2nd President of the United States, 1735–1826

I believe that banking institutions are more dangerous to our liberties than standing armies. Already they have raised up a money aristocracy that has set the government at defiance. The issuing power should be taken from the banks, and restored to the people to whom it properly belongs.

~ Thomas Jefferson
3rd President of the United States, 1801-1809

While boasting of our noble deeds were careful to conceal the ugly fact that by an iniquitous money system we have nationalized a system of oppression which, though more refined, is not less cruel than the old system of chattel slavery.

~Horace Greeley (1811-1872)
US Congressman and Founder of The New York Tribune

Whoever controls the volume of money in any country is absolute master of all industry and commerce…
when you realize that the entire system is very easily controlled, one way or another, by a few powerful men at the top, you will not have to be told how
periods of inflation and depression originate.

~ James A. Garfield,
20th President of the USA, Mar-Sept. 1881
Assassinated 1881

There today exists uncontrolled in the hands of a set of men a power to make dollars from nothing.

~ Thomas W. Lawson, Frenzied Finance, 1905

I was as secretive - indeed, as furtive - as any conspirator. Discovery, we knew, simply must not happen, or else all our time and effort would be wasted. If it were to be exposed that our particular group had got together and written a banking bill, that bill would have no chance whatever of passage by Congress.

~ Frank A.Vanderlip
President of the National City Bank of New York
(forerunner of Citi Bank)
~ Writing in 1935 of the secretive meeting that took place on Jekyll Island in 1910, to draft the bill that was passed as the Federal Reserve Act in 1913.

This (Federal Reserve) Act establishes the most gigantic trust on earth. When the President (Woodrow Wilson) signs the Bill, the invisible government of the Monetary Power will be legalised… The worst legislative crime of the ages is perpetrated by this banking and currency Bill.

~ Charles A. Lindbergh, Sr. (1859-1924)

I am a most unhappy man. I have unwittingly ruined my country. A great industrial nation is controlled by its system of credit. Our system of credit is concentrated. The growth of the nation, therefore, and all our activities are in the hands of a few men. We have come to be one of the worst ruled, one of the most completely controlled and dominated governments in the civilized world. No longer a government by free opinion, no longer a government by conviction and the vote of the majority, but a government by the opinion and duress of a small group of dominant men.

~ Woodrow Wilson,
28th President of the United States, 1913-1921
6 years after passing the Federal Reserve Act of 1913.

The real truth of the matter is, as you and I know, that a financial element in the large centers has owned the government of the U.S. since the days of Andrew Jackson.

~ Franklin D. Roosevelt, 32nd President of the US
in a letter written Nov. 21, 1933 to
Colonel E. Mandell House

It [the depression] was not accidental. It was a carefully contrived occurrence…. The international bankers sought to bring about a condition of despair here so that they might emerge as the rulers of us all.

~ Congressman Louis T. McFadden,
(Assassinated in 1936)

Chairman of the House Banking and Currency Committee
Each and every time a bank makes a loan, new bank credit is created - new deposits - brand new money.

~ Graham F.Towers
Gov of the Central Bank of Canada, 1934-55

If there were no debts in our money system,
there wouldn't be any money

~ Marriner Eccles,
1941, Gov. of the Fed

I have never yet had anyone who could, through the use of logic and reason, justify the Federal government borrowing the use of its own money…
I believe the time will come when people will demand that this be changed.
I believe the time will come in this country when they will actually blame you and me and everyone else connected with the Congress for sitting idly by and permitting such an idiotic system to continue.

~Wright Patman, Democratic Congressman 1928-1976, Chairman Committee on Banking and Currency 1963-1975

When you or I write a check, there must be sufficient funds in our account to cover the check, but when the Federal Reserve writes a check there is no bank deposit on which that check is drawn. When the Federal Reserve writes a check, it is creating money.

~ Federal Reserve Bank of Boston
"Putting It Simply", 1984

THE FEDERAL RESERVE

- The Fed is the 'independent' central bank of the US. It was created in 1913 with the passing of the Federal Reserve Act.
- It has a unique structure, part private and part government.
- It is supposed to be a politically independent, non-partisan entity within the government.
- While the Fed Board of Governors is appointed by the President and con irmed by Congress, **the decisions of the Fed do not need to be ratified by anyone. Yes, it is confusing!**

It consists of:

- The Federal Reserve Board of Governors
- 12 Federal Reserve Banks
- The Federal Open Markets Committee (FOMC), which is the monetary policy-making body.

The Fed is responsible for:

- Overseeing US monetary policy, promoting employment and stable prices.
- Regulating and supervising banking and financial institutions.
- Providing payments services to financial institutions.
- Promoting consumer protection and community development.

A NOTE ON THE FED CHAIR

- The Chair of the Federal Reserve also:
  - Chairs the Federal Open Market Committee (FOMC), which decides on the direction of US monetary policy (for eg: QE, interest rate hikes)
  - Is a member of the International Monetary Fund, the IMF
  - Is a member of the Bank for International Settlements, the BIS (the bank of central banks).
  - Is the finance minister of the G-7
  - Is the finance minister of the G-20
- A **whole** lot of power for one person!

FRACTIONAL RESERVE BANKING, INTEREST & LOANS

- **Fractional Reserve banking:** Until March 2020, banks were required to hold a reserve of 10%, and could loan out 90%.

- **Since March 2020, there is no reserve required, allowing banks to issue unlimited loans (!!!).**

- A loan is debt-based money, and you are required to pay interest on the loan.

- **Fun Fact 1:** The money to pay the interest on the loan is NOT created by the banks.
- **Fun Fact 2:** It is NEVER created.
- **Fun Fact 3:** There is NOT ENOUGH money in the world to pay back all the loans + the interest due on those loans.
- **Fun Fact 4:** There never will be!

A NOTE ON THE PETRO DOLLAR

- One could say **that until 1971 the dollar was backed by gold, and since 1974 it has been backed by oil, and by default, the US Military**.

- **In 1974 the US and Saudi Arabia entered into bilateral agreements to price the sale of oil in US dollars.**

- Since then, most global oil sales have been settled in US dollars.

- This has contributed greatly to the dollar becoming the strongest currency in the world.

- **It has thus been artificially propped up**, even during times when it would normally have struggled.

- While I was writing this, things were rapidly deteriorating as the Russian invasion of the Ukraine was heating up, and Russia and China were making deals for oil in the ruble/yuan, breaking away from using the dollar.

- It is very likely that this could be the beginning of the end of the petro dollar. What happens next remains to be seen…

ON QE (QUANTITATIVE EASING)

- Quantitative Easing is considered an 'unconventional monetary policy' used by Central Banks to 'stimulate the economy', whereby the Fed buys government bonds and other government securities.

- It was first used by Japan between 2001-2006. Following that, the US, UK, and the Eurozone used QE during the 2008 financial crisis.

- Since then, the only time the US has not had a QE program was between 2014-2019.

- As seen below, critics contend that **QE overwhelmingly benefits the already-wealthy.**

Credit: @RudyHavenstein on Twitter

CYCLES

- **In all of nature, there are cycles, natural ebbs and flows, expansions and contractions.**

- This **contributes to an overall, over-time, balance and sustainability** of the whole interconnected system, of all life on earth.

- **The debt-based, fiat currency system ignores the wisdom of natural cycles,** and instead is based on, and 100% reliant for its survival upon, unparalleled and unmitigated growth, in order to continue servicing its debts.

- In nature, this is cancer.

- In 'the economy', this unnatural trajectory is further supported by the government bailing out failing banks and large companies, rather than allowing them to fold, and be recycled into something new, something healthier.

- **The short-sightedness of bailing out failing companies is putting the whole economy at risk.** In essence, it is just kicking the can down the road, and the inevitable turmoil that lies ahead is likely to be far, far more intense than if natural cycles were allowed to play out.

- **We are indebted to Satoshi Nakamoto, and to the cypherpunks before and after him**, for having the vision, foresight, determination and skill to provide a lifeboat to carry us to new shores.

- Once we realize the gift that this is, it is up to us to jump on board, with full hearts and clear minds, to take the trip and build a new world with the Money of Peace.

- **Bitcoin fixes the money, it is up to us to fix the rest. And, to be clear, by having the money fixed, a LOT of other things will be fixed, by default.**

- The main one being that large-scale, government-initiated, kinetic war will no longer be profitable, or possible, without the support of the people.

- Additionally, there will naturally be less consumption, along with a switch over to real-value goods and services, free markets, real savings, & demonetization of housing and real estate, that was never meant to be monetized in the first place.

WE NEED bitcoin

BECAUSE INFLATION IS THEFT

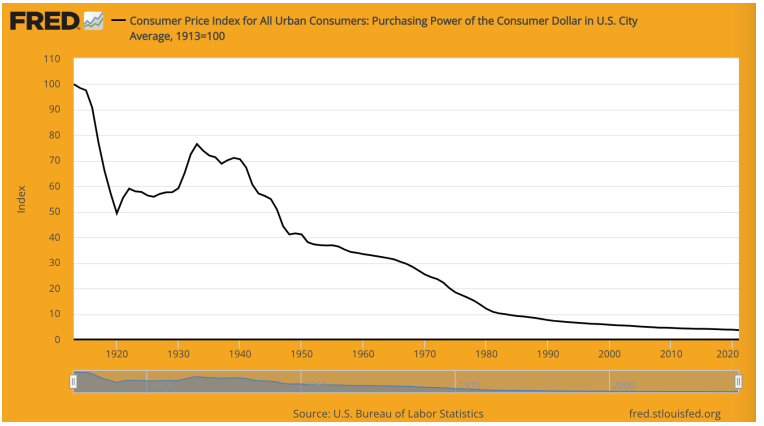


Chart showing the declining purchasing power of the dollar since the formation of the Federal Reserve in 1913. The cumulative rate of inflation since 1913 is around 2,525.4%. All central bank fiat currencies around the world are following a similar rate of decline.

- **The more money that is created out of thin air, the more all money loses value.**
- This is called **inflation.**
- Inflation is **time-theft**, literally. The value of your time is stolen when you save it in a currency that is inflated and manipulated.
- Inflation is also a **hidden tax.**
- This time-theft and tax affects all other countries' fiat currencies as well, since they are all pegged to the

US dollar, as it has been the world reserve currency since the Bretton Woods agreement in 1944.

- **In the USA, a 2% annual inflation rate is written into the Federal Reserve mandate.**
- This means that **you are GUARANTEED to be able to buy 2% LESS** with the same $20 bill each year.
- **In February 2022, the annual inflation rate was 7.9%,** (a lot more than 2%), which means you lost 7.9% of your purchasing power in the past year.
- Put another way, this means that on average, things went up in price by 7.9%.
- So, if a basket of groceries cost $50 in 2021, the same basket cost $53.95 in 2022.
- **If inflation was measured accurately, like it was done until the early 1980's, it would actually be closer to 15% right now in 2022, and your basket of groceries would be $57.50.**
- **When looked at by category, one can see inflation is actually a lot worse than 7.9% in many categories over the past year:**
- Energy - 25.6%
- Gasoline - 38%
- New vehicles - 12.4%
- Used cars and trucks - 41.2
- Food - 7.9% (largest since July, 1981)

Average Inflation over the past 50 years in the US:

Average Cost	1971	2021	% Increase
Salary	$9,400	$53,400	469%
House	$23,400	$408,000	1,643%
Gallon of Gas	$0.36	$3.60	1,000%
New Car	$3,400	$39,000	1,047%
College Degree	$1,400	$26,000	1,757%
Basket Groceries	$20	$133	565%
Electricity/kWh	$0.02	$0.14	600%

True Story:

~ A house was bought in 1976 for $58,000.

~ When accounting for 'official' inflation, this would be $279,000 in 2022 dollars,.

~ In 2022 the same house was recently valued at $2.09 million.

~ Ponder on that…

- **As inflation increases, your savings (if you are lucky enough to have savings), lose value.**

- Over time, they lose A LOT of value.

- If you started saving $100/month today, with the best available interest rate of 0.05%:
  - In 30 years you would have saved $84,019.
- When adjusted for the FED's mandated 2% inflation:
  - In 30 years your savings would have an **effective purchasing power** of just $46,384.
- Adjusting for today's 'actual' inflation of 7%:
  - Your $84,019 worth of savings would have the purchasing power of just $11,037 in 30 years!

- **In effect this means that ~six out of seven hours of your work have been stolen = *Time Theft*.**

Another way to look at it is the following:

- In 1971, the cost of a house = 2.5 times an average annual salary.
- In 2021, the cost of a house = 8 times an average annual salary.
- In 1971, a new car cost about 1/3 of an average salary.
- In 2021, a new car cost nearly 2/3 of an average salary.

I trust that it is now clear that
inflation
does not
work in your favor.

Note: All of these numbers are averages, and variable based on many factors. The point remains, inflation has sky-rocketed and shows no signs of slowing down, thanks to the ongoing money printing. Inflation is a hidden tax and is time-theft on our real labor and production.

Hard money fixes this.

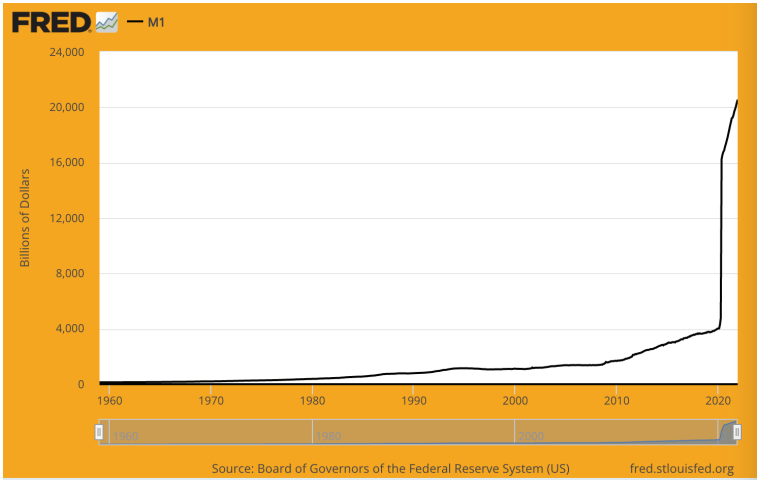
Bitcoin is hard money.

WE NEED bitcoin

TO REPLACE THE CENTRALLY CONTROLLED, MANIPULATED, DEBT-BASED ECONOMY

I don't believe we shall ever have a good money again, before we take the thing out of the hands of government, that is, we can't take them violently out of the hands of government, all we can do is by some sly roundabout way introduce something they can't stop.

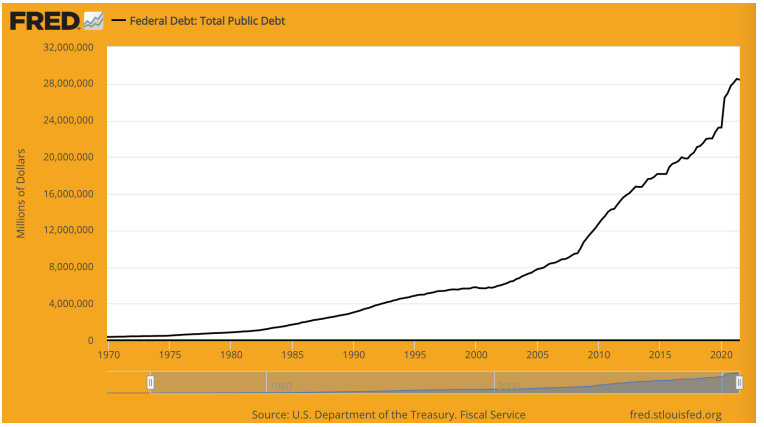
~ Friedrich Hayek
~ Austrian Economist, Philosopher and Author



Graph showing M1 Money Supply increase from $4 trillion to over $20 trillion since March 2020!

Blow your mind here: https://usdebtclock.org/

- **45% of all the US dollars in existence were printed in the past 21 months, April 2020-Jan 2022!**
- Printed out of thin air that is, remember?
- Fiat money is centrally controlled by the state, and the supply is easily manipulated.
- **It took 205 years for the US National Debt to reach $1 trillion.** (1776 > 1981)
- It took just **31 more years for the** US National Debt **to reach $30 trillion!** (1981 > 2022)



Graph showing Total Public Debt 1970-2021 in the US.

Global debt, measured by the Institute of International Finance, now totals $303 TRILLION. This is our planet on debt-based fiat. By the way, global GDP is only $84 trillion.

~ Nik Bhatia, Author of 'Layered Money', 2021

- For reference:

If you have:	You can spend $1/second	
$1 Million	for 11 days	= 11 days
$1 Billion	for 11,680 days	= 32 years
$1 Trillion	for 11,680,000 days	= 32,000 years

- We are all at the mercy of those who have the power to decide when to print more, and what interest rates to charge.

- If the Fed raises the interest rates, then getting a loan for a house or a car becomes suddenly more expensive, which slows down spending, leading to stagflation.

- If they keep the rates artificially low, we enter a period of depression

- Allowing the central bank to create the financial 'weather', takes away our freedom to let the market decide what is of value, and what is not.

- In addition, **when they bail out banks and corporations, they artificially prop up the economy.** It is only a matter of time before the house of cards falls.

- The original argument for having a central bank was that there needed to be a Lender of Last Resort when the economy wobbled.

This has turned into the central bank being a Ruler of First Resort, with unparalleled, unelected, ultimately authoritarian power.

All money is political, except for Bitcoin. Fiat currencies, banking instruments, fintech credits, other cryptocurrencies, and even gold are all controlled by governments, corporations, or small groups. Having an exception will prove very useful as we head into the future.

~ Alex Gladstein @gladstein
Chief Strategy Officer for the Human Rights Foundation

Bitcoin links together 8 billion people, links together a hundred million companies, it synchronizes the world across political jurisdictions, and it returns rationality to the entire financial system, and it returns freedom and property rights to the entire human race.

~Michael Saylor, CEO Microstrategy

WE NEED bitcoin

TO BANK THE UNBANKED

For 953 million people in 20 countries with weakening currencies, Bitcoin represents something greater than a treasury asset. For them, it's more like an ark of encrypted energy to escape the flood.

~ Michael Saylor
CEO of Microstrategy

- Approximately 30% of the adults in the world are unbanked, about 1.9 billion people!

- This means they have no access to banking services and cannot use ATM's, debit cards, credit cards or checks.
- In addition, they are not able to get loans to start a business, to buy a car or a house etc.

- Sending and receiving money, or cashing checks, is expensive.

- They have to use money-transfer and check cashing services like Western Union, that charge high rates and take time to process.

- It is **especially expensive for people sending money home to their families** in other countries (remittances), which can cost up to 10%.

- It is **expensive and time-consuming for those receiving remittances**, as they need to pay for transport and go to the money-transfer office, often far from where they live, to get the money their family member sent.

- Oftentimes it is not safe for them to travel to these offices.

- Bitcoin, over the Lightning Network, provides an instant solution to these problems now!

#bitcoin fixes this

> *When has a technology that empowers people ever been stopped?*

~Jeff Booth
Author of: The Price of Tomorrow

WE NEED bitcoin

TO HELP PEOPLE ESCAPE TYRANNY AND CURRENCY COLLAPSE

- As we have seen, over these past months even in 2022, governments can and do freeze the bank accounts of those they disagree with.

- **This shows that, in essence, your money in the bank is nothing more than an IOU that can be stolen from you at any time.**

- In addition, when inflation runs rampant, as we are currently seeing in Venezuela, Sudan, Lebanon, Syria, Argentina, Zimbabwe, Turkey and more, people's life-savings are vaporized, sometimes overnight, and there is nothing they can do about it.

- For people experiencing any of the above, **bitcoin becomes a real, immediate solution to an otherwise untenable problem**.

- **Considering that both tyranny and inflation is on the rise in many places, one would be wise to hedge against them by buying bitcoin now.**

WE NEED bitcoin

TO AVOID CBDCS

- You may have heard that **central banks are starting to create CBDC's, Central Bank Digital Currencies.** In May 2020, 35 countries were exploring this option.

- At the time of this writing, February 2022, 87 countries are actively looking at, or have already launched, a CBDC.

- In the US it is called Project Hamilton.

- **CBDCs are very similar to the electronic money you see in your online bank account, except that by being *natively digital*, they are *programmable* and *100% controllable.***

> *A key difference with CBDCs is central banks would have* ***absolute control****..*
>
> ~Agustin Carstens
> GM, BIS (Bank for International Settlements)
> (The bank of all banks)

- **This means the government can program an expiration date on your money,** forcing you to spend it before it expires.

- **They can also program other things into it**, like only allowing it to be spent at certain shops, websites or jurisdictions, and not at others.

- **They could link it to**: your credit score, your health pass, digital ID and other social scores.

- **Following this, they can program any restrictions they see fit,** based on your specific score in one area, or on your 'overall score', or on what they deem the 'economy' needs.

- In addition, they will be able to surveil every single thing you do with your money.

We don't know who's using a $100 bill today and we don't know who's using a 1,000 peso bill today. The key difference with the CBDC is ***the central bank will have absolute control on the rules and regulations that will determine the use*** *of* ***that expression of central bank liability****, and also* ***we will have the technology to enforce that****.*

~Agustin Carstens
GM, BIS - Bank for International Settlements

- **Note:** Saying **"that expression of central bank liability"** implies that your value, your life force, stored as money, is actually 'owned' by the central bank. (Um, no!)

WE NEED bitcoin

TO SAVE THE GARDEN

- **Bitcoin plucks out, at the root, THE biggest issue we face, the Fiat Lie.**

- This is the lie of corrupted fiat currency, usury and all that comes with it to steal your time, while greatly enriching those closest to the money printer (known as the Cantillon Effect).

- The **Fiat Lie** is like a giant **monster weed** in your garden, **sucking** all the nutrients from the soil, **killing** all the mycelium, and **blocking** the sunlight so that the other plants cannot thrive, and are struggling to survive.

- Suddenly when this noxious, monster Fiat Lie weed is gone, Truth enters!

- All the plants (**the people**) can begin to recover.
- The soil (**being peoples' creativity, real goods and services**) can regenerate.
- The mycelium (**being authentic connection between people**) will regrow.
- And the sunlight (**unmediated life force**) will shine down once again upon us all!

WE NEED bitcoin

TO FIX THE WORLD

- This is not a joke. **#bitcoinfixesthis** is a running meme on BT (Bitcoin Twitter), for good reason.

- While this might sound somewhat 'grandiose', let me explain. When one considers the 'way things are', even before 2020, **anyone could, still can, see that 'something is very wrong'**.

- Rampant destruction, environmental degradation, splintered families and communities, loss of cultures, languages, traditions, poverty increasing, massive wealth concentration amongst the hands of the (very) few, over-consumption, infinite money backing politicians, lack of food and clean water for millions, ever-increasing obesity and auto-immune disorders, seemingly endless wars …

- One would think that with the exponential growth in NGOs, non-profit organizations, charitable foundations and so-called government-backed institutions, these issues would be getting less severe.

- Instead, **they are largely becoming more severe.**

bitcoin FIXES THIS

FINANCIAL INCLUSIVITY

- With bitcoin, everyone has access to the same financial system, with the same rules for everybody.
- No loopholes or backdoors or special deals for anyone.
- Everyone has the potential to be compensated for the value they provide with the same real money, created and maintained with the same rules.
- Bitcoin is accessible to anyone, anywhere with an internet connection.

ADDING VALUE TO THE WORLD

- Bitcoin incentivizes people to add real value to the community and the marketplace, as this is the only way to make more money.
- If one is satisfied with less, one still benefits by working for a fair wage, and when one saves, those savings maintain their value over time.

bitcoin FIXES THIS

ENVIRONMENT

- Sound money, with a hard-capped supply, creates a very different dynamic to that which we see today.

- Instead of an unstoppable drive to consume ever more, in a race to the bottom to pay compounding interest rates on loans and debt that will ultimately never get paid off, **bitcoin provides an off-ramp to a world where a low-time preference is sought after.**

- **Rampant environmental destruction is replaced with less consumption, less waste, and a considered approach to production, where the market decides what holds true value, and things are therefore built to last.**

- This is a net benefit to people, plants and animals!

bitcoin FIXES THIS WAR

- The fiat money system is what makes 'forever-wars' possible and profitable. Since the people are mostly in the dark about how war spending works, or where the money for war comes from, there is little to no accountability on the part of government. Wars can drag on for years in remote places, with no real oversight.

- Starting with Vietnam, wars have become 'credit card wars' (h/t @AlexGladstein), since the government borrows money to fund the wars, and then borrows more money to pay the interest on the initial loans.

- **On a bitcoin standard, it would require the people of a country to be willing to help pay for a war. They would likely only do so if it was absolutely and clearly necessary, to defend their family and country, with an end-goal in site.**

- Since there would be no undue profits to be made, government officials and corporations would not be incentivized to promote or engage in war as a viable option.

- **Efforts would greatly increase to find ways to come to peaceful, low-cost resolutions instead.**

bitcoin FIXES THIS

TIME PREFERENCE

- High-time preference leads to personal, societal and environmental destruction. When our money is losing value each day, we are 'forced' to spend it as quickly as possible, before it loses more value. When our time is devalued by an ever-inflating fiat currency, we lose connection to the value of our time.

- This leads to disconnection, and an undercurrent of stress.

- Attempts to alleviate the stress, and find meaning, are distorted and become distractions such as over-consumption of drugs, alcohol, shopping, porn, fast food, short attention spans, addiction to screens/ social media etc.

- Sound money on the other hand, which holds its value over time and properly measures our contributions through our work, leads to a low-time preference, thoughtful quality of life, with meaningful relationships, less consumption, deeper connection, more profound conversation and increased creativity.

WHAT IS bitcoin ?

"Writing a description for this thing for general audiences is bloody hard. There's nothing to relate it to."

~ Satoshi Nakamoto 2010-07-05

Total circulation will be 21,000,000 coins. It'll be distributed to network nodes (miners) when they make blocks, with the amount cut in half every 4 years.

first 4 years: 10,500,000 coins
next 4 years: 5,250,000 coins
next 4 years: 2,625,000 coins
next 4 years: 1,312,500 coins etc...

When that runs out, the system can support transaction fees if needed. It's based on open market competition, and there will probably always be nodes willing to process transactions for free.

~ Satoshi Nakamoto 2009-01-09

- **Bitcoin is freedom money**... in the sense that it has the potential to free us all from the overarching manipulation by, and control of, the central banking system.

- **In bitcoin, the monetary rules are the same for EVERYONE, EVERYWHERE.**

- Bitcoin is **inclusive**, in the sense that anyone with an internet connection can participate in the network, and has to **play by the same rules.**

bitcoin IS:

- DECENTRALIZED
- TRULY SCARCE
- CENSORSHIP RESISTANT
- A DISTRIBUTED LEDGER
- INCORRUPTIBLE

This group of five properties distinguish bitcoin from every other cryptocurrency!

- PERMISSIONLESS
- AUDITABLE
- TRANSPARENT
- IMMUTABLE
- BORDERLESS
- HARD TO COUNTERFEIT
- PSUEDONYMOUS
- FRICTIONLESS
- TRUSTLESS
- PEER-TO-PEER

- **Bitcoin is decentralized.**
- **It is run on thousands of nodes worldwide, by thousands of people who don't know each other.**
- No one person, government or company can ever control it.
- You can run a node too, it's easy ;)
- By running your own node, you help secure the network, while also having the ability to verify your own transactions

Don't trust. Verify.

- **Bitcoin (upper case 'B')** is a monetary network.

- **bitcoin (lower case 'b')** is the currency, or monetary asset, that is issued on, and runs on the Bitcoin network.

- Bitcoin is the great incentivizer.

- The genius of Satoshi was such that in bitcoin, for the first time, both good and bad actors are incentivized to play by the rules.

> *"The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU proof-of-worker than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth."*
>
> ~ Satoshi Nakamoto 2008-10-31

- Bitcoin is the first *digitally native money.*
- Unlike your online checking account, which is just a digital form of central bank fiat.
- Bitcoin is **decentralized** digital currency.
- Bitcoin has **no central authority**.
- Bitcoin is **stateless.**
- Consider the implications ...

> *Bitcoin is a decentralized digital currency that enables instant payments to anyone, anywhere in the world. Bitcoin uses peer-to-peer technology to operate with no central authority: transaction management and money issuance are carried out collectively by the network.*

~ Bitcoin Wiki
en.bitcoin.it

- Bitcoin is magic internet money.
- No seriously, **Bitcoin is the way we are going to fix the world.**
- Seriously? Yes.

- Bitcoin is a way to transfer value
  - of any amount
  - securely
  - instantly (on the Lightning Network)
  - between any two parties
  - anytime
  - 24/7
  - anywhere
  - yes, anywhere
  - Think about that.

> *With e-currency based on cryptographic proof, without the need to trust a third party middleman, money can be secure and transactions effortless.*
>
> ~ Satoshi Nakamoto 2009-02-11

Bitcoin is (almost) costless to move with certainty.
I know with 100% certainty what I am receiving.

~ Michael Saylor CEO of Microstrategy

- You can send $1.13, or 46c or 359 sats or 500,000,000 sats or $1 million to anyone, anywhere, anytime … instantly and almost free, via the Lightning Network, built on Bitcoin.

- **And no one can stop you.**

- Can you do that with gold, silver, USD/GBP/EUR/YEN/CYK/ZAR or any other central bank fiat currency? (No)

- **Bitcoin is historical.** This is the first time in history that a truly decentralized, censorship-resistant, immutable, borderless, permissionless, and incorruptible monetary system with an absolute hard cap (21 million coins) has ever been created.

- Bitcoin is **as significant to decentralizing power and increasing financial inclusion**, as the invention of the printing press, and later the World Wide Web, **was to decentralizing and increasing access to information.**

A lot of people automatically dismiss e-currency as a lost cause because of all the companies that failed since the 1990's. I hope it's obvious it was only the centrally controlled nature of those systems that doomed them. I think this is the first time we're trying a decentralized, non-trust-based system.

~ Satoshi Nakamoto 2009-02-15

- **Bitcoin is a distributed, decentralized, transparent and immutable, ledger.**

- Which simply means it is a way where anyone in the world can see who owns what, at any given moment, and it cannot be changed.

- Except the 'who' isn't a name, it is an address made up of numbers and letters.

- An example of a bitcoin address:

bc1qar0srrr7xfkvy5l643lydnw9re59gtzzwf5mdq

- **Bitcoin is therefore pseudonymous.**

- Bitcoin is
  - an impartial issuer of assets
  - a store of value
  - a medium of exchange
  - and soon to be a unit of account
  - *as well as*
  - *the means* of exchange.

- It is the issuer, the gold, the cash, the debit card AND paypal, the bank, venmo, cashapp, western union

ALL ROLLED INTO ONE!

- **Bitcoin is a record keeper that uses mathematics and computer science, instead of bankers, bookkeepers and accountants.**

- It eliminates the middlemen, banks, govts, overdraft fees, checking account fees, limited hours of service, potential for censorship, frozen accounts, manipulation of the money supply, interest rates, the IMF, the WEF, brick-and-mortar buildings, ATMs, checks, corruption, usury, the petro dollar, the euro dollar, bank seignorage, bonds, equities, fractional reserve banking, visa, mastercard, amex, western union, the BIS, days of waiting for your wire transfer to go through.

- **Instead of having someone between you and the person whose hand you want to shake, you can just shake their hand directly.**

- **No need to ask permission to send your own money!**

- You can now do so how, when and where you choose, instantly, with final settlement occurring immediately!

Put Simply...

- Bitcoin is digital property that no one can take from you.

- Owning bitcoin means owning the right to send value from a specific address that you control with your private key, to ANY other address you choose.

> *Bitcoin is a property right that is independent of the monopoly on violence.*
>
> ~ Robert Breedlove @breedlove22

- And, we can repurpose tens of thousands of brick & mortar bank buildings worldwide, to be community centers, libraries, concert halls, artist studios, & anything else we can imagine to enrich and enliven our communities!

- Bitcoin is a once-in-a-species event.

- The discovery of Bitcoin 14 years ago, is to human financial freedom and sovereignty, as the discovery of fire was to human flourishing over 500,000 years ago, and the printing press was to decentralizing access to human knowledge nearly 900 years ago.

- Bitcoin is choice.

- Bitcoin engenders sovereignty.

- **Bitcoin is a true store of value.**

- It stores your most precious resource, your time, in such a way that you can access it again later.

Bitcoin is like a high bandwidth conduit of energy to your future self ... you can work today and Bitcoin will deep freeze your energy for later use.

~ Robert Breedlove

The root of money is time
And the root of time is value

~ Guy Swann

- **Bitcoin is a timechain**, literally.

- You can measure time in blocks, since one block is mined every ~10 minutes.

- Our time is our most scarce and precious resource.
- It is our literal life force.
- True Money allows us to store our time!

- It is the way we can acknowledge the time we 'spent'.

- We trade our time for money, which is simply a record of our time and effort.

- It is magic, this ability to preserve our time such that we have 'access' to it, later in life when we are no longer able to work as we once did.

- When Inflation occurs, it steals the value of our time from us.

- Bitcoin is a **store of value**.
- Bitcoin is a **medium of exchange**.
- Bitcoin **will one day be a unit of account**.
- Bitcoin **will one day be *THE unit of account***.

- **Bitcoin is scarce.**
- It has a hard cap of 21,000,000 coins.
- There will never be more.
- Code is law here.*

* While it is 'technically' possible to change the code, Satoshi's genius prevents that, since increasing (inflating) the supply would only serve to decrease the value of all coins in circulation. This therefore incentivizes everyone to implicitly agree to maintain the 21,000,000 hard cap supply.

- **Bitcoin is infinitely divisible.**
- It is currently divisible to the eighth decimal: 1.00000000
- There are 100,000,000 satoshis in 1 bitcoin.
- 1 satoshi = ₿ 0.00000001
- You can buy sats (satoshis) in any amount.

- **Bitcoin is the hardest, soundest money we have ever known.**

- It is even sounder than gold, since gold is not easily divisible or portable, has low velocity (moves slowly) and is not easily verifiable.

- **Bitcoin has the most superior monetary properties of any asset ever known.**

Properties of Money	Bitcoin	Gold	Fiat
Verifiably Scarce	✓	✗	✗
Easily Portable	✓	✗	✗
Instantly Verifiable	✓	✗	✓
Easily Divisible	✓	✗	✓
Durable over Time	✓	✓	✗
Fungible Everywhere	✓	✓	✗
Censorship Resistant	✓	✗	✗
Difficult to Counterfeit	✓	✓	✗
High Velocity	✓	✗	✓

- Bitcoin is the antidote.
- Attempting to 'stabilize' the economy with bailouts, money printing, QE and interest rate manipulation is like having it on artificial life support.
- This 'machine' can only go on so long, before becoming more and more expensive to maintain, and less and less sustainable, leading to a serious breakdown.
- Bitcoin fixes this.
- Bitcoin is better money.

- **Bitcoin is anti-fragile.**
- And it gets more so with every attempted attack, with every government ban, with every piece of mainstream media FUD (fear, uncertainty, doubt).
- Bitcoin has never been hacked.*
- Though many have tried.

* Although you may have heard of hacks, it is the exchanges that have been hacked.

Remember: Not your keys, not your coins
>> **Always** withdraw your sats to your **own wallet**.
And **very best** to buy peer-to-peer >> Bisq works.
1000% worth the time to learn how!

- Bitcoin is a combination of:
  - cryptography
  - mathematics
  - networking
  - game theory
  - economic incentives …
- … that all work together to create trust in a trustless, decentralized environment to support a secure digital currency.

- **Bitcoin is a deep, deep rabbit hole**, causing you to question most everything you thought you knew ;)

- Bitcoin is self-contained.

- **Bitcoin simply is.**

- **Bitcoin is a symbiotic relationship** between: humans <-> a perfect solution to transfer and store time/ value.

- Humans need Bitcoin, bitcoin needs humans.

- **Bitcoin is the solution to the Byzantine General's problem.**

- This was thought to be an unsolvable problem in computer science.

- This problem arises in decentralized systems, where it was thought impossible to prove that message sent = message received, since the 'man-in-the-middle' could be a bad actor and falsify the message.

- In other words, it seemed impossible to form consensus amongst a network of distributed and independent computers.

- By using the timestamp along with the cryptographically secured distributed ledger, Satoshi solved this problem.

- His solution is known as **Nakamoto's consensus.**

- **Bitcoin is the solution to the double-spend problem.**

- This means that when you send bitcoin, the receiver can be sure that you actually owned the bitcoin you sent, and, that once you sent it to them you cannot spend those coins again by sending them to someone else (double-spending).

- Just like me giving you an orange.

- Once it leaves my hands and is in your hands, I no longer have the orange to give to someone else.

> *..double-spends are never accepted into the transaction pool, so every node bears witness to which transaction it saw first by working to put it into a block.*
>
> ~ Satoshi Nakamoto 2010-12-09

- **Bitcoin is a bearer asset**, like cash or gold, held by the bearer (owner) directly.

- **This means that, once sent (given), it goes directly to the new bearer (owner), with no middleman (bank) needed to process the transaction.**

- **Bitcoin is P2P (peer-to-peer).**
- Bitcoin is censorship-resistant.
- **This means that no one has the power to hold up, or to prevent a transaction from going through to the new bearer.**
- Bitcoin flows freely.
- There can be no gatekeepers.

Bitcoin is trustless.

> *The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust.*
>
> ~ Satoshi Nakamoto on the importance of Bitcoin's trustless nature.

- Bitcoin is code.
- Code is speech.
- Be amazed here: Check out **github.com/bitcoin**
- Click around to view the code, the pull requests, the reviews, the commits, by the amazing developers who are working on, maintaining and improving the creation that is bitcoin.

- **Bitcoin is the internet of money.**

- When one stops to consider that everything else is going/has gone digital, including:

  - music
  - books
  - banking
  - movies
  - education
  - photos
  - phone calls
  - maps
  - and the list goes on ... for better or for worse…
  - … then one sees how it is really a logical step for money to follow.

    (**BUT** we need BITCOIN, ***NOT*** CBDCs!)

SATOSHI's GENIUS

- Bitcoin is **ALL** of the following:
  - A **decentralized, distributed ledger**
  - And a **payment system**
  - And the **value *itself* being transferred**.

- Outside of bitcoin, **money creation** (issuance), and **accounting** (keeping track of money received/spent), **is centralized**, and includes the following separate layers:
  - **Central Bank issuance** of money
  - **The type** of money being traded (gold, silver/ USD/EUR/YEN/ZAR etc)
  - **The amount** of money being traded
  - **The ledger of account**, whether written or digital
  - **The trusted parties** who enter the numbers into the ledgers
  - **The trusted parties** who keep the physical ledgers safe, or who maintain the computer databases
  - **The trusted security teams** who work to prevent hacking of the databases

- With bitcoin, **all these layers are folded into one!**

- While this might sound more centralized, Satoshi's genius made it such that the opposite is true.

- It is 100% Decentralized!

- Bitcoin has NO central point of failure.

- The only way it could all be rolled into one, and be decentralized, is that the distributed ledger is maintained by a voluntary, world-wide, ad hoc group of people voluntarily mining and/or running full nodes.

- And, the incentives of the network encourage everyone to play by the rules.

- You can join us!

Bitcoin is
a peaceful revolution

Bitcoin is Hope

HOW DOES bitcoin WORK?

Rules not Rulers

tik-tok/
/next block

Cryptography (noun) /krɪpˈtɑːgrəfi/
: the enciphering and deciphering of messages in secret code or cipher
: the computerized encoding and decoding of information

~ Merriam Webster Dictionary

Hashing (verb) /ˈhæʃɪŋ/
: a method of encryption
: the process of using a mathematical algorithm against data to produce a numeric value (a hash digest) that is representative of that data.

~ crsc.nist.gov

Remember:

The bitcoin ecosystem includes >>

bitcoin: the digital **monetary asset**

Bitcoin: the **payment network** of miners and nodes

1 bitcoin = 100,000,000 satoshis (sats)
(**You can buy sats, a fraction of a bitcoin**)

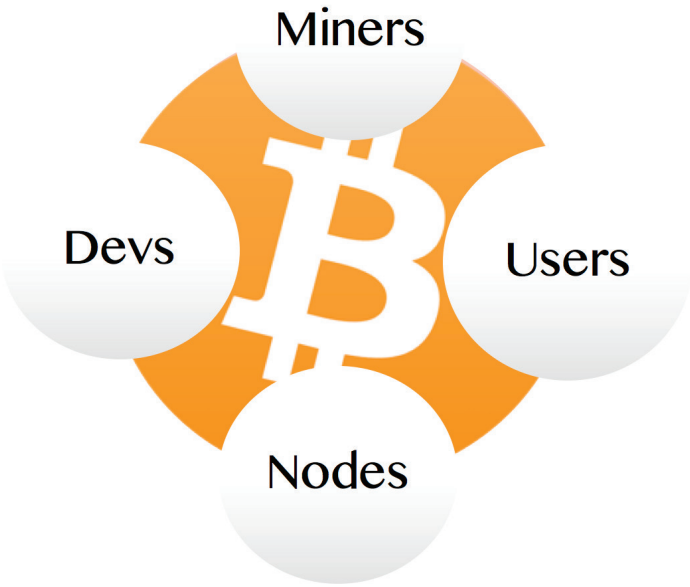
- Bitcoin uses **proof-of-work**, **public-key cryptography** and **peer-to-peer networking**, to process and verify payments in a global, distributed, online ledger.

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

~ Satoshi Nakamoto
Bitcoin White Paper, Pt.2, 2008
Describing how a bitcoin transaction works
in the distributed ledger

THE BITCOIN ECOSYSTEM..

consists of Miners, Nodes, Users, Developers
all working independently,
and simultaneously *inter*dependently,
to enliven that which is
BITCOIN!



MINERS

- **Specialized nodes (computers) that 'mine' the blocks** that become part of the bitcoin blockchain.

- In so doing, they **confirm the verified transactions made by users, mint new bitcoins and secure the entire network.**

USERS

- **You and me. All of us.** The people. **Acknowledging and appreciating value provided**, by transacting, giving, and receiving this energy money.

- **Storing our energy** for use later, as needed.

NODES

- **Nodes make up a decentralized, global, voluntary network of thousands of computers**, large and small, each independently **running the bitcoin blockchain, verifying transactions (thereby preventing double-spending), and helping to secure the system.**

DEVELOPERS (DEVS)

- **Coders, programmers, digital authors and seers, working to maintain and scale the network, improve security, privacy and user interface, translating code** to language and visuals that the rest of us can comprehend and utilize.

A BITCOIN TRANSACTION:

Ali wants to send Benji some bitcoin:

1. Ali **opens the bitcoin wallet** app on her phone and **clicks 'Send'**.
2. Benji **opens his wallet app** and **clicks 'Receive'**.
3. **If they are together:** Ali scans the QR code on the wallet app on Benji's phone.
4. **If they are not together:** Ali copies and pastes the address Benji texts her, into the address field in her wallet.
5. Ali **enters the Amount to send**, and hits '**Send**'.
6. **A few seconds later**, Benji will see the amount pending in his wallet.
7. If it was sent through Lightning it will be confirmed almost instantly, and is almost free.
8. If it was sent 'on-chain' (on the Bitcoin mainchain), it includes a small fee, and usually takes around 10 minutes to be confirmed. It can take longer, depending on traffic.

A BITCOIN TRANSACTION UNDER THE HOOD:

(Definitions of terms follow)

1. When Ali sends those sats to Benji, the payment **transaction** is **broadcast** to the network.

2. **The transaction gets verified by nodes** that make sure Ali really has the bitcoin to send, and that it has not previously been spent (to prevent double-spending).

3. Once verified by a node, it **waits in the mempool** with other people's transactions.

4. The transactions in the mempool **get added in a block to the blockchain** when a **miner** finds a **nonce** that satisfies the **difficulty algorithm**.

5. **Each block has a timestamp**.

6. This **creates immutability, and helps protect the difficulty algorithm adjustment from being manipulated.**

7. **Each block represents one confirmation** for the transactions included in it.

8. As blocks are created and added, approximately every ten minutes, the immutability of the blockchain increases.

TRANSACTION ~ Sending/receiving bitcoin

- A transfer of value in the form of satoshis, from one bitcoin holder to another.

NODE ~ A 'branch' of the bitcoin 'bank'. Anyone can run a node.

- Nodes, along with miners, users and developers, form the peer-to-peer Bitcoin network.
- Imagine **each full node as a ledger containing the balances of every private key.**
- They interact, and reach consensus (agree) with one another by accepting and validating transactions from other nodes, along with blocks from miners, and then relaying these onward to other nodes.
- Nodes are run by an ad-hoc group of thousands of volunteers around the world. A full node is one that has independently validated the entire Bitcoin blockchain, since the Genesis Block mined by Satoshi in 2009. It currently takes about 2-3 days and ~390GB of space.
- The more active nodes there are, the more distributed, and therefore resilient, the whole network becomes.
- There are **currently over 15,000 reachable, full nodes worldwide, & far more unreachable ones.**
- All participating nodes are equal.

BROADCAST ~ Letting the network know you are sending bitcoin to someone.

- When you click 'Send', your wallet signs the transaction with your private key, and lets all the other nodes know of your intention to transfer value so that they can validate it.

MEMPOOL ~ A transaction waiting room

- This is the 'waiting room' where validated transactions are sent to be picked up by a miner and added to a block.

BLOCK ~ A 'page' in the bitcoin ledger

- The Bitcoin distributed ledger is made up of digital 'blocks'. Each block contains verified bitcoin transactions that keep the global ledger accurate and current. They also contain the nonce, a timestamp and a hash of the previous block, all of which contribute to the immutability of the bitcoin blockchain.

BLOCKCHAIN ~ The whole bitcoin ledger

- The bitcoin blockchain is the distributed ledger that contains every block, and every bitcoin transaction ever made since the Genesis block was mined by Satoshi in 2009.

MINER ~ A specialized node that both confirms transactions and issues new bitcoins.

- Bitcoin miners are specialized computers. They direct lots of computing power (hashrate) in a digital lottery to guess a number that will satisfy the current difficulty algorithm, thereby 'mining' a 'block' (a piece of the ledger).
- A mined block is timestamped and added to the blockchain (aka timechain).

DIFFICULTY ALGORITHM ~ A special, adaptive design that helps keep new bitcoin issuance predictable.

- This was one of Satoshi's genius solutions to help protect the bitcoin issuance from outrunning itself, as more advanced computers are developed.
- When more miners come online, the target number (nonce) in the 'lottery' gets smaller, and therefore more difficult to find.
- When less miners are online, it gets easier.
- The algorithm **adjusts automatically every 2016 blocks** (about every two weeks), to ensure a predictable rate of supply, where one block is mined approximately every ten minutes.

NONCE ~ A 32-bit random number

- A 32-bit random number that miners add to the end of the hashed list of transactions, to attempt to satisfy the difficulty target to mine a block.
- When a miner finds a nonce that leads to generating a hash below the current target number, they have mined a block and get to add it to the blockchain and claim the bitcoin block reward.

TIMESTAMP ~ Stamps the time

- Every block mined has a timestamp added to it.
- This is for added security, immutability and to help establish the difficulty adjustment.

IMMUTABILITY ~ Cannot be changed.

- This means the blockchain is 'set in digital stone'.

PROOF-OF-WORK (PoW) ~ Cryptographic proof that difficult work was done to satisfy an algorithm.

- Miners use the PoW algorithm to prove they have used a lot of computational power via electricity (work), in order to achieve consensus in a decentralized manner, and to prevent corrupt actors from spamming the network.

PUBLIC KEY CRYPTOGRAPHY ~ A process that creates the digital keys to access your bitcoins

- This is a system whereby two keys are created through a cryptographic algorithm.
- **One key is public** - Like your bank account number, that you can give people to send bitcoin to you for goods, gifts or services.
- **The other key is private** - Only you have a copy, and you use it to unlock your account to access your bitcoin, just as a password unlocks your online bank account.

PEER-TO-PEER (P2P) NETWORK ~ A decentralized network with no middlemen

- Full nodes (peers) collaboratively maintain a peer-to-peer network for block and transaction validation. In this type of network, each node is able to both request/provide data from/to its peers. There are no gatekeepers.

LIGHTNING NETWORK ~ A network built on bitcoin, that makes it possible to send/receive sats very fast and almost for free.

- Lightning is a Layer 2 scaling solution. This means it provides a way for bitcoin to scale, giving it the potential to process millions of transactions per second (TPS)

WALLET ~ A 'wallet' is a software app that holds the cryptographic keys to access your bitcoin.

- It can be on a phone, computer or on a separate small hardware device.
- A bitcoin wallet would more accurately be called a signing device. Your bitcoin never actually leaves the blockchain, the digital ledger.
- When you wish to send or spend your bitcoin, the wallet will sign and broadcast the transaction to the network, so that it can be verified and added into a block on the blockchain.

DEVELOPERS ~ Computer programmers

- Cypherpunks/programmers that maintain the network, improve security, check for bugs, submit pull requests (for new updates or features), review pull requests, audit the code.

PUBLIC KEY ~ Like a bank account number for receiving bitcoin.

- You can give it to people to send you bitcoin, just like you would give your account number to someone so they can send you fiat.

PRIVATE KEY ~ For securing, accessing and sending bitcoin, like the key to a safety deposit box.

- A bitcoin private key is a secret string of numbers and letters that allows you to send/spend your bitcoin.
- Only you have a copy. **It is very important to keep it very safe and secure, as anyone who obtains a copy can spend your bitcoin.**

DISTRIBUTED LEDGER ~ A ledger maintained by everyone who wishes to help maintain it.

- Instead of a centrally-controlled ledger that is invisible to the public, like one that a bank maintains, Bitcoin is a transparent, open, decentralized ledger visible to anyone, anytime.
- The addresses are strings of letters and numbers, with no names attached.
- While pseudonymous, it is possible to track transactions, especially if the bitcoin was bought from a centralized KYC exchange.
- One must trust that the banks are keeping their ledgers honestly.
- The Bitcoin network, on the other hand, is trustless and anyone can audit it anytime.

MORE ON MINING

- Bitcoin is 'mined' by specially designed, powerful computers all over the world called ASIC miners, Application Specific Integrated Circuit miners.

An Antminer S9 ASIC bitcoin miner

- **Miners devote computing power AKA hashrate, via electricity to the network**, to add blocks to the Bitcoin blockchain.

- These computers run 24 hours a day, usually in sets of a few, to a few hundred or thousand.

- **They are basically running a lottery. When one of them guesses an answer** (the nonce), that generates a hash that satisfies the current difficulty target, **they get to add the next block to the timechain**.

- **All the above is the proof-of-work (PoW) needed to birth new bitcoins.**

BITCOIN BLOCK REWARD

- For their work, they get:
  - A reward in the form of freshly minted bitcoins.
  - All the fees from the verified transactions included in that block.

- **When you send bitcoin to someone, that transaction includes a fee** and needs to be verified by a miner, and then included in a block.

- The **bitcoin block reward** gets cut in half every four years.

- It is **currently 6.25 bitcoin** per block that is mined.

- **The next 'halving' will be in 2024**, at which point the block reward will drop to 3.125 bitcoin per block mined.

- As mentioned before, **this keeps the issuance stable.**

- **In the year 2140, the last piece of bitcoin will be mined.**

- After that, miners will only get the fees from the transactions they verify in each block.

In a few decades when the reward gets too small, the transaction fee will become the main compensation for nodes (miners).

~ Satoshi Nakamoto

- **Miners will always be needed to verify transactions, thereby keeping the network secure.**
- It is getting easier for anyone to mine at home.
- While one needs to be aware that there are costs involved, and profitability is low for home miners, it is a powerful way to help secure and keep the network decentralized.

- Miners last quite a few years. There are currently many Antminer S9's for example, that have been running for over 6 years.

- When miners are retired **they can easily be taken apart and recycled.**

- **Tons of fascinating innovation is happening, with people using miners to heat their homes, saunas and even hot tubs!**

A WORD ON THE LIGHTNING NETWORK

- **Bitcoin blocks are intentionally small*** (1MB each), resulting in the bitcoin main-chain being able to process about 7 transactions per second (TPS).

- Visa processes about 4000 TPS.

- Also, **it generally takes a minimum of 10 minutes for the first confirmation to go through on a main-chain transaction** (since a block is mined every ~10 minutes).

- This is not practical if you are at a store and want to make a quick payment for your goods.

*** Important Detail:** The reason the blocks are small, is to keep **the blockchain small enough for anyone to run their own node at home**, which **helps keep the network decentralized. Satoshi realized the importance of this ↓**

> *Bitcoin users might get increasingly tyrannical about limiting the size of the chain so it's easy for lots of users and small devices.*
>
> ~ Satoshi Nakamoto, 2010-12-10

➢ **READ**: 'The Blocksize War' by Jonathan Bier

- Enter, the **Lightning Network (LN), a Layer 2 *bitcoin scaling solution.***
- **'Layer 2'** means **it is built on top of bitcoin**.
- **'Scaling Solution'** means it allows the network to:
  - **Vastly increase the speed of processing.**
  - **Vastly increase the number of transactions it can process per second.**
  - **Make micropayments possible.**

- The Lightning Network can be (sort of) thought of like a tab you might keep with some friends at the bar.

- You keep track between all of you who owes what (like a Lightning Network channel), and at the end of the night your group settles with the barman ('the main-chain').

- **Lightning channels can stay open for days, weeks or months before being 'settled' on the main chain.**

BENEFITS OF ⚡:

- **VOLUME** ~ The volume of transactions per second is in essence limitless, as countless channels can be opened at the same time, each keeping their own 'tab'.

- **MICROPAYMENTS** ~ You can send as little as 1 satoshi (currently $0.0003).

- **SPEED** ~ It usually takes between a millisecond and a few seconds to receive a payment.

- **PRIVACY** ~ Transactions are not stored on the open, public bitcoin blockchain. In some ways it is even more private than cash, because with Lightning, even the other party does not necessarily know who you are, as your payment 'hops' through different channels to reach the receiver.

  To be clear, I am not saying it is 100% impossible to uncover, just far more so than with payments on the bitcoin main-chain. It would take an immense of time and energy to establish with certainty who was making payments to whom, and it would not always be possible to do so at all.

  - **Enjoy an amazing visualization** of the Lightning Network at: lnrouter.app/graph

Bitcoin itself cannot scale to have every single financial transaction in the world be broadcast to everyone and included in the blockchain. There needs to be a secondary level of payment systems which is lighter weight and more efficient.

~ Hal Finney, 2010-12-30
Early cypherpunk & the second person to run Bitcoin

Think of it like this:

- Bitcoin: **Savings Account** ~ Slower transactions for larger amounts.
- Lightning: **Checking Account** ~ Very fast transactions for smaller amounts.

Bitcoin enhanced by Lightning can be viewed as both a product (digital property) and a service (open monetary network). The ability to transfer monetary energy through time and space without government intervention or conventional banking is enormously valuable to humanity.

~ Michael Saylor @saylor
CEO Microstrategy

HOW TO bitcoin

To Bitcoin: (verb) /tuːˈbɪtkɔɪn/

I hereby propose making 'to bitcoin' a verb, that encapsulates the fullness of participating in the bitcoin/Bitcoin eco-system.

Ok, now that you have, hopefully ;) been orange-pilled, and are ready to become your own bank, participating in the world's first global freedom money, here comes the fun part!

BECOMING YOUR OWN BANK

- This is where the **really epic shift** in becoming financially self-sovereign lies, and, it can take time to fully grok what it means.

- Some **intention and dedication is required to understand how to do this in the most secure way possible.**

- In the spirit of keeping this book 'the simplest bitcoin book ever written', I will provide an outline here, and then I offer resources at the end for you to dive in to, that go much deeper than the scope of this primer.

> HODL: (verb) /ho'dill/
>
> : to hold on to your bitcoin
> : to not sell
>
> (from a 2013 bitcointalk.org post, where the poster professed to be drunk, and misspelled 'HOLD'
> - Google it, worth the read ☺)

While the network is still growing, there is much value in the millions of global hodl'rs of last resort.

ACQUIRING BITCOIN

- **Bitcoin enters the market by miners selling some of the bitcoins they receive as rewards**, in order to pay for their operating costs.

- **You can acquire bitcoin by buying on a peer-to-peer trading platform, by accepting it as payment for goods or services you offer, as a gift, or by mining it**. (A very last resort, not recommended, is from an exchange).

- When you receive it, you are technically receiving the private keys with which to access your bitcoin.

- **The bitcoin itself never leaves the blockchain.**

- You can acquire bitcoin either anonymously, or with ID verification (KYC - Know Your Customer)

- KYC is required by law to fulfill AML (anti-money laundering laws) when buying from exchanges.

- **Being that bitcoin is freedom money, I highly recommend buying non-KYC bitcoin.**
- **This preserves your right to privacy in the future.**

Non-KYC >> Anonymously

How to Get non-KYC Bitcoin (No ID):

RECOMMENDED

1. Select a bitcoin-only wallet app.
2. Choose a method (see below).
3. Buy, receive or mine bitcoin.
4. Withdraw your bitcoin to your wallet.
5. HODL

- **Buy it from Bisq or HodlHodl**. Check out bisq.wiki to learn how. It can take a little time to master, but it is sooo worth it! Stay KYC-free!

- **Buy it from a bitcoin ATM** >> Be sure to check, as some require ID. Others just ask for a name and number (you can use a temporary phone #).

- **Buy an Azteco voucher.** Visit azte.co for location

- **Earn it for work you do** ~ Ask to be paid in bitcoin. Offer to discount your price.

- **Buy it in person at a bitcoin meet-up**.

- **Mine it** ~ It is getting easier to mine at home, or you can join a mining pool, but then DYOR to stay KYC-free.

KYC >> ID Verification Required

How to Buy KYC Bitcoin (with ID):

NOT RECOMMENDED

1. Select a bitcoin-only wallet app.
2. Choose a bitcoin-only exchange.
3. Create an account.
4. Link a payment method.
5. Fulfill the KYC requirements.
6. Buy bitcoin.
7. Withdraw your bitcoin to your own wallet.
8. HODL

- **Be aware that your bitcoin will be forever linked to your identity** if you buy it this way.
- If you choose this method, I recommend finding a reputable ***bitcoin only exchange***.
- ***Be sure the exchange allows you to withdraw your bitcoin to your own wallet!***
- **Exchanges are required by law to 'KYC' you.**
- They will take **your full name, address, social security number, email, phone number and often a photo of you holding your ID**.
- **Confirm that the exchange has both phone and email support** for customer service.

- Have them walk you through sending your bitcoin from your account with them, to your own wallet, so that you are self-custodying your bitcoin = **Holding your own keys.**

> - **This does NOT erase the fact you bought bitcoin from them…ever.**
> - **Transactions are traceable on-chain, and in many countries you are liable for taxation when spending your bitcoin.**

- **Avoid buying through Venmo and Paypal**, as **you cannot currently withdraw your sats** to your own self-hosted wallet.

- As they say on BT (bitcoin twitter):

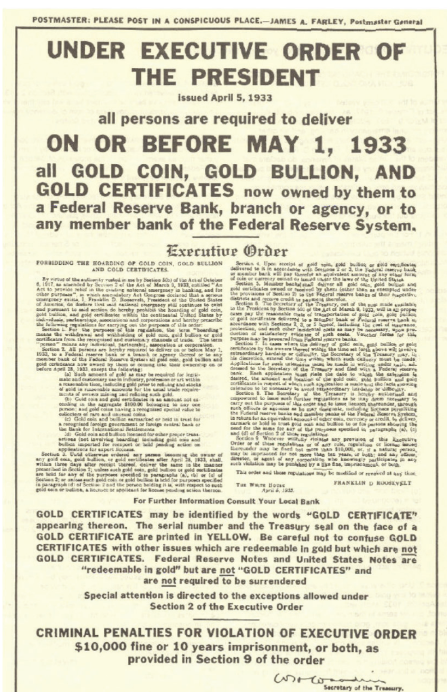
> **"No keys, No cheese"** or
> **"Not your keys, Not your bitcoin"**

- What this means is, so long as a centralized service is holding the private keys to your bitcoin, there remains the possibility that their platform gets hacked, or that they undergo regulatory capture and you lose your bitcoin.

EO 6102

- This happened with gold in 1933. **President Roosevelt issued Executive Order 6102, which required every US citizen to turn in most of their gold in exchange for bank notes.**

- The gold was valued at $20.67/oz. The following year, the government increased the price of gold to $35/oz with the Gold Reserve Act of 1934, effectively devaluing the notes people had received, since the value of their notes never went up with the inflated gold price.



POSTMASTER: PLEASE POST IN A CONSPICUOUS PLACE.—JAMES A. FARLEY, Postmaster General

UNDER EXECUTIVE ORDER OF THE PRESIDENT

Issued April 5, 1933

all persons are required to deliver

ON OR BEFORE MAY 1, 1933

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

Executive Order

FORBIDDING THE HOARDING OF GOLD COIN, GOLD BULLION AND GOLD CERTIFICATES.

THE WHITE HOUSE
April 5, 1933.

FRANKLIN D. ROOSEVELT

For Further Information Consult Your Local Bank

GOLD CERTIFICATES may be identified by the words "GOLD CERTIFICATE" appearing thereon. The serial number and the Treasury seal on the face of a GOLD CERTIFICATE are printed in YELLOW. Be careful not to confuse GOLD CERTIFICATES with other issues which are redeemable in gold but which are not GOLD CERTIFICATES. Federal Reserve Notes and United States Notes are "redeemable in gold" but are not "GOLD CERTIFICATES" and are not required to be surrendered

Special attention is directed to the exceptions allowed under Section 2 of the Executive Order

CRIMINAL PENALTIES FOR VIOLATION OF EXECUTIVE ORDER $10,000 fine or 10 years imprisonment, or both, as provided in Section 9 of the order

Secretary of the Treasury.

U.S. Government Printing Office: 1933

- It took until 1975, 42 years, for EO6102 to be repealed.

- While this is unlikely, it is not impossible. At this stage, we have little idea how the regulators are going to respond to bitcoin as it continues to gain popularity and more widespread adoption.

- So far, there has been a mixed reception. For the time being however, it seems that many understand, or perhaps just accept, that bitcoin cannot ultimately be stopped.

- There are a number of politicians starting to speak in support of bitcoin as part of their platform. There are also some against it.

- Ultimately, it would be in the interest of every government to embrace it and add it to their balance sheets, as a hedge against their rapidly inflating, debasing fiat currencies.

- El Salvador is way ahead at this point, having made it a form of legal tender in 2021.

- It is exciting to see which country will be next!

SECURELY STORING BITCOIN

- Once you have taken the life-changing step of buying your first ₿ (congratulations!), you need to decide how to **securely store it**.

- **Being your own bank is a powerful form of self-sovereignty.**
- And it **needs to be taken seriously**!

- *** Please DYOR > Do Your Own Research < beyond my basic recommendations here***

- The **bitcoin ecosystem is evolving every minute.**

- Twitter is a good place to stay on top of the latest developments (until a better, decentralized app gains traction).

CHECK OUT THESE SITES FOR TUTORIALS:

- BTC Sessions on You Tube
- Bitcoiner.guide
- Armantheparman.com

BITCOIN-ONLY WALLETS

- Bitcoin is best stored in your own
  - **self-hosted**
  - **non-custodial**
  - **bitcoin-only** 'wallet'
- A 'wallet' is actually a piece of software which is a signing device. It contains your private keys which it uses to sign a transaction you send (broadcast).

HOT WALLET

- **This is an online bitcoin wallet app, that you download to your phone or computer.**
- It is best used for smaller amounts, for day-to-day spending.

COLD STORAGE WALLET

- **This is an offline wallet**. Also known as a hardware wallet.
- It is a separate hardware device on which to store your keys. This is like a safety deposit box.

> - **Please DYOR to compare the features and trade-offs between the wallets.**

- While both work well, it is generally recommended to make use of a cold wallet once you have over $500-1000 worth of bitcoin, as it is more secure.

- **HOT WALLET APPS** - Non-Custodial

  Muun Wallet, Blue Wallet, Samourai Wallet (Android only), Sparrow Wallet, Green Wallet, Phoenix Wallet

- **COLD STORAGE WALLETS**

  Cold Card, Trezor, Passport, Keystone, Blockstream Jade, Seed Signer, Bitbox,

- ALWAYS purchase your cold storage wallet **direct from the manufacturer,** to be certain it has not been tampered with.

WALLET SET-UP

- **Follow BTC Sessions on YouTube** for excellent tutorials on wallet set-up (and lots more).

- When setting up your wallet, be sure to ***write down the 12- or 24-word Seed Phrase on paper.***
- *Keep it offline. Never take a screenshot of it.*
- STORE THE SEED PHRASE VERY SAFELY.
- VERY, VERY SAFELY!

- **Many companies make metal seed plates into which you can punch your seed phrase for added fire/water protection.**

- If you were to lose access to your hot or cold wallet, you can restore it with the seed phrase and recover your funds.

- You can do so on any wallet that supports the same type of BIP39 seed phrase (12/24 words).

- Best practice would be to store the derivation path of your wallet in addition to your seed.

- Remember: *Anyone who has the seed has access to your bitcoin!*

ON PRIVACY

- Privacy when **buying (non-KYC), securing, storing and spending** bitcoin is becoming more and more important, especially in light of recent events with bank accounts being seized/frozen.

- In addition, **general digital privacy is critical if you wish to gain online sovereignty, and protect yourself from undue surveillance and fraud.**

- Below are some current privacy focused services. It is beyond the scope of this book to go deeply into each of the following, so absolutely DYOR, and follow the accounts I mention below on Twitter for updates.

Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world.

~Eric Hughes, From 'A Cypherpunk's Manifesto'

PRIVACY GUIDES

- Bitcoiner.guide @BitcoinQ_A
- Econoalchemist.com @econoalchemist
- Sethforprivacy.com @sethforprivacy
- diverter.hostyourown.tools @Diverter_NoKYC
- Citadeldispatch.com @ODELL
- KYCnot.me
- Lopp.net @lopp > Click Resources > Privacy
- Privacytools.io
- Enegnei.github.io
- Restoreprivacy.com @ResPrivacy
- Keepitsimplebitcoin.com @KISBitcoin
- @SovrnBitcoiner
- K3tan.com @_k3tan

VPN (Virtual Private Network to Obscure your ISP)

- Mullvad.net - Pay with bitcoin

TWO-FACTOR AUTHENTICATION APPS

- Authy
- Google Authenticator
- Yubi Key

PRIVACY-FOCUSED BROWSERS

- TOR
- Firefox
- Brave

ENCRYPTED 'NOTES' APP

- StandardNotes.com

PRIVACY-FOCUSED SEARCH ENGINES

- Duck Duck Go
- Firefox
- Startpage
- Qwant

PRIVACY-FOCUSED MESSAGING APPS

- Signal
- Session
- Element

RUNNING YOUR OWN NODE

- Bitcoin Core
- Ronin Dojo
- Run Citadel
- Raspi Blitz
- Umbrel - If you just run your bitcoin node on it.

MIXING SERVICES

- Coinjoin
- Paymarket
- Coinswap

CELL PHONES/SINGLE USE PH #'S

- Run Calyx OS on an Android Pixel
- Text Verified

PRIVATE SPENDING

- Pay with Moon
- Bitrefill
- Paxful

PRIVATE RECEIVING ADDRESS BOT

- PayNym

DECENTRALIZED SOCIAL MEDIA

- Mastodon
- Zion (monthly fee, will have bitcoin added as a payment option)

The possibility to be anonymous or pseudonymous relies on you not revealing any identifying information about yourself in connection with the bitcoin addresses you use. If you post your bitcoin address on the web, then you're associating that address and any transactions with it with the name you posted under.

If you posted under a handle that you haven't associated with your real identity, then you're still pseudonymous.

~ Satoshi Nakamoto 2009-11-25

For greater privacy, it's best to use bitcoin addresses only once. You can change addresses as often as you want.

~Satoshi Nakamoto 2009-11-25

DISPELLING bitcoin FUD
(Fear Uncertainty Doubt)

- Below are some common arguments against, or fears about, bitcoin.
- These are largely unfounded, resulting from ignorance, or perhaps incomplete understanding.
- I provide brief rebuttals to each here, and at the end you will find pointers to more in-depth resources rebutting all the FUD.

BITCOIN USES TOO MUCH ENERGY

> *The heat from your computer is not wasted if you need to heat your home… It's equal cost if you generate the heat with your computer.*
>
> ~ Satoshi Nakamoto 2010-08-09

> *At first, the production of a commodity simply because it is costly seems quite wasteful. However, the unforgeably costly commodity repeatedly adds value by enabling beneficial wealth transfers. More of the cost is recouped every time a transaction is made possible or made less expensive. The cost, initially a complete waste, is amortized over many transactions.*
>
> ~ Nick Szabo
> Cypherpunk

- 'Too much' energy is a value proposition that must consider how we value the *purpose* of the energy use.

- When one considers that the Christmas lights in the US use as much electricity as the entire Bitcoin network, then perhaps one can see that it is all relative!

- Using energy, even a whole lot of energy, to secure the hardest, most censorship-resistant money humanity has ever known, is 1000% worth it!

- In comparing bitcoin energy usage to that used by the legacy system, we also need to consider the 'full stack' on both sides:

Bitcoin Ecosystem	Legacy Fiat System
ASIC Miners	BIS
Nodes	Central Banks
Hardware Wallets	National/Regional Banks
Software Wallet Apps	Military Industrial Complex
	Backup Data Banks
	Physical Money Printing
	Online Banking Apps
	Network of ATMs

- By using bitcoin, we will ultimately reduce energy usage in a multitude of other areas, most notably by no longer needing the Military Industrial complex to protect the petro dollar.

> *Bitcoin is a property right that is independent of the monopoly on violence.*
>
> ~ @breedlove

- Also, the rampant consumerism that is required to keep the debt-based system afloat, will over time be curtailed, as **hard money naturally incentivizes prudent spending and saving** (since your savings will actually hold their value, a concept we have not experienced since being off the gold standard).

- **Lastly, and importantly, bitcoin mining is already reducing pollution by capturing flared natural gas and using it to power the miners**. Since miners seek low electricity costs, it is also likely to be the biggest driver toward renewable low cost energy, since the incentives match up.

- **Informed deep dives on Bitcoin and Energy** have been written by Nic Carter, Troy Cross, NYDIG, the video 'This Machine Greens' by Swan Bitcoin on YouTube, and an excellent episode of the 'What is Money' show (WiM161) with B.Quittem.

BITCOIN IS A PONZI

- **Bitcoin is not a Ponzi:**
  - Old investors are not paid any money by new investors.
  - When buying bitcoin, no one is promising a return on your investment.
  - There is no leadership or promotions team.
  - There was no pre-mine.
  - **Read:** 'Why Bitcoin is Not a Ponzi' by Lyn Alden for more.

BITCOIN IS TOO SLOW

- While the Bitcoin base layer is slow, the 2nd layer **Lightning Network built on the base layer is … lightning fast!**

- Bitcoin's network can process about 7 transactions per second (TPS).

- The Visa network claims it can process up to 24,000 TPS, although 4,000 TPS is closer to actual usage.

- **The Lightning Network, a second layer solution built on Bitcoin, has the capacity to process millions of transactions per second!**

GOVERNMENTS COULD BAN BITCOIN

- Some governments have tried, like China, India and Nigeria for example. In each case, the use of bitcoin rises rapidly by the people of said country.

- **There is no way for governments to truly 'ban' bitcoin,** as it is by its nature permissionless and censorship-resistant. It is code and code is speech.

- That said, governments can make it harder to buy and sell with, and into fiat. They can also tax it as a commodity, like they do in the US.

- **Ultimately, it will not be in their favor to try and ban it, since bitcoin is inevitable and they are starting to see that.** They would be far smarter to add it to their country's balance sheet as a hedge against their inflating fiat currencies.

> *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

- **Great Article:** Can Government Stop Bitcoin? by Alex Gladstein, CSO of the Human Rights Foundation

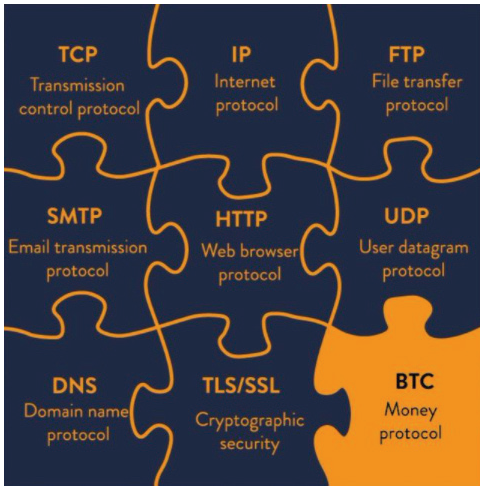
BITCOIN IS OLD TECH

- **More like 'ultimate tech'**, with regards to digital scarcity, decentralization and solving both the double-spending problem and the Byzantine General's problem. Once discovered, it cannot be re-discovered.

- **Once the wheel was invented, it could never be reinvented.**

- The TCP/IP protocol that the internet runs on has been the standard for all computer networking since 1983. It is likely to continue being the standard for a long time.

- Once a prefect-solution, base layer technology is discovered that works optimally, it can last for hundreds, or thousands of years.



Credit: @DecouvreBitcoin

BITCOIN IS USED BY CRIMINALS

- **So is the dollar, and every other fiat currency in the world.** While these activities sadden me greatly, it is simply incorrect to attribute them to bitcoin itself. **Bitcoin is a tool, just like a knife, and it is up to each one of us how we use it.**

- Note: Since the Bitcoin blockchain is auditable, it is actually a really bad choice for criminal activity.

QUANTUM COMPUTING COULD BREAK BITCOIN

- While this is a possibility one day in the future, **developers are already working on solutions for post-quantum encryption.** These would be implemented once needed.

- Bitcoin is only one of a multitude of online applications that rely on SHA-256 hashing for security. Even the military uses it, so there is massive incentive beyond the bitcoin community to develop new encryption protocols.

- In addition, if SHA-256 is broken, we will have a lot else to worry about beyond bitcoin.

BITCOIN HAS NO REAL VALUE

"Bitcoins' value is driven by its enforceable scarcity"

~ Fidelity Digital Assets

- **Rarity is the value. All money over all time has been valued because it had some measure of scarcity.**

- In addition, it was backed by the belief that it would hold its value, such that it could be traded in the future for something else of value.

- As the Bitcoin network grows, backed by the superior monetary properties it embodies, the network effect grows exponentially.

- The larger the network effect, the more value it, as a scarce asset, offers. Value is a reflection of demand, and as demand increases, value increases.

SOME PEOPLE HAVE TOO MUCH

- It is true that some people have far more than others. **In releasing the protocol openly, Satoshi allowed it to roam freely, and those that understood the potential it held either mined, or bought in early. It was the fairest and most organic way possible to present it to the world.**

- Over time, when the world is hyperbitcoinized, meaning we are living on a bitcoin standard, those that have more will naturally spend it into the economy.

- Even though at a certain point one will no longer be able to buy it with fiat, people will get paid for their work in bitcoin. Being paid in truly sound money will allow us to have real savings that will not be debased over time by inflation.

- While there will always be those with more wealth and those with less, due to a vast number of factors, **a bitcoin standard will make the membrane between wealth classes permeable,** as Aleks Svetsi says. This will allow both upward and downward mobility to be far, far more fluid than it is today.

- **Having been born into, and swimming our whole lives in a fiat world, it is almost impossible to imagine, and fully grok the implications of having a money that cannot be debased or manipulated!**

BITCOIN IS TOO VOLATILE

- **This is normal during the price discovery phase of a new monetary asset.** There is no other way for growth to happen when it is organic and emergent (as opposed to top down and ordained).

- In addition, at this stage of human existence, with exponential shifts happening in all spheres, it makes sense that something as rEVOLutionary as bitcoin will have wild swings.

- While those of us deep down the rabbit hole see it as the future, currently only about 1-2% of the global population holds bitcoin at this time. This makes it vulnerable to immense volatility.

- As it matures, and adoption increases, the volatility will decrease, and eventually it will stabilize and become a unit of account.

> *I'm sure that in 20 years there will either be very large transaction volume or no volume.*
>
> ~ Satoshi Nakamoto 2010-02-14

YOU CAN'T TOUCH A BITCOIN

- **This is a feature, not a bug.** The very fact that bitcoin is not physical is one of the biggest factors contributing to it's unconfiscatability!

BITCOIN COULD GET HACKED

- In the 14 years since it was launched, it has never been hacked.

- There have been hacks at exchanges however, so I highly recommend moving your bitcoin to your own self-custody wallet as soon as possible.

- It has been estimated that to break the SHA-256 encryption (that bitcoin uses) within 24 hours, a quantum computer would need 13,000,000 physical qubits. At this time, the current qubit record held by IBM is just 127 qubits.

- It is widely assumed that a quantum-safe encryption method will be developed well before it is needed.

> *Being open source means anyone can independently review the code. If it was closed source, nobody could verify the security. I think it's essential for a program of this nature to be open source.*
>
> ~Satoshi Nakamoto 2009-12-10

MORE ON DEBUNKING FUD HERE:

- Endthefud.org
- Bitcoinmythbusters.org
- Casebitcoin.com
- Safehodl.github.io/failure/
- Lopp.net - Misconceptions

Bitcoin is fundamentally different from any other digital asset. No other digital asset is likely to improve upon bitcoin as a monetary good because bitcoin is the most (relative to other digital assets) secure, decentralized, sound digital money and any "improvement" will necessarily face tradeoffs.

~ Fidelity Digital Assets Report, 'Bitcoin First', Jan 2022
Chris Kuiper, CFA, Director of Research
Jack Neureuter, Research Analyst

ON THE PRICE OF BITCOIN

- I see hodling (holding) bitcoin like having a long-term savings account.

- The daily price doesn't matter, as it is expected to be volatile (go up and down) for some years yet.

- As I mentioned previously, this is normal for a new asset undergoing price discovery.

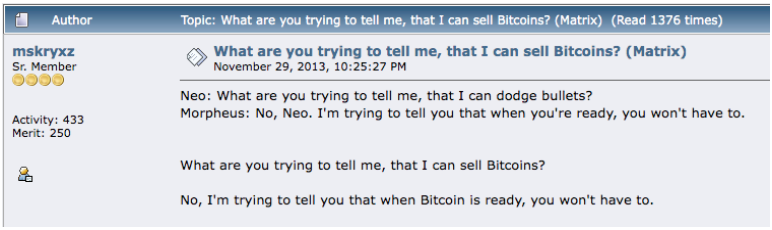
- If one zooms out on the BTC/USD price chart, you will see that it has increased by +31,296% since 2009, averaged out to ~200% per year.

- The price swings reflect various news articles, regulatory updates, market demand, fear and excitement. It's a roller-coaster!

- The longer you hodl, the more you learn and understand the fundamentals, and the more you realize the profound implications of having sound money, the less the price matters.

- In the end, 'price' won't matter at all, as bitcoin will be the unit of account.

- That said, I must add this disclaimer: General advice is to put in only what you 'can afford to lose', since there are, of course, no guarantees.



Original bitcointalkforum.org source for one of the most classic bitcoin memes of all time.

IN THE MEANTIME, ON TAXES

>> **Disclaimer**: This is **not** financial or tax advice!

- In the US tax code, bitcoin is currently seen as a commodity, so there are potential tax implications if you sell it back into fiat, or even if you buy something with your bitcoin.

- If the price went down before you sold/spent it, you can claim a loss.

- If the price went up, you are supposed to claim a capital gain, and pay between 10-30% CGT (Capital Gains Tax).

- The amount depends upon several factors, such as how long you held it before selling or spending, and in which tax bracket you land.

- If you plan to sell or spend bitcoin, especially larger amounts, you may want to consider consulting with a tax professional.

- If you simply buy and hold, you currently do not have any taxable events regarding bitcoin.

- And if you buy non-KYC…

WHY bitcoin ONLY?

Of the over 20,000 (yes, 20,000!) cryptocurrencies out there, bitcoin is the ***only one*** that is:

- **TRULY decentralized**
- With a **TRULY distributed ledger**
- A **TRULY hard capped supply**
- A **TRULY immutable ledger**
- A **network effect** built over 14 years
- And a **monetary policy that cannot be f*cked with!**
- **Every other cryptocurrency has a small, centralized group who controls the supply, and/or has the power to change the base layer protocol (monetary policy).**
- **This is just like the central fiat banking system we see today.**
- Centralized power like this begs for manipulation and corruption.
- See the altcoin pump/dump scam described on the following page.
- Also:

  Stephan Livera Pod (SLP306) with Guy Swann
- A list of altcoin/defi rug-pulls:

  https://rekt.news/leaderboard/

ALTCOIN PUMP AND DUMPS

- Sadly, these are real, and happen daily with 'cryptos/tokens' other than bitcoin.
- There are various iterations, but one of the most common types is the following:

- **Token Created:** A new crypto token gets made (this is far easier than it sounds!)

- **Website:** Often, a shiny, fancy website is created to make the token look legit.

- **Paid Influencers:** Promote it on social media.

- **Paid Insider Groups:** The info is sent to leaders of some of the hundreds of 'Trading' or 'Investment' Groups, where people pay monthly or annual fees to get 'insider intel'.

- **Pre-Launch:** The paid influencers and paid group leaders buy first, at the bottom price.

- **Launch:** The token is 'launched' by these influencers/group leaders, who tell their followers: "Quick, buy now!"

- **Pump:** The price pumps fast as their followers scramble to get in early.

- The rapidly rising price entices regular people to buy in, in the hopes of making their fortune.

- Which in turn has the effect of pumping the price further.

- **Dump:** This sad part usually happens fast. At a certain point, the paid group leaders sell their tokens, 'at the top'. Then they tell their followers to sell.

- Because so many people sell at the same time, and liquidity is generally low since it is a new coin, the price drops fast.

- **Panic:** The price drop causes panic amidst the general public, who have no idea of these back-door shenanigans, and they start to panic-sell.

- **Bag Holders:** The end of this sad story is that those left 'holding the bag', will likely be holding their bags forever.

- Without any real value or fundamentals, most of these tokens never recover a market price.

SECURITY & AVOIDING SCAMS

- **Stick with bitcoin only.**
- **Be super vigilant** about your cyber security!
- **Do your own research** and **secure your bitcoin** with utmost care.
- **NEVER give your seed words to anyone you wouldn't give the key to for your stash of gold!**
- **NEVER click on any links** in your email that ask you to confirm account details of any kind. **Instead go to the official website directly** and check if you have any notices requiring any actions.
- **BE AWARE** that there are endless imitations of accounts with large followings on social media. If an influencer randomly DMs you, it is probably a scam.
- **AVOID all the scams popping up on social media** accounts, promising to double your bitcoin if you send some to them! Not happening!
- **AVOID those same 'double your crypto' scams** on You Tube.
- **BE CERTAIN** about the address you are sending your bitcoin to, as transactions are irreversible.

SATOSHI'S NUMBERS
369 CLOCK

Bitcoin is designed to mine 6 blocks per hour >> one block every ~10 minutes.

- 24 hours in a day

  2+4=**6**

- That works out to 144 blocks per day

  1+4+4=**9**

- 52560 blocks per year

  5+2+5+6+0=18
  1+8=**9**

- 52704 blocks per leap year

  5+2+7+0+4=18
  1+8=**9**

- 21 Million coins:

  2 + 1 + 0 + 0 + 0 + 0 + 0 + 0 = **3**

- 33 Halvings:

  3 + 3 = **6**

- Difficulty adjusts every 2016 blocks:

  2 + 0 + 1 + 6 = **9**

  ~ Based on a Tweet by @level39

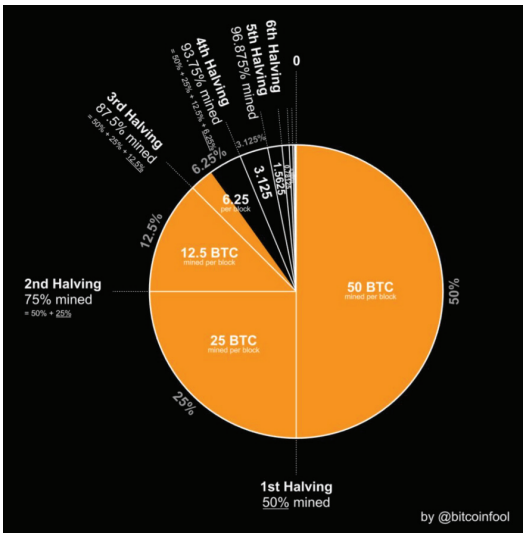
- The block reward halving happens every 210,000th block (every four years)

  2 + 1 + 0 + 0 + 0 + 0 = **3**

"If you only knew the magnificence of the 3, 6 and 9, then you would have the key to the universe."
~ Nikola Tesla

BLOCK REWARD = % OF SUPPLY

- The block reward (number of bitcoins rewarded for each new mined block) represents the percentage of the total supply that will be mined during that epoch.
- For example, the current block reward between 2020-2024 is 6.25 bitcoin.
- In these same four years, 6.25% of the 21 million bitcoins will be mined.
- Satoshi, you continue to amaze!



Credit: @bitcoinfool

REWARD EPOCHS

Every four years, the bitcoin rewards get halved for each block mined. A Reward Epoch is that four year period.

- **Reward epoch 1**: 2009-2012

  = (50 bitcoin * 210,000 blocks) = 10,500,000 bitcoin
  1+0+5+0+0+0+0+0 = 6

- **Reward epoch 2**: 2012-2016

  = (25 * 210,000) = 5,250,000 bitcoin
  5+2+5+0+0+0+0 = 12
  1+2 = 3

- **Reward epoch 3**: 2016-2020

  = (12.5 * 210,000) = 2,625,000 bitcoin
  2+6+2+5+0+0+0 = 15
  1+5 = 6

- **Reward epoch 4**: 2020-2024

  = (6.25 * 210,000) = 1,312,500 bitcoin
  1+3+1+2+5+0+0 = 12
  1+2 = 3

- **Reward epoch 5**: 2024-2028

  = (3.125 * 210,000) = 656,250 bitcoin
  6+5+6+2+5+0 = 24
  2+4 = 6

- **Reward epoch 6**: 2028-2032

  = (1.5625 * 210,000) = 328,125 bitcoin
  3+2+8+1+2+5 = 21
  2+1 = 3

- **Reward epoch 7: 2032-2036**

  = (0.78125*210,000) = 164,062.5 bitcoin
  1+6+4+0+6+2+5 = 24
  2+4 = 6

SATOSHI'S BIRTHDAY

- *April 5, 1975* is the date Satoshi claimed as his birthday.

- While we cannot know if this was indeed his true birth date, it is very interesting.

- *April 5th* (1933) was the day that Executive Order 6102 was signed by US President Franklin D. Roosevelt "forbidding the hoarding of gold coin, gold bullion, and gold certificates within the continental United States."

- *1975* was the year EO 6102 was finally repealed, and US citizens were once again allowed to hold more than 5oz of gold, more than four decades later.

A NUMERIC PALINDROME 6102-2016

- *6102* was the number of the above-mentioned Executive Order.

- *2016* is the number of blocks mined during each difficulty adjustment (approximately 2 weeks).

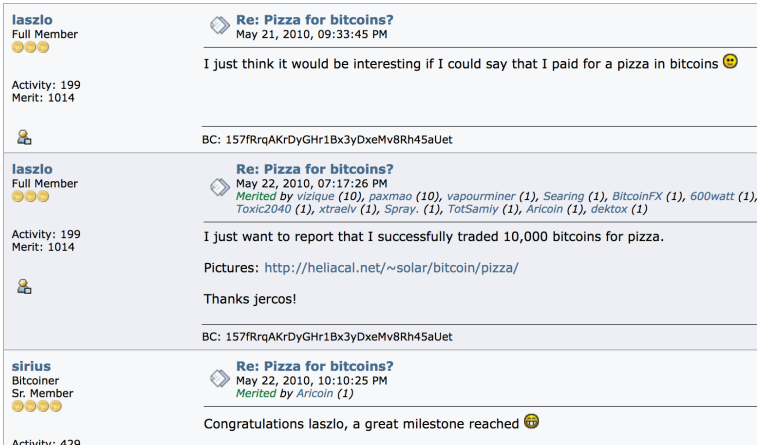
    - In both of the above examples, one could postulate that Satoshi was using numbers to indicate a reversal, an unwinding of the damage inflicted by government overreach.

BITCOIN PIZZA DAY

- May 22 is known as Bitcoin Pizza Day. This was the day that a guy, named Laszlo Hanyecz, announced on bitcointalkforum.org that he had successfully traded 10,000 bitcoin for pizza! Back then that was about $40.

- In today's prices, that would be ~$420,000,000 ☺

- It was a milestone for bitcoin, in that it was the first known incidence of someone trading bitcoin for a good or service. What a long way we have come!



laszlo
Full Member

Activity: 199
Merit: 1014

Re: Pizza for bitcoins?
May 21, 2010, 09:33:45 PM

I just think it would be interesting if I could say that I paid for a pizza in bitcoins

BC: 157fRrqAKrDyGHr1Bx3yDxeMv8Rh45aUet

laszlo
Full Member

Activity: 199
Merit: 1014

Re: Pizza for bitcoins?
May 22, 2010, 07:17:26 PM
Merited by vizique (10), paxmao (10), vapourminer (1), Searing (1), BitcoinFX (1), 600watt (1), Toxic2040 (1), xtraelv (1), Spray. (1), TotSamiy (1), Aricoin (1), dektox (1)

I just want to report that I successfully traded 10,000 bitcoins for pizza.

Pictures: http://heliacal.net/~solar/bitcoin/pizza/

Thanks jercos!

BC: 157fRrqAKrDyGHr1Bx3yDxeMv8Rh45aUet

sirius
Bitcoiner
Sr. Member

Activity: 429

Re: Pizza for bitcoins?
May 22, 2010, 10:10:25 PM
Merited by Aricoin (1)

Congratulations laszlo, a great milestone reached

5184x3456 (1/60) f/5.6 f(35)=78mm (flash)
2010-05-22 15:01:22 -0400

Download: IMG_0985.jpg

5184x3456 (1/60) f/5.6 f(35)=78mm (flash)
2010-05-22 15:01:29 -0400

Download: IMG_0986.jpg

BITCOIN CALENDAR OF NOTABLE DAYS

2008-08-18 ~ The domain name bitcoin.org was registered. (2+0+0+8+0+8+1+8 = 27, 2+7 = 9)

2008-10-31 ~ **Bitcoin White Paper Day:** The White Paper, titled "Bitcoin: A Peer-to-Peer Electronic Cash System"was published by an anonymous cryptographer named Satoshi Nakamoto, on the cryptography mailing list at metzdowd.com (2+0+0+8+1+0+3+1 = 15, 1+5 = 6)

2009-01-03 ~ **Bitcoin's Birthday:** The Bitcoin network was launched, when Satoshi mined the Genesis block. (2+0+0+9+0+1+0+3 = 15, 1+5 = 6)

2009-01-12 ~ The first bitcoin transaction took place, when Hal Finney received ten bitcoins from Satoshi. (2+0+0+9+0+1+1+2 = 15, 1+5 = 6)

October 5, 2009 ~ Bitcoin has a market price for the first time, of $0.001 per coin.

2010-05-22 ~ **Bitcoin Pizza Day:** The first known occurrence of bitcoin being used to buy a good or service, when Lazslo Hanyecz paid 10,000 bitcoin for two Papa John's pizzas! (2+0+1+0+5+2+2 = 12, 1+2 = 3)

2010-12-12 ~ The last confirmed time that Satoshi wrote on the bitcointalk.org forum. (2+0+1+0+1+2+1+2 = 9)

February 8, 2011 ~ Bitcoin reaches parity with the US Dollar for the first time.

March 3, 2017 ~ Bitcoin reaches parity with an ounce of gold.

August 21, 2021 ~ 1st **Annual Bitcoin Infinity Day** suggested by Knut Svanholm's meme:

Everything divided by 21 million. $\frac{\infty}{21{,}000{,}000}$

2021-09-07 ~ El Salvador becomes the first country to make bitcoin legal tender. (2+0+2+1+0+9+0+7 = 21, 2+1 = 3)

that was just a start…

here are more

RESOURCES FOR THE bitcoin RABBIT HOLE

"Curiouser and curiouser!" said Alice

MOVIES

- You can find these movies on You Tube

BITCOIN MOVIES:

- The Great Reset and the Rise of Bitcoin (2022)
- Where Did Bitcoin Come From (2021)
- This Machine Greens (2021) About Bitcoin & Energy
- Bit X Bit: In Bitcoin We Trust (2018)
- Bitcoin Big Bang (2018) About the 2014 Mt Gox hack
- Magic Money: The Bitcoin Revolution (2017)
- Banking on Bitcoin (2016)
- Deep Web (2015) About Silk Road & Ross Ulbricht
- The Bitcoin Gospel (2015)
- Bitcoin: The End of Money as We Know It (2015)
- The Rise and Rise of Bitcoin (2014)
- Bitcoin in Uganda (2014)

FIAT MONEY SYSTEM MOVIES:

- How is Money Created (2020)
- Hidden Secrets of Money Series - Mike Maloney ('13-'18)
- Who Controls All of our Money (2017)
- How the Economic Machine Works - Ray Dalio (2013)
- Inside Job (2010) - On events leading up to 2008 crash
- The Money Masters (1996)

BOOKS

About Bitcoin:

- **Layered Money** by Nik Batia
- **21 Lessons** by DerGigi
- **The Bullish Case for Bitcoin** by Vijay Boyapati
- **The Bitcoin Standard** by Saifedean Ammous
- **Bitcoin Clarity** by Kiara Bickers
- **Inventing Bitcoin** by Yan Pritzker
- **Independence Reimagined** & **Bitcoin: Sovereignty Through Mathematics** by Knut Svanholm
- **Check Your Financial Privilege** by Alex Gladstein
- **Hard Money You Can't F*ck With** by Jason A.Williams
- **Why Buy Bitcoin** by Andy Edstrom
- **Bitcoin Audible:** If you prefer listening to reading, Guy Swann, reads Bitcoin books and articles.

ABOUT THE CURRENT FIAT DEBT-BASED MONEY SYSTEM:

- **The Price of Tomorrow** by Jeff Booth
- **The Sovereign Individual** by JD Davidson and Lord W Rees-Mogg (not only about money)

PODCASTS

Listen on Fountain app to stream sats to hosts!
If not yet on Fountain, find these on Spotify and iTunes.

- **Citadel Dispatch** with Matt Odell
- **BitBuyBit Podcast** with Max Buybit
- **Bitcoin Rapid Fire** with John Vallis
- **The 'What is Money' Show** with Robert Breedlove
- **Stephan Livera Podcast**
- **This is Bitcoin Podcast** with Bitcoin Gandalf
- **Wake Up Podcast** with Aleks Svetski
- **The Bitcoin Standard Podcast** with Dr S. Ammous
- **Bitcoin Magazine Podcast**

- **The Bitcoin Matrix** with Cedric Youngelman
- **Bitcoin Fixes This** with Jimmy Song
- **Orange Pill Podcast** with Max Keiser and Stacy Herbert
- **What Bitcoin Did** with Peter McCormack
- **Bitcoin Audible** with Guy Swann reading books/articles

FREE COURSES

- **Saylor Academy** - Bitcoin for Everybody
- **Looking Glass Education** - Money & Bitcoin Courses
- **Bitcoin Magazine** - 21 Days of Bitcoin Daily Lessons

WEBSITES

Each of these have a great compilation of resources:

- Nakamotoinstitute.org
- Bitcoinmagazine.com
- Bitcoin-only.com
- Bitcoin Wiki - En.bitcoin.it
- Lopp.net
- Casebitcoin.com
- Bitcoiner.guide
- Bitcoin.tv
- Learnmeabitcoin.com - Great simple btc tech explainer!
- Hope.com
- Bitcoin-resources.com
- My irstbitcoin.io (Available in Spanish too)
- Whatisbitcoin.com

Inside Bitcoin's beating heart:

- github.com/bitcoin

BITCOIN ATMS

- **Coin ATM Finder** - coinatmfinder.com
- **Coin Radar** - coinatmradar.com

ARTICLES

- **Bitcoinmagazine.com** - Excellent, new articles daily!
- **SatoshisJournal.com** - Bitcoin education, news, stories!
- Many Twitter accounts below write on Medium, Substack

BT ~ BITCOIN TWITTER

Some cypherpunks, geniuses, goats & wild ones to follow!
Through these accounts, you will find 1000's of plebs and other deep thinkers,
all on the journey.
BT is largely where this experiment is growing, unfurling in real time, across time and space, in the ethers of cyberspace, connected to the physical,
through all of us,
humans,
sharing a vision.
Then there are the quieter ones, developers working behind the scenes
without whom
none of this would be possible.
All of us
together
unleashed,
as bitcoin was unleashed upon us,
a blessing beyond measure.

TOPICS INCLUDE: Bitcoin, Proof-of-Work, Privacy, Philosophy, Monetary History, Code, Bitcoin Mining, Sociology, Game Theory, Austrian Economics, Bitcoin Education, Lightning Network, Regulatory Environment, Bitcoin's Energy Use, Core Devs, Bitcoin Communities, Bitcoin's Future.

Be warned: It helps to have a somewhat thick skin on Twitter, and know this, there is a lot of passion in defense of bitcoin. Keeping a clear line between it and all the altcoins takes work. Maintaining the clarity, security and purity of the only truly sound money the world has ever known is critical if we are to have a chance in these times a'coming.

Adam Back - @adam3us
Allen Farrington - @allenf32
Anil - @anilsaidso
Arman the Parman - @parman_the
Beautyon - @Beautyon_
Bitcoin Gandalf - @BTCGandalf
Bitcoin Q+A - @BitcoinQ_A
BTC Sessions - @BTCsessions
BTC Times - @btc
Brandon Quittem - @Bquittem
D++ - @D_plus__plus
Deterministic Optimism - @nvk
Dylan Le Clair - @DylanLeClair_
Gigi - @dergigi
Greg Foss - @FossGregfoss
Guy Swann - @TheGuySwann
Hugo Nguyen - @hugohanoi
Jack - @jack
Jameson Lopp - @lopp
Jeff Booth - @JeffBooth
Jimmy Song - @jimmysong
Knut Svanholm - @knutsvanholm
Luke Dash Jr - @LukeDashjr
Lyn Alden - @LynAldenContact
Marty Bent - @MartyBent
Matt Odell - @ODELL
Michael Saylor - @saylor
Natalie Brunell - @natbrunell
Nick Szabo - @NickSzabo4
Nik Bhatia - @timevalueofbtc
Parker Lewis - @parkeralewis
Pavlenex - @pavlenex
Pleb Lab - @PlebLab
Preston Pysh - @PrestonPysh
Robert Breedlove - @breedlove
Tomer Strolight - @TomerStrolight
Troy Cross - @thetrocro
Vijay Boyapati - @real_vijay

Thank you all for teaching me every day!

bitcoin COMMUNITY PROJECTS

- Below are some of the grassroots projects around the world that are working to create a circular, local economy with bitcoin.

- Follow them on Twitter to learn more or to donate:

- **Bitcoin Beach El Zonte** - El Salvador - @Bitcoinbeach

- **Bitcoin Ekasi** - Mossel Bay, South Africa - @BitcoinEkasi (Supports Surfer Kids NGO)

- **Bitcoin Beach Brazil** - Jericoacoara, Brazil -@BitcoinBeachBR

- **Bitcoin Jungle Costa Rica** - Dominical, CR - @BitcoinJungleCR

- **Bitcoin Venezuela** - Venezuela - @btcven

- **Bitcoin Smiles Dentistry** - El Salvador - @BitcoinSmiles

- **Saul M - El Salvador** - Chalatenango - @saulhodl

- **Apata Johnson - Nigeria** - @LumiExc

- **Bitcoin Lake** - Lake Atitlan - @LakeBitcoin

bitcoin INDUCED PONDERINGS

Shout out to
Satoshi
and all the
orange-pilled
dreamers
seers
cypher punk wizards
poets for freedom
keepers of wisdom
sovereign individuals
hodlers of last resort
fearlessly forging forward
alone together
for freedom
Vires In Numeris!

A RABBIT HOLE PONDERING

Bitcoin is really a rather fascinating 'thing'
Except it is not a 'thing'
In the sense that you cannot touch it
Yet it is touching millions of us
Around the world
Soon to be billions..
It is true that
It is digital bits and bytes
Algorithms and code
0's and 1's
And that if every single node
Mining node, full node and light node
Were somehow
Destroyed
It would no longer exist
In the way we know it
Are able to perceive it..
It would, however, still 'exist'
In the sense that quantum physics
Or gravity
Exists
Regardless of human perception..
In the sense that mathematics existed
Before humans codified it
Chose symbols to represent it..
Truth
Does not need us

WHY WILL ALL VALUE ACCRUE TO BITCOIN

- There are some interesting game theories that appear to converge when it comes to bitcoin, making the likelihood of it's growth and increased value over time more and more certain.

SCHELLING POINT

- Introduced in the 1960s by the American economist, Thomas Schelling, the Schelling point basically asserts that **people who cannot necessarily communicate with one another, can still converge on a decision or course of action, especially when a compelling solution to a problem presents itself** (-> bitcoin)

- In addition, as more people are drawn to the Schelling point, it attracts ever more people (-> bitcoin)

LINDY EFFECT

- In essence, the Lindy Effect states **that the longer an idea, a technology or a business has been around, the longer it is likely to endure**.

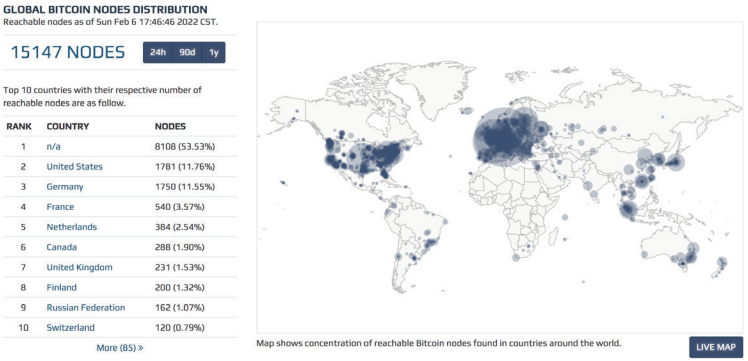
METCALFE'S LAW

- Popularized by Robert Metcalfe, who invented Ethernet, among other things. Metcalfe's law states that **a network becomes proportionally more valuable the more users it has**. Utility increases exponentially as more and more users join, strengthening the web.

THE P2P NETWORK

It is a global distributed database, with additions to the database by consent of the majority...

~ Satoshi Nakamoto 2009-02-18



GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Sun Feb 6 17:46:46 2022 CST.

15147 NODES 24h 90d 1y

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	n/a	8108 (53.53%)
2	United States	1781 (11.76%)
3	Germany	1750 (11.55%)
4	France	540 (3.57%)
5	Netherlands	384 (2.54%)
6	Canada	288 (1.90%)
7	United Kingdom	231 (1.53%)
8	Finland	200 (1.32%)
9	Russian Federation	162 (1.07%)
10	Switzerland	120 (0.79%)

More (85) »

Global reachable Bitcoin Nodes distribution

The result is a distributed system with no single point of failure. Users hold the crypto keys to their own money and transact directly with each other, with the help of the P2P network to check for double-spending.

~ Satoshi Nakamoto 2009-02-11

BITCOIN, NONVIOLENT COMMUNICATION & PERMACULTURE

I see **Bitcoin**, brought to us by Satoshi Nakamoto, as being the foundation layer for a healthy society with regards to:

- communicating value
- transacting and exchanging
- storing our time/life energy

in an emergent, organic, honest unfolding.

I see **Nonviolent Communication**, brought to us by Marshall Rosenberg PhD, as the foundation layer for a healthy society with regards to:

- communicating feelings and needs
- deep listening, empathy
- finding co-creative solutions

in an emergent, organic, honest unfolding.

I see **Natural Farming and Permaculture**, brought to us by our Ancestors, and more recently, Masunobu Fukuoka and Bill Mollison as being the foundation layer for a healthy society with regards to:

- communication with the earth
- growing food, healing the soil
- tending the wild

in an emergent, organic and honest unfolding.

Each of these technologies, one mathematical, taking us beyond mathematics, one linguistic, taking us beyond language, one biological, taking us beyond biology, are based in Truth.

It is up to us to make use of them, to live into them, and to allow them to guide us deeper and deeper into the profound potential we feel tingling at the tips our perception.

May we find the courage, the strength,
the wisdom and the grace
to move forth fearlessly
on the journey.

A Cypherpunk's Manifesto

by Eric Hughes

Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world.

If two parties have some sort of dealings, then each has a memory of their interaction. Each party can speak about their own memory of this; how could anyone prevent it? One could pass laws against it, but the **freedom of speech, even more than privacy, is fundamental to an open society**; we seek not to restrict any speech at all. If many parties speak together in the same forum, each can speak to all the others and aggregate together knowledge about individuals and other parties. The power of electronic communications has enabled such group speech, and it will not go away merely because we might want it to.

Since we desire privacy, we must ensure that each party to a transaction have knowledge only of that which is directly necessary for that transaction. Since any information can be spoken of, we must ensure that we reveal as little as possible. In most cases personal identity is not salient. When I purchase a magazine at a store and hand cash to the clerk, there is no need to know who I am.

When I ask my electronic mail provider to send and receive messages, my provider need not know to whom I am speaking or what I am saying or what others are saying to me; my provider only need know how to get the message there and how much I owe them in fees. When my identity is revealed by the underlying mechanism of the transaction, I have no privacy. I cannot here selectively reveal myself; I must always reveal myself.

Therefore, **privacy in an open society requires anonymous transaction systems. Until now, cash has been the primary such system. An anonymous transaction system is not a secret transaction system. An anonymous system empowers individuals to reveal their identity when desired and only when desired; this is the essence of privacy.**

Privacy in an open society also requires cryptography. If I say something, I want it heard only by those for whom I intend it. If the content of my speech is available to the world, I have no privacy. To encrypt is to indicate the desire for privacy, and to encrypt with weak cryptography is to indicate not too much desire for privacy. Furthermore, **to reveal one's identity with assurance when the default is anonymity requires the cryptographic signature.** We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy out of their beneficence.

It is to their advantage to speak of us, and we should expect that they will speak. To try to prevent their speech is to fight against the realities of information. Information does not just want to be free, it longs to be free. Information expands to fill the available storage space. Information is Rumor's younger, stronger cousin; Information is fleeter of foot, has more eyes, knows more, and understands less than Rumor.

We must defend our own privacy if we expect to have any. We must come together and create systems which allow anonymous transactions to take place. People have been defending their own privacy for centuries with whispers, darkness, envelopes, closed doors, secret handshakes, and couriers. The technologies of the past did not allow for strong privacy, but electronic technologies do.

We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money.

Cypherpunks write code. We know that someone has to write software to defend privacy, and since we can't get privacy unless we all do, we're going to write it. We publish our code so that our fellow Cypherpunks may practice and play with it.

Our code is free for all to use, worldwide. We don't much care if you don't approve of the software we write. We know that software can't be destroyed and that a widely dispersed system can't be shut down.

Cypherpunks deplore regulations on cryptography, for encryption is fundamentally a private act. The act of encryption, in fact, removes information from the public realm. Even laws against cryptography reach only so far as a nation's border and the arm of its violence.

Cryptography will ineluctably spread over the whole globe, and with it the anonymous transactions systems that it makes possible.

For privacy to be widespread it must be part of a social contract. People must come and together deploy these systems for the common good. Privacy only extends so far as the cooperation of one's fellows in society. We the Cypherpunks seek your questions and your concerns and hope we may engage you so that we do not deceive ourselves. We will not, however, be moved out of our course because some may disagree with our goals.

The Cypherpunks are actively engaged in making the networks safer for privacy. Let us proceed together apace.

Onward.
Eric Hughes <hughes@soda.berkeley.edu>
9 March 1993

(Emphasis in **bold** is mine)

SOME OF THE EARLY CYPHERPUNKS

we can thank for contributing to the development of digital peer-to-peer cash

- **Satoshi Nakamoto** - Anonymous cypherpunk who introduced bitcoin to the world in 2009.
- **Nick Szabo** - Bit Gold 2005
- **Hal Finney** - 2004 Reusable Proof of Work (RPoW), Author of PGP 2.0. Second person to run the bitcoin client. Received the first bitcoin transaction of 10 bitcoins from Satoshi Nakamoto
- **Wei Dai** - B-money 1998
- **Dr Adam Back** - HashCash 1997 - CEO Blockstream
- **Douglas Jackson and Barry Downey** - E Gold 1996
- **John Gilmore**
- **Timothy C.May**
- **Eric Hughes**

} Founders of the Cypherpunk movement and mailing list in 1992.

- **Philip Zimmermann**: 1991 PGP 1.0, the most widely used email encryption in use.
- **David Chaum** - Ecash 1983 and DigiCash 1989

The bitcoin White Paper

Presented to the world on metzdowd.com
2008-10-31

by Satoshi Nakamoto

A pseudonymous cypherpunk, who last communicated with the cypherpunk community on the bitcointalk.org forum on 2010-12-10.

By leaving, he allowed Bitcoin to be a true experiment in the wild. Everyone who works on it is a volunteer in some sense <-> inspired by the potential of freeing humanity from the shackles of a manipulated, debt-based money system, and instead, participating in a global, trustless, permissionless, censorship-resistant, truly scarce, peer-to-peer, decentralized money and monetary payment network, that is inspiring an emergent order to rise out of the fiat ashes.

We are all Satoshi

The Times 03/Jan/2009 Chancellor on brink of second bailout for banks

~ Text of a headline from The Times of London, etched into the Bitcoin Genesis block by Satoshi Nakamoto on 2009-01-03

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

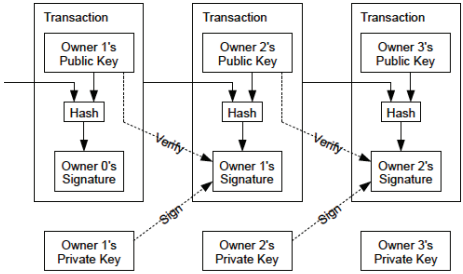
1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

2. Transactions

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

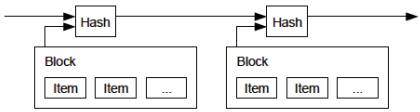


The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank.

We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions. In the mint based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced [1], and we need a system for participants to agree on a single history of the order in which they were received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.

3. Timestamp Server

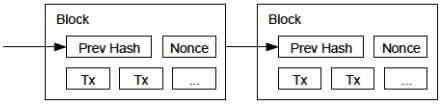
The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.



4. Proof-of-Work

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.



The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes. We will show later that the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added.

To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases.

5. Network

The steps to run the network are as follows:

1) New transactions are broadcast to all nodes.
2) Each node collects new transactions into a block.
3) Each node works on finding a difficult proof-of-work for its block.
4) When a node finds a proof-of-work, it broadcasts the block to all nodes.
5) Nodes accept the block only if all transactions in it are valid and not already spent.
6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proof-of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

New transaction broadcasts do not necessarily need to reach all nodes. As long as they reach many nodes, they will get into a block before long. Block broadcasts are also tolerant of dropped messages. If a node does not receive a block, it will request it when it receives the next block and realizes it missed one.

6. Incentive

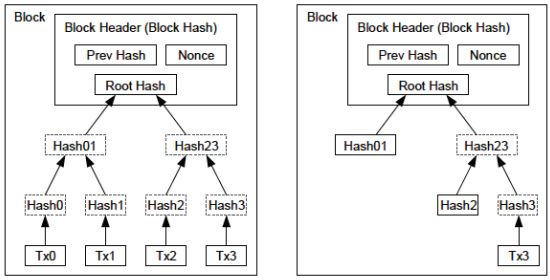
By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them. The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended.

The incentive can also be funded with transaction fees. If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction. Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free.

The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.

7. Reclaiming Disk Space

Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space. To facilitate this without breaking the block's hash, transactions are hashed in a Merkle Tree [7][2][5], with only the root included in the block's hash. Old blocks can then be compacted by stubbing off branches of the tree. The interior hashes do not need to be stored.



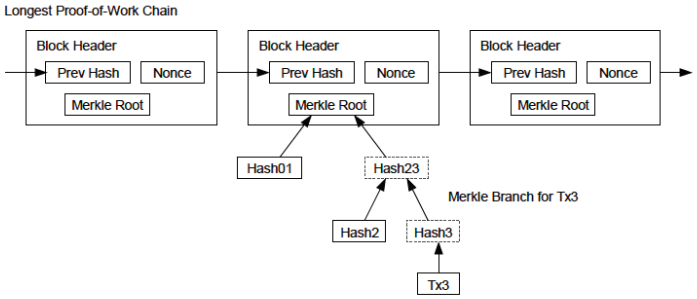
Transactions Hashed in a Merkle Tree

After Pruning Tx0-2 from the Block

A block header with no transactions would be about 80 bytes. If we suppose blocks are generated every 10 minutes, 80 bytes * 6 * 24 * 365 = 4.2MB per year. With computer systems typically selling with 2GB of RAM as of 2008, and Moore's Law predicting current growth of 1.2GB per year, storage should not be a problem even if the block headers must be kept in memory.

8. Simplified Payment Verification

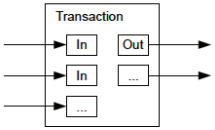
It is possible to verify payments without running a full network node. A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's timestamped in. He can't check the transaction for himself, but by linking it to a place in the chain, he can see that a network node has accepted it, and blocks added after it further confirm the network has accepted it.



As such, the verification is reliable as long as honest nodes control the network, but is more vulnerable if the network is overpowered by an attacker. While network nodes can verify transactions for themselves, the simplified method can be fooled by an attacker's fabricated transactions for as long as the attacker can continue to overpower the network. One strategy to protect against this would be to accept alerts from network nodes when they detect an invalid block, prompting the user's software to download the full block and alerted transactions to confirm the inconsistency. Businesses that receive frequent payments will probably still want to run their own nodes for more independent security and quicker verification.

9. Combining and Splitting Value

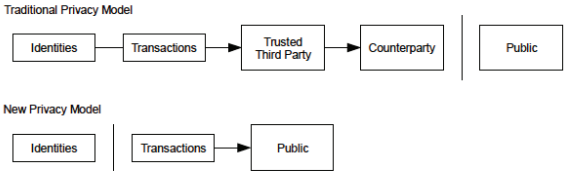
Although it would be possible to handle coins individually, it would be unwieldy to make a separate transaction for every cent in a transfer. To allow value to be split and combined, transactions contain multiple inputs and outputs. Normally there will be either a single input from a larger previous transaction or multiple inputs combining smaller amounts, and at most two outputs: one for the payment, and one returning the change, if any, back to the sender.



It should be noted that fan-out, where a transaction depends on several transactions, and those transactions depend on many more, is not a problem here. There is never the need to extract a complete standalone copy of a transaction's history.

10. Privacy

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.



As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.

11. Calculations

We consider the scenario of an attacker trying to generate an alternate chain faster than the honest chain. Even if this is accomplished, it does not throw the system open to arbitrary changes, such as creating value out of thin air or taking money that never belonged to the attacker. Nodes are not going to accept an invalid transaction as payment, and honest nodes will never accept a block containing them. An attacker can only try to change one of his own transactions to take back money he recently spent.

The race between the honest chain and an attacker chain can be characterized as a Binomial Random Walk. The success event is the honest chain being extended by one block, increasing its lead by +1, and the failure event is the attacker's chain being extended by one block, reducing the gap by -1.

The probability of an attacker catching up from a given deficit is analogous to a Gambler's Ruin problem. Suppose a gambler with unlimited credit starts at a deficit and plays potentially an infinite number of trials to try to reach breakeven. We can calculate the probability he ever reaches breakeven, or that an attacker ever catches up with the honest chain, as follows [8]:

p = probability an honest node finds the next block
q = probability the attacker finds the next block
q_z = probability the attacker will ever catch up from z blocks behind

$$q_z = \begin{cases} 1 & \text{if } p \leq q \\ (q/p)^z & \text{if } p > q \end{cases}$$

Given our assumption that $p > q$, the probability drops exponentially as the number of blocks the attacker has to catch up with increases. With the odds against him, if he doesn't make a lucky lunge forward early on, his chances become vanishingly small as he falls further behind.

We now consider how long the recipient of a new transaction needs to wait before being sufficiently certain the sender can't change the transaction. We assume the sender is an attacker who wants to make the recipient believe he paid him for a while, then switch it to pay back to himself after some time has passed. The receiver will be alerted when that happens, but the sender hopes it will be too late.

The receiver generates a new key pair and gives the public key to the sender shortly before signing. This prevents the sender from preparing a chain of blocks ahead of time by working on it continuously until he is lucky enough to get far enough ahead, then executing the transaction at that moment. Once the transaction is sent, the dishonest sender starts working in secret on a parallel chain containing an alternate version of his transaction.

The recipient waits until the transaction has been added to a block and z blocks have been linked after it. He doesn't know the exact amount of progress the attacker has made, but assuming the honest blocks took the average expected time per block, the attacker's potential progress will be a Poisson distribution with expected value:

$$\lambda = z \frac{q}{p}$$

To get the probability the attacker could still catch up now, we multiply the Poisson density for each amount of progress he could have made by the probability he could catch up from that point:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & \text{if } k \le z \\ 1 & \text{if } k > z \end{cases}$$

Rearranging to avoid summing the infinite tail of the distribution...

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

Converting to C code...

```
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k <= z; k++)
    {
        double poisson = exp(-lambda);
        for (i = 1; i <= k; i++)
            poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

7

Running some results, we can see the probability drop off exponentially with z.

```
q=0.1
z=0     P=1.0000000
z=1     P=0.2045873
z=2     P=0.0509779
z=3     P=0.0131722
z=4     P=0.0034552
z=5     P=0.0009137
z=6     P=0.0002428
z=7     P=0.0000647
z=8     P=0.0000173
z=9     P=0.0000046
z=10    P=0.0000012

q=0.3
z=0     P=1.0000000
z=5     P=0.1773523
z=10    P=0.0416605
z=15    P=0.0101008
z=20    P=0.0024804
z=25    P=0.0006132
z=30    P=0.0001522
z=35    P=0.0000379
z=40    P=0.0000095
z=45    P=0.0000024
z=50    P=0.0000006
```

Solving for P less than 0.1%...

```
P < 0.001
q=0.10   z=5
q=0.15   z=8
q=0.20   z=11
q=0.25   z=15
q=0.30   z=24
q=0.35   z=41
q=0.40   z=89
q=0.45   z=340
```

12. Conclusion

We have proposed a system for electronic transactions without relying on trust. We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending. To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power. The network is robust in its unstructured simplicity. Nodes work all at once with little coordination. They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis. Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone. They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism.

References

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In *20th Symposium on Information Theory in the Benelux*, May 1999.

[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In *Journal of Cryptology*, vol 3, no 2, pages 99-111, 1991.

[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In *Sequences II: Methods in Communication, Security and Computer Science*, pages 329-334, 1993.

[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In *Proceedings of the 4th ACM Conference on Computer and Communications Security*, pages 28-35, April 1997.

[6] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7] R.C. Merkle, "Protocols for public key cryptosystems," In *Proc. 1980 Symposium on Security and Privacy*, IEEE Computer Society, pages 122-133, April 1980.

[8] W. Feller, "An introduction to probability theory and its applications," 1957.

Bitcoin Genesis Block ~ Raw Hex Version 2009-01-03

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

and so,
a new era,
was unleashed

Profound gratitude to Satoshi, the cypherpunks past,
present and future, the BT vortex, the toxic
maxis, the non-toxic maxis, the meme-lords and -ladies,
the believers, the cynics, the seers...
and always,
my beloved family, friends,
and the One who breathes through us all,
for always seeing me through,
more precious than anything, even bitcoin

Check out the paperback at:
thesimplestbitcoinbook.net

Feel free to send comments, questions,
updates, feedback to:
TheSimplestBitcoinBook@proton.me

Can't promise I will get to it in a timely fashion ...
might be barefoot on a mountain somewhere

Stack sats
Stay strong
Stay true

in the end, Love

Block # 728922

Hey there!

If you found value reading this and
would like to buy the printed book,

or donate some sats to support me
as I create new content,

please visit my website by
scanning the QR code below.

Thank you!

THE
SIMPLEST
bitcoin
BOOK
EVER
WRITTEN

Keysa Luna