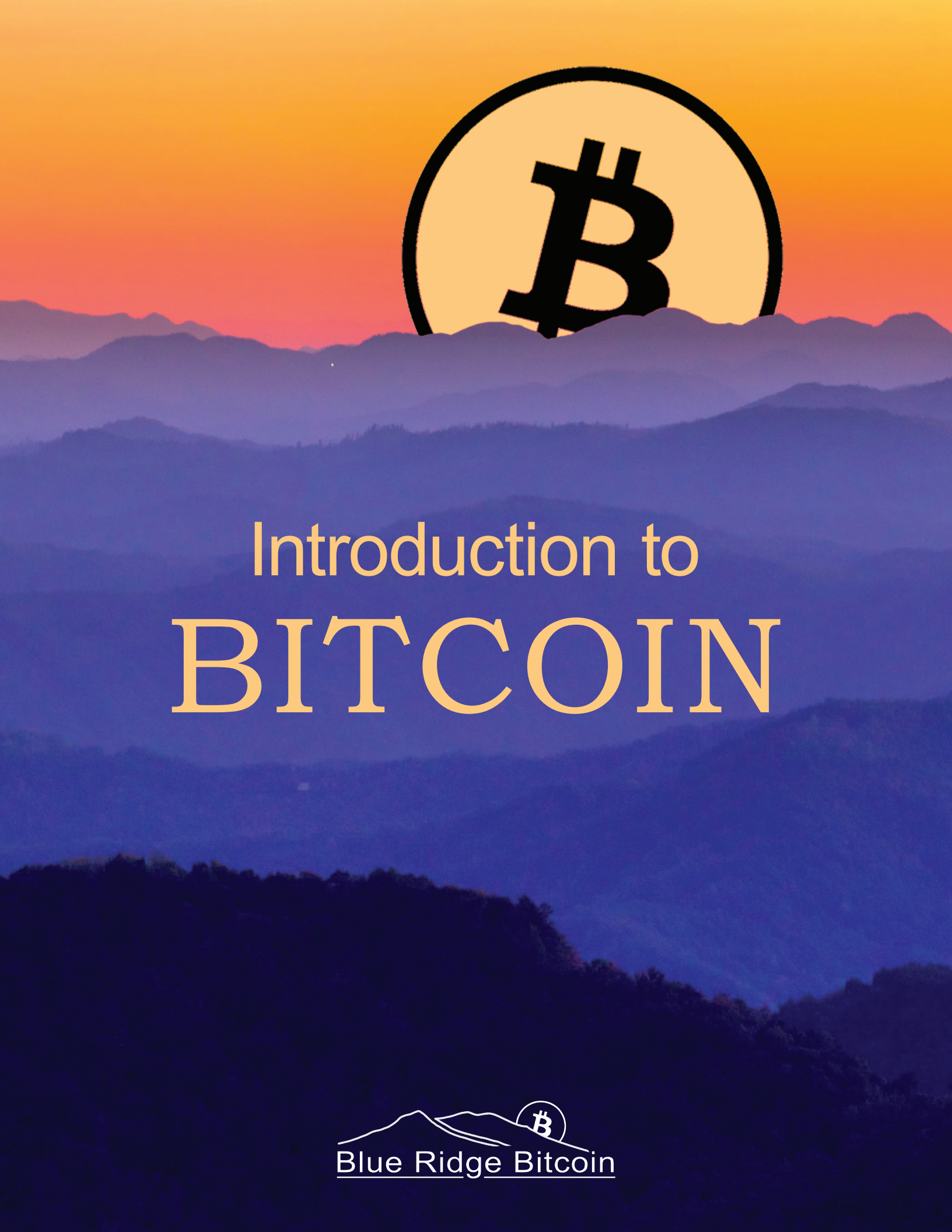
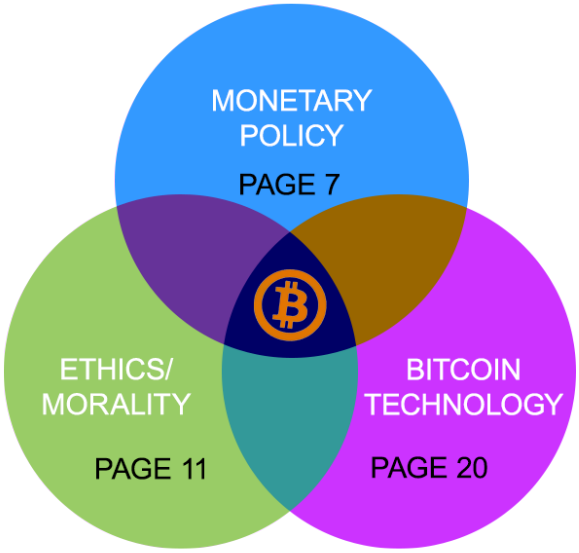

Introduction to
BITCOIN
Blue Ridge Bitcoin

Introduction to

Bitcoin

Last Update: 1.12.2025

Contents


MONETARY
POLICY
PAGE 7
ETHICS/
MORALITY
PAGE 11
BITCOIN
TECHNOLOGY
PAGE 20

Scriptures Addressing Money

You shall not steal.
-Exodus 20:15

Do not steal. Do not lie. Do not deceive one another.
-Leviticus 19:11

The rich rule over the poor, and the borrower is slave to the lender.
-Proverbs 22:7

Do not use dishonest standards when measuring length, weight, or quantity. Use honest scales and honest weights, and honest ephah and an honest hin. I am the Lord your God, who brought you out of Egypt.
-Leviticus 19:35-36

Do not have two different weights in your bag, one heavy and one light. Do not have two different measures in your house, one large and one small. You must have accurate and honest weights and measures so that you may live long in the land the Lord your God is giving you. For the Lord your God detests anyone who does these things, anyone who deals dishonestly.
-Deuteronomy 25:13-16

A good man leaves an inheritance for his children's children, but a sinner's wealth is stored up for the righteous.
-Proverbs 13:22

Honest scales and balances belong to the Lord. All the weights in the bag are of his making.
-Proverbs 16:11

If you lend money, you shall not be like a moneylender (banker) to him, and you shall not exact interest from him.
-Exodus 22:25
The Lord detests differing weights, and dishonest scales do not please him.
-Proverbs 20:23

Be not one of those who gives pledges, who puts up securities for debts.
-Proverbs 22:26

Anyone who has been stealing must steal no longer, but was work, doing something useful with their hands, that they may have something to share with those in need.
-Ephesians 4:28

A good man leaves an inheritance for his children's children, but the wealth of the wicked is laid up for the righteous.
-Proverbs 23:22

Hear this, you who trample the needy and do away with the poor of the land, saying, "When will the New Moon be over that we may sell grain, and the Sabbath be ended that we may market wheat?" – skimping on the measure, boosting the price and cheating with dishonest scales.
-Amos 8:4-5

Am I still to forget your ill-gotten treasures, you wicked house, and the short ephah which is accursed? Shall I acquit someone with dishonest scales, with a bag of false weights? Your rich people are violent; your inhabitants are liars and their tongues speak deceitfully.
-Micah 6:10-12

The Lord has a charge to bring against Judah; he will punish Jacob according to his ways and repay him according to his deeds… The merchant uses dishonest scales and loves to defraud.
-Hosea 12:2;7

You are to use accurate scales, an accurate ephah, and an accurate bath.
-Ezekiel 45:10

The Lord detests dishonest scales, but accurate weights find favor with him.
-Proverbs 11:1

Your silver has become dross, your choice wine is diluted with water.
-Isaiah 1:22

Then Peter said, "Ananias, how is that Satan has so filled your heart that you have lied to the Holy Spirit and kept some of the money you received for the land? Didn't it belong to you before it was sold? And after it was sold wasn't the money at your disposal?
-Acts 5:3-4

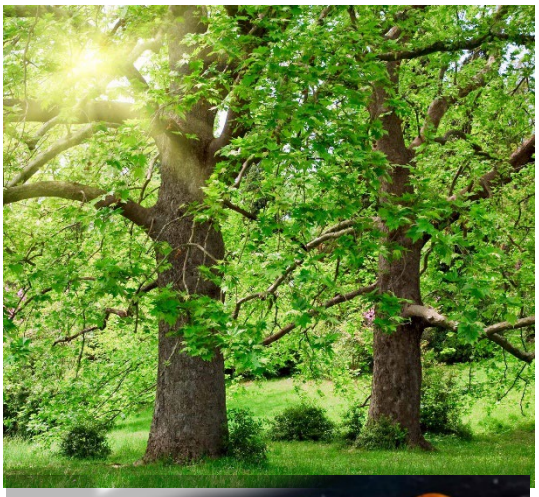
And forgive us our debts, as we forgive our debtors.
-Matthew 6:22

PART 1: WHAT IS MONEY?

Scarcity and Value

Have you ever asked yourself: *What is money?* Why are dollars money? Or Euros? Why don't we use leaves as money? Or gravel?

We don't use leaves or gravel as money because leaves decompose and both leaves and gravel are very abundant. In order to be good money, the object used as money must be *durable* and *scarce*. The scarcer something is, the more valuable it is. Leaves are neither durable nor scarce. Gravel is durable, but it is not scarce.



For thousands of years, gold served as money because gold is durable and scarce. However, gold is still being mined, and new gold is added to the existing supply by 2-4% each year. This means that gold is slowly becoming less scarce over time and is losing value. In addition, gold is difficult to verify. Gold bars and coins must be melted down, x-rayed, or subjected to other expensive treatments to confirm they are genuine.

Other things have been used as money. Many years ago, both salt and seashells were used as money. Back then, both were hard to obtain and durable. We get the word "salary" from the Latin word for salt (*sal*).

What Makes Good Money?

Leaves and gravel would make terrible money. Salt and shells were reasonable for a time, but gold was used as money for thousands of years. Good money is scarce and durable and performs three main functions: it is 1) a *unit of account*, 2) a *medium of exchange*, and 3) a *store of value*.

1. Unit of Account.
'Unit of account' means we price things in our monetary units. Roughly, a candy bar is worth $2; a cell phone is worth $500; and a car is worth $25,000. It is usually difficult to price things in more than one monetary unit and only one form of money is usually used by a coherent society.

2. Medium of Exchange. How much money do you want? In reality, zero. Good money has no other value than what you can buy with it. So, you don't want money, you want what you can *obtain* with money (free time, vacations, material possessions,

and even power and influence). Dollars are just paper and ink, but dollars allow you to buy the things you want or need. It is something you can *exchange* for the things you want or need. Suppose you own an apple orchard and need a new car; you could trade apples for the car, but the car seller may not want apples. And how many apples would it take to equal a car? Using a medium of exchange (i.e., money) avoids the problems with barter.

3. Store of Value (SoV)
Good money stores value into the future. In 1850, one ounce of gold ($18) would buy you a new, high-end suit. Today, one ounce of gold ($2,500) will buy you a new, high-end suit. The cost of a suit has changed a lot in terms of dollars, but not in terms of gold. You can see that gold has been a better *store of value* (SoV) than dollars.

Salability Across Scale, Time, and Space
1. Salable across scale means that a money can be easily divided or grouped to easily make both small and large purchases. The US dollar is surprisingly unsalable in scale: the largest unit ($100 bill) is only 10^4 times larger than the smallest unit (one penny). The only reason this lack of salability is not obvious is because we usually perform transactions digitally or by check. Consider using cash (i.e., physical paper bills) to buy a new car or house. It would require a suitcase of $100 bills.

2. Salability across time means your money holds its value into the future. We said that one ounce of gold would buy you a nice suit in 1850, 1900, 1950, and today. So, if you put one ounce of gold in a vault and save it for 50 years, it will buy the same amount then as it does now. Gold is a good store of value over time.

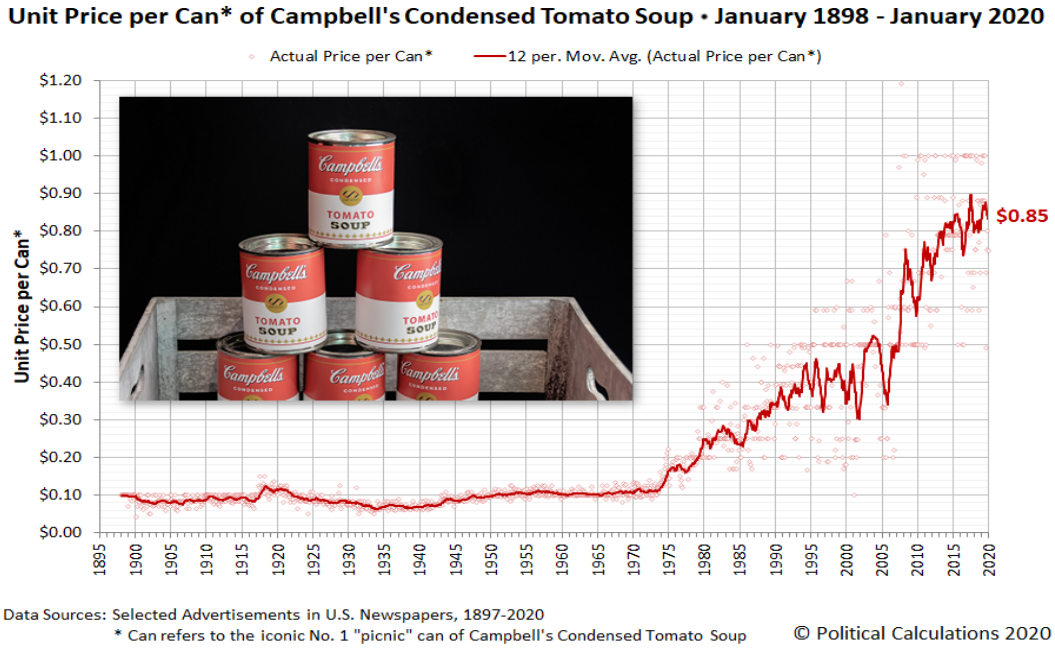
3. Salability across space means that the chosen money is easy to transport. Here, the dollar beats gold hands down. Gold is heavy and therefore difficult to carry on your person in significant amounts. It is also dangerous to transport over long distances. Indeed, piracy was a major problem during the Golden Age. Paper money is much lighter, and since paper money can be printed, stolen money can be easy to replace when insured. Digital dollars are even easier to carry and send over long distances.

So What's Wrong With the Dollar?
1. Inflation
The dollar has lost a lot of purchasing power in the past 100 years. In other words, the dollar has failed miserably at salability across time and being a store of value (especially since 1971). Your grandfather could buy many household items at a 5 and Dime store; today, not even the Dollar Store sells anything for just a dollar. In 1850, an ounce of gold was worth $18. In 2020, an ounce of gold

was worth 18 *hundred* dollars. Today, an ounce of gold is worth $2,600 and rising quickly. Actually, the value of gold is not changing; the value of the dollar is *dropping* quickly. For hundreds of years, the purchasing power of gold has remained constant, while the value of the dollar has declined 97% since 1913 (when the Federal Reserve central bank was created by the US Congress).

Year	Gold		Dollars
1850	1 oz	=	**18 x $1**
2020	1 oz	=	**18 x $100**

For many years the dollar held a steady value because it was backed by gold. The price of a can of Campbell's tomato soup was constant from 1895 to 1970; it cost your great-grandfather $0.10 in 1900 and your father $0.10 in 1960. But something happened in the 1970's (1971 to be exact), and in 2024 a can of tomato soup costs $1.29. We'll see what happened in 1971 in a moment.



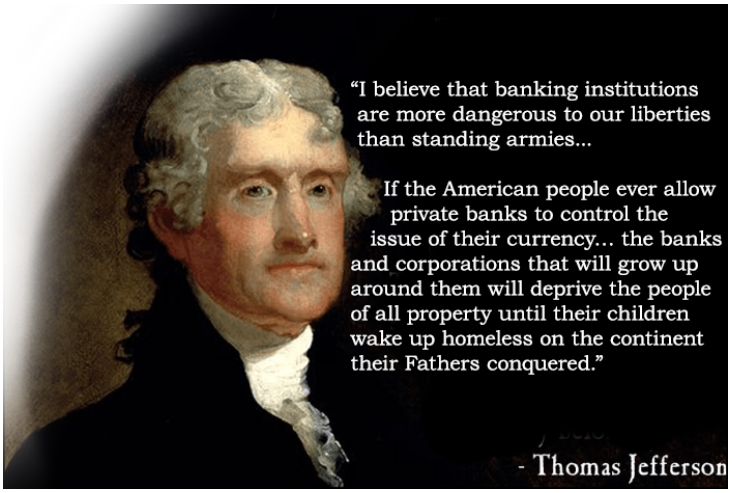
2. The Federal Reserve

The Federal Reserve is the central bank of the United States. It is a coalition of *private* banks; thus, it is not part of the Federal government. It also has no reserves, so the name is a complete lie. As a coalition of private entities with monopoly control over the issuance of money, it is quite literally a cartel. A cartel that, through the coercive power of government, requires us to use *their* money under *their* rules.

The Federal Reserve was created by an act of Congress in 1913. (Coincidently the same year the income tax was created). The United States did not have a central bank prior to that except for a brief

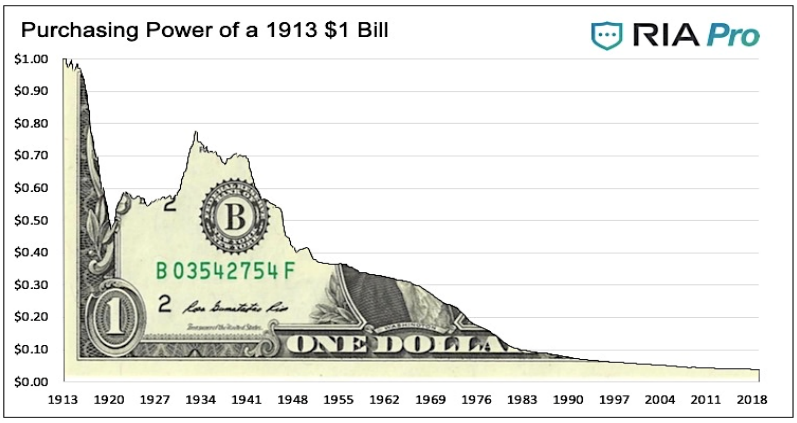
period in the early 1800's. Thomas Jefferson believed that central banks are more dangerous to freedom than standing armies.

One mandate of the Federal Reserve central bank is to preserve the value of the dollar. It has obviously failed. The purchasing power of a 1913 one-dollar bill is now just three pennies. In other words, the dollar has lost about 97% (or 30x) of its purchasing power since the Fed was created. This is why the price of Campbell's soup has gone up from ten cents to $1.29.



If the dollar lost 30x its purchasing power, why has soup only gone up 15x in price? Because the production cost of soup has *decreased* 2x due to technological advancements. Without inflation created by the Federal Reserve, the price of soup should have dropped from $0.10 to less than $0.05. In fact, without the Fed, the price of *everything* would go down over time, not up.

Backed by Gold?



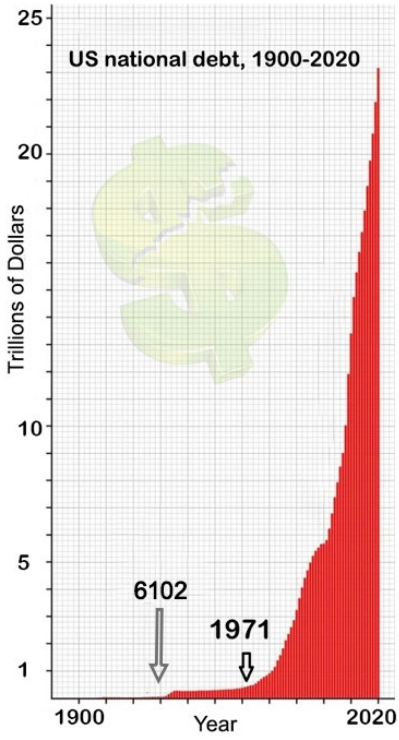
Data Courtesy: St. Louis Federal Reserve

The dollar used to be pegged to gold. When the Federal Reserve was created, dollars were fixed at $18 per ounce of gold. Of course, the government couldn't resist the urge to spend more money than they collected in taxes, and the Fed was happy to print the difference. When they could no longer hide this theft, Franklin D. Roosevelt confiscated (i.e., stole) every American's gold via an executive order (EO 6102). The gold was collected and placed into Fort Knox for safekeeping. Shortly after, gold was legalized again but repriced to $38 per ounce. In other words, the value of the dollar was cut in half almost overnight by the stroke of a pen.

During World War 2, many Europeans countries, threatened with the prospect of losing a war and being looted, decided to move their gold to Fort Knox for safekeeping. As the war came to a close, an international agreement called Bretton-Woods established the US dollar as the global reserve currency, meaning all countries would conduct international trade in dollars. This created a global demand for dollars, and the dollar Ponzi scheme began in earnest. By printing dollars and

Fort Knox has not been audited since the early 1970's. And even then, only a small fraction of the vaults was inspected. Do you think the gold is still there, or do you think it was looted by politicians and bankers long before the 1970's?

exporting them to the world, Americans benefitted from money printing while exporting the effects of inflation. In other words, we were getting rich at the expense of the rest of the world.



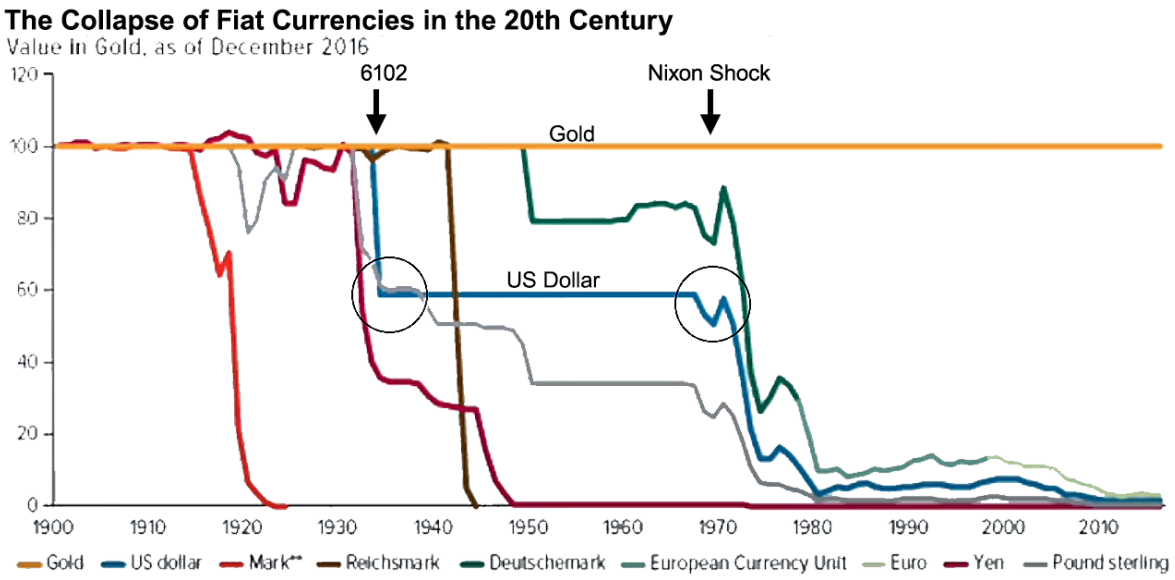
What Happened in 1971?

When countries started to catch on to this scheme in the 1960's, several demanded their gold back. The French even sent warships to New York Harbor to pick up their gold. Instead, on August 15, 1971, Richard Nixon de-pegged the dollar from gold and sent them back with paper dollars. This event is called the Nixon Shock, and it converted the dollar into *fiat money*. Fiat money is backed by nothing but the "full faith and credit" of the issuer.

Once the dollar was de-pegged from gold, the money printer could really go brrrr. Trillions of dollars have been printed since 1971 and our national debt has soared. Today, the national debt is over $35 trillion and rising by about $1 trillion every 100 days.

PART 2: MONEY MORALITY

In addition to a ballooning national debt, printing money has destroyed the middle class and widened the gap between the haves from the have-nots. The poor, who have no assets and save in dollars, are getting poorer every year. The rich put their wealth into inflation-beating assets like real estate and stocks. Worse, the rich get cheaper loans than the average person. In 2024, the average mortgage rate is 6.5-7%, but Blackrock gets mortgage rates less than 1% to buy up houses. This favoritism for the rich and those closest to the money printer is called the Cantillon Effect, and results in the rich getting richer while the poor get poorer.

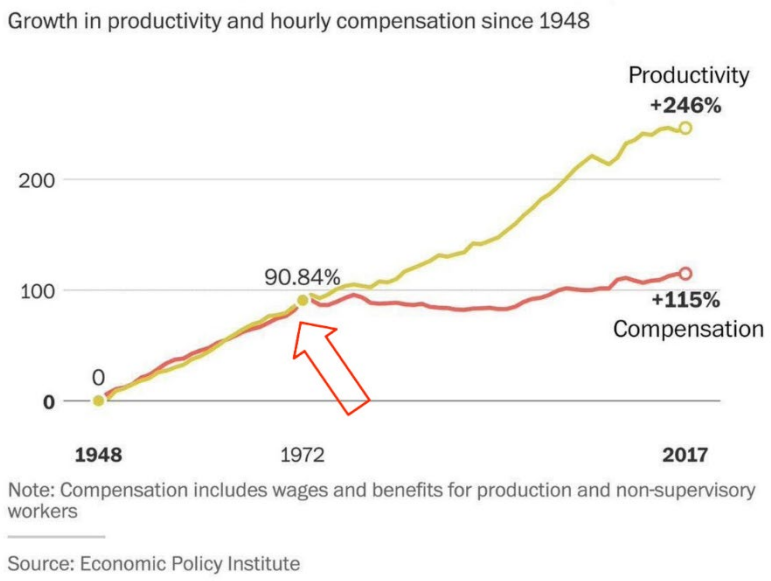


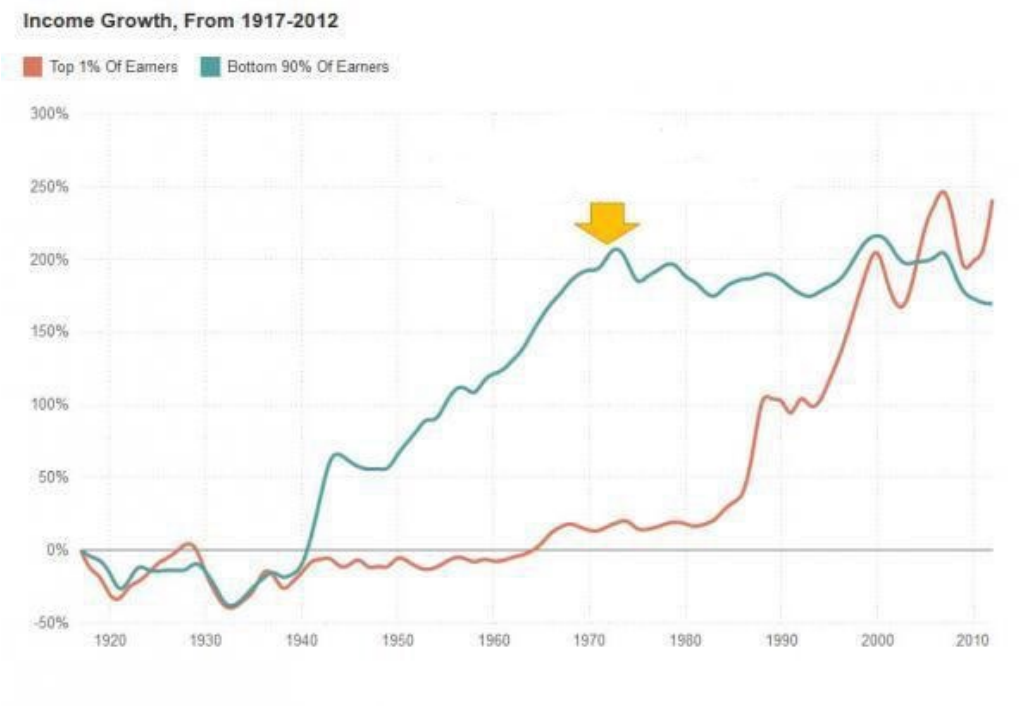
The US dollar is not the first fiat currency. Many nations have tried it, and all have failed. The average lifespan of a fiat currency is just 20 years. The US dollar has been fiat now for 50 years, but its unusual longevity is explained by its unique status as the world reserve currency. We have delayed the effects of fiat money printing by exporting those dollars to the world. But the gig is up. Inflation is rising and many nations are reconsidering the reserve status of the dollar. In October 2024, the BRICS nations met to discuss de-dollarization. If/when the rest of the world stops using the dollar, it will collapse almost overnight. Ironically, this process has been undoubtedly accelerated by the Biden administration weaponizing the dollar. Russia, like most countries, holds dollars in reserve as a national asset. The Biden administration first froze the movement of those dollars internationally, then wholly confiscated them. To add insult to injury, they gave the confiscated dollars to Russia's enemy: Ukraine.

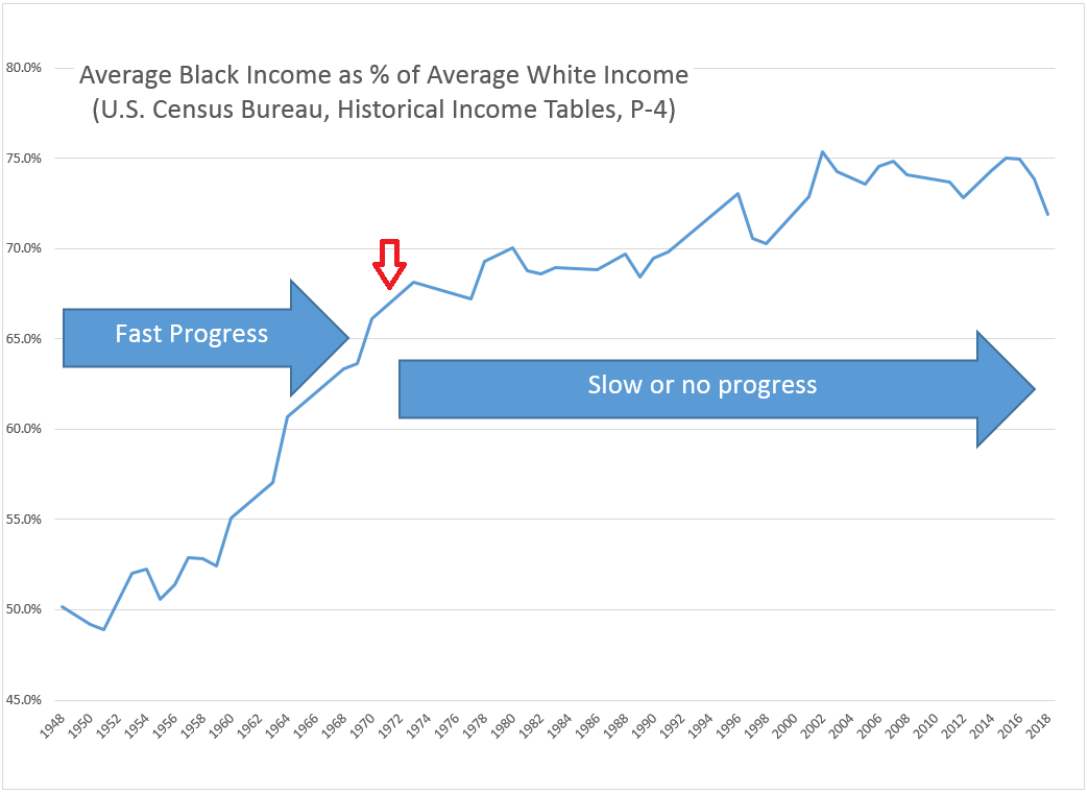
There is a global coalition of banks called the International Monetary Fund (IMF). The IMF purportedly exists to help third world countries develop into first world nations. It does this by providing loans, but unsurprisingly the loans come with strings attached. The loans are designed to end in default, and when that inevitably happens the resources of the country (e.g., copper mines, ports, or oil fields) are possessed as repayment. In its 50-year history, the IMF has not lifted a single nation out of poverty – not one. But it has siphoned 64 TRILLION DOLLARS from third world countries into the coffers of banks and the corporations around them. Such predatory lending is not simply immoral, it is evil.

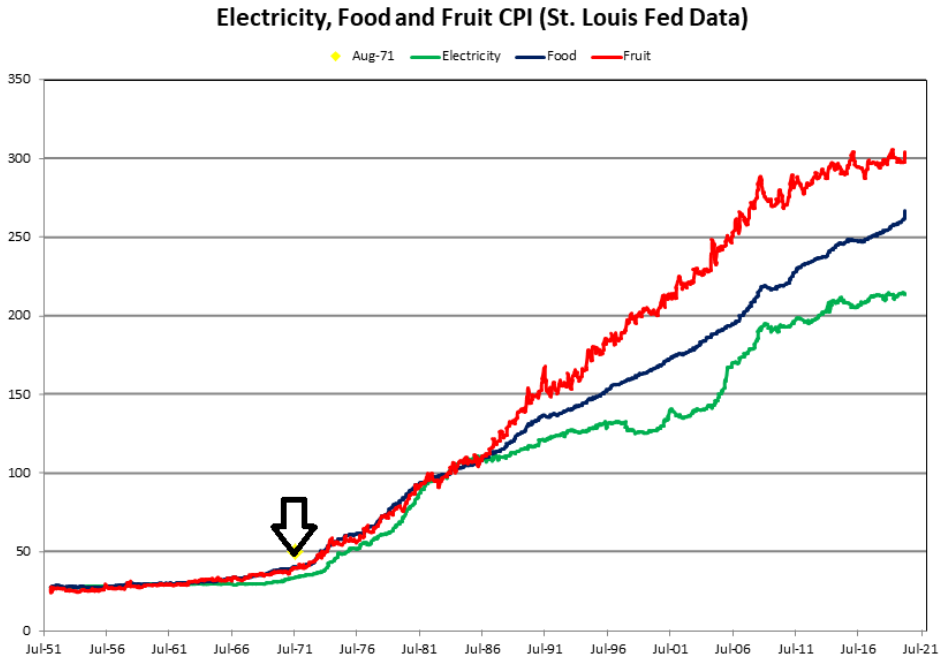
Legalizing money printing (i.e., counterfeiting) by a monopoly bank does not make counterfeiting moral or magically abolish the consequences. Because those closest to the money printer will benefit disproportionately from the counterfeiting (via the Cantillon effect), money is slowly transferred from the poor to the rich.

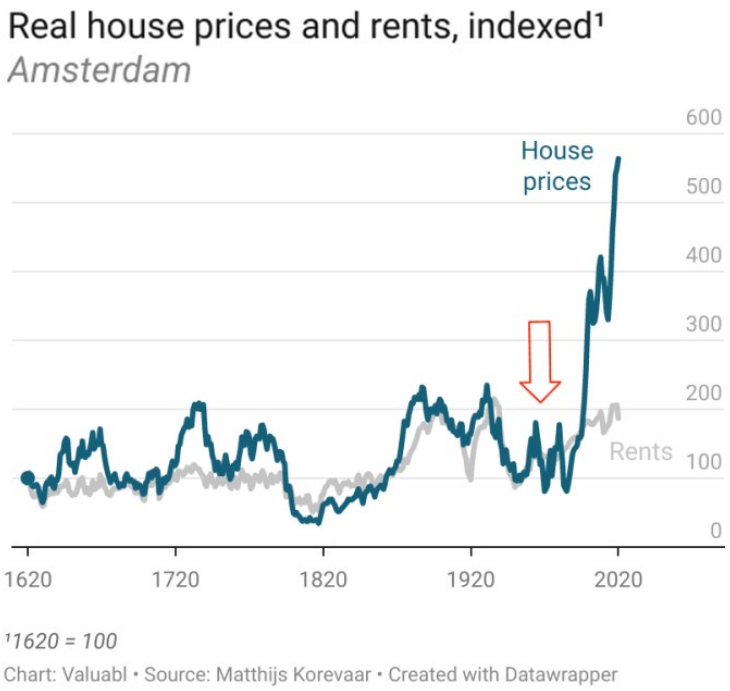
The detrimental effects of decoupling the dollar from gold can be seen in the following graphs.








Electricity, Food and Fruit CPI (St. Louis Fed Data)
Aug-71
Electricity
Food
Fruit
350
300
250
200
150
100
50
0
Jul-51
Jul-56
Jul-61
Jul-66
Jul-71
Jul-76
Jul-81
Jul-86
Jul-91
Jul-96
Jul-01
Jul-06
Jul-11
Jul-16
Jul-21
The92ers.com


Real house prices and rents, indexed¹
Amsterdam
600
500
400
300
200
100
0
House prices
Rents
1620
1720
1820
1920
2020
¹1620 = 100
Chart: Valuabl • Source: Matthijs Korevaar • Created with Datawrapper

Commodity Money
Good money should be a commodity, something not controlled by any one person or group. Oil, corn, and gold are all commodities; they are products of nature that anyone can drill, grow, or mine to acquire. No one holds the patent on oil, or the copyright for corn. Of these three examples, gold is the best for money because it is scarce and durable.

When you hold gold as money, you can physically possess it. It is a *bearer instrument*. When you transact with gold, you exchange your gold for a good or service you desire and thus transfer ownership to the seller. When the buyer and seller go their separate ways, the seller now has possession of the gold. The transaction was both final and instantaneous. So, gold is a bearer instrument that permits *instantaneous final settlement* during transactions. So far so good but remember that gold is cumbersome and dangerous to carry.

Because gold is cumbersome and dangerous to carry, banks offered to keep your gold and provide you with written receipts. Traveling with these receipts is both easier and safer. Buyers and sellers trade receipts which can be exchanged for real gold at any time at the bank. Like gold, cash is a bearer instrument that permits instantaneous and final settlement.

From the perspective of bankers and politicians, gold and cash both come with a problem: transactions cannot be monitored or controlled. This is why governments are trying, overtly and covertly, to create cashless societies. In Europe, cash transactions over $1000 are literally illegal. In America, some politicians wanted an accounting of every $600 we spend. (Thankfully, they failed).

From the perspective of users, gold and cash come with a serious limitation: buyer and seller must be physically present to transact. In today's world, most purchases are made using digital dollars over the internet, so you no longer need to be physically together. Obviously, governments also love digital dollars because those transactions can be tracked and controlled. Dollars are under the complete control of our central bank, the Federal Reserve. The decisions of a handful of bankers decide whether you retire at 65, or not at all, by setting the value of the dollar and massively manipulating the economy.

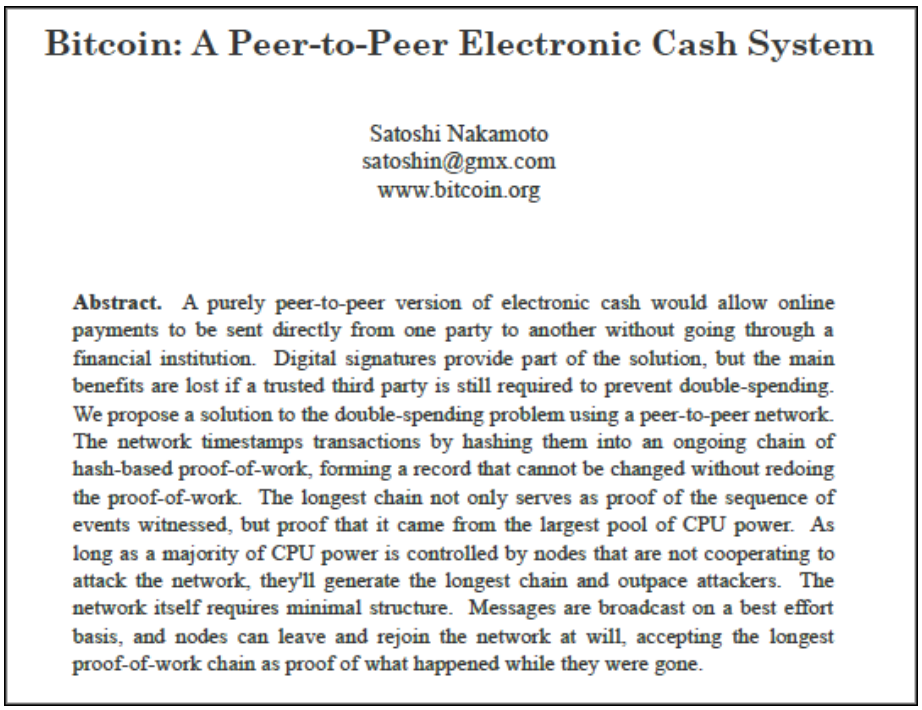
But there's another major problem cash – physical or digital. Remember that banks offered to hold your gold and provide receipts in exchange. That's how paper cash got started, and it worked well until something went terribly wrong.

Bankers realized they could write more receipts than they actually held as gold in the vault. They wrote these extra receipts and gave them out as loans. This slight-of-hand is called *fractional reserve banking*. For most of the past 100 years, banks in the USA were required to hold only $1 in gold for every $10 dollars they loaned. Since the invention of the computer, paper receipts no longer even need to be physically printed; most are "printed" digitally. During COVID, as the money printer overheated with digital printing, the 10% reserve was reduced to zero. Banks literally create money out of thin air to loan out. You, however, have to pay it back with money you earn by the sweat of your brow.

Bitcoin Fixes This

Money is literally one half of every purchase we make. Money is so pervasive that bad money can destroy a society, while good money will foster a healthy society. That's why Bitcoiners like to say, "*Fix the money, fix the world*."

But what is Bitcoin?



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.

Bitcoin is a digital currency created in 2008 by an unknown creator going by the pseudonym Satoshi Nakamoto.

Creating a workable, digital cash was something of a holy grail for computer programmers. The "problem" with computers is that all files and data are easily copied. When you send someone an email, for example, you actually send them a copy and you also retain a copy on your device. If you send a photo to Facebook, the original stays on your device while a copy goes to Facebook. And anyone can download many copies after that. So how do you create a digital file that cannot be copied? Satoshi solved the problem using a combination of new technologies, including digital signatures, hashing, public/private key cryptography, decentralized networks, and a blockchain. The details are fairly complicated but suffice it to say it has worked (almost) flawlessly for over 15 years now.

Prior to Bitcoin, digital payments could be (and still are) conducted online, but as Satoshi pointed out, they all require a trusted third party. This works fine if the trusted third party is trustworthy, but all experience shows that they are not. Payments are denied if the trusted third party, or a government, doesn't like what you are buying. Or if you protest. Or if you don't get vaccinated. Etc. Etc.

Bitcoin takes buying and selling out of the control of a third party and puts it back in control of the buyer and seller. It takes the best of cash and puts it online, while simultaneously removing some of the dangers of cash. It provides the safety of distance and immediate settlement but avoids the risk of blocked payments. Like cash, Bitcoin is a bearer instrument. He who holds it, owns it.

A Digital Commodity
Bitcoin is a digital commodity. Like other commodities (e.g., gold or wheat), it is owned by no one and available to everyone. Unlike other commodities, Bitcoin is *inelastic*, which means the supply is fixed (at 21 million bitcoins) and cannot be altered. If demand for gold or wheat increases, the production of gold or wheat will also increase to meet the new demand. As demand goes up, prices go up, but as supply saturates demand, prices go down again. Since Bitcoin is inelastic, supply *cannot* be increased no matter how much the demand goes up. The only thing that can change is the price. This makes the Bitcoin price volatile, but only during its current 'discovery phase.'

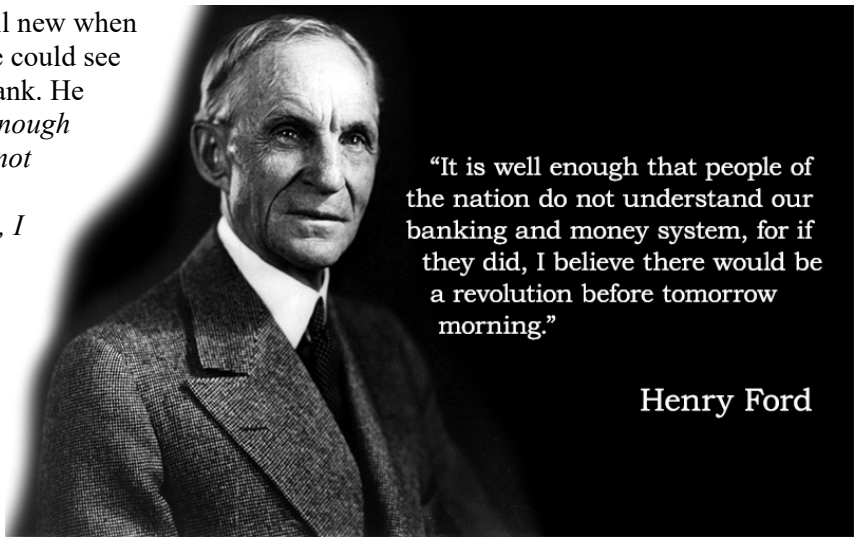
Cash Payments	**Third-party payments**
Must be done in person	Can be done remotely (online)
Immediate and final settlement	Final settle takes months
Requires no trust between parties	Requires trust in a third party
Requires trust in the money issuer (Fed)	Requires trust in the money issuer (Fed)
No fees	Costs additional fees (for third party)
Potentially dangerous	Much safer (from physical attack)
Payments cannot be blocked	Payments can be blocked
No need to share personal information	Must divulge lots of personal information

A Fair and Equitable Distribution
Anyone can participate in the Bitcoin ecosystem. Anyone can mine for gold, anyone can grow wheat, and anyone can mine bitcoins. All it takes is a computer. These days it takes a special computer, but in the early days any computer would do. Satoshi did not treat himself to a pile of bitcoins when it was launched, he mined them just like everyone else. Most of the other cryptocurrency copycats begin with a pre-mine, a stash of coins given to the creators before the token goes public. These are scams designed to make the creators rich at the expense of gullible buyers. Bitcoin is the only true digital, commodity money with a fair and equitable distribution. Also, the Bitcoin network has no knowledge of a person's gender, age, race, religion, or any other characteristic; Bitcoin literally cannot discriminate.

Backed by Energy
The dollar was once backed by gold, and this kept the value of the dollar steady for many decades. Bitcoin is backed by energy.

Henry Ford, creator of the assembly line and Ford Motor Company, once proposed an energy-backed form of money. Unfortunately, the technology didn't exist to make it possible. Today, it is possible and is achieved by Bitcoin, which uses electricity to mine new coins and to secure the blockchain. (The blockchain is a public record of all Bitcoin transactions.) A difficulty adjustment in the Bitcoin protocol ensures that coins will be mined at a fixed pace, so coin production is completely predictable. As more computers join the network, the mining difficulty is increased to make sure coins are not created too quickly. If many computers leave the network, the difficulty is decreased to guarantee coins still get mined. So many computers are mining bitcoins today that the Bitcoin network is the most powerful computing network on Earth, by many orders of magnitude.

The Federal Reserve was still new when Henry Ford was alive, but he could see the problem with a central bank. He once mused that *"it is well enough that people of the nation do not understand our banking and money system, for if they did, I believe there would be a revolution before tomorrow morning."*



Summary of Bitcoin vs Dollar

Bitcoin	**Dollar**
Digital commodity	Fiat
Fixed supply	Infinite supply
Backed by energy	Backed by violence (i.e., law)
Native to the internet (digital)	Physical (digital requires trusted third party)
Audited every 10 minutes	Fed has never been audited
Fair distribution	Unfair distribution / Cantillon Effect
Cannot be debased	Debased by inflating money supply
Decentralized control	Centralized in Federal Reserve
Rules-based protocol	Controlled by central bank 'elites'
Deflationary forever	Inflationary by design
Becomes more valuable over time	Becomes less valuable over time
Salability scale: 10^8	Salability scale: 10^4

Generational Theft

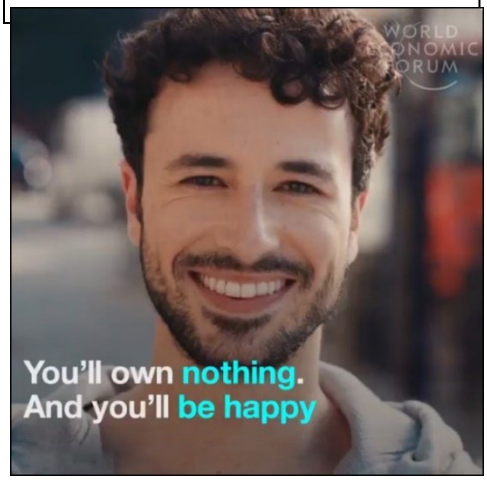
At least a dozen Scriptures reveal God's heart regarding money. Proverbs 11:1 summarizes them succinctly: "The Lord detests dishonest weights, but accurate scales are a delight to Him."

Money that steals from the future is immoral. A monetary system designed to transfer wealth from the poor to the rich is immoral. A debt-based currency is immoral. Fractional reserve banking and rehypothecation are immoral. Truly, the dollar and it's elite-controlled monetary policy may be the most corrupt, immoral money the world has ever known. Debasement was achieved by money-clipping in times past, but those methods of theft pale in comparison to the modern monetary policy of the US dollar. The dollar is backed by violence, and the military-industrial complex has kept the United States in continual war for nearly a century, resulting in untold death, destruction, and global misery all to prop up the Almighty Dollar.

In 1970, my father bought a newly constructed house for $17,500. If my father had taken the advice of Proverbs 13:22 and set aside $18,000 for his grandson to buy a house in 2024, that money would not even be enough for a downpayment. This scale of theft is unconscionable. We've been told it's just natural for things to get more expensive over time. *That is a lie*. It's natural for things to get *cheaper* over time. In the 1960's, a man with a high school education could support a wife at home

with children. By the 1990's, it was impossible to run a household on just one income, and kids were put into daycare. Today, it's nearly impossible to even get married and have a family at all. And the World Economic Forum (WEF) proclaims that soon "you'll own nothing, and you'll be happy." This is their plan for us. It's called Agenda 2030.

> *A good man leaves an inheritance to his children's children.*
>
> - Proverbs 13:22

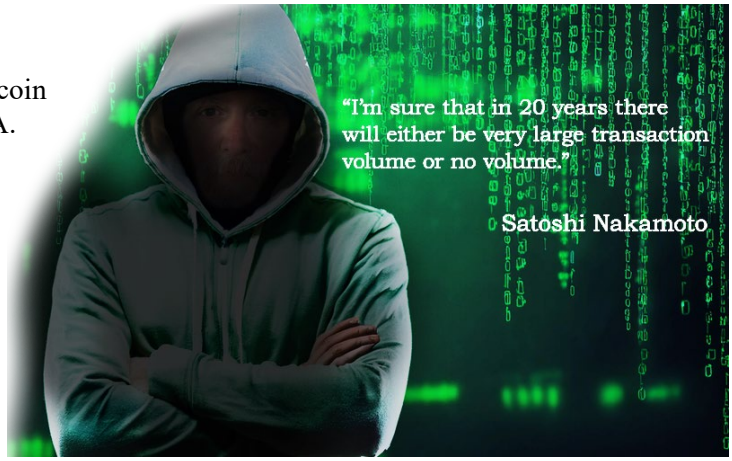


Bitcoin cannot be debased by inflation. Bitcoin is a voluntary system that is not forced upon anyone by coercion. The distribution of new bitcoins is just and fair and equitable. Bitcoins cannot be looted, nor can transactions be thwarted. Bitcoin encourages cooperation and peace. It is the polar opposite of fiat money.

We've seen that fiat money steals from the working and productive members of society to enrich bankers, financiers, and wealthy investors. This is wealth transfer from the poor to the rich, and it's immoral. Eventually, fiat money completely destroys the middle class, leading to masses of impoverished and a few wealthy overlords. As the rich get richer and the poor get poorer, it creates social unrest and political upheaval. It creates stress in families – arguments over money are the leading cause of divorce. It leads to more abortions – the cost of raising a child is a leading cause of terminating a pregnancy. Even art and architecture suffer under fiat money, as glorious cathedrals and magnificent bridges give way to drab cubes and tiny houses.

The Inevitability of Bitcoin

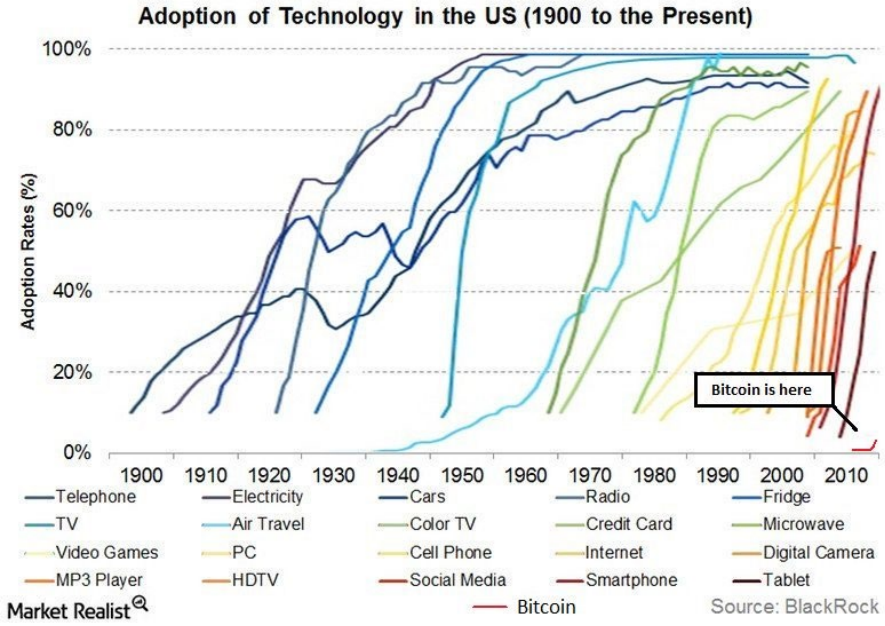
In 2008, it was uncertain if Bitcoin would succeed. It was programmed to be the hardest money in the world, and history shows that the hardest money always wins in a free market. But other digital monies had been tried and failed. Yet Bitcoin's monetary policy was fair, just, and moral and the code seemed promising. Soon after it launched in January 2009, Satoshi predicted that "*in 20 years there will either be very large transaction volume or no volume."*



Today, it is obvious there is "very large volume" on Bitcoin. The network has a market cap of $1 trillion. Last year, Bitcoin completed more transactions than VISA. Yet Bitcoin is still in its infancy. The same number of people are using Bitcoin today as were using the internet in 1998, and yet Bitcoin adoption is growing *faster* than the internet did. Global adoption of Bitcoin has increased annually by 1000% for the past several years. In 2021, El Salvador made Bitcoin legal tender. In the United States, an estimated 50 million Americans own some bitcoin and in 2024, two presidential candidates and other prominent politicians spoke at the largest Bitcoin Conference in America. In January 2024, nine bitcoin ETF's were launched and were the most successful ETF launches in history. As for the

computer code itself, almost 1 million blocks have been added to the blockchain with near flawless execution (there was one glitch in 2010 and another in 2013). The hashrate has risen steadily and continues to reach all-time highs. (The hashrate is a measure of network health). The network has never been hacked or forcibly stopped. It is safe to say that Bitcoin is succeeding while the dollar is collapsing. And it is not a stretch to conclude that Bitcoin will one day (soon) replace the dollar as the global reserve currency, or perhaps be used to back the dollar as gold once did. When Bitcoin replaces the dollar, it will usher in a new 'golden' era of peace and prosperity because Bitcoin incentivizes cooperation rather than conflict.

As a technology, Bitcoin seems to be working. At this point, it seems inevitable that Bitcoin will win because it is a superior form of money. Just as the car replaced the horse and the computer replaced the typewriter, newer and better technologies always replace older, lesser technologies.



PART 3: BITCOIN TECHNOLOGY

Open-source vs Proprietary Code

Computer software can be either *open-source* or *closed-source* (proprietary). With open-source software, the code is freely available to the public (most are deposited to github.com). Thus, the software can be scrutinized by any interested computer programmers and hackers to look for mistakes or secret backdoors. The code for proprietary software is not available to the public.

Bitcoin is an open-source project. The software is not only viewable, but any programmer can alter the code and suggest changes to the Bitcoin community. These suggested changes are called Bitcoin Improvement Proposols (BIPs). One of the most famous BIPs is BIP-039 which allows bitcoin private keys to be converted into 12 or 24 English words. This makes it much easier and safer to store private keys and back them up.

Public / Private Cryptographic Keys
To access your bank account online, you need an account number and a password. There are no banks in Bitcoin, only wallets. To access your funds in a wallet, you need a *public key* and *private key* instead of an account number and password. If you want someone to send money to your bank account, you give them your account number, but you would never share your password. Likewise, if you want to receive bitcoin, you may share your public key but never your private key. Anyone with access to your private key can take your bitcoin.

Transactions are the transfer of bitcoins from one wallet to another. All transactions are recorded on the *blockchain*, which is a public ledger of all bitcoin transactions.

There are bitcoin wallets available for computers (Windows, Apple, and Linux) and for phones (Android and iOS). Once installed, these wallets will create a private key and a mathematically related public key for you.

The public key is used to derive bitcoin addresses. A new bitcoin address is generated for every bitcoin transaction (i.e., whenever you send or receive bitcoin). Examples of an actual private key, public key, and bitcoin address are shown below:

Private key: E9873D79C6D87DC0FB6A5778633389532133O3DA61F20BD67FC233AA33263
Public key: FC7492E739D810291293098B38A74F0B82901369D937A798E4898D93987C9
Bitcoin address: bc1qyg0fck9g5640dwksff3scvvc50r65zeutpz0r7

Bitcoin addresses are usually converted to QR codes by your wallet. You simply present the QR code to the sender and they can send you bitcoin. Or you can scan someone else's QR code to send them bitcoin.

bc1qyg0fck9g5640dwksff3scvvc50r65zeutpz0r7

Decentralized vs Centralized control
Satoshi described Bitcoin as a "peer-to-peer electronic cash system." The electronic coin is defined as a chain of digital signatures. Eash owner transfers the coin to the next owner by digitally signing a transaction. The signed transaction is broadcast to computers called *nodes* that make up the "peer-to-peer" network. To date, there are over 10,000 nodes visible on the internet scattered across the globe. (There may be as many as 100,000 additional nodes hidden on the dark web).

Recent transactions are broadcast to the network of nodes and stored temporarily in the *mempool*. Computers called *miners* select transactions (usually based on a fee) from the mempool to put into a block, and then perform work to get that block into the blockchain. The work performed in called hashing. The miner that wins the hash race has their block of transactions added to the blockchain and receives a reward of freshly minted bitcoins (called the *block subsidy*). The block subsidy decreases over time; it is currently 3.125 bitcoins. Basically, miners do the hard work of building a securing the blockchain, and nodes keep the miners honest (because they will reject any blocks or transactions that do not follow the rules).

Nodes and miners are just computers. Anyone can run them. Because nodes and miners are scattered all over the planet and no single computer is in charge, the Bitcoin network is *decentralized*. There is no single point of failure and no central authority to be coerced. Bitcoin is a completely open and transparent system.

By contrast, the dollar monetary system is highly centralized and opaque. The Federal Reserve central bank can decide which transactions are allowed and which ones are not. They can seize funds, freeze transactions, and sanction individuals and States. The Federal Reserve has never once been audited in its entire existence.

Hash Functions

A *hash* is mathematical function that takes any size input and produces an output of a fixed, predetermined size. The SHA256 algorithm used by Bitcoin produces a 256-bit output. You can input a single character or an entire novel into the algorithm and it will produce a 256-bit output unique to each input. This is important: no two inputs will ever produce the same output.

In the Bitcoin program, the 256-bit binary number is converted to a hexadecimal number. The input 'Blue Ridge Bitcoin" results in the following hexadecimal hash:

84918d83f85d7b8e201929857d2813476e145f1db6e6c7a93f3593e4c52a9aa2

Adding the number 1 (i.e., Blue Ridge Bitcoin 1) results in:

3620456c2bfe10d5d11c536a753a1dee5084eac577f1852a75b2e39855ee5f6a

---

Example Hashes:

Blue Ridge Bitcoin 10
Hash = 0dc0dc79b2fc9075e36dfa71bbc770d80c4970ef72ff11a0500ecb4b59cec672dc

Blue Ridge Bitcoin 22
Hash = 00ef3c1bbe4176a7298968c28846f9dadd8edfc3d3e914ad62017f31c762661a

---

The Bitcoin program uses incoming transactions as inputs for SHA256 hashing. Approximately 3,000 transactions are gathered into a *block* and hashed to generate a 256-bit output. To "win" the block, a miner must obtain a hash below a certain target value, called the *difficulty*. The difficulty can be adjusted by the protocol. In simple terms, you need a certain number of leading zeros in the hash to win a block. "Blue Ridge Bitcoin 1" did not result in any leading zeros. The number 1 is replaced with 2 and the block is re-hashed. The input "Blue Ridge Bitcoin 10" produces one leading zero, and the input "Blue Ridge Bitcoin 22" produces two leading zeros. The number added (called a *nonce* for 'number used once') is continually adjusted until a hash is reached with the required number of leading zeros.

			9		2			
	4						5	
		2				3		
2								7
			4	5	6			
6								9
		7				8		
	3						4	
			2		7			

Sudoku puzzle

There are many miners around the world competing for the next block. The first miner to produce a hash with the requisite number of leading

zeros wins the block and their block of transactions is added to the blockchain. As a reward, the winning miner is given the block subsidy, and any transactions fees.

Hashing is used in Bitcoin because it is somewhat like a Sudoku puzzle: it is difficult to solve a Sudoku puzzle but extremely easy to confirm a winning solution. Likewise, it is difficult to find a winning hash, but it's easy for nodes to confirm a winning hash.

Difficulty Adjustment

The *difficulty level* determines the number of leading zeros needed to win a block. If many new miners are added to the network, they will mine blocks too quickly. If many miners leave the network, the remaining ones will mine new blocks too slowly. The program is designed to add one new block to the blockchain every 10 minutes. To keep the pace of block production steady, the difficulty is adjusted every 2,016 blocks (about 2 weeks). This is called the *difficulty adjustment*. At the time of writing, the current difficulty is 101 trillion, meaning that 19 zeros are required to win a block! The hash for block 869,206 is

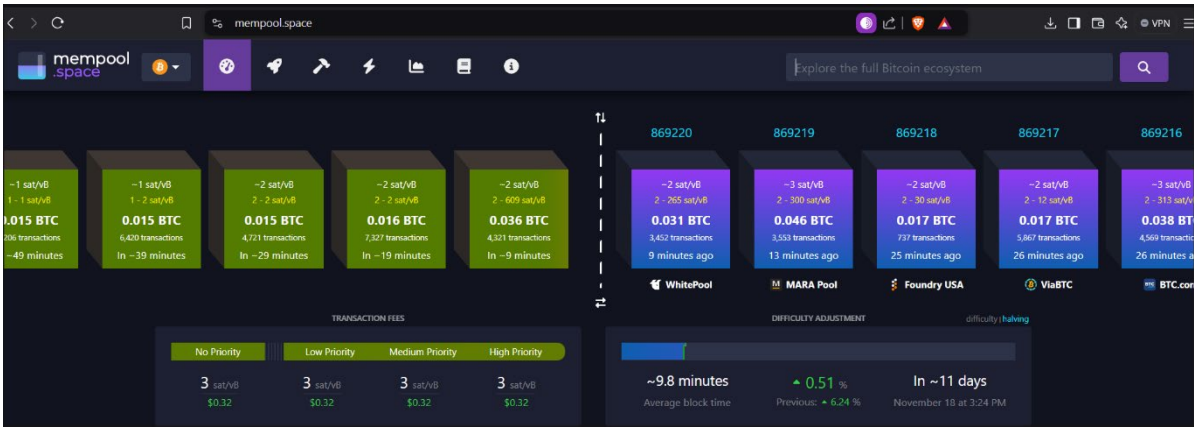
000000000000000000102415becd6036ecf68ef0e516715c222bbbb7bb3d182

Proof of Work

Finding a hash of the requisite difficulty is called *proof of work* (POW) because it can only be accomplished by expending real-world energy (i.e., electricity). Since the difficulty adjustment ensures it takes 10 minutes of energy consumption to find a valid block, finding a block 'proves' you consumed the energy, or did the work. Proof of work is what links the virtual currency to the real (physical) world. If a bad actor tried to alter a past transaction, they would have to redo the POW which would incur real-world energy costs. Trying to undo more than one block would be prohibitively expensive, even for nation states. Consequently, the blockchain is an unalterable history of bitcoin transactions.

Blockchain

The blockchain is the record of all bitcoin transactions; a public ledger that can be audited by anyone at any time. As described above, blocks are bundles of transactions used as an input for a hash function. The hash of each newly found block contains the hash of the previous block, thus linking the blocks into a chain. Satoshi actually called this the *timechain* rather than blockchain.



Miners and Nodes
The nodes described above are more precisely called *validating nodes*, or *validators.* These small computers (usually just laptops or raspberry pi's) broadcast bitcoin transactions and check all transactions and blocks to ensure they are valid. If any block or transaction does not follow the rules of the protocol, it is rejected.

Miners are extremely powerful computers that perform hash operations quickly (trillions of hashes per second). They are called *miners* because they can create new bitcoins like mining for gold; however, a better term would be simply *hashers*. These computers consume large amounts of energy to secure the blockchain, but the energy they consume is rather green. Miners are incentivized to find the cheapest energy possible and that is usually stranded energy or energy that would normally be wasted (e.g. methane flares). Because bitcoin miners are portable, they can go wherever cheap, abundant energy is located.

Scaling Bitcoin
The blockchain and all transactions within it are called the *base layer* of Bitcoin. Because blocks can only hold about 3,000 transactions and new blocks are added every 10 minutes, the base layer can only process about 5 transactions per second. The VISA network, by contrast, regularly processes 65,000 transactions per second. Given the (intentionally) slow speed of the blockchain, how can Bitcoin scale to be a global monetary network?

Second layer solutions such as the *lightning network* and *sidechains* have been developed to speed up bitcoin transactions. These are transactions that occur off chain. A business wishing to accept bitcoin payments must certainly use a second layer to make real-time sales. Lightning is easy to use as a customer, but working the backend as a merchant can be complicated. For this reason, custodial solutions are usually preferred, at least until you become more proficient with the technology. Likewise, sidechain solutions are often custodied.

Bitcoin Wallets
The three participants in the Bitcoin network are miners, nodes, and wallets. Wallets have become increasingly sophisticated and easy to use over the years. There are two main types of wallets: *hot wallets* and *cold wallets*. A hot wallet is connected to the internet. There are hot wallets designed for laptops and computers, but most hot wallets are designed for cell phones. These wallets are typically used for small purchases, not long-term storage.

A cold wallet is one that never connects to the internet. These are used for long-term storage and storing large amounts of bitcoin. Think of a hot wallet as a checking account and a cold wallet as a savings account. Wallets can also be *custodial* or *non-custodial*. You hold your own Bitcoin private keys with a non-custodial wallet. A custodial wallet is one where someone else holds your keys for you. This can be useful if you don't trust yourself to keep your bitcoins safe, but it comes with a third-party risk, which moots the point of using Bitcoin. As Bitcoiners say: "Not your keys, not your coins."

It is absolutely essential that you backup your wallet's private key. If you lose your phone or it's stolen, or if the computer holding your wallet crashes, you will lose your bitcoin if you do not have your private key backed up. With your private key, however, you can restore your wallet on a new device.

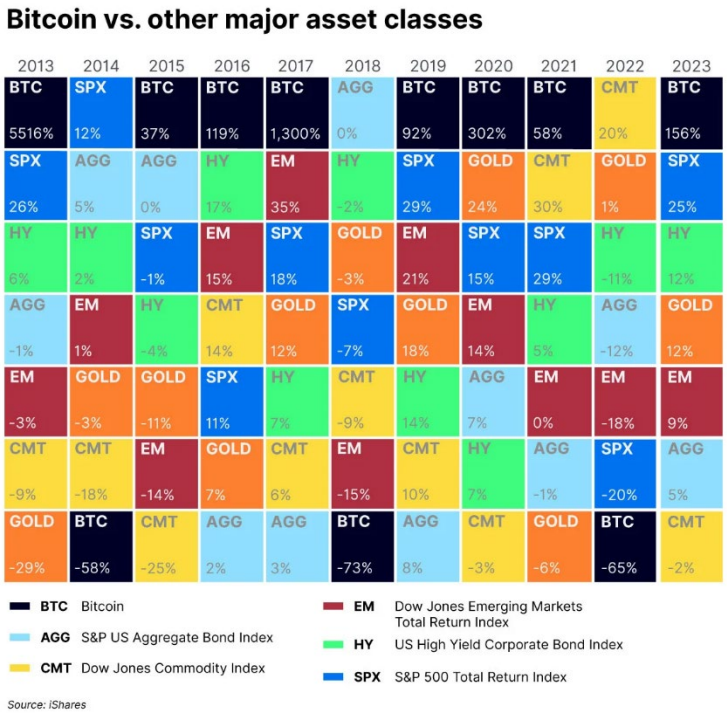
The private key is long and difficult for humans to read and copy by hand, yet you NEVER want to make an electronic copy of your private key – not even by taking a picture of it. Any electronic copy might be hacked. To make backing up your private key by hand easier, a Bitcoin Improvement Proposal (BIP) has been adopted by virtually all wallet makers. The protocol converts the long hexadecimal private key into a series of 12 (or 24) English words. It is much easier to write down (or even memorize) 12 English words than a string of hexadecimal numbers and letters. To back up your wallet, write down the English words (in order!) *by hand* and save them in a very safe place. Some place where you might store large amounts of cash, or expensive jewelry. If someone asks you for your 12 words (called a *seed phrase*, or *seed words*), NEVER give it to them, unless you want them to control your bitcoin.

1. umbrella
2. random
3. purpose
4. lift
5. rugged
6. season
7. mystery
8. airplane
9. jungle
10. silence
11. tool
12. energy

Final Thoughts

The dollar is in a precarious position. It is a fiat money that has been debased continually by a central bank inflating the money supply. It has been weaponized. History shows us that when a fiat currency collapses, it happens quickly (in a matter of days). We could wake up one day soon to find the dollar collapsing. In an effort to maintain their control over money, governments will try (are trying) to implement Central Bank Digital Currencies (CBDCs), which are everything bad about fiat money on steroids. CBDC's are surely the 'mark of the beast' money. Whether Bitcoin replaces a collapsed dollar or provides a parallel economy against CBDC's, it might not hurt to have some.

On the other hand, the dollar may languish on for decades more. After all, our politicians are good at kicking the can down the road. Even if the dollar continues for years to come, it is guaranteed to lose value. In that case, Bitcoin seems to be a good investment to hedge against inflation. It has been the fastest horse in the race – by far – for 9 of the past 11 years (including 2024).



A Deep Rabbit Hole

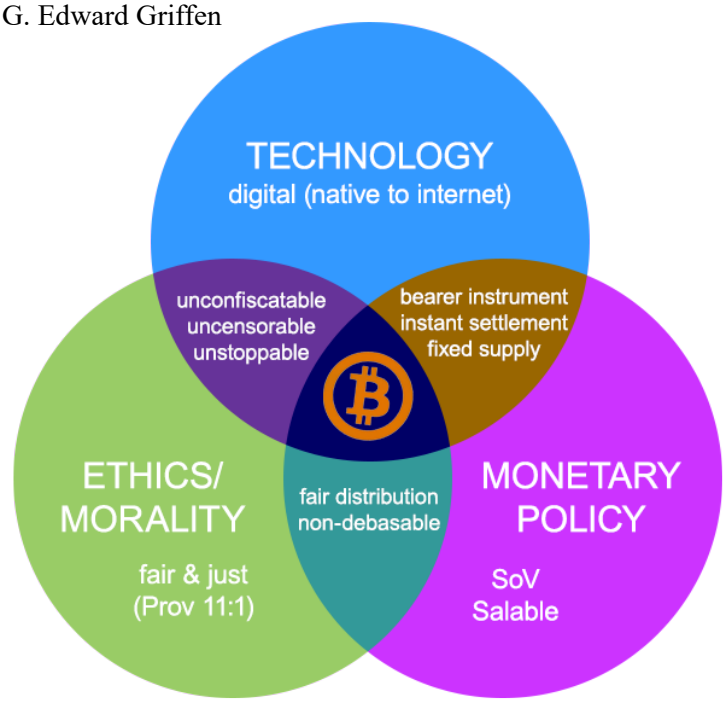
There is much more to learn about Bitcoin, as a technology and as a money. If you would like to know where and how to buy or earn Bitcoin, and how to hold is securely, we can help at Blue Ridge Bitcoin. Here are some additional resources to help you on the journey.

Books:

The Bitcoin Standard, by Saifedean Ammous
Thank God for Bitcoin, by Breedlove et al.
Broken Money, by Lynn Alden
The Creature from Jekyll Island, by G. Edward Griffen
End the Fed, by Ron Paul

YouTube channels:

Simply Bitcoin
Prof St Onge
Swan Bitcoin
Bitcoin University
BTC Sessions



Thank you for reading this **Introduction to Bitcoin** by Blue Ridge Bitcoin. We would love to get you started on your Bitcoin journey today!

www.BlueRidgeBitcoin.com