December 23, 2024

Pablo Ortiz

Why Bitcoin

During WW1, the US raised money through taxes and liberty bonds to pay for the war effort. Government debt almost 10x [1], America prospered during the roaring 20s.

The market increased to unsustainable levels and crashed to start the great depression (1929-1939). The government started its intervention in the economy through wage-fixing, price-controls and increased government spending. High fixed wages caused severe unemployment, price controls created supply shortages and surpluses, increased spending inflated away citizen's purchasing power. This is the start of increasingly destructive business cycles, caused by the US government adopting a Keynesian approach to the economy. This means more intervention to try and "stabilize" the economy. To get themselves out of the great depression the government leaned into more budget deficits and increased spending from 3.2% to 9.3% of GDP by 1936 [2].

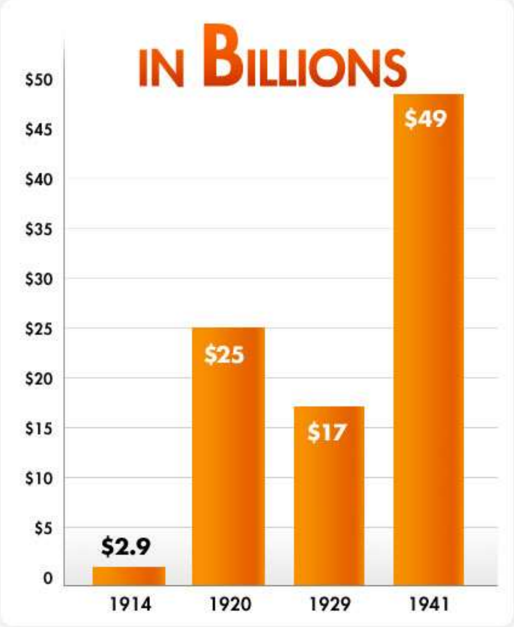


Figure 1: US Public Debt

At this time, the US was on the gold standard, therefore increasing spending was not that easy, the federal reserve act of 1913 required 40% gold backing of dollars in circulation. The government could either issue more gold backed currency, but they were pretty much at the 40% limit, or they could borrow more. They did borrow more, but there wasn't an unlimited demand for that newly issued debt.

To get around this problem FDR forced the American citizens to pay through currency devaluation and closed off the only escape, gold. He signed executive order 6102 in 1933, making it a crime for an American citizen to "hoard" gold (punishment of $10,000- or 10-years imprisonment, or both) [3]. Many citizens turned in their gold in at the market price of $20/ounce.

A year later, he signed the Gold Reserve Act, which gave the president the power to establish the value of a gold ounce, with no one else's approval [4]. As soon as he signed this act, he changed the price of gold from $20/ounce -> $35/ounce. That represented a 43% increase in the price of gold. The way I see it is people who turned in their gold out of fear, had their purchasing power eroded by 43%. This incentivized everyone around the world to sell their gold to the US government. This increase in gold reserves + an inflated price allowed the government to issue much more gold backed dollars, M1 money supply grew at 12% per year from 1933-1937. That means 12% more dollars chasing an almost inelastic supply of goods and services each year [4]. FDR's strategy technically worked, Gross National Product increased (mostly because prices were inflated), lower borrowing costs and increased government spending did in fact lift the US out of the depression. This marks the first time the government eroded its citizen's purchasing power to "fix" their own f-up caused by irresponsible monetary policy during WW1.

Wars are very expensive, up until WW1 war efforts were carefully planned and restricted by the budget, issuing new currency was limited by gold redemptions and the max tax rate has always been 100%. Most major countries gave into temptation and halted gold convertibility. They were no longer limited by what was in their treasuries, theoretically they were limited only by their citizen's wealth, which they could capture through inflation. It is not unreasonable to imagine this conflict staying contained and resolving within a year or so once governments ran out of gold and maxed out tax income. The chart below shows the exchange rate of 6 currencies vs the Swiss Franc which remained on the gold standard [5].

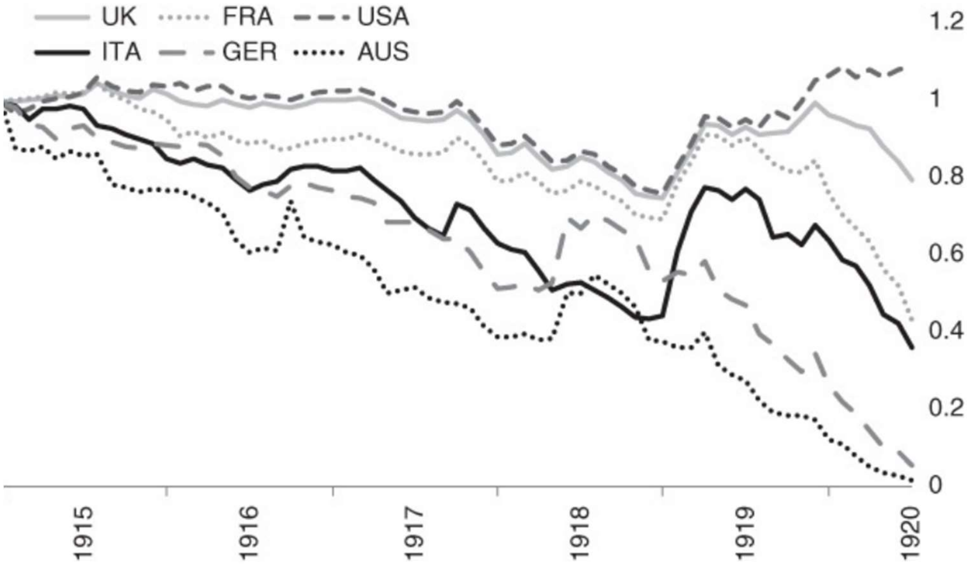


Figure 2: Exchange rates vs Swiss Franc. Exchange rate in June 1914 = 1

Pre-WW1 money flowed easily between nations, since all currencies were redeemable for a specific weight of gold, currency exchange was simply gold weight ratios (eg: 1 unit of currency1=100g, 1 unit of currency2 = 200g, the exchange ratio is then 2-1). After halting gold redemptions, there was no standard for these exchange rates, "currency manipulation emerges as a tool of trade policy, with countries seeking to devalue their currencies in order to give their exporters an advantage “ [5]. To combat this, governments enacted trade barriers. There was no longer a gold standard that could be used to easily exchange goods, trade frictions increased.

After WW2, representatives from 44 countries met in Bretton woods, NH to come up with a global currency to facilitate international trade and address their own f-up: Forex frictions. Other countries had already been selling their gold to the US due to FDR’s repricing of gold. The US had accumulated a disproportionately large amount of gold reserves (around 2/3s of all global reserves). The US dollar was selected as the global reserve currency. Governments would be able to trade in an ounce of gold for $35 dollars and redeem $35 dollars for an ounce of gold [6]. Dollars would be globally accepted for international trade.

This gave the US an advantage over the rest of the world, they were able to inflate the money supply (issue more currency than the gold in their vaults), without the usual consequence of inflation. Initially, this power was used on cold war “activities. Soon enough, those with the power to issue currency realized they could buy votes through strategic government spending. Backed by the artificial demand for US dollars around the world, this misalignment of incentives led to astonishingly irresponsible levels of spending. Figure 3 shows the increase in government spending over the last century [7].

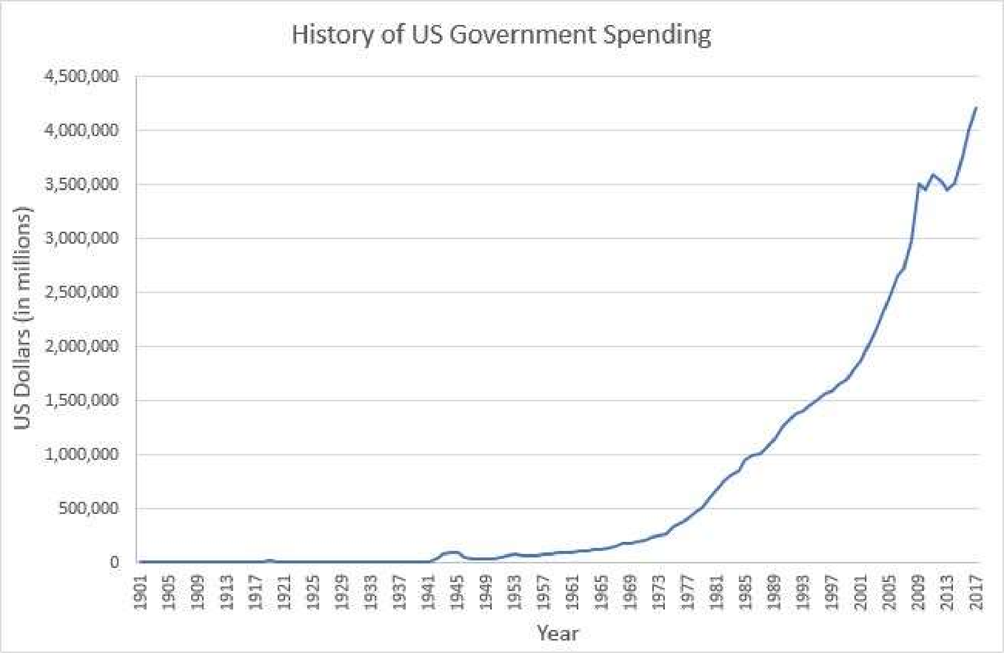
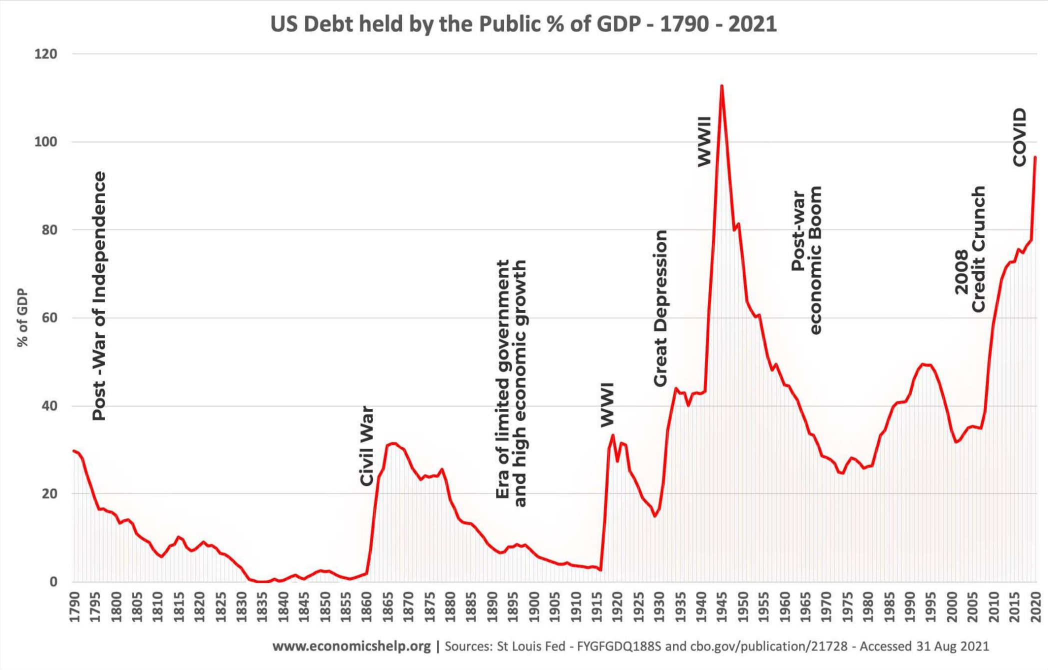


Figure 3: Look at the steep increase after 1971, keep that in mind for later

Figure 4 shows the national debt as a percentage of GDP [8], I don’t love this measure, because GDP before and after Bretton woods isn’t equivalent in my opinion. I don’t think printing money to increase GDP “counts” but that is just my opinion, you can see what I mean in Figure 5, which shows how government spending went from 8% to 35% of GDP between 1929 and 2011. With that in mind, Debt as a % of GDP has still trended up since Bretton Woods.



www.economicshelp.org | Sources: St Louis Fed - FYGFGDQ188S and cbo.gov/publication/21728 - Accessed 31 Aug 2021

Figure 4: National debt as a % of GDP

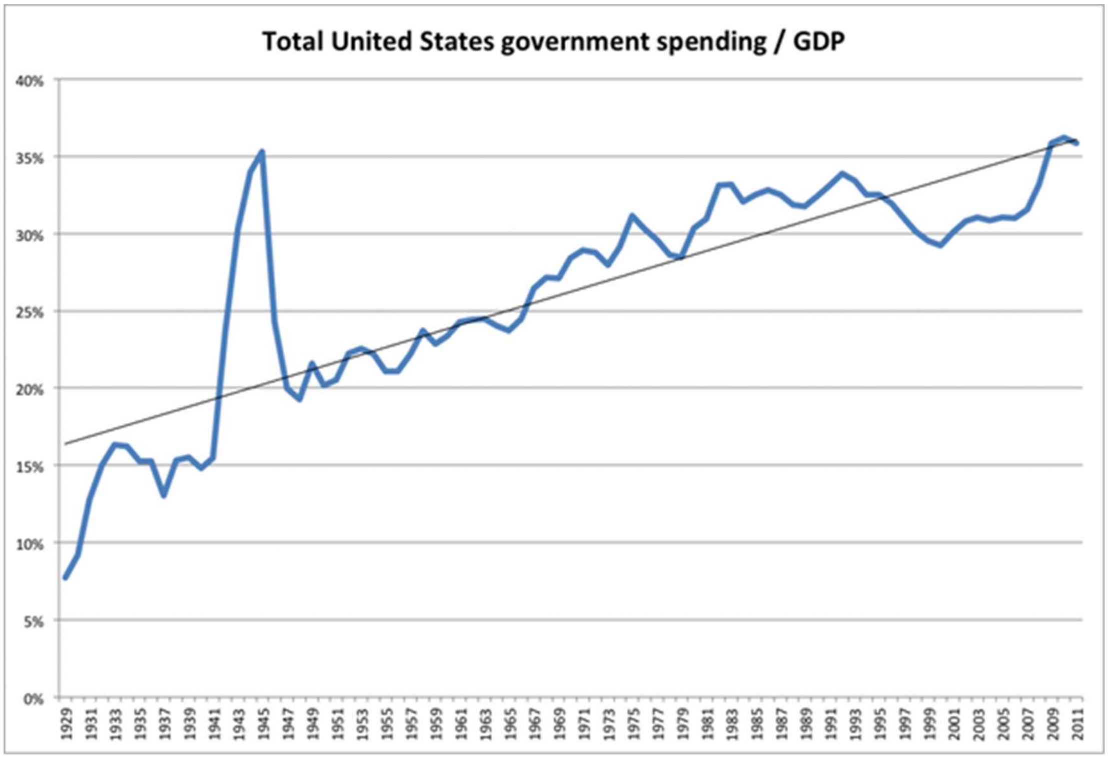


Figure 5: This is like me funding my son's investment account to make it look like its growing

Other governments noticed their dollars decreasing in purchasing power and started demanding their gold back from the US. Charles de Gauls, president of France even sent a French military carrier to New York to get his gold back in the 1960s [9]. The US obviously didn't have enough gold reserves for all countries to redeem their gold, so when the Germans tried to get their gold back, Nixon closed the US's vaults. On August 15, 1971, Nixon announced that the US would no longer redeem gold for dollars. He finished the slow process that had started in WW1 to get off the gold standard. The US had defaulted on its promise, a nice way of saying they stole everyone's gold.

I would recommend you take a scroll through this website, there is a chart for every single measure of general wellbeing, from divorce rates to wealth gaps. It is possible that some charts are cherry picked, or formatted to exaggerate the effect, but it gets across the general idea that since 1971, statistical measures of a society's well being have gotten worse.

https://wtfhappenedin1971.com/

In 2008 the Emergency Economic Stabilization Act was passed by congress in response to the subprime mortgage crisis. This authorized the Treasury to buy up to 700 billion of distressed assets, in the end *only* 300-400 billion was used [10].

Margot Robbie does a great job explaining the crisis, so go watch that scene if you need a refresher. Figure 5 was published by the federal reserve on house prices since 1900, you can see the volatility that is unleashed starting 1971 [11].

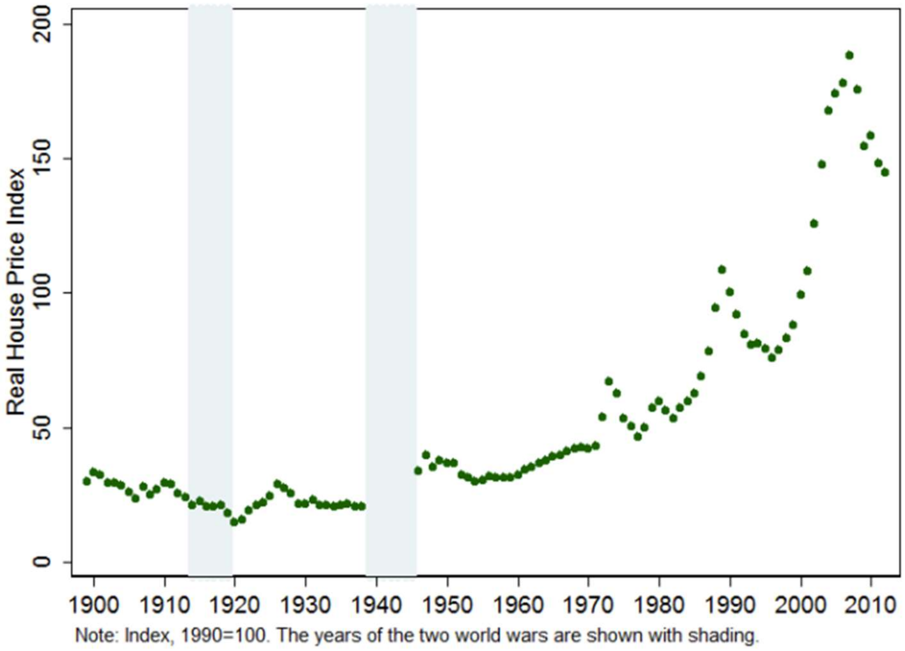


Figure 5: Real Estate Prices in US Dollars

Sure, the crash was caused by sub-prime loans in mortgage-backed securities, but my argument is that none of this would have happened if people didn't flee to assets like real estate or gold starting in 1971. I won't try and give an opinion on the ethics of bailing out wall street, that horse has been beaten to death.

The cost of housing is absurd, the price of real estate no longer reflects just the value of its utility as a place to live. There is a massive monetary premium on houses above their utility value. This has driven out middle- and lower-income families from the real estate market.

Same reasoning can be applied to gold, it would be worth a fraction of what it is today if it was only used for its industrial applications/jewelry. But it isn't, it has a monetary premium that represents a store of value. An ounce of gold went from $20 to $2,623. And it is not because we discovered gold cures cancer, it represents the devaluation of its denomination (dollars). In fact, if you look at the price of anything denominated in gold vs in dollars you will see what I mean. Below is a chart of food priced in gold since 1960, look at the steep decline from 1970. This website shows you the price of anything in gold.

https://pricedingold.com/food/

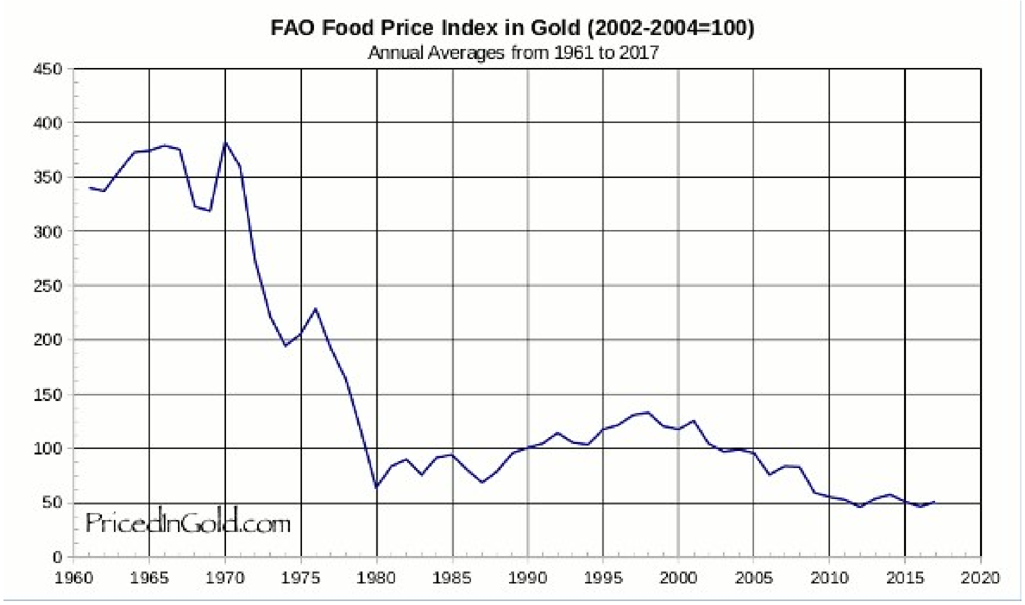


Figure 6: Food priced in gold

If you have been storing all your money in gold, you have not experienced inflation, things have in fact gotten cheaper representing both increased productivity and gold's monetary premium expanding.

I won't cover the inflation caused by spending in 2021 and how every Canadian now gets 250 dollars and no sales tax.

Conclusion is that since WW1 governments gave up sound money and adopted the Keynesian view that the state of the economy is determined by aggregate spending (essentially GDP). Nonstop spending creates crises, crises are remedied by more spending, and the cycle repeats.

It has been nonstop printing, spending and therefore inflation, and now we cannot stop, if we stop the house of cards will fall. I don't pretend to have a solution, I don't blame the current appointed officials either, they are simply playing a game that was started a long time ago. J Powel and Janet Yellen are just trying to keep the boat afloat.

I accept that this is the current state of the world, we need to keep inflating away the debt. With that in mind I will try and minimize inflation's negative impact on my life by holding something that cannot be inflated away by anyone. This argument doesn't just apply to bitcoin as a store of value, it has always been the argument for gold.

Gold's saleability (Saleability is the ability of an item to be sold or its marketability) is awesome, great store of value but highly inconvenient. This is why the whole, "*you store your gold with me I gave you a paper receipt" thing* started, nobody wants to transact with physical gold. The "custodian" of that gold, with enough time, will inevitably lie about how much gold they have, the incentives are misaligned. In my opinion, bitcoin has better saleability than gold due to its superior portability and divisibility.

If the Treasury held bitcoin, we would all be able to audit their holdings by looking at the blockchain, you can't walk into Fort Knox and start counting gold bars. I don't know how or if that would ever happen, simply an example to illustrate bitcoin > gold as a reserve asset.

This covers my argument for why the demand for bitcoin will keep increasing, the devaluation of currencies cannot stop. In my opinion Bitcoin is the best alternative/escape to keep your purchasing power from being eroded away. Now, I will explain how bitcoin's decreasing supply works.

Bitcoin is programmed to produce a block of transactions every 10ish minutes, a block contains around 500 transactions, the reward for each block was 50 bitcoins in the first 4 years of the network's operation (2009-2013). The 10 minutes is maintained by a difficulty adjustment, every 2,016 blocks (about every 2 weeks) the network will compute the average time to find a block over the last two weeks and adjust the difficulty accordingly.

Every 210,000 blocks (about every 4 years), the block reward is cut in half during what has been coined "Halving Events". Basic supply and demand dictate that lower supply = higher price if all else is equal. Figure 8 shows how the price of bitcoin has reacted to the last 4 halving events (doesn't include the latest one) [12].

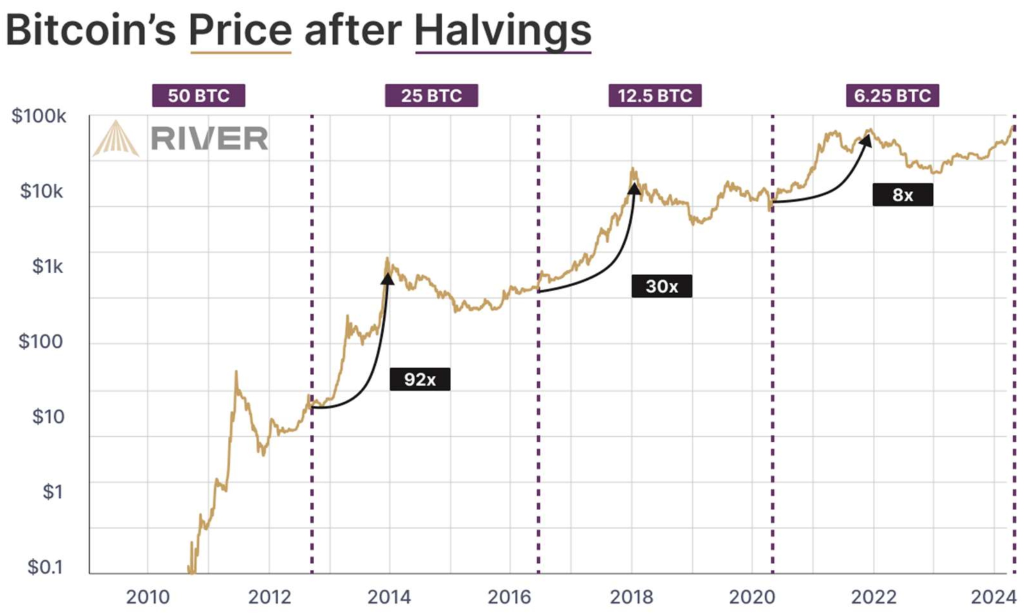


Figure 7: Bitcoin price after halving events

Currently the bitcoin reward is 3.125 BTC per block. You can calculate an estimate of how much bitcoin has been mined with the equation in Figure 9 by replacing 32 with the current epoch (4 as of this writing).

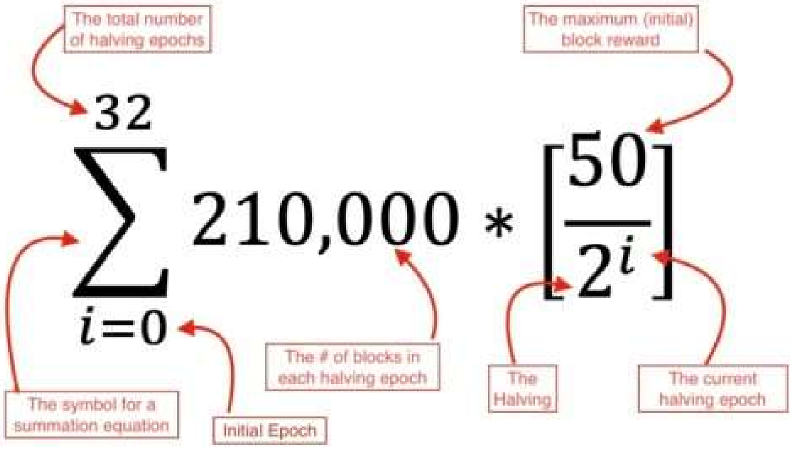
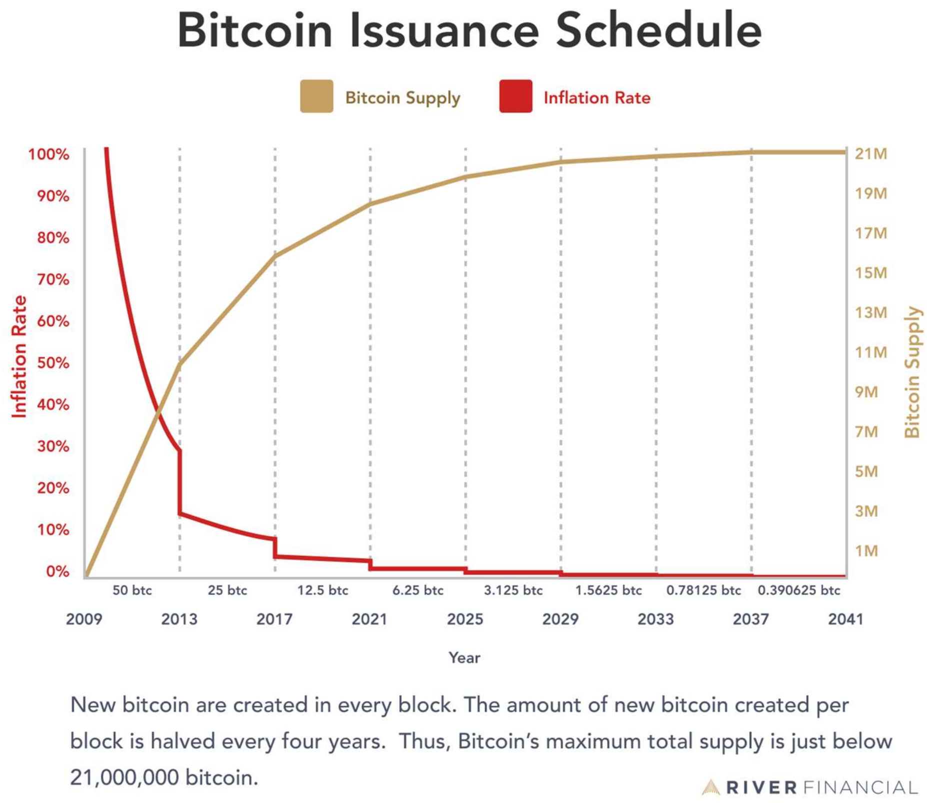

The total number of halving epochs
The maximum (initial) block reward
$\sum_{i=0}^{32} 210{,}000 * \left[\frac{50}{2^i}\right]$
The symbol for a summation equation
Initial Epoch
The # of blocks in each halving epoch
The Halving
The current halving epoch

Figure 9: Mined bitcoin formula

Figure 10 shows you the bitcoin supply, and inflation rate overtime. You can see its supply follows an exponential decay due to the 2^n in the denominator of the formula in Figure 9 [13].



New bitcoin are created in every block. The amount of new bitcoin created per block is halved every four years. Thus, Bitcoin's maximum total supply is just below 21,000,000 bitcoin.

Figure 10: Bitcoin supply and Inflation Rate

If you divide the amount of bitcoin produced annually, by the amount of bitcoin in circulation you get an inflation rate, the number of new coins added to circulation every year. For context gold's inflation rate has historically been 1-3% depending on if gold prices are up or down that year. With 3.125 Bitcoins per block, the inflation rate is 1.8%, the previous halving was an important milestone, as it marked bitcoin's inflation rate matching/beating golds. At the next bitcoin halving, sometime mid-2028, the inflation rate will come down to .9% with a 1.5625 block reward.

Every time any money that has ever existed (gold, silver, seashells, glass beads, tobacco, the US dollar) increases in value, producers of that money are incentivized to make more of it. That could be increasing gold mining or printing more dollars. Bitcoin is the only asset with a long-term inelastic supply. Its supply will systematically decrease to 0, regardless of its price movements.

This covers how bitcoin's supply decreases over time, if you agree with my argument for why its demand will increase over time, you can conclude its price should also increase.

I buy bitcoin because it is the best escape from the government's attack on my purchasing power, I won't let them inflate away my hard-earned money. I believe the price will continue to go up, not as drastically as it has in the past (It is already 2 trillion in market cap), but I believe it will continue to outperform any other investment over the long term. It isn't priced in, because there has never been an asset with these supply and demand qualities, there is no model to compare to.

Here ends my economic argument, the rest of this document covers more technical details about the network.

The following is a simplified explanation of bitcoin mining. Users will create and sign transactions (like writing and signing a cheque), they publish those transactions to the network (like publishing a post on Facebook), miners will group around 500 transactions into a block (a list of all the transactions). To "mine" a block, a miner must find a SHA-256 hash for the block with a certain number of leading 0's. SHA-256 is a hash function that calculates a 256-bit long hash value for an input (in this case the input is the block/list of transactions). The output of SHA cannot be predicted other than running it for the input (one way function).

The miner starts by calculating the SHA-256 value for a block of characters. If the value has the required number of leading zeros, the miner is done and has "mined the block". If not, the miner will append some characters to the list of transactions, and re-run SHA-256, it will do this repeatedly until it finds the correct number of leading zeros. These additional characters the miner adds are called "nonce" and it is really the nonce that miners are trying to guess/find. Once found, the miner can append the block to the block-chain and will receive the block reward. Network participants can easily verify the miner isn't cheating by running their newly added block through sha-256 once and seeing the correct number of leading zeros.

You can play around with SHA 256 on this website, add characters to the string "Satoshi" to try and get a single leading zero, you are doing about .3 Hashes/second, the best bitcoin miner is doing 234 TH/s, that is 2.34 x 10^{14} Hashes/second.

https://tools.keycdn.com/sha256-online-generator

With a basic understanding of mining, lets analyze the feasibility of the most widely discussed attack on bitcoin, a 51% attack. This 51% attack would be either an attempt to censor someone's transactions (not include their transactions in the blockchain) or double spend (spend the same amount of bitcoin twice), like if I had 100 dollars in my bank account and sent 2 100-dollar e-transfers. Either of these attacks would break people's confidence in bitcoin and drop the price to 0, meaning the attacker would not gain any monetary compensation for attacking the network.

Due to halving events and increasing demand from people using it as a store of value, Bitcoin price has increased over-time. The increased price has attracted more miners, Figure 11 shows Hashes/second, a Tera Hash is one trillion hashes [14].

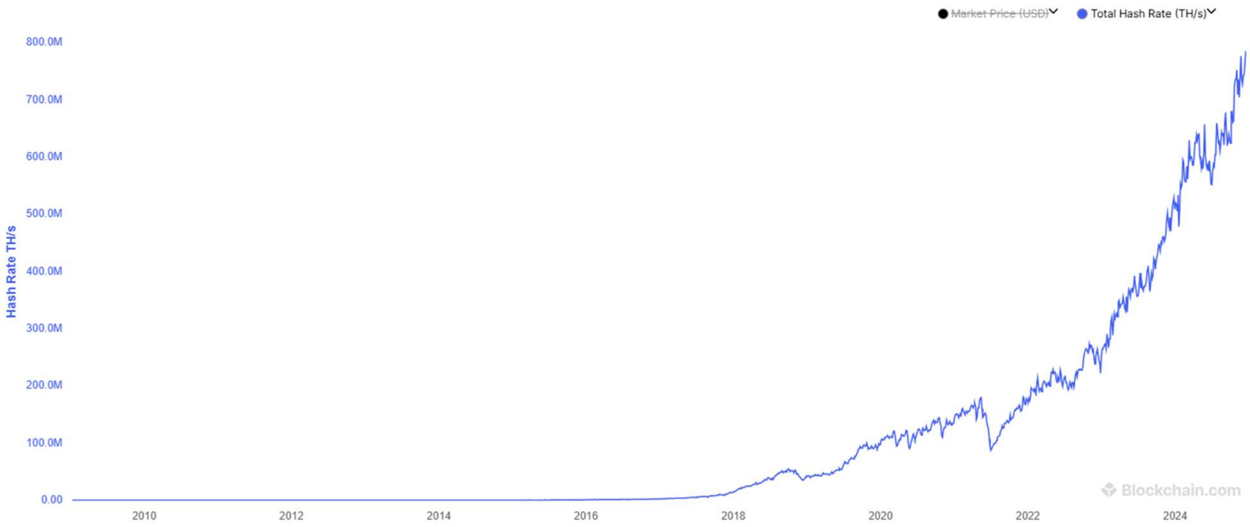


Figure 11: Bitcoin hash rate Hashes/Second

At the time of writing, 800 million Terra Hashes/Second are being performed by all miners. The best bitcoin miner, the Antminer S21 delivers a max hashrate of 234^{Th}/s, while consuming 3531 Watts of power. Since most people don't have the S21 we can approximate the average max hash rate of a miner is 110 (Based off the S19). Using this assumption we get 7.3 million miners. At a price-point of $2,500, 7.3 million S19s would cost 18.2 billion dollars. At a max power consumption of 3.25 KW and a reasonably cheap $.12/kWh, we get 2.9 million dollars/hour spent on electricity worldwide securing the bitcoin network. A 51% attack would go one of two ways.

One, an entity like a government is able to locate, confiscate and coordinate over 50% of miners. The US has the largest percentage of miners at 38% of all miners worldwide, next is China at 21% (Even though they tried to ban it). This means one entity would have to locate, confiscate and coordinate every single miner in the US and China at the same time, good luck.

Option two, buy and setup another 7.3 million miners, we can stop there on the fact that even with all the money in the world, supply wise that would be impossible. Just for fun, let's say it is possible, that is an initial 18-billion-dollar investment, next you need to setup the infrastructure. Bitcoin miners produce an incredible amount of heat, so they need sophisticated cooling systems. The s19 is about the size of a desktop computer and weighs 17 Kg. You must get a warehouse large enough to fit 57,670 Tons of bitcoin miners (A honda civic weighs 1,200 kg, that is 48,000 honda civics), this is without all the wiring and cooling systems that such a setup would require. Now find 23,725 Megawatts of electricity (Toronto's peak demand is 4,700 megawatts). Congratulations, you have found and connected 7x Toronto's electricity supply and now have a 51% chance of discovering the next block before the other 7.3 million miners at a cost of 3 million dollar/hour (Probably way more, you would be using a large amount of your country's electricity supply so electricity prices would skyrocket).

For extra precautions, all bitcoin wallets and most people in industry will get a transaction and wait for 3 more blocks to be added before they "confirm" they have received the bitcoin. For example, if I am buying bitcoin from someone, I will not send payment till their transaction gets included in a block AND 3 more blocks are added on top of that one.

What this means is this entity must find the next block, and then find the next three blocks. Remember, each time you have just 51% chance of discovering the next block. Multiplying the probabilities: .5 x .5 x .5 x .5= .0625. With your impossible setup, you have a 6.25% chance of attacking one block from the network. Divide the cost per hour to run your machines, $3,000,000/hour, by the probability, .0625, and you get 48 million dollars. That is the amount that you would spend just on the electricity for the miners (add the cooling and servers and that number could double) to theoretically attack one block of the network. That is just 15 hours (48/3). If you want to attack more than one block, keep multiplying by .5.

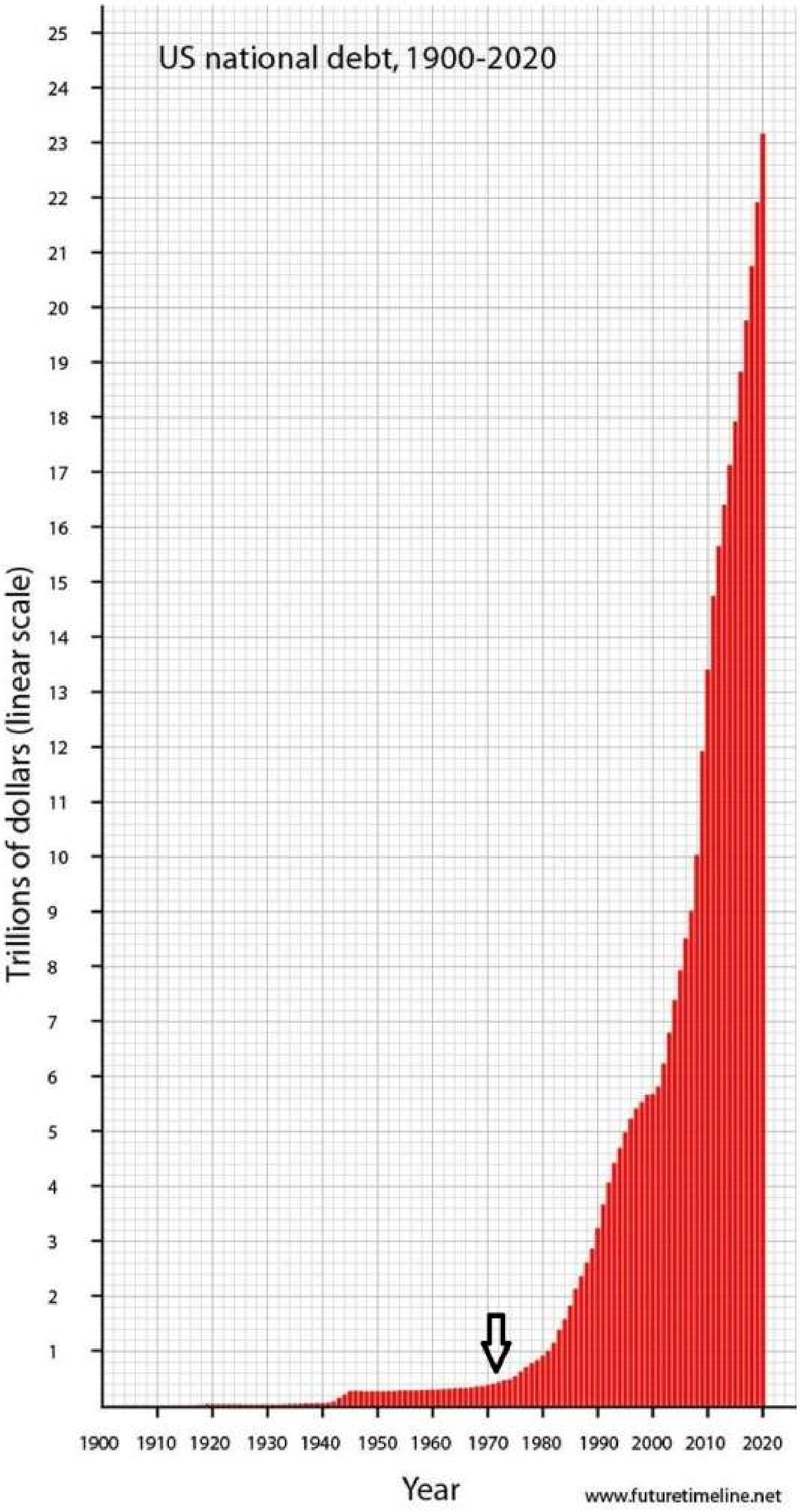
This exercise is pointless since you wouldn't get past the problems of finding 7.3 million more s19s, setting them all up along with their cooling systems and finding such an immense electricity supply at $.12/kWh. But it gives you an idea of the scale of the network and how much electricity is securing it.

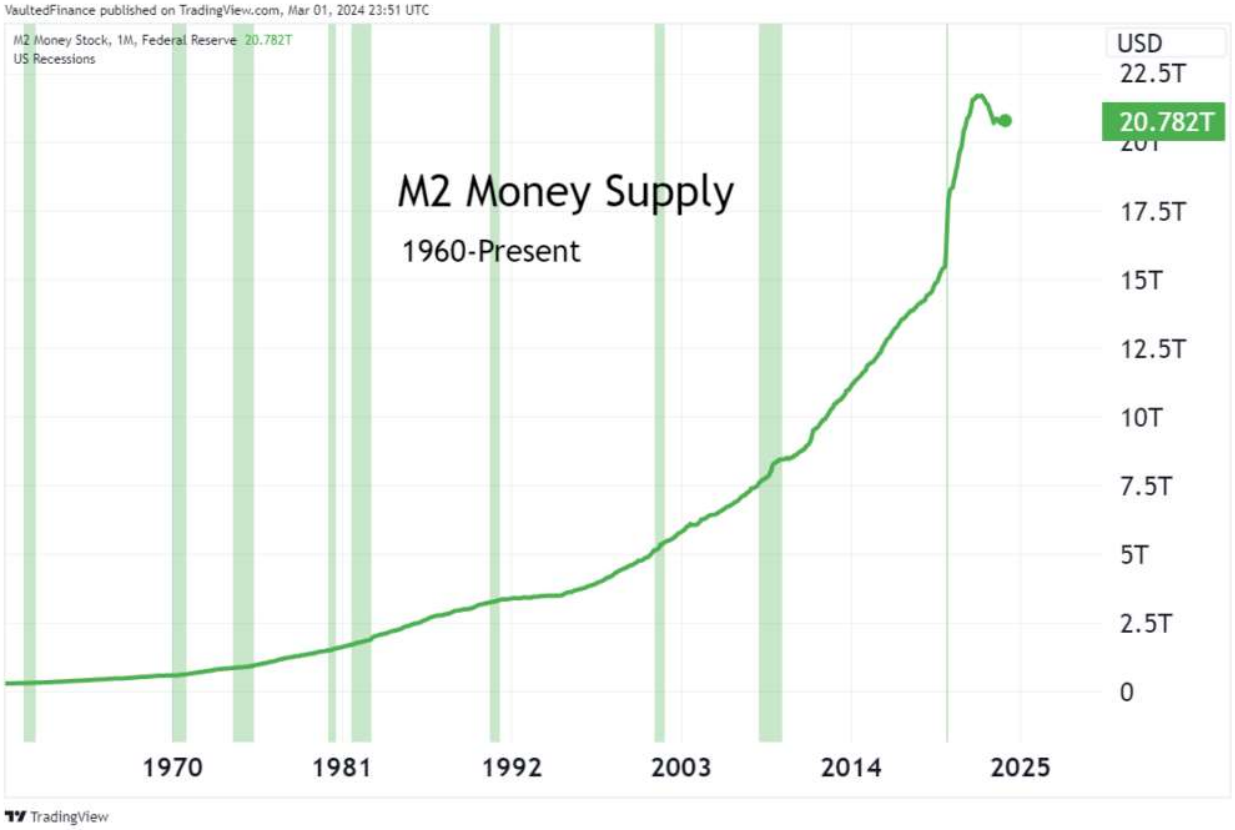
This is not an apples-to-apples comparison, but again just trying to put things in context, the US spends 830 billion annually on their military, that is their expense to secure the dollar network. Using our numbers, of $.12KwH and 7.3 million miners, the bitcoin network spends 64 billion annually on electricity to run and secure the network. Note, I am not counting how much it costs to run the Fedwire system (closest comparison of a value transmission network to BTC)

There is a lot missing from this document, I have not covered seed phrases, how transactions are signed, how public and private keys work, how changes to the source code happen, how nodes secure the network, how a wallet works, how the lightning network fixes the throughput/scalability problem, quantum threats, and so much more. This is already way too long, and it just scratches the surface, if you want to get an intelligent rendition of this that also covers all those topics read **Broken Money by Lynn Alden**.

If you disagree with anything I said let me know, I am very open to changing my mind.

Below are three more graphs that piss me the f-off, National debt, M2 money supply (amount of dollars in the system), and inflation. **Start stacking sats.**

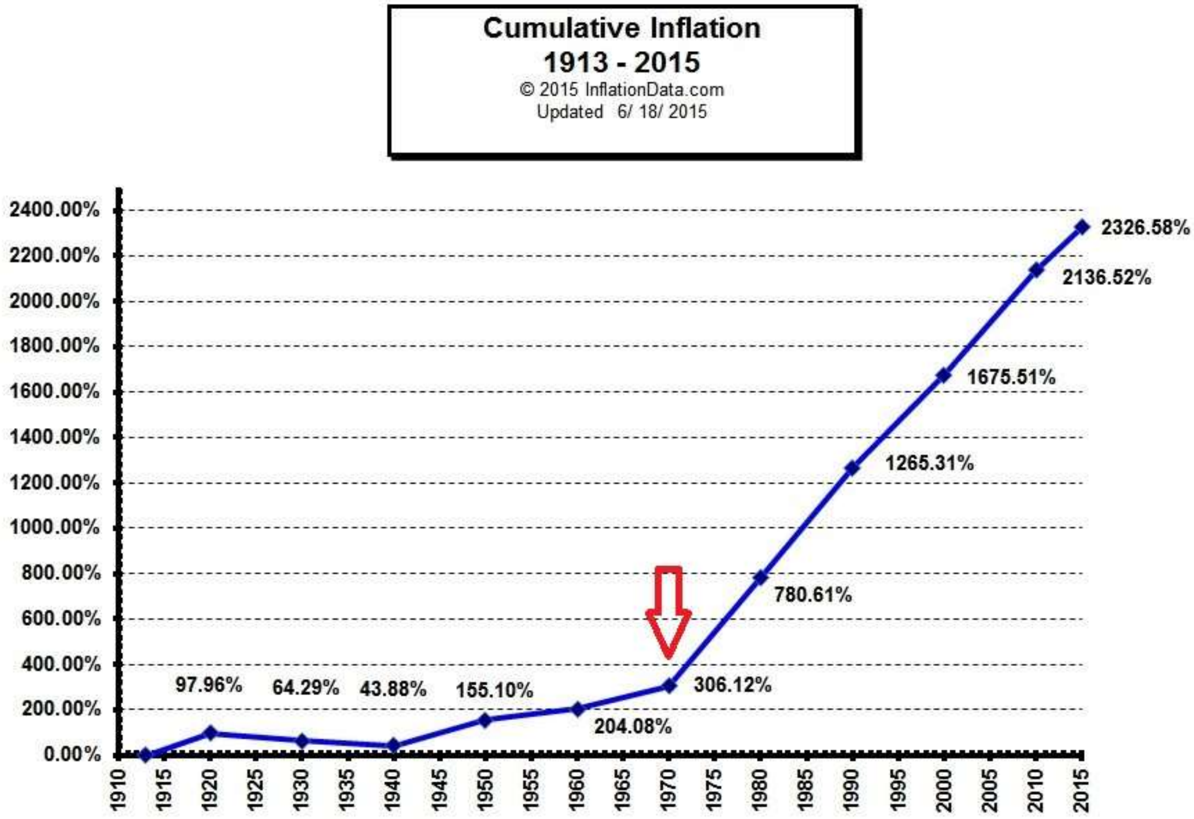




VaultedFinance published on TradingView.com, Mar 01, 2024 23:51 UTC

M2 Money Supply

1960-Present



Cumulative Inflation

1913 - 2015

© 2015 InflationData.com

Updated 6/ 18/ 2015

Bibliography

[1] "Public Debt WW1," [Online]. Available: https://www.treasurydirect.gov/kids/history/history_wwi.htm#:~:text=The%20Government%20also%20raised%20money,was%20more%20than%20%2425%20billion..

[2] "Saylor dot org," [Online]. Available: https://saylordotorg.github.io/text_macroeconomics-theory-through-applications/s11-05-policy-interventions-and-the-g.html#:~:text=In%20terms%20of%20fiscal%20policy,were%20financed%20by%20budget%20deficits..

[3] "Wikipedia 6102," [Online]. Available: https://en.wikipedia.org/wiki/Executive_Order_6102.

[4] "Wikipedia Gold Reserve Act," [Online]. Available: https://en.wikipedia.org/wiki/Gold_Reserve_Act#cite_note-GREEN-3.

[5] S. Ammous, The Bitcoin Standard.

[6] "Wikipedia Bretton woods," [Online]. Available: https://en.wikipedia.org/wiki/Bretton_Woods_system.

[7] W. c. t. U. g. s. t. increase?. [Online]. Available: https://www.higherrockeducation.org/blog/the-us-s-changing-priorities-reflected-in-the-government-budget.

[8] "History of US National Debt," [Online]. Available: https://www.economicshelp.org/blog/3018/economics/history-of-us-national-debt-gdp/.

[9] "Fifty Years Without Gold," [Online]. Available: https://www.rstreet.org/commentary/fifty-years-without-gold/.

[10] "Emergency Economic Stability Act," [Online]. Available: https://www.investopedia.com/terms/e/emergency-economic-stability-act.asp.

[11] "No Price Like Home," [Online]. Available: https://www.dallasfed.org/-/media/documents/institute/wpapers/2014/0208.pdf.

[12] "Bitcoin Halving," [Online]. Available: https://river.com/learn/what-is-a-bitcoin-halving/.

[13] "Who Create Bitcoin," [Online]. Available: https://river.com/learn/who-creates-new-bitcoin/.

[14] "Hashrate," [Online]. Available: https://bitcoinvisuals.com/chain-hash-rate.