THE BITCOIN SUPREMACY

How Bitcoin Becomes The World's Dominant Money

BY NICK GIAMBRUNO, Founder

FINANCIAL UNDERGROUND

The Bitcoin Supremacy

How Bitcoin Becomes the World's Dominant Money

By Nick Giambruno

Founder, The Financial Underground

Bitcoin has been likened to the platypus… which sounds like an odd comparison.

The platypus is a strange duck-billed mammal with webbed feet and a furry body like a beaver. It has characteristics of birds, mammals, and reptiles. Females lay eggs but also nurse their young with milk. Males produce a potent venom.

When Europeans discovered the platypus in Australia in 1798, they wrote letters to folks at home to describe this bizarre new animal. People thought the platypus was a joke or a hoax —because it didn't fit into the classification of animals at that time. But it was a real animal. People just didn't understand it because it was a new thing that didn't fit into the established paradigms.

Bitcoin is much the same. It doesn't fit into the framework of traditional financial analysis metrics. There is no P/E (price-to-earnings) ratio because Bitcoin has no earnings. There is no P/B (price-to-book) ratio because Bitcoin has no book value. Bitcoin has no CEO, no marketing department, and no employees.

Bitcoin is an entirely new asset people are adopting as money because of its superior monetary properties. The monetization of a new global money is genuinely unlike anything anyone alive has ever seen before. There is nothing else comparable. Like the platypus, Bitcoin is an entirely new animal. That's why Bitcoin confuses many people, including prominent investment professionals.

It's not uncommon for it to take years for someone to *really* get Bitcoin. It requires an understanding of economic incentives, technology, cryptography, financial markets, and other fields. But, by far, the most important way to understand Bitcoin is first to understand money, which anyone can do. I'll get to that in a moment.

Fortunately, it no longer takes years to understand Bitcoin. There is a wonderful body of knowledge that connects the dots in a way that wasn't available in the early years. I believe that anyone who does the homework to really understand Bitcoin will reap significant dividends in the future.

I think Bitcoin has revolutionary implications, as much or more than the printing press, the invention of gunpowder, the Internet, and other historical innovations that overturned established paradigms.

In this report, I am distilling many years of study into the most concise analysis possible that anyone—regardless of their background—should be able to understand. I'll take you down the Bitcoin rabbit hole and show you where I think it goes.

It is essential to start with the basics as a sound foundation and build from there in understanding Bitcoin. Doing it any other way will likely end with confusion or faulty conclusions.

My goal in this report is to make the case for two simple propositions that underpin our investment thesis in Bitcoin, Bitcoin mining stocks, and other businesses involved with Bitcoin.

1) Bitcoin is a superior form of money.

2) Bitcoin is unstoppable.

What Is Money?

Although people use money every day, few consider what it actually is or what makes for a good money.

Asking people, "what is money?" is like asking a fish, "what is water?"

The fish probably doesn't even notice the water unless it becomes polluted or something is wrong.

Money is a good, just like any other in an economy. And it isn't a complex notion to grasp. It doesn't require you to understand convoluted math formulas and complicated theories—as the gatekeepers in academia, media, and government mislead many folks into believing.

Understanding money is intuitive and straightforward. Money is simply something useful for storing and exchanging value. That's it.

Think of money as a claim on human time. It's like stored life or energy.

Unfortunately, today most of humanity thoughtlessly accepts whatever their government gives them as money. However, money does not need to come from the government. That's a total misnomer that the average person has been hoodwinked into believing.

It would be similar to transporting yourself back in time and asking the average person in the Soviet Union, "Where do shoes come from?"

They would say, “Well, the government makes the shoes. Where else could they come from? Who else could make the shoes?”

It’s the same mentality here regarding money today—except it’s much more widespread.

The truth is money doesn’t need to come from the government any more than shoes do.

People have used stones, glass beads, salt, cattle, seashells, gold, silver, and other commodities as money at different times.

However, for over 2,500 years, gold has been mankind’s most enduring form of money.

Gold didn’t become money by accident or because some politicians decreed it. Instead, it became money because countless individuals throughout history and across many different civilizations subjectively came to the same conclusion: gold is money.

It resulted from a market process of people looking for the best way to store and exchange value.

So, why did they go to gold? What makes gold attractive as money?

Here’s why.

Gold has a set of unique characteristics that make it suitable as money.

Gold is durable, divisible, consistent, convenient, scarce, and most importantly, the “hardest” of all physical commodities. In other words, gold is “hard to produce” relative to existing stockpiles and the one physical commodity most resistant to inflation of its supply. That’s what gives gold its monetary properties.

Bitcoin shares many of the same attributes of gold that make it attractive as money. That’s why it is often referred to as “digital gold.” Like gold, Bitcoin does not have counterparty risk, and nobody can arbitrarily inflate the supply.

At this point, some people might say, “wait, Bitcoin doesn’t have intrinsic value or industrial use. It’s more like fiat money. So how can it even be compared to gold?”

Before we go further, it’s important to make three clarifications to address common misunderstandings.

There is No Such Thing as Intrinsic Value

One of the first—and most important—things free-market Austrian economics teaches is that all value is subjective.

There is no such thing as inherent or intrinsic value.

Something only has value because individuals subjectively determine it has value to them.

For example, when people didn't understand what crude oil was, they'd find it in their backyards and think it was waste. So they'd pay to have it removed from their property.

Later, once people understood the economic potential of crude oil, it was transformed from unwanted waste into a lucrative commodity.

The oil didn't change; it was still the same oil. What changed was how people valued it.

Marxists differ in that they falsely believe that labor has inherent or intrinsic value. But this ridiculous notion is easily debunked.

The great economist Murray Rothbard explains this by asking people to try to make and sell mud pies—not the chocolate desserts, but pies literally made of dirt.

According to the Marxists, the pies have objective and intrinsic value because of the labor someone put into making them. But good luck getting someone to pay for them voluntarily.

The concept that all value is subjective applies to all goods, including monetary goods like gold and Bitcoin.

Bitcoin is Not Fiat Money

Bitcoin is a free-market form of money.

Over 100 million people worldwide have subjectively determined that Bitcoin has value to them. They voluntarily chose to exchange other forms of value for Bitcoin. They did not choose Bitcoin because legal tender laws or government decrees forced them to, as they do for fiat money.

The Oxford English Dictionary defines fiat money as "inconvertible paper money made legal tender by a government decree."

Bitcoin is clearly not fiat money.

Industrial Use Doesn't Make a Good Money

Many people incorrectly reason that Bitcoin can't be a good money because it doesn't have any industrial use or non-monetary utility.

However, that is not needed to make something money. The use of something as money itself is sufficient for it to be money.

The fact that gold has some industrial use doesn't give it its superior monetary properties. People value gold as money primarily because it's the one physical commodity most resistant to inflation—not because it's used in dentistry, electronics, or other industries.

On the contrary, I'd argue that gold's relatively small industrial uses do not enhance its monetary characteristics. If they did, then why aren't metals with more industrial use—like copper or nickel—more desirable as money?

When it comes to money, I'm only interested in its ability to store and exchange value. I'm not interested in something whose value is hostage to the whims of ever-changing industrial conditions.

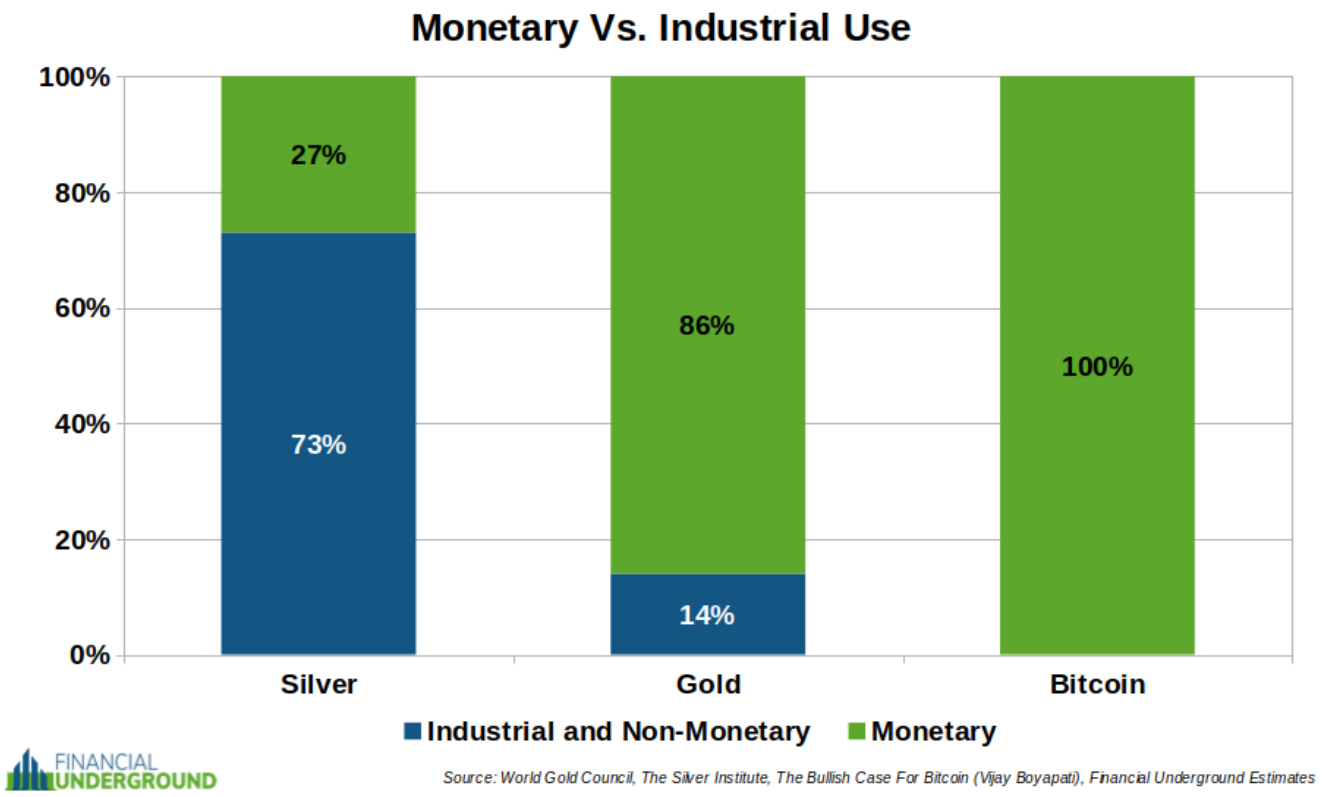
This is why industrial use is not a monetary benefit but, in fact, a potential detriment. Gold would be an even better money without the variation in its supply/demand that comes from its industrial uses, which are unrelated to its use as money.

According to the latest annual data from the World Gold Council, total gold demand is broken down into the following uses: jewelry (55.4%), investment (25%), central banks (11.3%), and industrial (8.2%).

According to the latest annual data from The Silver Institute, total silver demand is broken down into the following uses: industrial (51%), jewelry (17%), investment (27%), silverware (4%), and hedging (1%).

Indians, Chinese, and other Asians account for a large portion of global gold jewelry demand. While there isn't precise data, I estimate that many people are also using gold jewelry as a store of value—a monetary use.

Putting it all together, we can see in the chart below that gold is primarily a monetary good (86%). Industrial and non-monetary uses account for a relatively small part of its demand (14%). Silver is the opposite. Industrial and non-monetary uses account for 73% of its overall demand, with monetary use making up 27%. Finally, Bitcoin is a purely monetary good; it has no industrial or non-monetary utility.



With those clarifications in mind, let's look at Bitcoin's most important monetary characteristic, its hardness.

The Hardest Money the World Has Ever Known

Hardness is the most important characteristic of a good money.

Hardness does not mean something that is necessarily tangible or physically hard, like metal. Instead, it means "hard to produce." By contrast, "easy money" is easy to produce.

The best way to think of hardness is "resistance to inflation," which helps make it a good store of value—an essential function of money.

Would you want to put your savings into something that somebody else can create with no effort or cost?
Of course, you wouldn't.

It would be like storing your life savings in Chuck E. Cheese arcade tokens or airline frequent flyer miles. Unfortunately, putting your savings into government currencies isn't that much different.

What is desirable in a good money is something that someone else cannot make easily.

The stock-to-flow (S2F) ratio measures an asset's hardness.

S2F Ratio = Stock / Flow

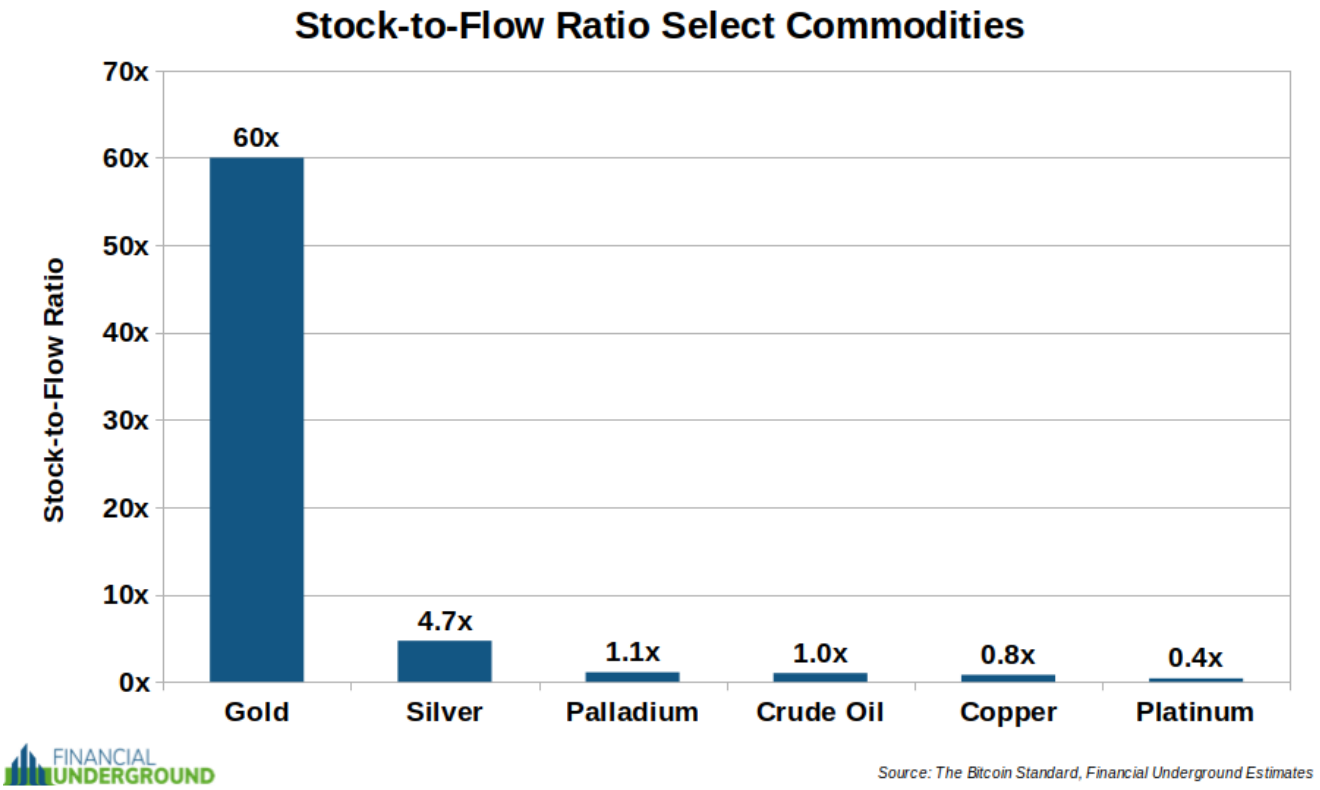
The “stock” part refers to the amount of something available, like current stockpiles. It’s the supply already mined. It’s available right away.

The “flow” part refers to the new supply added from production and other sources each year.

A high S2F ratio means that annual supply growth is small relative to the existing supply, which indicates a hard asset resistant to inflation.

A low S2F ratio indicates the opposite. A low S2F ratio means that new annual supply can easily influence supplies—and prices. That’s not desirable for something to function as a store of value.

In the chart below, we can see the hardness of various physical commodities.



Monetary commodities such as gold and silver have higher S2F ratios. On the other hand, industrial commodities have low S2F ratios, typically around 1x.

With an S2F ratio of 60x, it would take about 60 years of the current production rate to equal the existing gold supply.

Another way to think of it is to look at the inverse of the SF ratio, which is the rate of annual production relative to existing stockpiles. So, for example, gold’s yearly production is about 1.7% of its existing stockpiles.

In short, no other physical commodity comes close to gold's hardness or resistance to inflation.

Two things can explain gold's high S2F ratio.

First, gold is indestructible.

Unlike silver, gold doesn't decay or corrode. That means that most gold people produced even thousands of years ago is still around today and contributing to current stockpiles.

Second, unlike other metals, gold has a history of thousands of years of production.

These two factors make gold's existing stockpiles so large relative to new production. That means nobody can arbitrarily increase the gold supply, which helps make it a neutral store of value. It's what gives gold unique and unmatched monetary properties among other metals.

Here's the main point.

Hardness is the most important characteristic of a good money. All other monetary characteristics—durability, divisibility, consistency, convenience, and so forth—are meaningless if the money is easy for someone to produce.

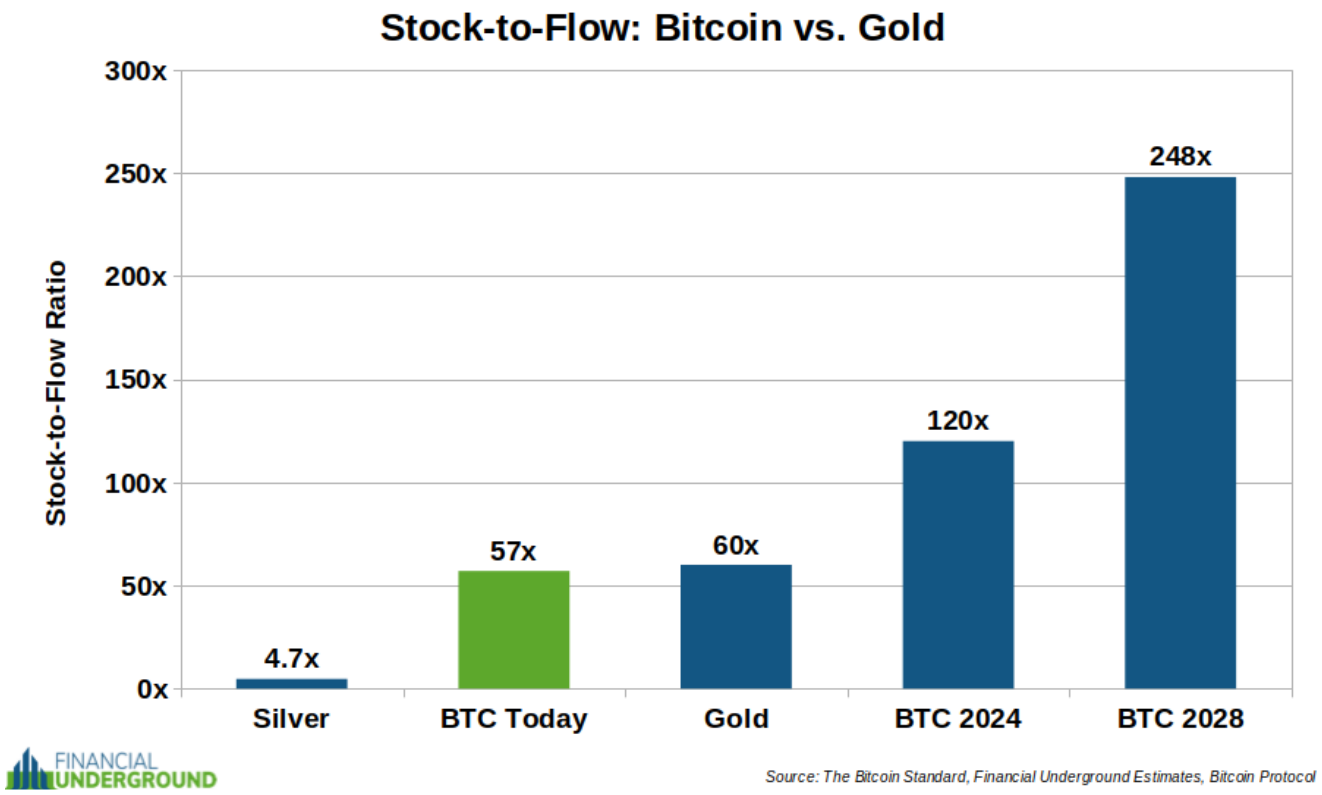
That's why the history of money is the history of the hardest asset winning and why gold has always reigned supreme. But now gold has a serious competitor…

Today, Bitcoin's S2F ratio is about 57x, slightly below gold's.

According to its fixed protocol, we know precisely how Bitcoin's supply will grow in the future. A key feature is that the new supply gets cut in half every four years, which causes Bitcoin's hardness to double every four years. It's a process known as the "halving"—or what I like to call "quantitative hardening."

The next time Bitcoin's supply growth will be cut in half will be in May 2024.

Bitcoin's hardness will be almost twice that of gold's when that happens.



That's how Bitcoin could become the hardest money the world has ever known in May 2024. And it will keep getting harder.

Scarcity is Not Hardness

It's important to clarify that hardness is not the same as scarcity. They are related concepts but not the same thing.

For example, platinum and palladium are scarcer than gold, but they are not hard assets. Current production is high relative to existing stockpiles. Unlike gold, stockpiles of platinum and palladium have not built up over thousands of years. It's the primary reason why new supply can easily rock the market.

Because of their low S2F ratios, platinum (0.4x) and palladium (1.1x) are even less suitable as money than silver. Their low S2F ratios indicate they are primarily industrial metals, which corresponds to how people actually use them today.

The Bitcoin Standard

The one resource that has been most influential on my thinking about Bitcoin and money is *The Bitcoin Standard: The Decentralized Alternative to Central Banking*. The author, Saifedean Ammous, is a sound Austrian economist and an old friend from when I lived in Beirut, Lebanon. I consider his book to be essential reading.

Absolute Scarcity

It's crucial to note that none of the other thousands of cryptocurrencies are genuinely scarce like Bitcoin.

They all have key players, insiders, and development teams that can inflate the supply or change the rules if they choose to.

In short, all other cryptos have artificial scarcity and are therefore not hard assets. Instead, they are more akin to frequent flyer miles and arcade tokens.

By contrast, Bitcoin takes humans out of the equation. Its non-discretionary monetary policy is in the hands of a fixed protocol.

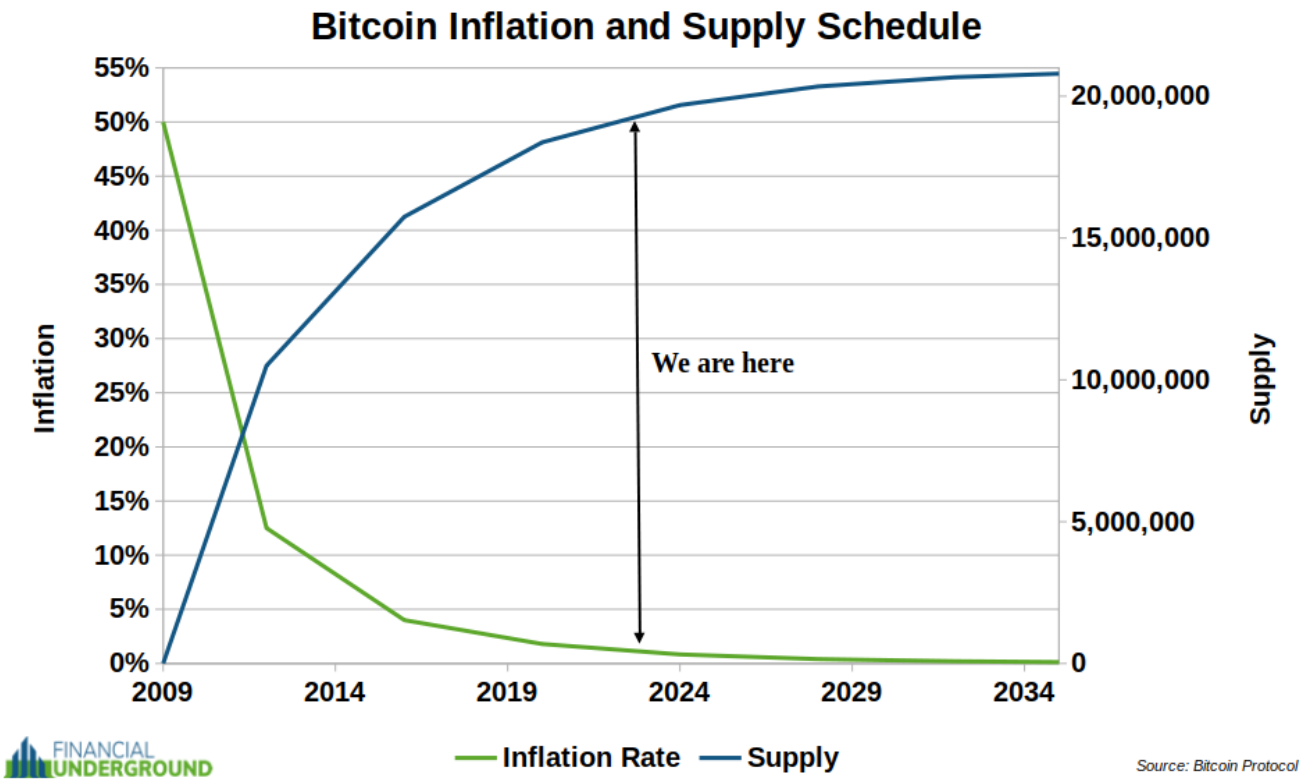
Nobody can change Bitcoin's supply—not even Elon Musk, Jeff Bezos, the Chinese government, the US government, or any of these powerful entities combined. Even if Satoshi Nakamoto—Bitcoin's anonymous cypherpunk creator—came back after disappearing in 2011, he would not be able to alter Bitcoin.

That's what gives Bitcoin genuine scarcity and credibility as a neutral money. It's the essential difference between Bitcoin and all other cryptocurrencies and why no other possesses the monetary properties of Bitcoin.

With Bitcoin, the current and future supply is finite and known to all. There will never be more than 21 million Bitcoins, and there is nothing anyone can do to change that.

The supply of Bitcoin won't grow much at all from here. The current supply is over 19 million, which means more than 90% of the total Bitcoin supply has already been created. By the end of this decade, over 98% of all Bitcoins will have already been created.

The remaining 10% will come on to the market at a preset, ever-decreasing rate until the last Bitcoin is created around 120 years from now, in 2140.



No other monetary asset has this kind of certainty of future supply. The closest comparison is with gold.

The World Gold Council estimates there are 6.4 billion ounces of mined gold globally and that annual production averages around 80 million ounces a year.

That much is what is known. However, we don't know how much gold is out there to be discovered and mined in the future.

For example, how many mined ounces of gold will be available on June 1, 2031? We can probably make a pretty accurate projection, but nobody can know.

What will the Bitcoin supply be on June 1, 2031? According to the immutable protocol, it will be around 20,589,121 Bitcoins.

Bitcoin has another unique scarcity attribute. It isn't just scarce. It is *absolutely scarce*.

For example, imagine the price of copper going 5x or 10x.

You can be sure that would spur increased production, eventually expanding the copper supply. Of course, the same is true of any other commodity.

The dynamic of higher prices incentivizing more production and ultimately more supply, bringing prices down, exists with every physical commodity. However, gold is the most resistant to this process.

That supply response is why most commodity prices tend to revert around the cost of production over time.

However, Bitcoin totally defies this dynamic because its supply is perfectly inflexible. It's the only commodity where higher prices *cannot* induce more supply.

In other words, Bitcoin is the first—and only—monetary asset with a supply that is entirely unaffected by increased demand. That is an astonishing and game-changing characteristic.

Here's the bottom line. Gold and other commodities are scarce, but only Bitcoin is absolutely scarce.

That means the only way Bitcoin can respond to an increase in demand is for the price to go up. Unlike every other commodity, increasing the supply in response to increased demand is not an option.

You might be wondering, that all sounds nice, but what gives Bitcoin's absolute scarcity credibility? Couldn't someone change the supply and other aspects of the protocol?

The key to understanding the **credibility** of Bitcoin's fixed monetary policy is with the full nodes and in the mining process, which combined form an ingenious system of incentives that secure the Bitcoin network in a genuinely decentralized fashion.

Bitcoin Miners and Full Nodes Create a Credible Monetary Policy

Let's start with the basics and build from there to get clarity on this often misunderstood topic.

Bitcoin is open-source software, which means its code is available for anyone to download, inspect, suggest changes, and run.

Think of the Bitcoin blockchain as simply a public database of transactions distributed to over 15,000 computers worldwide. The computers that retain the entire blockchain and run the Bitcoin software are called "full nodes."

Full nodes enforce the Bitcoin protocol and consensus rules—like its monetary policy. They can also verify and audit the entire supply and transaction history—without relying on third parties.

Bitcoin needs enough full nodes to protect against centralization and capture by hostile forces—like governments and financial institutions.

How many full nodes are enough to achieve this security? Nobody knows for sure. However, it seems the current number has been capable of doing the job.

If a hostile entity wanted to change Bitcoin's parameters, among other things, it would need to attack all the full nodes all around the world simultaneously.

For example, imagine that Bitcoin had only 15 full nodes, all located in China. It would be feasible for the Chinese government—or another attacker—to simultaneously target or compromise all 15 nodes. It would be the death of Bitcoin as we know it.

However, attacking 15,000 full nodes worldwide—some cleverly hidden—at the same time is an entirely different matter. So far, it's proved to be impossible.

The more full nodes there are, the more secure Bitcoin is. So it's crucial the average person can easily operate one.

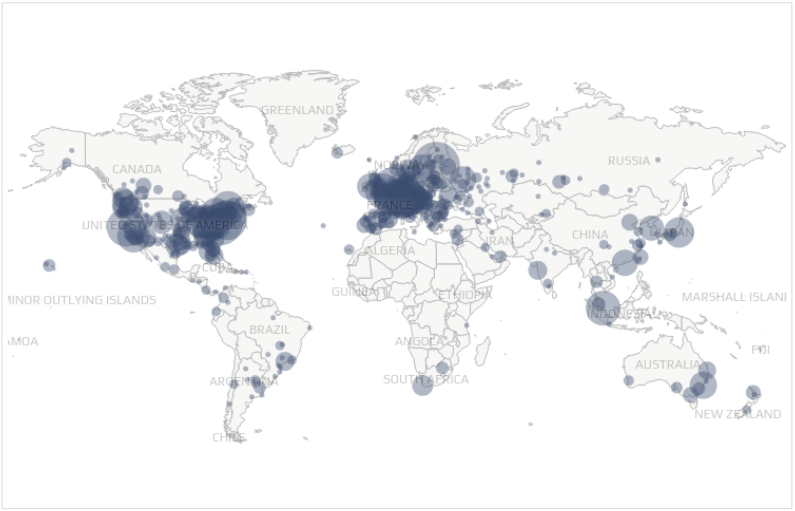
The table below lists the majority (53%) of nodes as "n/a," which means the node owners have taken measures to conceal their actual locations, improving privacy and making them much harder to attack.

REACHABLE BITCOIN NODES

15765 NODES CHARTS

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

RANK	COUNTRY	NODES
1	n/a	8402 (53.30%)
2	United States	2016 (12.79%)
3	Germany	1438 (9.12%)
4	France	528 (3.35%)
5	Netherlands	350 (2.22%)
6	Canada	331 (2.10%)
7	Russian Federation	241 (1.53%)
8	United Kingdom	233 (1.48%)
9	Finland	220 (1.40%)
10	Singapore	137 (0.87%)



Map shows concentration of reachable Bitcoin nodes found in countries around the world. LIVE MAP

Source: Bitnodes.io

To be honest, I am not a fan of the term "mining" because it confuses what is happening.

The process of Bitcoin mining is better thought of as a competition with finite rewards, like winning a gold medal in the Olympics.

About every 10 minutes, Bitcoin miners submit a new block—or set of transactions—to the full nodes, adding it to the existing database (blockchain), but only if the miner's block follows the protocol.

If the full nodes verify the block as valid, the miner will earn the **Block Reward**.

The Block Reward consists of the **Block Subsidy**—newly created Bitcoins in each block—and **Transaction Fees**.

The Block Subsidy is currently 6.25 Bitcoin per block and is cut in half every four years—or approximately 210,000 blocks—until it reaches 0 in the year 2140.

The Block Subsidy will remain 6.25 BTC until May 2024, when it will be halved to 3.125 BTC.

The other component of the Block Reward is the Transaction Fees.

Think of the digital space on each Bitcoin block as scarce real estate on an immutable ledger.

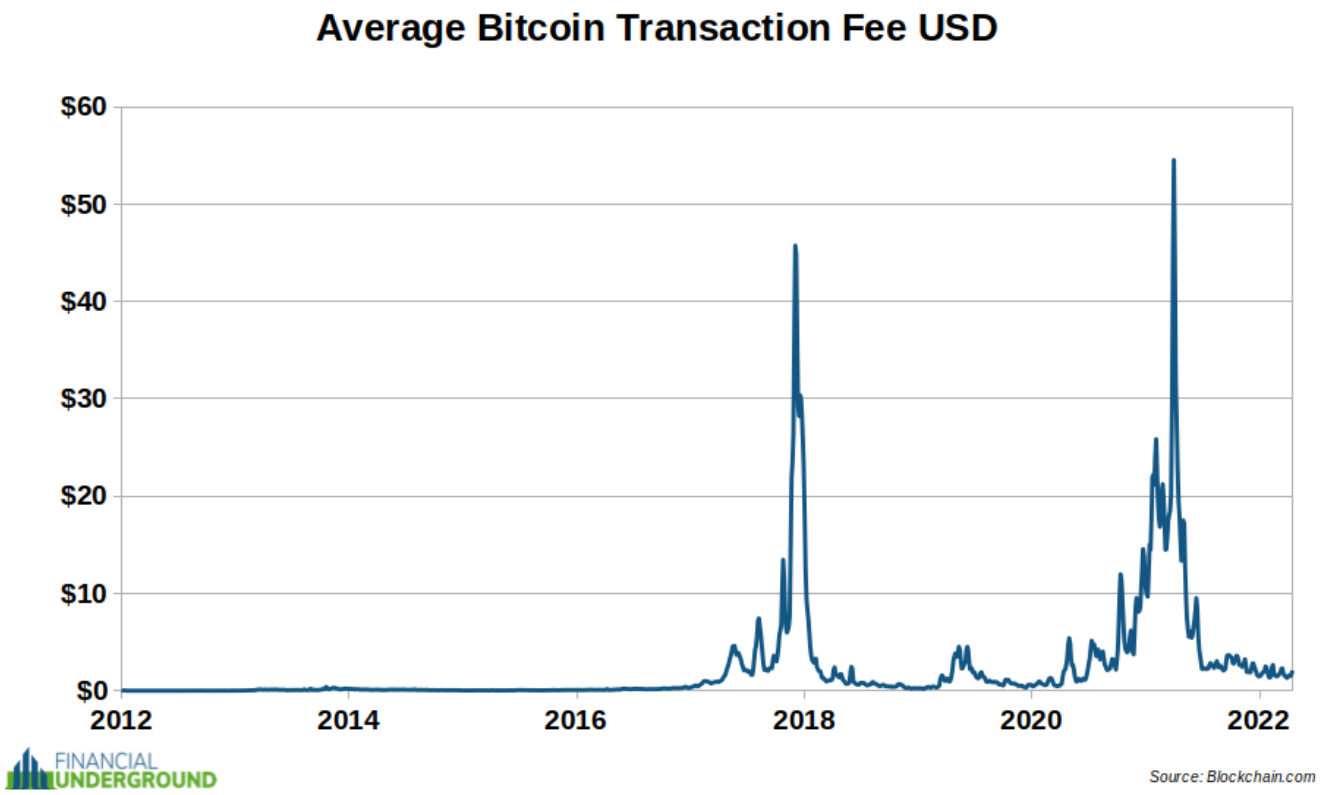
Whenever you make a Bitcoin transaction, you must pay a fee for Bitcoin miners to inscribe it onto the next block of the blockchain.

These transaction fees are a simple matter of economics—supply and demand for scarce Bitcoin block space. It's an excellent illustration of a competitive free market at work.

Whenever you make a Bitcoin transaction, you are bidding against everyone else in the world to get your transaction inscribed onto the next block through the transaction fee.

The higher the fee you pay, the faster miners will finalize your transaction, which means it has been added to the blockchain.

Naturally, transaction fees vary widely. It has swung from being as cheap as $0.05 to get your transaction included in the next block to over $40.



However, before a Bitcoin miner can submit a new block to the network of full nodes—and thus earn the rewards of 6.25 of freshly created Bitcoins and transaction fees—they must compete to solve complex math problems that are difficult to solve but easy to verify. The first miner to solve the math problem has the chance to propose a new block to the network and thus earn the rewards. The process then starts over again.

Depending on the aggregate amount of computing power miners are contributing, the Bitcoin protocol automatically adjusts the difficulty of these math problems every two weeks so that, on average, it takes about 10 minutes for miners to solve and thus generate a new block.

This brilliant feature—called the **Difficulty Adjustment**—is why, no matter how high the Bitcoin price goes, it cannot incentivize miners to produce more Bitcoins than what the protocol has preset.

At first glance, it all may seem unnecessary—as the complex math problems are unrelated to the transactions—but it's a crucial part of ensuring the Bitcoin network is self-sufficient, incentivized to be honest, and doesn't deviate from the consensus protocol. It's what makes Bitcoin work without anybody in charge of it.

Miners must incur real-world costs—expensive computer hardware and massive amounts of electricity—to solve these math problems and have the chance to submit a new block to the network to earn the rewards.

If the block they submit doesn't follow the Bitcoin protocol or is otherwise invalid, the network of full nodes will instantly reject it. If that happens, the miner will not earn any rewards despite incurring enormous costs to submit the block in the first place.

The genius of Bitcoin's security model is that it is difficult and expensive for miners to submit a new block, but easy, cheap, and fast for the network to verify whether that block is legitimate or not.

Bitcoin analyst Preston Pysh has come up with a helpful way to think of this.

Think of a Bitcoin miner like a person who puts together a large and complex jigsaw puzzle. It takes a lot of time and work to put it all together.

Then think of the global network full nodes as puzzle checkers. Each one of them verifies the work of the miners. It's like how someone can look at a complete jigsaw puzzle and quickly see that it was put together correctly. It's easier to check the work than to do the work.

In other words, it's quick, cheap, and easy for the puzzle checkers (full nodes) to verify that the miners completed the jigsaw puzzle correctly. That's the essence of the asymmetry in Bitcoin's security model.

If a miner ever tried to stray from the Bitcoin protocol or include invalid transactions in the block, the full nodes would easily detect and instantly reject it.

It would be not only a fruitless effort for the renegade miner but would impose actual costs on them. They would need to use an enormous amount of electricity and processing power to solve the math problem in the first place.

In other words, it takes a lot of effort and costs a lot of money to propose a new block to the Bitcoin network, and if the miner isn't following the protocol, then it will waste all of that money.

It's essential to clarify a common misunderstanding here. **Miners do not control Bitcoin**.

Bitcoin proponent Saifedean Ammous said it best: "Miners are Bitcoin's slaves, not masters."

Saifedean means that the miners need to satisfy the Bitcoin network—not the other way around. Miners must follow the Bitcoin protocol and be honest. If they don't, they will do nothing but waste money and eventually bankrupt themselves.

This is how Bitcoin's essential "**Proof of Work**" system works.

Satoshi once said, "Proof-of-work has the nice property that it can be relayed through untrusted middlemen."

Proof of Work makes it possible for a decentralized network of thousands of computers worldwide to reach a consensus on the entire transaction history—without the need for a trusted third party or any intermediary.

It's a truly revolutionary innovation in computer engineering and money.

Bitcoin's Proof of Work system solved the Byzantine Generals problem—a longstanding problem in computer science. In short, it's the problem of getting different people—who may be hostile to each other—to come to a consensus about something without a trusted arbitrator of truth.

Before Bitcoin, this was not possible. Obtaining consensus required a centralized party.

Think of a traditional bank that you use. The bank is needed to keep an internal ledger of accounts and balances, including your balance and transaction history. It would be impossible to keep accurate records without a trusted centralized entity determining what is true for everyone in this situation.

Now imagine an innovation that removes the need for the centralized entity (the bank) to keep an accurate record of all the accounts, balances, and transactions. It effectively allows everyone to be their own sovereign bank without the need for trusted third parties… and, at the same time, is the hardest money the world has ever known.

Now, that's a disruptive technology… and that's precisely what Proof of Work allows Bitcoin to do.

Proof of Work makes Bitcoin resistant to being captured, controlled, or manipulated. It's what makes Bitcoin credibly inflation-proof and absolutely scarce, which in turn is what gives it its superior monetary properties as a neutral hard money.

There is simply no substitute for Bitcoin's Proof of Work system. It's the only way we know of today to have a genuinely decentralized monetary system beyond anyone's ability to control.

Hash Rate

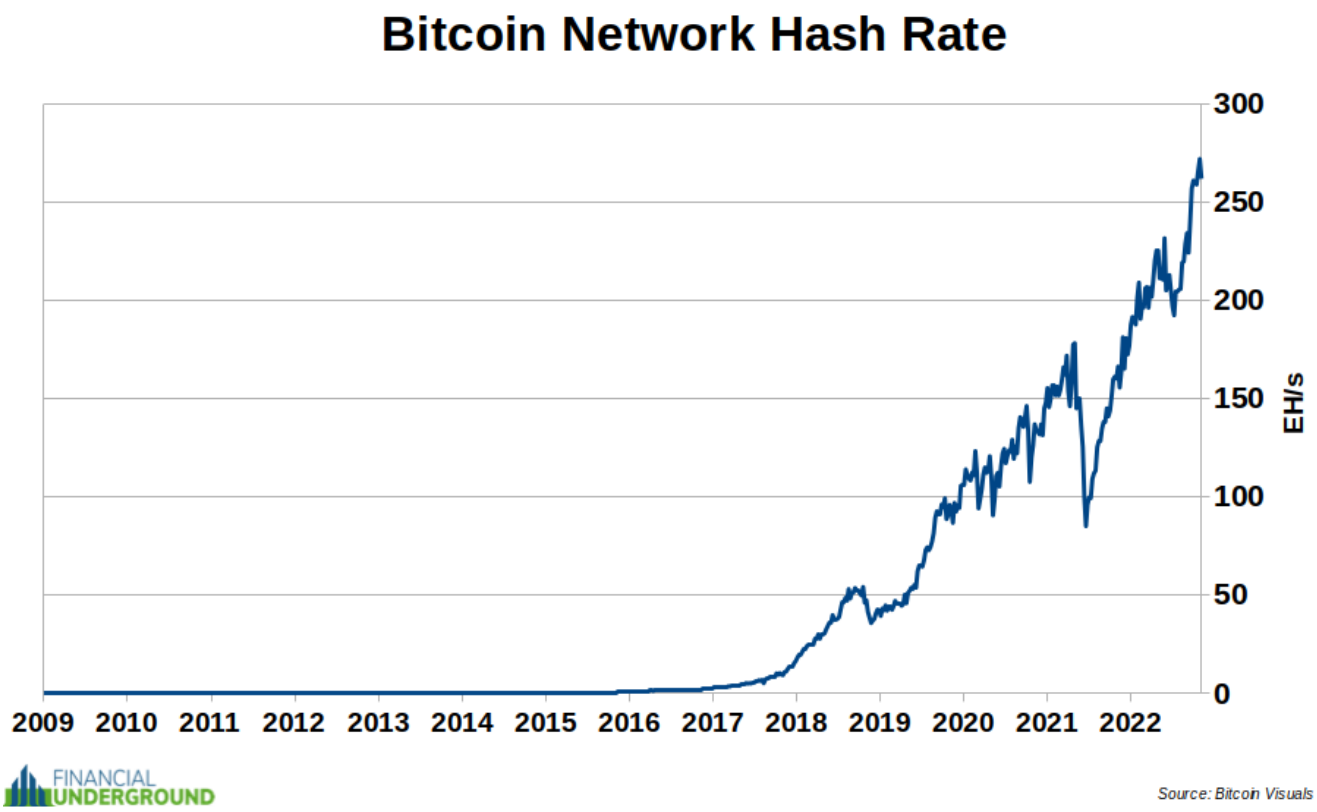
The cumulative computing power of all Bitcoin miners is the overall network's Hash Rate.

It refers to the number of hashes—or calculations—per second that Bitcoin miners dedicate to solving the Proof of Work math problems.

The chances of a miner solving the Proof of Work problem—and thus earning the rewards—is proportionate to its hashing power relative to the overall network.

A miner contributing 1% of the overall Hash Rate should earn 1% of the overall rewards, consisting of new Bitcoins created and the transaction fees.

The Hash Rate of the overall Bitcoin network recently exceeded 223 *quintillion* calculations per second, which is expressed in exahash per second (EH/s).



Let me put these numbers into perspective.

Few people know that a quadrillion comes after a trillion.

Even fewer know that a quintillion comes after a quadrillion.

That's partly because the human brain can't understand a number so large. It's also because there aren't many topics of conversation where these large numbers are relevant.

A trillion is an enormous, almost incomprehensible number.

A trillion seconds ago was about 30,000 BC.

It's common knowledge that the astronomical US government spending, deficit, and debt figures all reach into the trillions. But other than that, finding something that runs into the trillions is not something most people are familiar with.

What about a quadrillion?

A quadrillion seconds ago was about 32 million years ago.

It’s hard to think of anything so large that people measure it in a quadrillion (a thousand trillions). As far as I know, the only thing that reaches a quadrillion are some estimates of the total notional value of all derivatives in the world.

What about a quintillion?

A quintillion is one with 18 zeros behind it.

A quintillion seconds ago was about 32 billion years ago. For perspective, scientists believe the Big Bang, and thus the universe’s age, to be 13.8 billion years.

What topic of everyday conversation could possibly be so large that people measure it in quintillions?

I know of only one thing: the Bitcoin network’s Hash Rate of 223 quintillion calculations per second.

That’s an astonishing and mind-bending amount of computing power. It makes the Bitcoin network the world’s most powerful collection of processing power by orders of magnitude—and the most secure.

To even think of attacking Bitcoin, a potential attacker would need to obtain an improbable amount of electricity and computer hardware—over 51% of the network’s aggregate computing power (Hash Rate). And even then, they would still need to get over several daunting hurdles.

But let’s assume that happened. The most the attacker could do is double spend their transactions in some of the most recent blocks. They would not be able to create new Bitcoins or modify old transactions. This is what is known as a 51% Attack.

For practical purposes, a 51% Attack would be improbable because it would require compiling more computing power than any entity is capable of doing or conceivably could in the future.

According to some estimates, it would require an attacker to spend scores of billions on computer hardware—and that’s with the unrealistic assumption they could even source the equipment if they had the money—and tens of millions per day on electricity to even have a slight chance at tampering with Bitcoin’s recent transaction history.

But let’s say they did. The return on investment for the attacker would not be attractive. Even if the attack were successful, it would crash the value of Bitcoin. In short, it would be extremely expensive and challenging to execute with little or no monetary reward.

That’s how powerful economic incentives protect Bitcoin and make attacking it improbable and uneconomic.

Ultimately, anyone who wants to attack Bitcoin will realize that it will be more profitable to buy Bitcoin or mine it honestly than to try to attack it. In other words, if you can't beat them, join them.

Also, the cost to perform a 51% Attack is likely to grow significantly higher as the Difficult Adjustment increases the difficulty of solving the Proof of Work problems and thus the computing power and electricity required to attack the network.

Here's the bottom line. The amount of electricity required to run the Bitcoin network makes it the most secure computer network in the world.

It's all part of Bitcoin's ingenious economic incentives, which creates a virtuous cycle.

1. The higher the Hash Rate, the more difficult it is to attack Bitcoin and the more secure it becomes.

2. The more secure Bitcoin becomes, the more attractive it is as a reliable store of value.

3. The more attractive it is as a store of value, the more people will demand and hold it.

4. As more people hold and demand it, the higher the price goes.

5. The higher the price goes, the more people are incentivized to get into mining Bitcoin.

6. The more computing power dedicated to Bitcoin mining, the higher the Hash Rate and the more secure it becomes. Go back to step 1.

The Lightning Network Makes Bitcoin Easier to Use Than Visa

Every day there are over 2 billion consumer transactions around the world.

Visa, Mastercard, American Express, and other large companies process most of these payments.

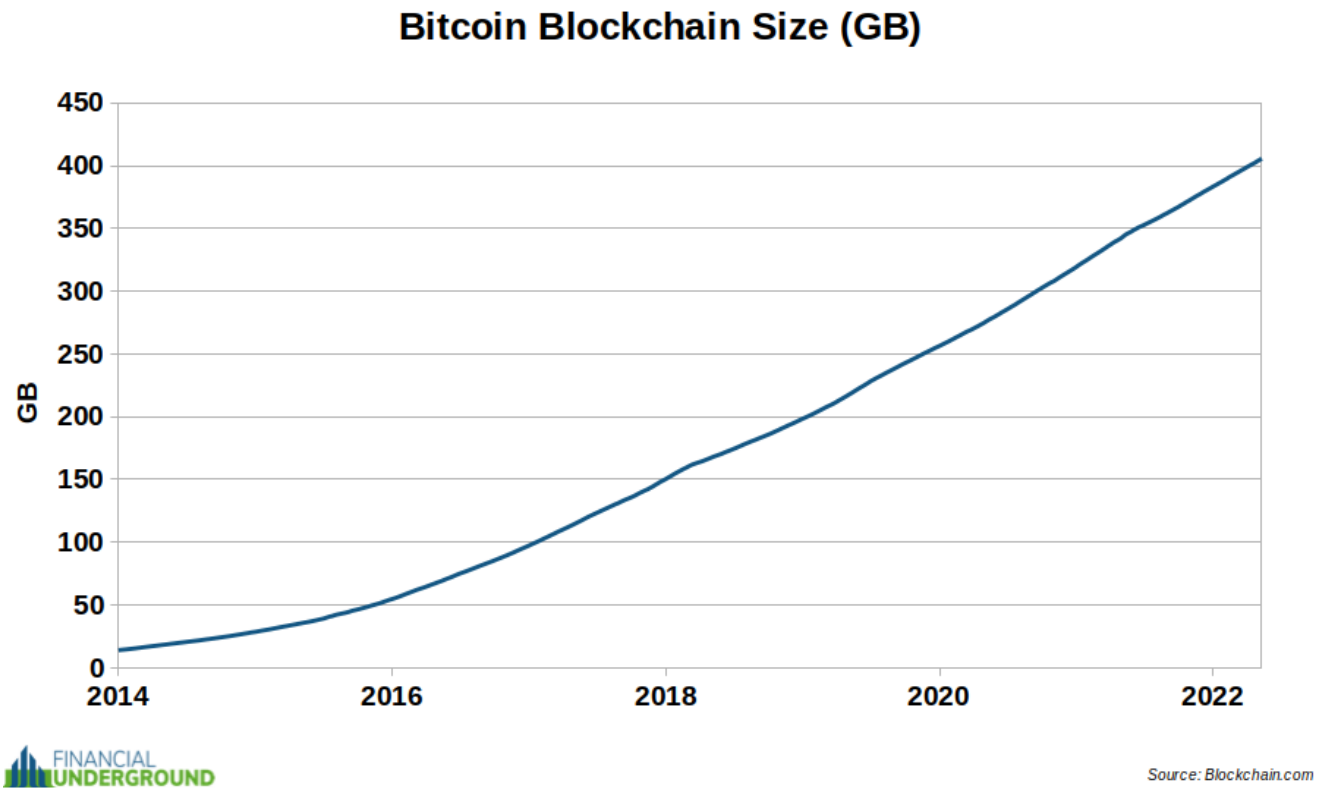
Bitcoin, on the other hand, does not have anywhere near the capacity to handle this kind of volume.

The Bitcoin protocol sets the maximum size of each new block at about 1 megabyte (MB).

That means there is a hard limit on the maximum number of transactions the Bitcoin network can process—about 375,000 transactions a day, or about 0.019% of all the world's consumer transactions.

That's why it was never possible to record every Starbucks or McDonald's transaction on the Bitcoin blockchain. It was also never desirable.

Today—after over 13 years of transaction history—the size of the Bitcoin blockchain has grown to about 405 gigabytes (GB). The small block size means that the Bitcoin blockchain grows slowly and is predictable. As a result, the average computer can easily handle running a full node now and in the future. That is crucial for Bitcoin to remain decentralized.



However, if Bitcoin needed to record every consumer transaction on its blockchain—or even a fraction of them—it would require an industrial-scale operation with expensive data centers. As a result, only large entities would be able to run full nodes. That means the average person would not be able to participate in enforcing the consensus parameters and the protocol. That would be the end of Bitcoin's decentralization because a few large entities would solely validate and enforce the protocol, which means they would be in charge.

In this scenario, Bitcoin might as well be another PayPal, Visa, or another centralized financial service where you need to ask for permission to do anything. Moreover, it would destroy the one thing that makes Bitcoin such a revolutionary innovation in money.

Remember, Bitcoin's primary value proposition as a global money is dependent on it being neutral, censorship-resistant, accessible to everyone, and controlled by nobody.

To have these properties, it's essential the average person can run a full node. That's why Bitcoin has a hard limit on the transactions it can handle each day. It needs to be this way so that the average laptop can easily handle running Bitcoin. That's what keeps Bitcoin genuinely decentralized and incorruptible, giving it its unique monetary properties.

Does that mean Bitcoin will never be able to scale and achieve widespread adoption? Absolutely not.

There's a working solution available to anyone today. It allows Bitcoin to scale to handle every transaction in the world—without compromising its decentralization and immutability. Moreover, it can process transactions instantly and at practically no cost.

Monetary Layers

When you use your credit card to buy a coffee at Starbucks, the money doesn't land in Starbucks' bank account when Visa approves the transaction.

Instead, a payment processor collects the money. It then aggregates a bunch of other transactions over a period. It then uses a commercial bank, which uses the Federal Reserve (the central bank of the US), to move the money from the payment processor's account to Starbucks' account for final settlement.

Aside from physical cash transactions, it's not practical for Starbucks to immediately obtain final settlement. The company doesn't have to clear with the Federal Reserve each cup of coffee it sells. Instead, it uses this layered approach with payment processors to facilitate everyday transactions.

All successful financial systems have used a layered approach to scale, including the one based on a gold standard, the current fiat currency system, and now Bitcoin.

Layer 1 – International Final Settlement

The key characteristic of Layer 1 financial transactions is finality. They represent the ability to perform irreversible transactions that can transcend borders.

In the current fiat currency system, Layer 1 involves the central bank clearing transactions for final settlement.

Under a gold standard, the central banks of two nations used to settle balances between themselves with physical gold. Once Country A delivered the physical gold to Country B, there was final settlement.

Transactions on the Bitcoin blockchain are comparable to these. They represent final international settlement and clearance.

Layer 1 transactions are typical for high-value transactions that need security and finality. However, they are inappropriate for most consumer transactions—it's unnecessary to use a wire transfer to pay for a cup of coffee—which instead can happen on Layer 2.

Layer 2 – Scaling and Convenience

Layer 2 transactions shouldn't be compared to Layer 1 transactions—they're totally different.

Layer 2 transactions involve systems built on top of Layer 1 that offer more convenience.

Using a credit card to pay for a cup of coffee is an example of a Layer 2 transaction. It involves a credit card company and a payment processor that enable convenient transactions on top of the Federal Reserve's clearance for final settlement.

Under a gold-based monetary system, exchanges of physical gold were Layer 1 transactions because they had final settlement. However, they were also inconvenient, especially for smaller purchases.

Transactions involving a gold-backed currency—which are more easily divisible and convenient for daily transactions—are examples of a Layer 2 solution under a gold-based monetary system.

The US dollar under the gold standard would be an example of a Layer 2 system.

As I mentioned earlier, not every transaction in the world will be put on the Bitcoin blockchain (Layer 1).

Consider that many cryptocurrency businesses—like exchanges—perform almost all transactions on their internal ledgers. They only use the Bitcoin blockchain for final settlement.

For example, if you would like to trade on an exchange, you'll typically deposit Bitcoin into your exchange account. That transaction will be recorded on the Bitcoin blockchain.

Once that deposit is complete, all other transactions you perform on the exchange will not be recorded on the Bitcoin blockchain. Instead, they'll be recorded on the exchange's internal ledger. You could then complete thousands of trades on the exchange, and none of them will go on the Bitcoin blockchain.

When you are finished trading on the exchange and would like to withdraw your Bitcoin to your wallet, that transaction will be recorded on the Bitcoin blockchain.

It's not just exchanges. Countless other Bitcoin businesses do the same thing. The idea here is that the Bitcoin blockchain is used for final settlement.

So, which Bitcoin transactions should be on Layer 1 and Layer 2?

Those are subjective decisions every individual must make. The competitive free market for the scarce resource of space on the Bitcoin blockchain will decide its most efficient use and, thus, which transactions should be on Layer 1 or Layer 2. In other words, whoever is willing

to pay the transaction fee to the miners can have their transactions inscribed onto the Bitcoin blockchain (Layer 1).

It's likely larger transactions that demand a high level of security will use the Bitcoin blockchain. Smaller consumer transactions will probably use more convenient Layer 2 solutions, just like they do now and did under the gold standard.

The idea is to keep Bitcoin's base layer secure and scale by building on top of it. It would make no sense to scale Bitcoin by compromising its Layer 1. That would be bad engineering.

Many Layer 2 solutions for Bitcoin will inevitably emerge. However, the Lightning Network is the most dominant one… and its adoption is about to go parabolic.

The Lightning Network

Numerous Bitcoin Layer 2 solutions are in development, but the Lightning Network is the most prominent and exciting. It's now ready for prime time.

The Lightning Network is an open, peer-to-peer network built on top of Bitcoin.

On the Lightning Network, people can perform an unlimited number of transactions without needing to add them to the Bitcoin blockchain. It's unnecessary to delegate custody of funds to a third party—you can always remain in control.

The Lightning Network can eventually handle every consumer transaction in the world—many millions per second.

Unlike Layer 1 transactions on the Bitcoin blockchain, which can take 10 minutes or longer to settle, the Lightning Network has nearly instantaneous speed and almost zero fees.

Unlike Layer 2 solutions under the gold standard and the fiat currency system, the Lightning Network is an open, permissionless network with zero counterparty risk.

It starts with two people opening a payment channel with each other by depositing Bitcoin and creating a smart contract.

(A smart contract is code that executes transactions automatically based on different conditions and inputs for a period of time. Various conditions can be applied to create complex spending rules with all sorts of financial applications.)

The two people can then transact with each other—and any other payment channels they are connected with—an unlimited amount of times. Those transactions are performed on the Lightning Network and will not be recorded on the Bitcoin blockchain.

At any point, either party can close a payment channel. The outstanding Bitcoin balance at that time will be returned to the two people. The transaction to close the payment channel will then be recorded on the Bitcoin blockchain.

In short, the only time Lightning Network transactions are recorded on the Bitcoin blockchain is when payment channels are opened or closed. Everything else occurs off-chain on the Lightning Network.
Think of it like keeping a running tab and then settling up on the Bitcoin blockchain when either party decides to.

Suppose you want to transact with someone but don't have a payment channel. It's possible to do so if the sender and receiver have enough connections in common to create a path to each other. If so, the Lightning Network will automatically find the shortest route and complete the payment without the need to open a payment channel.

It would look like the image below.

Person A wants to send Bitcoin to Person D, but they do not have a payment channel. They do have enough open payment channels with peers in common to create a path, though.

So, the Lightning Network will route the payment from Person A through Person B and Person C finally to Person D.

Source: Bitstamp

If this seems complicated, don't worry. This is just an explanation of how the Lightning Network works under the hood.

You can use the Lightning Network with a simple application on your phone. It does all of this in the background without the need for your input.

Here's the bottom line.

The Lightning Network makes Bitcoin a viable medium of exchange for everyday consumer transactions. It allows you to use the hardest, most inflation-resistant money mankind has known as easily as your Visa card.

Extreme Portability Helps Create a Safe Haven

If you were to send $1 billion worth of physical gold from New York to Beijing, complicated and expensive logistics would be required.

$1 billion worth of gold would weigh about 17,000 kilograms (or about 37,500 pounds). Transporting that much gold would likely involve multiple cargo flights and then armored trucks to transport it from the destination airport to the destination vault.

It would also require insurance, navigating regulations, paying import or export taxes, clearing customs, and thorough verification of the gold's purity, among other things.

It would also take a considerable amount of time, and it wouldn't happen overnight.

Transporting smaller amounts of gold is also problematic. For example, going through airport security with gold coins and bars is likely to generate unwanted attention.

These are some of the issues with gold's portability.

Bitcoin, on the other hand, is the most portable asset in the world. It is a digital bearer asset that can achieve final international settlement in 10 minutes for pennies.

You can send $1 billion worth of Bitcoin from New York to Beijing for less than $10 in fees, and it will arrive in 10 minutes. The transaction has no credit risk and no counterparty risk. You don't need to get anyone's permission or need to use—or trust—any third party whatsoever. And there's nothing anybody can do to block, freeze, reverse, or censor the transaction.

Going through airports and crossing borders with Bitcoin is also much more practical than other forms of wealth.

It's true that if you hold Bitcoin on your phone, laptop, or flash drive, it can be accessible to border agents if they search you and you reveal your password. However, those things are much less conspicuous than gold or stacks of cash.

Further, many popular Bitcoin wallets use a 12-word phrase as a way to recover your funds. If you can memorize the 12-word phrase, you can potentially store billions of dollars worth of value just in your head with nothing else.

When it comes to portability, Bitcoin isn't just slightly better. It's an upgrade orders of magnitude better than gold or fiat currency. It's an even more profound upgrade than when mankind moved from using horse carriages for travel to using Boeing 747 airliners. It's more like going from horse carriages to futuristic teleportation machines that can instantly beam you from one location to the next.

Bitcoin's portability is a big reason it has become a safe haven for ordinary people in crisis-stricken countries. They can easily use it to send and receive wealth. That might mean paying for goods and services when the local government currency becomes worthless or discreetly receiving a much-needed influx from relatives who have managed to get out.

When a crisis hits, the government can easily steal money from your bank account. It can also steal your purchasing power by inflating the currency. But it's next to impossible for it to steal Bitcoin or prevent people from using it because all anyone needs to use it is a cell phone and an internet connection.

That's why Bitcoin is popular in Argentina, Venezuela, Lebanon, Iran, Turkey, and other countries with high inflation or capital controls, which restrict money flowing into and out of a country. Capital controls have the effect of trapping people's money in rapidly depreciating currencies.

Whatever the particulars, Bitcoin allows anyone to bypass unsound banks, worthless currencies, and government confiscation schemes. That's because governments can't freeze, seize, or block the transactions.

Further, there is a tendency for people to be attracted to harder money over time. During financial crises or when government currency rapidly loses its value, the process is in fast motion. That's when people rush toward harder assets, and Bitcoin is set to become the world's hardest.

In short, this is how Bitcoin has become an essential escape hatch. It's a safe haven available to anyone anywhere in the world.

Nation State Adoption

In April 2022, the Central African Republic (CAR) became the second country—after El Salvador—to adopt Bitcoin as legal currency alongside the Central African CFA franc.

El Salvador and CAR are among the poorest countries in the world. But they now have a unique opportunity. These two countries have gained a tremendous head start in the race to accumulate the hardest money ever known by being first and second, respectively—and nobody will want to be last.

Bitcoin allows anyone with a cell phone to become their own sovereign bank that can send and receive payments from anywhere in the world. It gives ordinary people access to a form of money that nobody can confiscate or debase with inflation. Bitcoin could be transformative for many people in these countries.

It also illustrates an established trend of countries adopting Bitcoin as legal tender.

Both El Salvador and CAR do not have their own currencies. Instead, El Salvador uses the US dollar, and CAR uses the Central African CFA franc, a regional currency that Bangui does not control. That means neither government has the option to extract wealth from their citizens by printing money, an insidious practice known as seigniorage. In other words, the governments of El Salvador and CAR had nothing to lose by adopting Bitcoin as a legal currency.

That is a crucial factor in determining which country could be next to embrace Bitcoin as money. The most likely candidates will be those who don't benefit from seigniorage, like El Salvador and CAR. That could be because they've adopted the US dollar or another foreign currency. Or they have already inflated all the value out of the local currency.

Ecuador and Panama are top contenders, as they both use the US dollar as the official currency. In addition, Panama recently voted to remove all capital gains tax on Bitcoin, which is a big step towards making it legal tender.

Other countries in a similar situation include Belize, Liberia, Zimbabwe, and numerous other countries in the Caribbean, the Pacific, and Africa.

Venezuela, Turkey, Argentina, Pakistan, Lebanon, and Nigeria have lost any benefit from seigniorage due to rampant inflation. They have already squeezed as much value as they could through money printing. As a result, they might be more receptive to Bitcoin.

Bitcoin is also attractive to countries under US sanctions, such as Iran, Cuba, and Russia.

Countries dependent on remittances, like India, Mexico, Guatemala, and the Philippines, could be attracted to the savings that Bitcoin offers over Western Union. This was a significant consideration in El Salvador adopting Bitcoin.

Further, politicians in Paraguay, Tanzania, and Tonga have made statements about introducing legislation to make Bitcoin legal money in their countries.

In short, there's a whole slew of countries ripe for adopting Bitcoin.

Now that El Salvador and CAR have broken the ice, I don't think we'll have to wait long to find out who will be next.

Risks

Government Bans

> "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 it violently out of the hands of government, all we can do is by some sly roundabout way introduce something that they can't stop." – F.A. Hayek

Bitcoin has no central authority and single point of failure. Instead, it runs on a decentralized, voluntary, and growing network scattered around the world on over 15,000 computers—many of them are cleverly hidden—in nearly 100 countries.

With Bitcoin, there's no central location for a SWAT team to raid. There's no CEO to arrest. Governments can do nothing but play an endless game of whack-a-mole across the globe.

Even if the US and Russia engaged in all-out nuclear war, destroying most of the Northern Hemisphere, Bitcoin wouldn't miss a beat in the Southern Hemisphere.

No government can kill Bitcoin on its own. To even have a chance to stop Bitcoin, every government in the world would have to successfully coordinate simultaneously to shut down the entire Internet everywhere and then keep it off.

Even in that improbable scenario, the Bitcoin network can be communicated over radio signals, and small portable solar panels can power the computers running the network. Further, a network of satellites is constantly beaming the Bitcoin network down to Earth.

In short, all aspects of Bitcoin are genuinely decentralized and robust. Barring an inescapable, global return to the Stone Age, Bitcoin appears unstoppable.

The cat is out of the bag. Bitcoin is bigger than any government.

If the government can't shut it down, won't they ban it?

Algeria, Bangladesh, Bolivia, China, Ecuador, Egypt, India, Iran, Kyrgyzstan, Morocco, Nepal, Nigeria, Saudi Arabia, Thailand, Turkey, and others have tried to ban Bitcoin. However, they all failed miserably as adoption in those countries kept rising.

Could the US government try to outlaw Bitcoin?

It is certainly possible that US President could issue an Executive Order banning Bitcoin. Remember, Executive Order 6102 outlawed gold ownership for American citizens from 1933 until it was repealed in 1974.

However, I think that outcome is unlikely for several reasons.

First, Bitcoin is simply computer code. US courts have ruled computer code is equivalent to speech protected by the 1st Amendment of the US Constitution. On the other hand, the Constitution is not a reliable protector of rights, as the Covid hysteria, the War on Terror, and the War on Drugs have all proven. So, I wouldn't exclusively count on the US Constitution to protect Bitcoin. Nonetheless, the previous precedents ruling code as equivalent to speech complicates any attempts to ban it.

Second, the US government has defined Bitcoin as a commodity and property. The IRS, the SEC, the CFTC, and other agencies have given Bitcoin clear regulatory and tax frameworks. That's helped many large US businesses get into Bitcoin, including many large financial institutions. Reversing these guidelines would generate significant push-back and be challenging—but not impossible—to implement.

Third, banning Bitcoin is impractical. Government bans may restrict something, but they cannot make something valuable and desired by many people just go away by passing a law.

Consider governments in Argentina, Venezuela, and numerous other countries have laws restricting their citizens from accessing US dollars. However, these laws have little effect on their citizens' desire and ability to use them. Instead, these actions create a thriving black market or, more accurately, a free market.

Similarly, look at how successful governments have been in prohibiting cannabis over the decades. Despite their best efforts, cannabis has always been readily available in most big cities. Trying to enforce a prohibition on something digital and borderless like Bitcoin is entirely impractical. Bitcoin would be far more challenging for governments to ban than US dollars or a plant.

Even if it were practical to ban Bitcoin, it's already too late.

There's a critical mass of Bitcoin advocates among large corporations, politicians, and regular people. They bring all of their lawyers, lobbyist, and political connections to potentially advocate for Bitcoin. That's a lot of political firepower. And their numbers are only growing. According to a report from Gemini—the crypto exchange the Winklevoss twins founded—over 21 million adults in the US own cryptocurrencies.

Supporting a ban on Bitcoin means going against tens of millions of Americans—no small number are wealthy, powerful, and well-connected.

In short, outlawing Bitcoin will not help anyone win an election. I think Bitcoin has already reached escape velocity. In other words, it's too politically popular to outlaw, and every day it gets stronger as adoption grows.

Here's the bottom line.

The US government doesn't like Bitcoin. Even though banning it would be politically unpopular and unconstitutional, it still might consider the move if it could do so effectively—but it can't. So, I think the US government will have to adapt to that reality. As I've shown above, it already has been by giving Bitcoin a clear regulatory framework for businesses and investors.

Central Bank Digital Currencies (CBDC)

Despite all the hype, CBDCs are nothing but the same fiat money system with a new label. It's old wine in new bottles.

CBDCs will make it even easier for the government to inflate the currency and impose deeply negative interest rates, which are really just a euphemism for a tax on saving money.

If governments can implement CBDCs, they'll have a new powerful tool to confiscate and redistribute wealth. It would be foolish to expect them not to use it that way. So, we can expect much more inflation if CBDCs arrive.

However, it's doubtful CBDCs can save otherwise fundamentally unsound currencies—as I believe all fiat currencies are.

For example, it's implausible that a CBDC would have positively affected the Venezuelan bolivar or the Lebanese lira. In fact, CBDCs would have made it even easier for the Venezuelan and Lebanese governments to create more currency units.

There are a lot of bad things that come with CBDCs. But there's a silver lining. CBDCs are going to introduce and familiarize people with using digital currencies. It's then only then a matter of time before they discover Bitcoin.

CBDCs and Bitcoin share some characteristics. For example, they are both digital and facilitate fast payments from a mobile phone. But that is where the similarities end.

The reality is that CBDCs and Bitcoin are entirely different in the most fundamental ways.

You need the government's permission and blessing to use a CBDC, whereas Bitcoin is permissionless.

Governments can (and will) create as many CBDC currency units as they want. With Bitcoin, there can never be more than 21 million, and there is nothing anyone can do to inflate the supply more than the predetermined amount in the protocol.

CBDCs are centralized. Bitcoin is decentralized.

Governments can censor transactions and freeze, sanction, and confiscate CBDC units whenever they want. Bitcoin is censorship-resistant. No country's sanctions or laws can affect the protocol.

There is no privacy with CBDCs. However, with Bitcoin, if you take specific steps, it is possible to maintain reasonable privacy.

CBDCs are government money that are easy to produce and give politicians a terrifying amount of control over people's lives. On the other hand, Bitcoin is non-state hard money that helps liberate individuals from government control.

In short, CBDCs are a pathetic attempt to compete with Bitcoin. CBDCs make an inferior form of money even worse, but at the same time, it's an excellent Trojan Horse for Bitcoin.

It doesn't take much imagination to see that once governments inevitably inflate their CBDC units, censors transactions, freeze people's accounts, and confiscates funds, it will push people to look for better digital alternatives, first and foremost Bitcoin.

That's how, contrary to conventional wisdom, CBDCs could be an enormous catalyst for Bitcoin adoption.

Breaking Bitcoin's Cryptography

Unbreakable cryptography helps secure Bitcoin.

But how secure is its cryptography?

First, it's important to note that cryptography—or the practice of encoding information—is as old as civilization itself.

Many people think encryption popped up in the digital age. However, cryptography has been around for thousands of years. After all, people have always had sensitive information to conceal.

One of the oldest known cryptography uses dates back to around 600 BC when the ancient Spartans would pass encrypted messages on thin papyrus sheets. The recipient could wrap the papyrus around a scytale (a cylinder of varying dimensions) to decrypt the message.

The words written on the papyrus itself were gibberish. But you could “decrypt” the code if you had the right scytale. This is how the Spartans sent and received secret military plans.

Today, computers allow for radically more sophisticated cryptography.

At this point, no one—including the US government or any other government—can break properly used encryption. That’s why the US government uses it to secure its digital information. The only difference now is that this powerful technology is readily available to the individual when previously, it was not.

NSA whistleblower Edward Snowden—who knows a thing or two about encryption—puts it like this:

> “Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on.”

For all practical purposes, Bitcoin’s cryptography is not a risk today. If Bitcoin’s cryptography were at risk of being broken, it would also be an existential problem for every bank, brokerage, central bank, email provider, and every aspect of modern digital life.

I would put this risk in the same category as an alien invasion—something theoretically possible but not relevant to investment decisions today.

But let’s suppose a hypothetical problem of quantum computing—or some new technology—posing a threat to Bitcoin’s cryptography. A hypothetical solution exists. It would be possible to upgrade Bitcoin’s cryptography to make it resistant to quantum computing or whatever new technology threatens it.

Hard Forks and Changing Bitcoin

If Bitcoin is unchangeable, how is it possible for it to upgrade? That’s an excellent question.

The fact that no single—or group of—individuals, corporations, or governments can change the Bitcoin protocol is why it is unique. Moreover, it’s why Bitcoin is desirable as a neutral form of money and has a real chance of becoming the world’s dominant currency.

Although it is highly improbable, the Bitcoin protocol can theoretically be changed.

It’s similar to saying that nanotechnology could make gold as common as the aluminum foil in your kitchen drawer. Theoretically, that could happen, but it is so improbable right now that it makes it irrelevant to our investment decisions.

Understanding how difficult it would be to change the Bitcoin protocol is crucial to understanding the credibility of its monetary properties.

Bitcoin's protocol indeed is all but impossible to change. That's just a function of its technical specifications and unique economic incentives that keep a globally decentralized system functioning—and growing exponentially—with nobody in charge.

Satoshi Nakamoto once correctly said:

> "The nature of Bitcoin is such that once version 0.1 was released, the core design was set in stone for the rest of its lifetime."

This doesn't mean that it's impossible to make changes that don't affect the protocol or improve Bitcoin.

To understand how Bitcoin upgrades—and what makes it different from every other cryptocurrency—it's essential to grasp the basics.

There are generally two ways a cryptocurrency updates itself, a **hard fork** and a **soft fork**.

A hard fork is a drastic change to the protocol and is not backward compatible, which means previous software versions are not compatible after the hard fork.

For example, suppose the developers of XYZ cryptocurrency implemented a hard fork on July 15. After that date, anyone who didn't update their software to contain the new changes will not be able to access their funds or participate in the network.

A hard fork means someone is tinkering with the core aspects of the protocol. It means someone is in control and can change the rules.

On the other hand, a soft fork is an upgrade that is backward compatible, which means the previous versions of the software are compatible and will still work after the soft fork. That's because soft forks don't contain drastic changes that would render older versions unusable.

Aside from Bitcoin, when a cryptocurrency's development team announces a hard fork, everyone usually goes along and implements their suggested changes.

But sometimes, hard forks can be contentious. For example, certain people may disagree with the proposed changes and refuse to implement them. When that happens, the cryptocurrency splits into two totally different ones.

A contentious hard fork is not favorable because it splits the community and resources. It can make everyone weaker. A contentious hard fork is a more considerable risk if the cryptocurrency predominantly relies on hard forks to update—which almost all do except for Bitcoin.

On the other hand, soft forks can help avoid the disastrous splits from a contentious hard fork since they are backward compatible. That means users who choose not to go along with the soft fork will still have access to their funds and can interact with the network.

As a practical matter, anyone can hard fork any cryptocurrency whenever they want. All you have to do is take the open-source code available to anyone and make your desired tweaks to the protocol. But that doesn't mean anyone will follow your lead or value your new cryptocurrency.

For example, I can easily make a hard fork of Bitcoin that changes the supply from 21 million to 22 million and call it "Bitcoin 2.0" or BTC2. But that doesn't mean I can inherit the economic and technical properties of the original Bitcoin or benefit from its established network effects. People are unlikely to assign any value to BTC2.

In short, anyone can create a cryptocurrency in minutes. That's the easy part. Making one that nobody controls is the hard part.

If someone wanted to propose a change to the Bitcoin protocol—which would require a hard fork—they would need to get the agreement of a majority of the over 15,000 full nodes which enforce the protocol. Otherwise, they would just create an increasingly worthless knock-off.

That makes it improbable that any individual, corporation, or government—or groups of them—could get together to enforce their will on the network by coercing the full nodes.

The Blocksize Wars, which culminated in 2017, was an excellent example. That's when an overwhelming majority of the Bitcoin miners (primarily based in China)—and other prominent insiders and large companies—tried to get together and change Bitcoin's protocol, which would require a hard fork.

Even though they represented most of the miners, some of the most powerful insiders, the most prominent influencers, and large corporations, the decentralized network of full nodes successfully rejected their attempted hostile takeover and did not follow their hard fork. Instead of forcing a destructive change in Bitcoin—as they desired to—they just created an increasingly worthless knock-off known as Bitcoin Cash. Recently, the market cap of Bitcoin Cash was less than 1% of the real Bitcoin's and is trending towards 0%.

The effort to change Bitcoin's protocol during the Blocksize Wars was an abysmal and embarrassing failure.

After the 2017 Blocksize Wars, it became apparent that nobody controls Bitcoin, not even the vast majority of its most powerful insiders. It became clear Bitcoin was genuinely neutral and apolitical. This is only the case because of the network of full nodes.

For more on this incredible and important story, I suggest you check out the book *The Blocksize War: The battle over who controls Bitcoin's protocol rules*.

So, yes, it is theoretically possible for a hard fork to change Bitcoin. But it would require the consensus of an overwhelming majority of the network participants, including over 15,000—and growing—full nodes across the world.

If someone tried to change Bitcoin, they wouldn't succeed at anything except creating their own worthless crypto with no following.

Getting the consensus of the full nodes to accept a hard fork would be very difficult and impossible in almost all situations.

Imagine someone wanted to change the policy of the National Rifle Association (NRA). Suppose they said to the NRA members, "Hey, let's get rid of real guns, and everybody can have Nerf guns and water pistols instead. Would you guys agree to implement a policy that enshrines this?"

NRA members might embrace such a dramatic transformation—nothing is impossible. But it would be so improbable that it's irrelevant.

Getting the consensus of the full nodes to change the Bitcoin protocol with a hard fork—to say, alter the fixed supply of 21 million—is even less probable than NRA members agreeing to give up their guns.

It's important to emphasize that most of the Bitcoin community—the people running the full nodes—is highly resistant to change. They have a deep conviction in Bitcoin's potential as hard money and wouldn't want to undermine that by agreeing to tinker with a protocol proven to work. They also are likely to hold Bitcoin and wouldn't want to undermine its value. In other words, Bitcoin is resistant to change from a technical and economic standpoint and social and cultural ones.

The point is that a hard fork is not impossible in Bitcoin. Still, it is implausible to happen unless perhaps there was a genuinely existential situation where the entire network agreed on it simultaneously.

Bitcoin developers cannot simply propose a hard fork—which would immediately generate contention—and expect the full nodes to accept it blindly. This resistance to change gives Bitcoin's monetary properties credibility. It's what sets Bitcoin apart from every other cryptocurrency.

Here's the bottom line. The sovereignty in Bitcoin is not with the developers, the miners, insiders, influencers, large holders, or any individual or group. It's with the globally decentralized network of full nodes, which anyone can operate.

For every other cryptocurrency, the opposite is true. The sovereignty is with the developers and insiders. It is trivial for them to perform a hard fork and change the protocol. That's why most cryptos—aside from Bitcoin—perform hard forks as part of their routine upgrade

process. The developers simply tell everyone they need to upgrade, and there is effectively no choice as everyone goes along with it.

If a hard fork is easy to perform, that means a group of people can change the rules—such as the supply—whenever they want. They may choose not to for now, but they can.

That's why Bitcoin is different. The ability to enforce—and potentially change—the protocol is decentralized and not under the control of anyone.

It is not an easy task to perform a hard fork and thus change the rules in Bitcoin. It's basically impossible at this point. That is what gives Bitcoin genuine scarcity and credible monetary properties. If Bitcoin didn't have these attributes, it would be worthless.

For all practical purposes, Bitcoin's protocol is unchangeable. But that doesn't mean Bitcoin cannot upgrade. It just has to do so in a way that doesn't alter the protocol and is backward compatible, so users who do not upgrade are not left behind. This is why Bitcoin's upgrades occur with a soft fork.

It's a crucially important distinction that most people—even those familiar with cryptocurrencies—don't understand. It's how Bitcoin can upgrade while retaining its decentralization and immutability.

Misleading Narratives About Bitcoin's Energy Consumption

It's a fact that the Bitcoin network consumes an enormous—and growing—amount of electricity. This has triggered hysterical articles in the mainstream media about how Bitcoin wastes energy and dubious claims that it harms the environment.

The risk is that this misleading narrative could lead to government and corporations imposing restrictions that would hinder adoption.

However, we can easily debunk this misleading narrative.

First, let's start with the basic facts and the correct framing.

According to Our World in Data, the world consumes about 160,000 terawatt-hours (TWh) of energy from all sources each year.

According to the University of Cambridge, the Bitcoin network currently consumes around 127 TWh of electricity each year.

That means Bitcoin represents less than one-tenth of one percent or 0.08% of the world's total energy consumption. With that in mind, Bitcoin's energy consumption is not as big as the critics make it out to be.

Further, the energy Bitcoin consumes is legitimate and worthwhile. Bitcoin's energy consumption represents a free market of voluntary buyers and sellers of electricity.

As I discussed earlier, Bitcoin's energy consumption is a feature, not a bug. It represents the security of the network.

Stone Ridge Holdings is an asset manager that holds Bitcoin as part of its cash reserve strategy. In a letter to shareholders, they specifically addressed Bitcoin's energy consumption. I thought they were spot-on:

> "Bitcoin is a better technology for performing central banking than the current government monopolies on central banking. In the same way that cars consume far more energy than the bikes and horses they replaced, and electric lights replaced candles, and central heating replaced chimneys, and computers replaced typewriters, Bitcoin's better monetary system consumes far more energy than the current central banking system. Throughout history, energy use has grown whenever free people making free choices have decided for themselves that the price of the extra energy for the new technology they wanted was worth it. Today, every day, 24/7, Bitcoiners around the world make the decision that the price of Bitcoin's energy use is worth it because Bitcoin is better technology for money."

The truth is that Bitcoin represents a revolution in energy. Here's why.

Bitcoin mining is a cut-throat business. The most crucial factor influencing a Bitcoin miner's profitability is electricity costs. Some estimates put electricity costs at over 90% of a miner's operating costs. Therefore, only miners with reliable access to the cheapest electricity in the world—generally under $0.03 per kilowatt-hour (kWh)—can mine Bitcoin profitably. Everyone else will eventually go bankrupt as the mining machines' costs will exceed their revenue. For perspective, the average cost of electricity in the US is around $0.13 per kWh.

The reality is that Bitcoin miners are really in the energy arbitrage business. Advancements in satellite internet connections mean they can set up their operations anywhere on Earth.

Bitcoin miners seek out places where energy is overproduced with no buyers and provide a bid regardless of location. Then, they take this energy and convert it into Bitcoin, a hard money that people accept worldwide. In other words, Bitcoin mining has become the cheapest and easiest way to export energy.

That means that Bitcoin miners are the "energy buyer of last resort." They're a guaranteed buyer of cheap energy that nobody else wants to buy. Profitable energy production doesn't need to take place near population centers. There is no such thing as "stranded energy" anymore.

Never before in human history has energy production been profitable regardless of location. But, thanks to Bitcoin mining, now it is. That has world-changing implications.

If there is an inaccessible source of cheap energy that can't be economically transported—say, an isolated river or waterfall as a source of hydroelectric power—Bitcoin miners could be there to provide a bid to monetize the project.

Remember, Bitcoin miners need access to the cheapest energy on Earth to be competitive. That's why many of them are turning to renewable hydroelectric power.

Hydroelectric power generates electricity using flowing water, typically with water behind a dam that drives a turbine. While hydroelectric power is immobile and expensive to transport, it provides a cheap electricity source to those nearby.

The problem is that many sources of hydroelectric power are isolated from energy consumers. That means many hydroelectric power sources create a significant amount of excess, cheap electricity whether people use it or not. That's excellent news for energy-hungry Bitcoin miners.

It is easy to debunk misleading narratives about Bitcoin's energy use with this critical context in mind. Nevertheless, these narratives remain prevalent.

That's why Bitcoin mining companies and other industry players formed the Bitcoin Mining Council, which aims to educate and provide data and context to policymakers, the media, and anyone else. For example, the Bitcoin Mining Council estimates that 58% of Bitcoin mining utilizes sustainable sources of electricity, whereas that number for the overall grid in the US is only 31%.

These misleading narratives remain a risk insofar as they cause politicians or companies to create policies that would hinder Bitcoin adoption. But that risk is mitigated by the factors mentioned earlier.

Privacy and Taint

Perhaps the biggest drawback to Bitcoin is that every transaction ever made is known to all. Anyone can go online to a website with the details of the public Bitcoin blockchain to analyze and view the transaction history.

The information on Bitcoin's blockchain doesn't explicitly show your name, address, and other personal information. However, it does contain Bitcoin addresses and transaction IDs that can look something like this:

bc1qqzwmc4u2cajs27cnx3spr2r2227hca0ac38269

9be967b54cdd16ec3935b4cd2b4bffc7f10b55f2b851ce655103bc3cd846d70e

Suppose it were to become known that a particular Bitcoin address was associated with you. In that case, outsiders could track your balance and every transaction you make, which is incredibly sensitive financial information. Click the above Bitcoin address and transaction ID to examine them yourself.

If you buy Bitcoin off of a regulated exchange like Coinbase, and you have given them your ID, it is a certainty that they will have this information and pass it along to governments. They could also pass it on to other parties, or hackers could access it and use it to blackmail you.

Buying Bitcoin from a regulated exchange is not the only way to get Bitcoin. For example, you can obtain Bitcoin in a peer-to-peer transaction or mine it yourself without giving away personal information. But that's not how most people obtain it.

Aside from the privacy concerns, it is possible that specific Bitcoins could become "tainted" through transactions that governments don't like. For example, suppose you received a Bitcoin with a transaction history linking it to someone in North Korea, Iran, or another sanctioned entity. In that case, it might cause you complications.

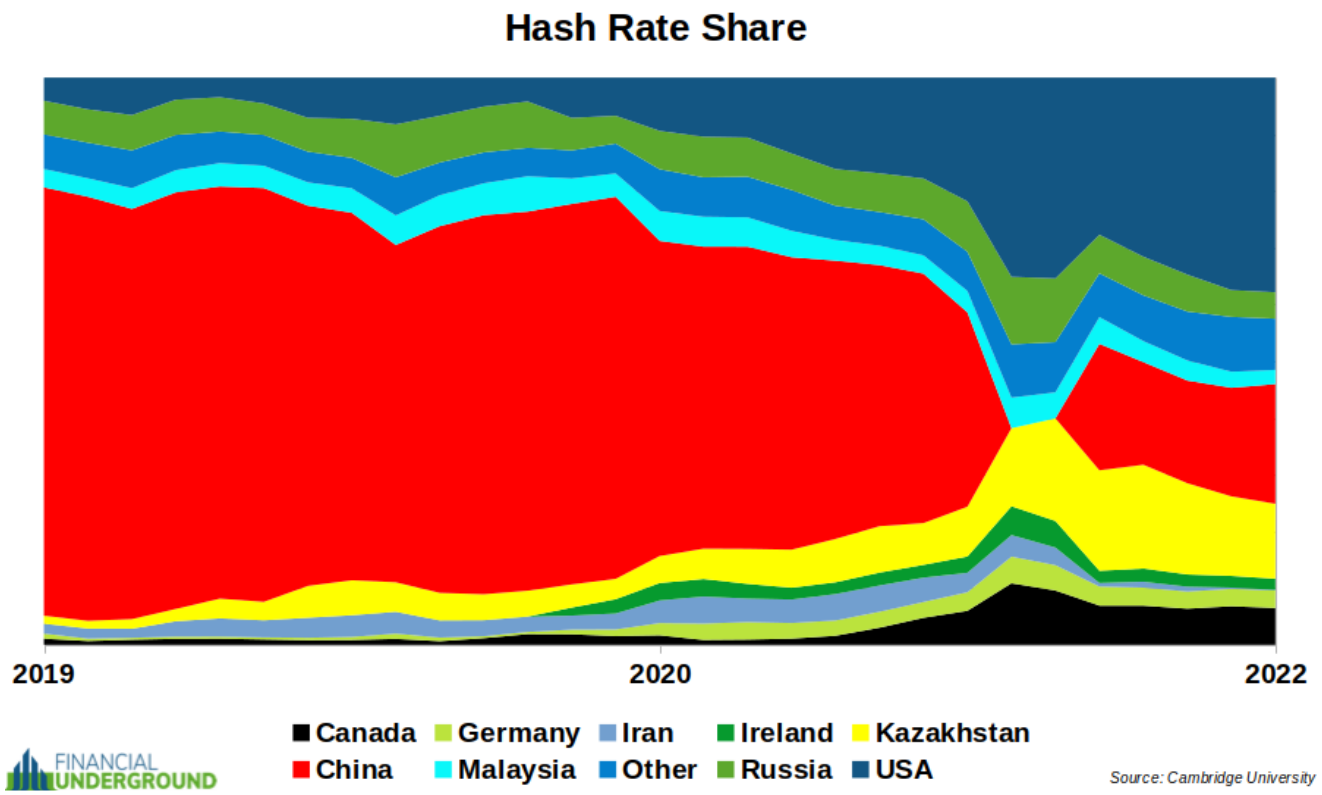
Thankfully, there are innovations in Bitcoin that help break the transaction history that are available today. However, they are for more advanced users, and they are not foolproof.

I expect developments that will significantly increase Bitcoin's fungibility and privacy for all users in the next couple of years. But the fact remains that this is an evident weakness for Bitcoin today.

51% Attack and Falling Hash Rate

While a 51% Attack is currently unlikely in the extreme, there is a risk it could become more feasible if Bitcoin's Hash Rate were to fall significantly.

It's also important that the Hash Rate is geographically dispersed. Below is a chart that estimates the countries in which Bitcoin's computing power is located.



We can see that China previously held a dominant position, but now the Hash Rate is more diversified.

It's also worth noting that just because a particular country is responsible for a certain percentage of the Hash Rate does not mean all miners within that country are controlled by a single entity within that country.

Nonetheless, a falling Hash Rate and miner concentration represent potential risks to the Bitcoin network. But for now, those risks are mitigated.

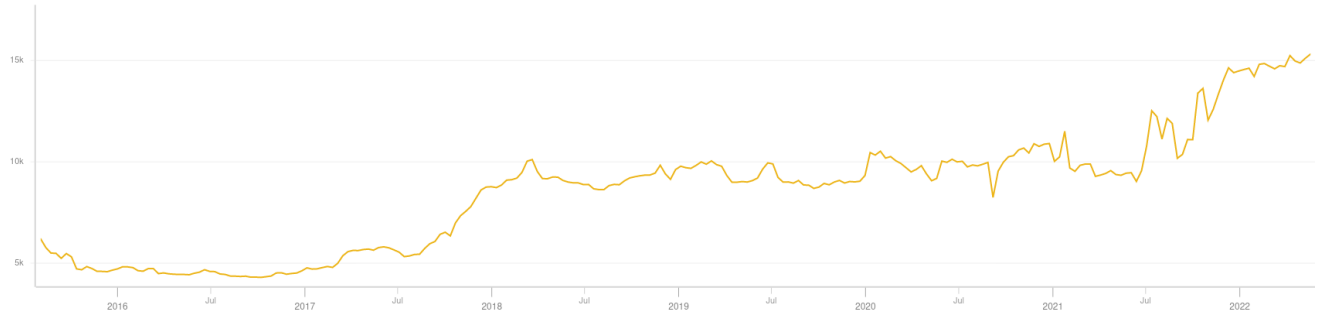
Falling Full Nodes

As discussed early, full nodes are crucial to ensuring Bitcoin remains decentralized.

If the number of full nodes was to drop significantly, it would represent a risk to Bitcoin. Similarly, anything that makes it more difficult for the average person to run one would be a risk.

As we can see in the chart below, the number of full nodes is over 15,000 and on an upward trajectory.

Bitcoin Full Nodes



Source: Coin.Dance

All or Nothing and Dubious Claims of a "Better Bitcoin"

Bitcoin is either useful as money, or it is worthless. That's because Bitcoin is purely a monetary good with no industrial or other non-monetary uses.

Further, the competition to be the world's dominant monetary network is essentially winner-take-all. Anything else would amount to an inefficient barter system, which is why monetary networks tend to converge on one thing as a dominant money.

The current status quo for Bitcoin seems untenable. Over the long-term, Bitcoin will either grow to become the dominant form of money or end up at $0 as a superior money beats it out.

Today, there are over 20,000 altcoins—cryptocurrencies other than Bitcoin.

So, what about the risk of a so-called "better Bitcoin?"

At this point, I am not worried about it.

Remember, anyone can make a crypto token in minutes. That's the easy part. Making one that nobody controls is the hard part.

Simply put, no other cryptocurrency comes even close to challenging Bitcoin's immutability, decentralization, hardness, liquidity, economic incentives, network effects, and most importantly, the credibility of its apolitical monetary policy.

It's crucial to remember two simple facts about altcoins.

First, altcoins are decentralized in name only (DINO). It is trivial for a small group of developers and insiders to change the supply and rules. That's why altcoins are in no way scarce or "hard to produce," which disqualifies them as candidates for good money.

Second, altcoins are not equity and do not represent any ownership stake or claim on any asset whatsoever.

But suppose altcoins did represent an ownership stake or a claim on an asset. They would then undoubtedly be “securities,” which means their developers must register with the government. (I think the SEC should have been abolished yesterday, but I also think it’s stupid to flaunt them).

Many people are confused about altcoins. However, once you understand those two basic facts, it’s easy to see why altcoins are akin to frequent flyer miles and arcade tokens.

In short, Bitcoin and altcoins are two entirely different things.

But suppose an altcoin came along that was a genuine competitor to Bitcoin. To disrupt Bitcoin’s established dominance as a monetary network, it would have to be not just a little bit better, but orders of magnitude better. According to renowned author Jeff Booth, a new competitor to an established network must be at least 10x better to convince enough people to leave the existing one and join the new network.

There have been dubious claims of a “better Bitcoin” for years, usually from people who simply don’t understand Bitcoin or disreputable altcoin promoters. I am not inclined to believe such claims until there is solid evidence that something could potentially have much better monetary properties than Bitcoin. So far, nothing has come close.

Governments Embracing Gold

Perhaps the most significant risk to Bitcoin would be if governments were to embrace gold as money. That would make government currencies a much more worthy monetary competitor. However, that is unlikely to happen unless the current fiat monetary system collapses and governments have no other alternative, which is certainly a plausible scenario in the years ahead.

Even if that were to occur, Bitcoin is still better than gold in two key monetary attributes, hardness and portability.

Valuation

The Bitcoin phenomenon is the birthing of a new free-market asset that became a significant global money in less than a decade.

Bitcoin has gone from having no market value when it was launched in 2009… to being used to purchase two pizzas in 2010, the first commercial exchange… to today generating over $35 billion in daily transaction volume around the world.

Many thousands of merchants accept Bitcoin as payment, including Overstock.com, Expedia, Microsoft, and Starbucks. That number is rapidly growing.

If it were a government currency, Bitcoin would be the 29th-largest currency by the market cap of its monetary base, just ahead of the South African rand. In other words, Bitcoin is already bigger than most national currencies.

Large corporations and nation states are starting to hold Bitcoin as a reserve asset in their treasuries. In addition, two countries have adopted Bitcoin as legal tender, and many more are likely on the way.

This is what the process of a new asset becoming money looks like, and it's just getting started.

To value Bitcoin and understand where it could be headed, we must consider what Bitcoin is and what it is competing with.

Bitcoin has a crystal clear use case. It's a hard money monetary system accessible to anybody and controlled by nobody. It works in the real world, and it probably solves mankind's biggest problem, which is storing and exchanging value reliably.

It's my contention that Bitcoin has superior monetary attributes compared to alternative monetary goods and is undergoing a process of monetization. I like to think of Bitcoin as hard money with an attached call option on its further monetization.

Remember, the monetization of new global monetary good is genuinely unlike anything anyone alive has ever seen before.

Gold has a 2,500-year history as money. You can take gold to any country in the world, and most will instantly recognize it. Bitcoin doesn't have this established history and recognition. It's only been around since 2009. But it's actually an opportunity for Bitcoin when you think of it.

It took gold centuries to achieve monetization. Bitcoin has a good chance of undergoing monetization in a much shorter period—and it's already well on its way. With Bitcoin, it's as if you discovered gold before most of the world understood that gold was useful as money—something to store and exchange value.

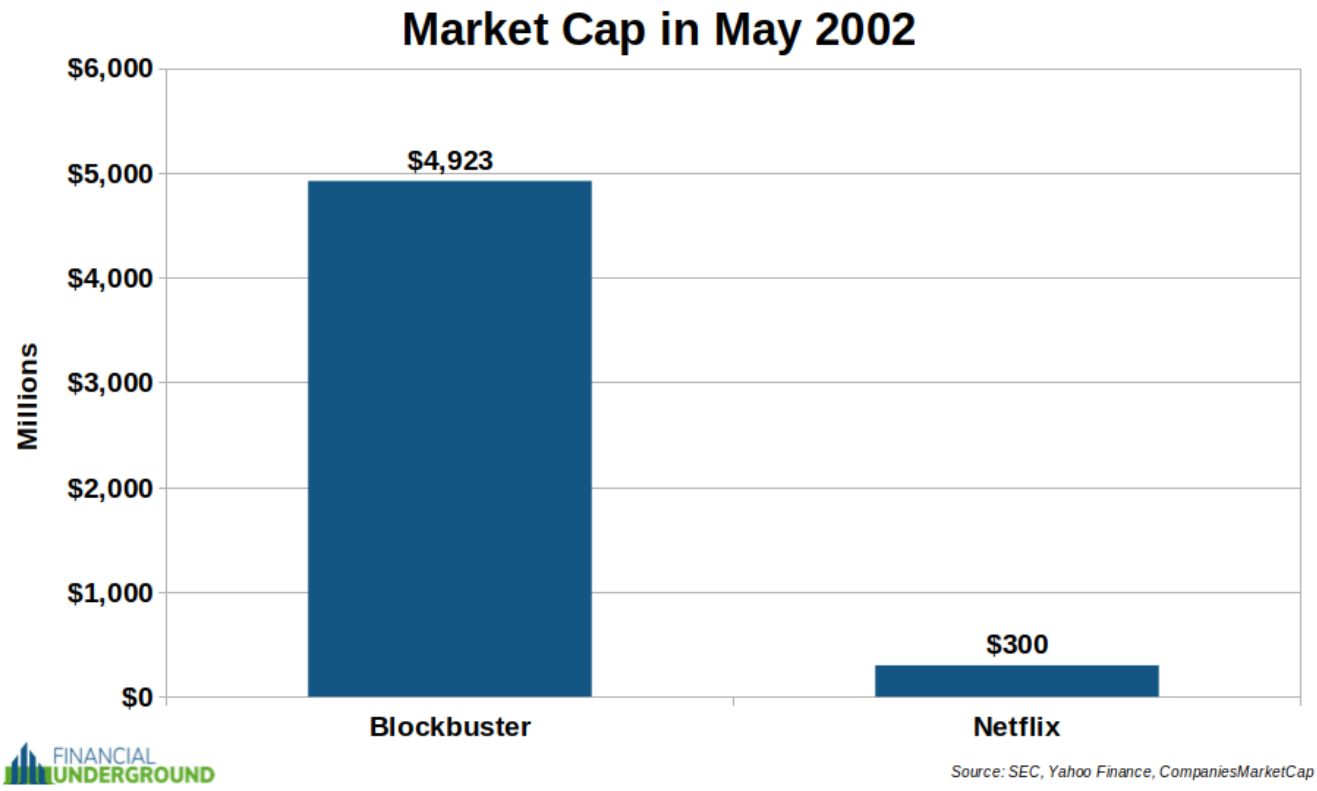
What we have with Bitcoin is an entirely new asset that millions—potentially billions—of people are adopting as money because of its superior monetary properties, primarily its total resistance to inflation and portability.

How big is the opportunity?

One analogy I like to make is that of Netflix and Blockbuster.

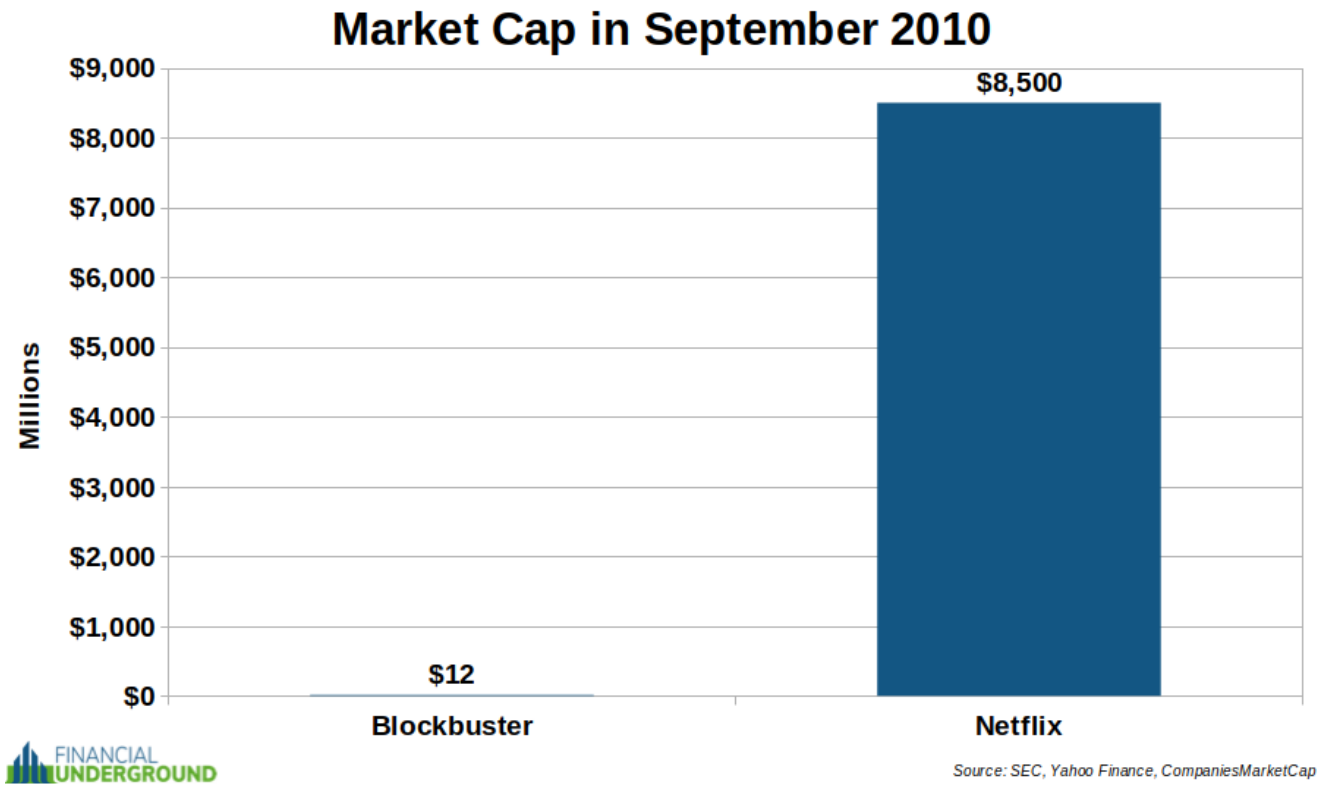
When Netflix went public in May of 2002, Blockbuster was the dominant player in the video rental industry.

Netflix's market cap was barely 6% of Blockbuster's.



A little over eight years later and Netflix didn't just absorb Blockbuster's market cap, it nearly doubled it as it disrupted the video rental market to become the new industry dominator.

Blockbuster filed for bankruptcy in September of 2010.



Netflix didn't just stop with Blockbuster.

It gobbled up the rest of the existing video rental industry and expanded it.

By late 2021, Netflix's market cap skyrocketed to a peak of over $305 billion, over 3,448%—or more than 35x its value in late 2010 after it had vanquished Blockbuster.

That's around a stunning 101,566% peak increase—or more than 1,016x—from its IPO.

That's enough to turn every $1,000 invested into over $1 million.

Now, that is with the unrealistic assumption that someone could buy the Netflix IPO, hold it for nearly 20 years, and then sell at the top. And past performance is not an indication of future results for any investment.

However, it does illustrate what can happen when a new force not only disrupts an industry but goes on to dominate it. Even a small position can have explosive potential.

The key is understanding a fundamental disruption before most others do, investing early, and having small enough position sizes to ride the megatrend without worrying about volatility whipsawing you out at the worst possible time.

I think an analogy can be made with Bitcoin.

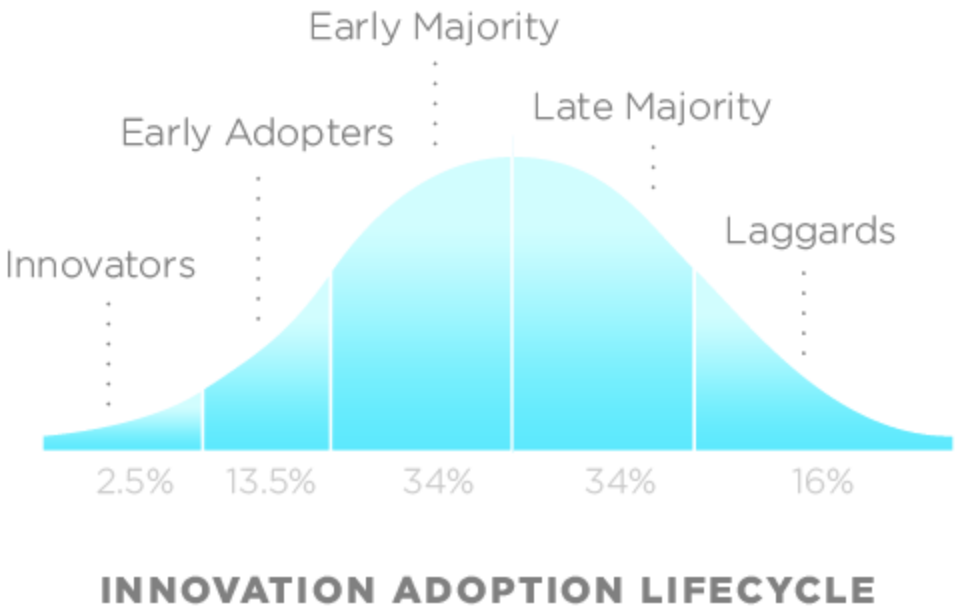
However, it could be even more profound—by orders of magnitude.

We're not talking about rendering the neighborhood video rental store obsolete.

We're talking about disrupting money itself as Bitcoin potentially renders all other inferior forms of money obsolete.

Bitcoin's total addressable market (TAM) is anyone who uses money, potentially 8 billion people.

Yet, *The Wall Street Journal* estimates only 114 million people worldwide own Bitcoin or about 1.4% of humanity. With that in mind, Bitcoin is still in the earliest phase (Innovators) of the adoption curve, comparable to where global internet adoption was in 1996.



INNOVATION ADOPTION LIFECYCLE

Remember, there can never be more than 21 million Bitcoin. So there would not be enough for every millionaire to own a whole Bitcoin. Also, recall that each Bitcoin can be divided into 100,000,000 units called satoshis (or sats).

Considering a TAM of 8 billion people and a fixed supply of 21 million, if Bitcoin were equally divided, there would only be 0.002625 BTC per person—or 262,500 sats.

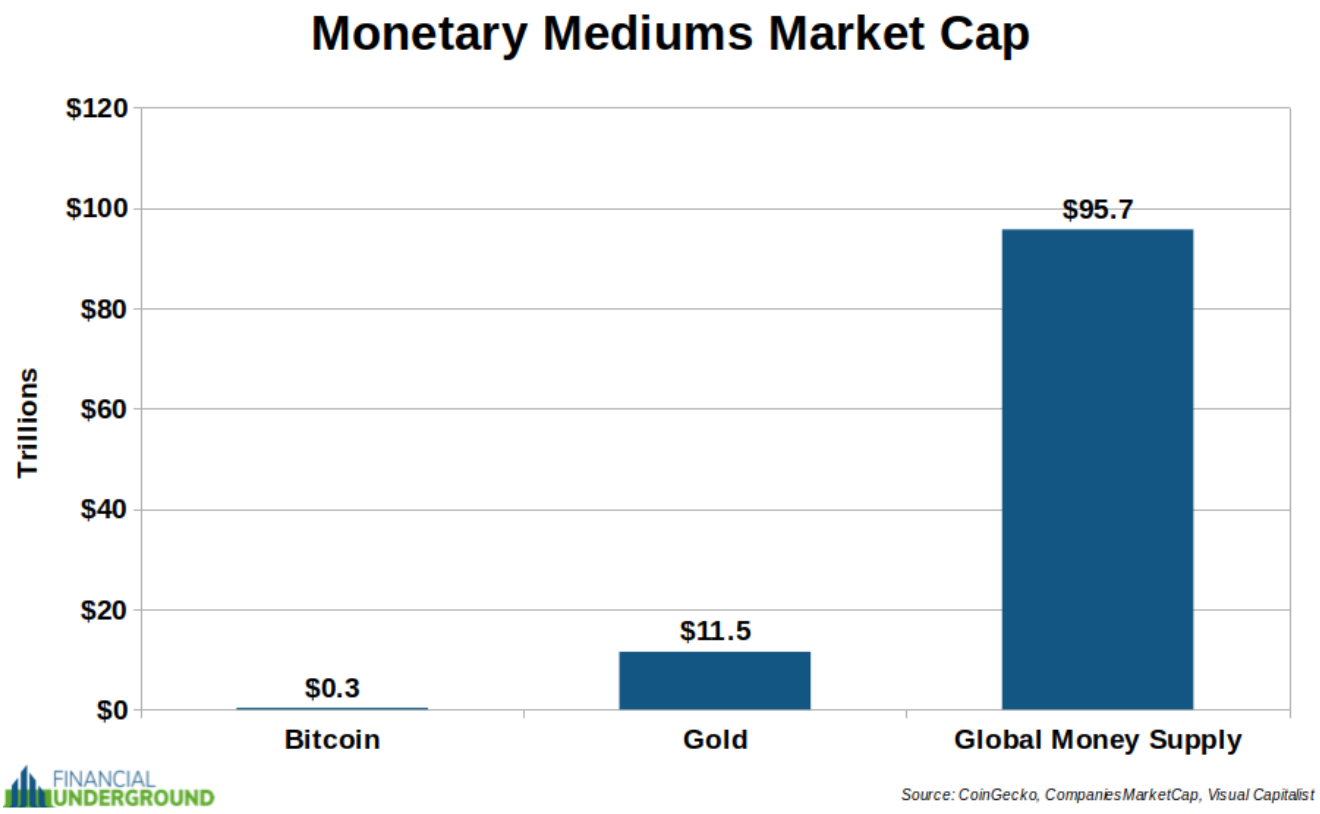
Today, Bitcoin only has around 114 million users. Imagine the draw of Bitcoin's scarcity and the power of its monetary network as its users double and reach 500 million people, a billion people, and more.

Capital is attracted to hard assets, and Bitcoin will become the world's hardest in 2024—and will become even harder. The economic incentives that attract people to harder money are impossible to resist. It's more powerful than any individual, corporation, or government.

Think of Bitcoin's increasing hardness like a black hole sucking in capital from competing monetary goods and other assets. The bigger the Bitcoin monetary network gets, the more powerful its gravitational pull becomes. I think this process will continue and accelerate exponentially in the years ahead.

Some proponents believe the endgame for Bitcoin is to eventually emerge as the world's dominant form of money—a process called "hyperbitcoinization"—or what I like to call The Bitcoin Supremacy.
It's a global, voluntary transition from inferior money to a superior one.

With that Big Picture view in mind, I think it's clear we are still in the early days of Bitcoin. Bitcoin's market cap is barely a blip in terms of global monetary assets, as you can see in the following chart.



If Bitcoin is going to become a more dominant global money in the years ahead, its market cap must grow substantially.

If Bitcoin's market cap rises to that of gold's, the price of a single Bitcoin would be worth $547,619 in today's dollars.

If The Bitcoin Supremacy happens, and Bitcoin's absorbs all the value in the fiat currency monetary network, a single Bitcoin would be worth over $4.5 million in today's dollars. Each satoshi would be worth about $0.05 in today's dollars. That means Bitcoin can absorb the monetary base of all fiat currencies quite easily.

Further, many people, particularly in Third World countries, use real estate above and beyond what they need for housing. They use it to store and exchange value—a monetary use. That's because real estate is a better vehicle for preserving their savings than their government currencies, which are continuously inflating away. In other words, fiat currency has led to the monetization of real estate—and other assets—that wouldn't necessarily be monetized under hard money.

In addition to absorbing the market cap of gold and all fiat currencies, Bitcoin could absorb the monetary demand embedded in real estate and other assets that fiat money has unnecessarily monetized.

That means Bitcoin's potential upside from here is truly mind bending. It could easily go up many multiples from today's prices.

Although The Bitcoin Supremacy has developed at warp speed since 2009, it's essential to keep in mind that it's a long-term megatrend that could take many years to play out fully. Therefore, investors should have a time horizon of at least one halving cycle (four years) and ideally two (eight years) or more.

Perfect Financial Collapse Insurance

As told in the movie *The Big Short*, a group of hedge fund managers who saw the housing crash coming used Credit Default Swaps (CDS) to make a fortune.

These exotic financial instruments conveyed information crucial to seeing the 2008 financial crisis in advance. That knowledge allowed astute speculators to get positioned for massive profits as the crisis unfolded.

In the coming crisis—which has already started—I expect CDS will again play a key role in telegraphing important information shrewd speculators can use to their advantage.

A CDS is a contract between two parties. Think of it like an insurance policy against a borrower—typically a large company or a government—defaulting. One party underwrites the insurance policy, and another buys it. If the borrower defaults, the CDS issuer pays out the CDS buyer.

CDS trade in the open market and reflect investor expectations of the default probability of a particular borrower. The more likely the underlying entity is to default, the more expensive the insurance (CDS) will cost.

The seller of the CDS collects a premium and bets that the underlying entity will not default. Conversely, the buyer of the CDS is betting that the underlying entity will default or become more distressed so that he can sell the insurance policy in the market for a higher price than he paid it for.

For example, in 2006, a CDS to insure $10 million of Lehman Brothers debt against default cost around $9,000. That CDS contract exploded in value to over $6 million in September 2008 as Lehman went bankrupt.

In short, that is how CDS work. They can deliver enormous profits, and their prices provide crucial market information.

Greg Foss is a 35-year veteran of the credit markets. He is an accomplished risk analyst with some of Canada's most prominent financial institutions. Greg is also a passionate Bitcoiner and has said:

> "Bitcoin is the best asymmetric trade I have ever seen."

Greg has devised a simple—yet clever—way to value Bitcoin using the CDS market. It reveals critical information about Bitcoin and the entire fiat currency monetary system.

The CDS market—and the information it conveyed—was crucial for making fortunes during the last crisis, and I suspect it will be for the next crisis as well. Likewise, I believe the information in Greg's valuation model is key to getting positioned for big profits in the months ahead.

Bitcoin Is a Cheap CDS on the Entire Fiat System

Greg Foss thinks Bitcoin should be considered default insurance on the entire global fiat currency system—like a CDS on the US dollar, Canadian dollar, British pound, euro, yen, yuan, and all the rest of the government currencies.

Why?

Because Bitcoin is an alternative and superior form of money compared to government confetti.

Think of Bitcoin's superior monetary properties—namely its total resistance to inflation—like a black hole sucking in capital and monetary energy from other forms of money. The bigger the Bitcoin monetary network gets, the more powerful its gravitational pull becomes. I think this process will continue and accelerate exponentially in the years ahead.

In short, as the risk to fiat currency continues to rise, so does Bitcoin's value proposition. As a result, it will benefit similar to a CDS as the fiat currency system defaults.

Legendary value investor Bill Miller has called Bitcoin "an insurance policy against financial disaster." He's correct.

Consider the example of Lebanon, which recently experienced hyperinflation, bank failures, and capital controls as its fiat system collapsed.

For over 20 years, the Lebanese government pegged the local currency, the lira, to the US dollar at a rate of 1,500.

That all began to change in the middle of October 2019, and many Lebanese would soon find themselves financially ruined.

As the banking system became insolvent, Lebanon imposed capital controls, preventing most people from sending their funds abroad.

The lira's artificial peg to the dollar became untenable, and a thriving underground market developed and revealed the real exchange rate. Recently, this free market is trading the lira at around 39,750 to the dollar.

In other words, the Lebanese lira has lost over 96% of its value since October 2019.

Now, let's look at how Bitcoin could have served as insurance against a collapse in the fiat system in Lebanon.

Imagine there was an astute Lebanese individual, let's call him Marwan, who saw the writing on the wall and knew trouble was imminent.

After all, similar banking and currency crises had occurred previously in Argentina, Greece, Cyprus, and other countries in recent years. So it didn't take much imagination to understand that Lebanese bank deposits and the lira could soon lose most or all of their value.

Suppose Marwan had the equivalent of $100,000 USD in his lira savings account at a Lebanese bank in October 2019 and decided to convert half of it—the equivalent of $50,000—into Bitcoin when the price was about $8,333 per BTC.

Marwan would then have around 6 Bitcoins that he could use to send and bring with him anywhere in the world without depending on the whims or permissions of any bank, central bank, government, or third party.

Fast forward to today.

The other $50,000 Marwan left in his Lebanese lira bank account is now worth about $2,000.

Marwan's 6 Bitcoins are now worth around $100,730 today, more than double his $50,000 investment and more than his $100,000 in total savings at the start of the crisis.

Had he not converted half of his money into Bitcoin, his $100,000 in total savings would have collapsed 96% to just $4,000. Instead, he has $102,730 thanks to Bitcoin.

That's how Bitcoin could have served as insurance against the collapse of the fiat system in Lebanon.

Undoubtedly, Bitcoin saved many people in Lebanon—I know several of them.

But Bitcoin is not just like default insurance against the fiat system in Lebanon. It's like a CDS on the entire global fiat currency system. As this system falters in many countries, the value of such insurance could become mind-bending.

However, Bitcoin is even better than a CDS.

That's because Bitcoin has no counterparty risk, and it never expires.

Typically, a CDS expires after five years and has significant counterparty risk.

For example, consider the lucrative CDS on Lehman Brothers debt I discussed earlier. These insurance contracts became incredibly valuable as Lehman Brothers became more distressed and sank into bankruptcy.

Owning a CDS on Lehman Brothers in 2008 was a winning trade… except for one big problem: counterparty risk.

The sellers of the CDS contracts on Lehman Brothers found themselves in big trouble as they had to pay them out as Lehman went bust. As a result, many, including Bear Stearns, became distressed, which brought into question whether they could fulfill the contracts.

Counterparty risk is a big problem with the fiat currency financial system in general and with CDS in particular.

Even if you get the trade right, your counterparty could default, which means you'd pay the insurance premium for the CDS but not get the payout.

That's why Bitcoin is even better than a CDS.

It provides insurance against the failure of the entire worldwide fiat currency system, has no counterparty risk, and doesn't expire.

Bitcoin is about as close to perfect financial collapse insurance as you can get.

Valuing Bitcoin Using the CDS Market

Greg Foss says that if Bitcoin is like a CDS on the entire fiat currency system, then we can use the data in the CDS market to create a fair price valuation for Bitcoin.

Here is how Greg's valuation model works in five simple steps…

Step 1: Calculate Total Obligations Needing To Be Insured

The US federal government has over $31 trillion in debt and about $173 trillion in unfunded liabilities.

That's around $204 trillion in total obligations that default insurance would need to insure.

Step 2: Obtain US Five-Year CDS Costs

In the open market, US five-year CDS are trading at 29.98 basis points, which means it costs $29,980 to insure $10 million worth of US federal government obligations. It's essential to remember that this number is constantly changing depending on market conditions.

Step 3: Estimate 20-Year CDS Cost

The obligations of the US federal government do not occur only over five years. Greg thinks a 20-year period is more appropriate.

Since there is no such thing as a 20-year CDS, the best Greg can do is make a calculation to estimate what the price would be using the market data of the five-year CDS. He does this by dividing the cost of the five-year CDS by five and then multiplying it by 20.

Therefore, the estimated cost of a 20-year CDS for the US is 119.92 basis points—or $119,200—to insure $10 million worth of US federal government obligations.

Step 4: Calculate the Cost To Insure All US Federal Obligations

There is $204 trillion worth of US federal government obligations.

Therefore the estimated cost to insure all US federal government obligations against default is $204 trillion x 119.92 basis points or about $2.45 trillion.

Step 5: Implied Bitcoin Valuation

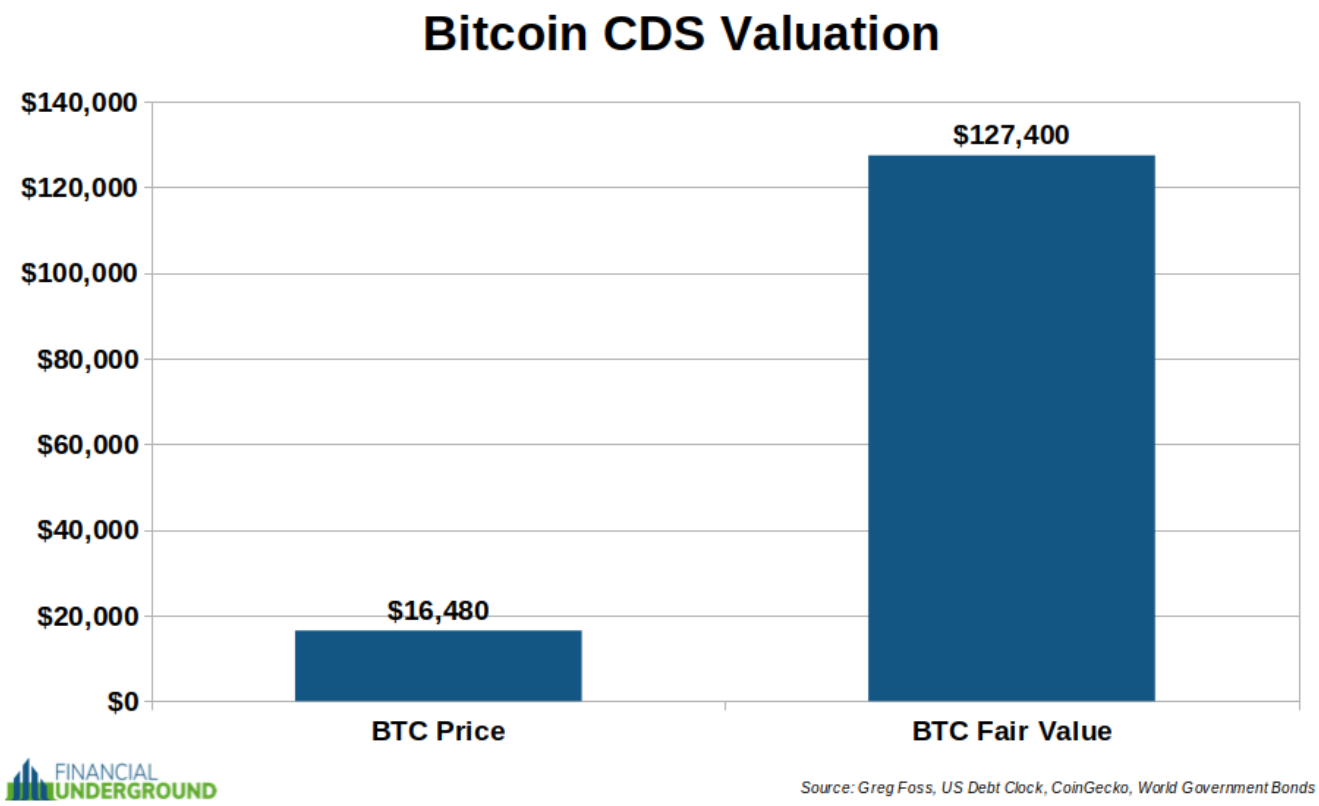
If Bitcoin is like a CDS on the global fiat currency system, the fair value of all outstanding Bitcoin should be at least $2.45 trillion or $127,400 per BTC at the current supply.

And that is a conservative estimate because we are just calculating the value of default insurance on the US, not the rest of the fiat currencies.

Bitcoin's current market cap is around $317 billion, and the price is about $16,480 per BTC.

That means, at current prices, we are getting default insurance on the US at an 87% discount while at the same time getting protection against the failure of all the rest of the fiat currencies for free.

In other words, with Bitcoin, we are getting perfect financial collapse insurance at an 87% discount to fair value at current prices.



That doesn't mean Bitcoin can't go higher than $127,400. That is only the model's fair value valuation at today's CDS prices.

As the fiat currency system in the US and other countries becomes more distressed, it's obvious the cost to insure their obligations will increase. That means higher CDS prices and a higher fair value for Bitcoin.

With all the chaos going on right now—which will likely only get worse—it seems prudent to buy Bitcoin to obtain some financial disaster insurance, especially since it is so cheap.

As the fiat currency system falters in the months ahead, buying Bitcoin now could be an even better trade than buying a counterparty-free CDS on Lehman Brothers in 2006.

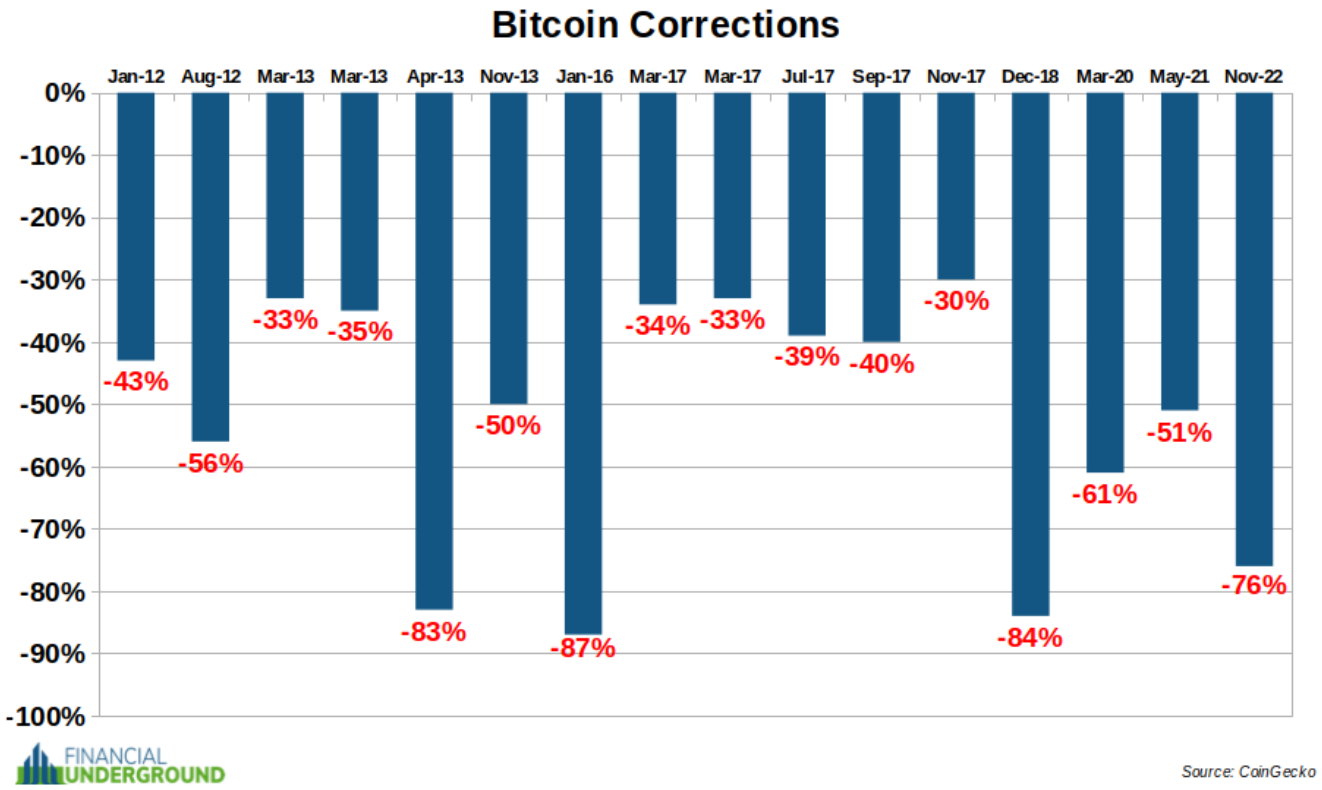
Volatility

Monetization doesn't happen overnight, and it's inherently a volatile process.

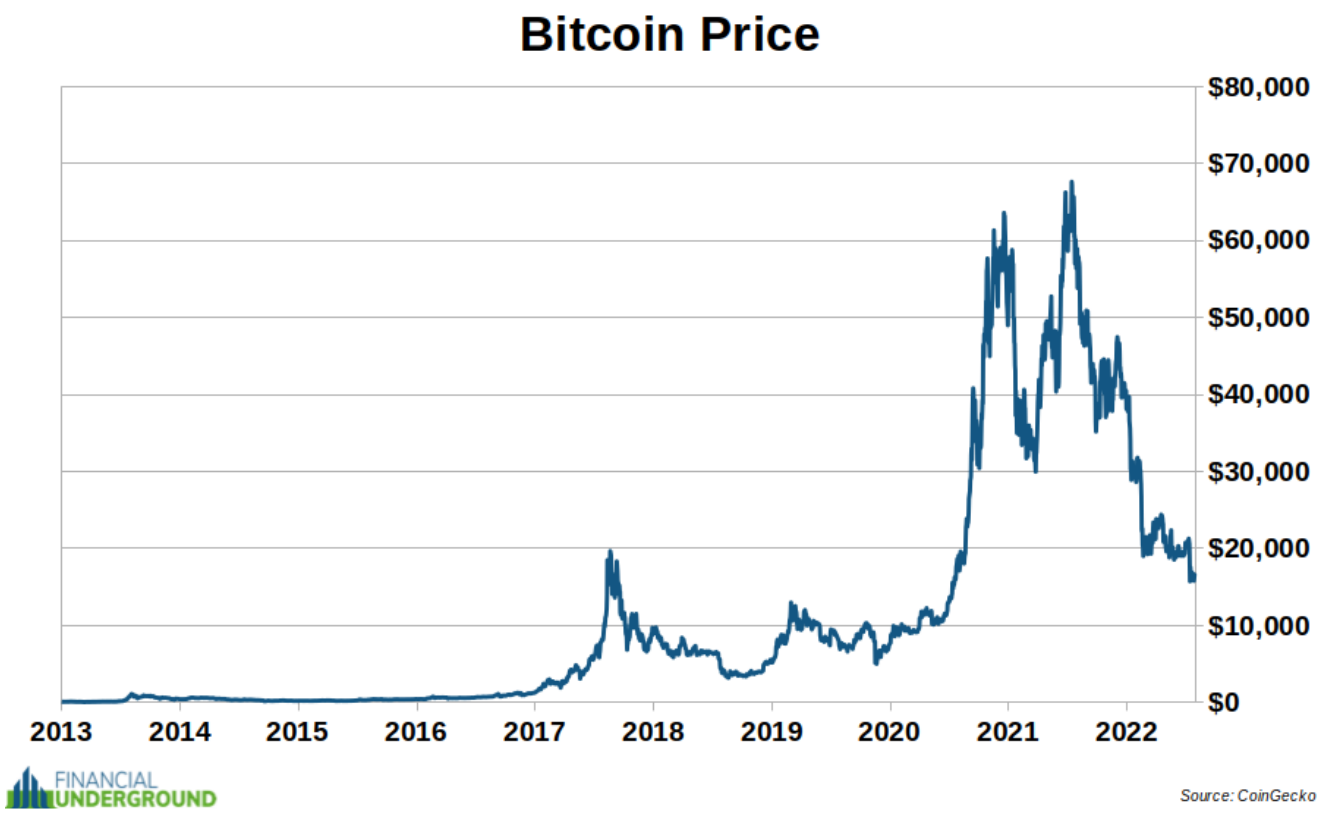
Something doesn't go from having no value to being significant global money without volatility. For example, Bitcoin went from having no value in 2009 to over $67,000 in 2021.

It is not uncommon for Bitcoin to have significant corrections of 50% or more, which has happened eight times. Further, there have been three occasions where Bitcoin has declined 80% or more.

Here is a chart showing Bitcoin's biggest corrections over the years to put its volatility into perspective.

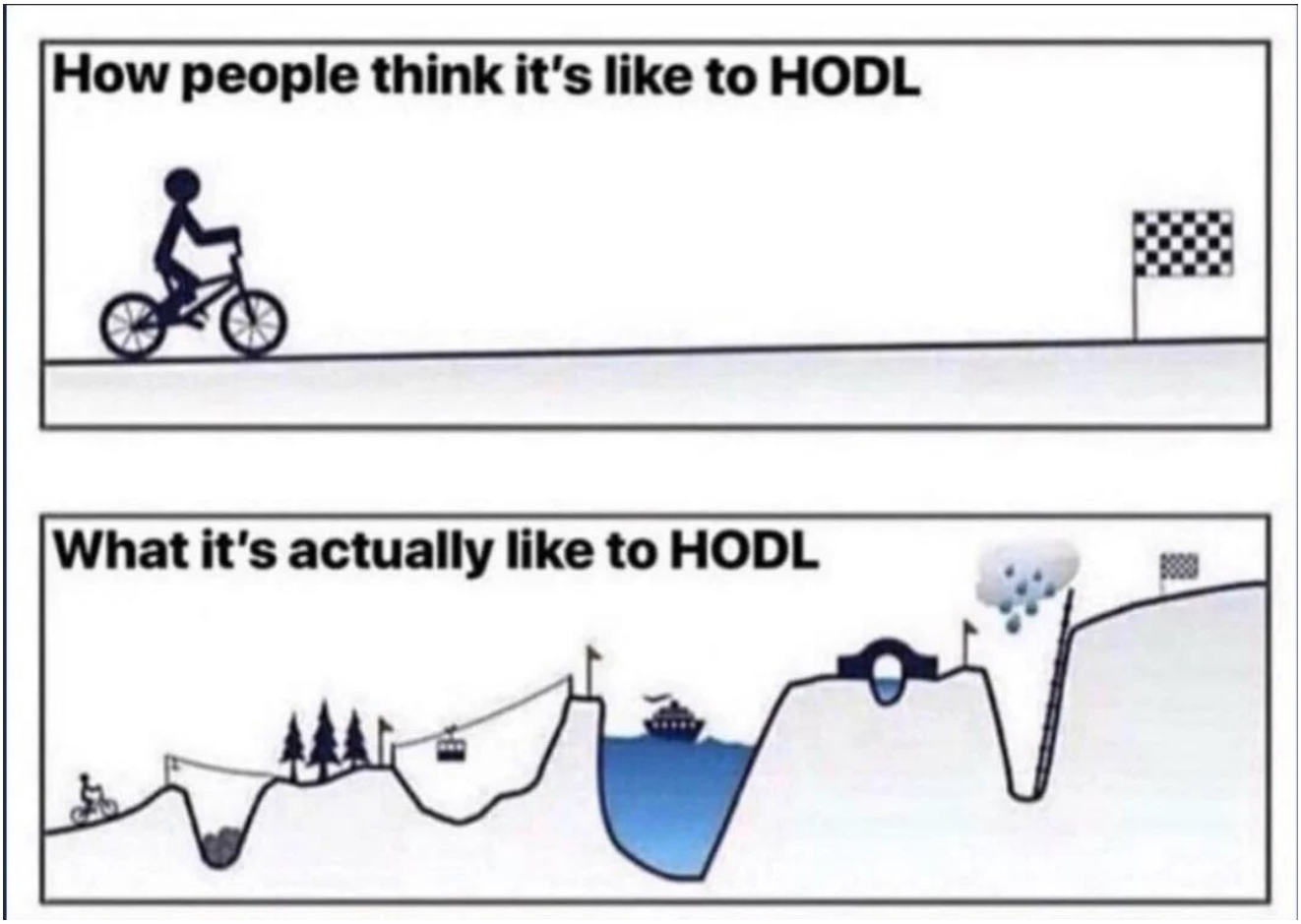


If you zoom out and look at the Big Picture, Bitcoin's volatility has mainly been to the upside over the long term.



As adoption grows and Bitcoin becomes more established as money, the volatility should smooth out—but probably at a much higher price. That's why you want to buy Bitcoin—and the best Bitcoin mining stocks—before the rest of the world figures out its superior monetary properties.

It will be a wild ride—like a violent roller coaster—but I believe it will reward patient investors. Stomaching Bitcoin's volatility is the price we must pay to earn outsized gains as it undergoes the process of monetization.



There are a couple of ways to help tame Bitcoin's volatility.

First, instead of buying your desired amount of Bitcoin in one large transaction, use dollar cost averaging (DCA) to spread it out over time. For example, suppose you'd like to invest $10,000 into Bitcoin. Instead of buying $10,000 at once, make a purchase of around $192 each week for a year.

DCA significantly reduces the risk of buying too much at the top of a cycle and not buying at the bottom. That's how DCA can turn Bitcoin's volatility in your favor.

Swan Bitcoin offers a convenient platform that automates dollar cost average purchases for you—including withdrawals to your own wallet, which is essential to eliminate counterparty risk. I've personally used it and found their service useful.

More details can be found at the link below, including a helpful calculator that displays how a DCA strategy performed in the past and a $10 bonus of free Bitcoin for signing up with this link.

https://www.swanbitcoin.com/nickg/

Second, plan on holding for at least four years—through one halving cycle. There has rarely been a period in which the Bitcoin price was lower than it was four years ago. But, of course, past performance is not an indication of future results.

Third, whenever you see volatility in the Bitcoin price, ask yourself two things:

1) Does Bitcoin still have superior monetary properties (total resistance to debasement)?

2) Is Bitcoin still unstoppable?

If the answer to those two questions is “Yes,” I would not be worried.

Nonetheless, it is helpful to have perspective when Bitcoin experiences volatility—both to the downside and upside.

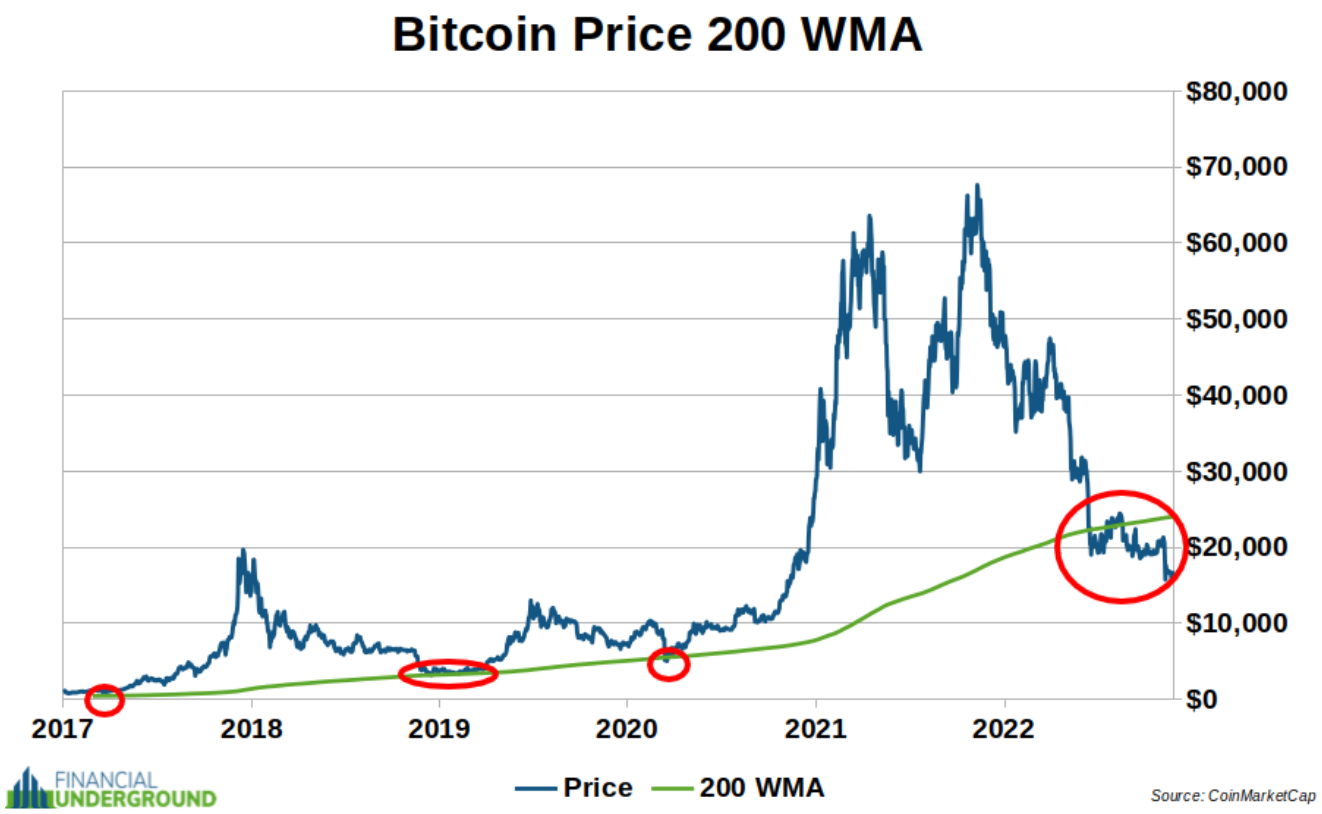
Below I discuss two indicators helpful in gauging the Bitcoin price at a given moment.

Indicator #1: 200-Week Moving Average

There has rarely been a period when the Bitcoin price was lower than it was four years ago. That’s why the 200-Week Moving Average (200 WMA) is a helpful metric, as it contains nearly four years of price data—around the length of a halving cycle.

Think of the 200 WMA as a floor on the Bitcoin price. Historically it has marked the bottom.

Will it mark the bottom in the future too? Nobody knows for sure, but I think it’s a reasonable proposition. As always, though, past performance is not an indication of future results.



In its history, the Bitcoin price has touched the 200 WMA a few times, and they were fantastic buying opportunities.

Indicator #2: Mayer Multiple

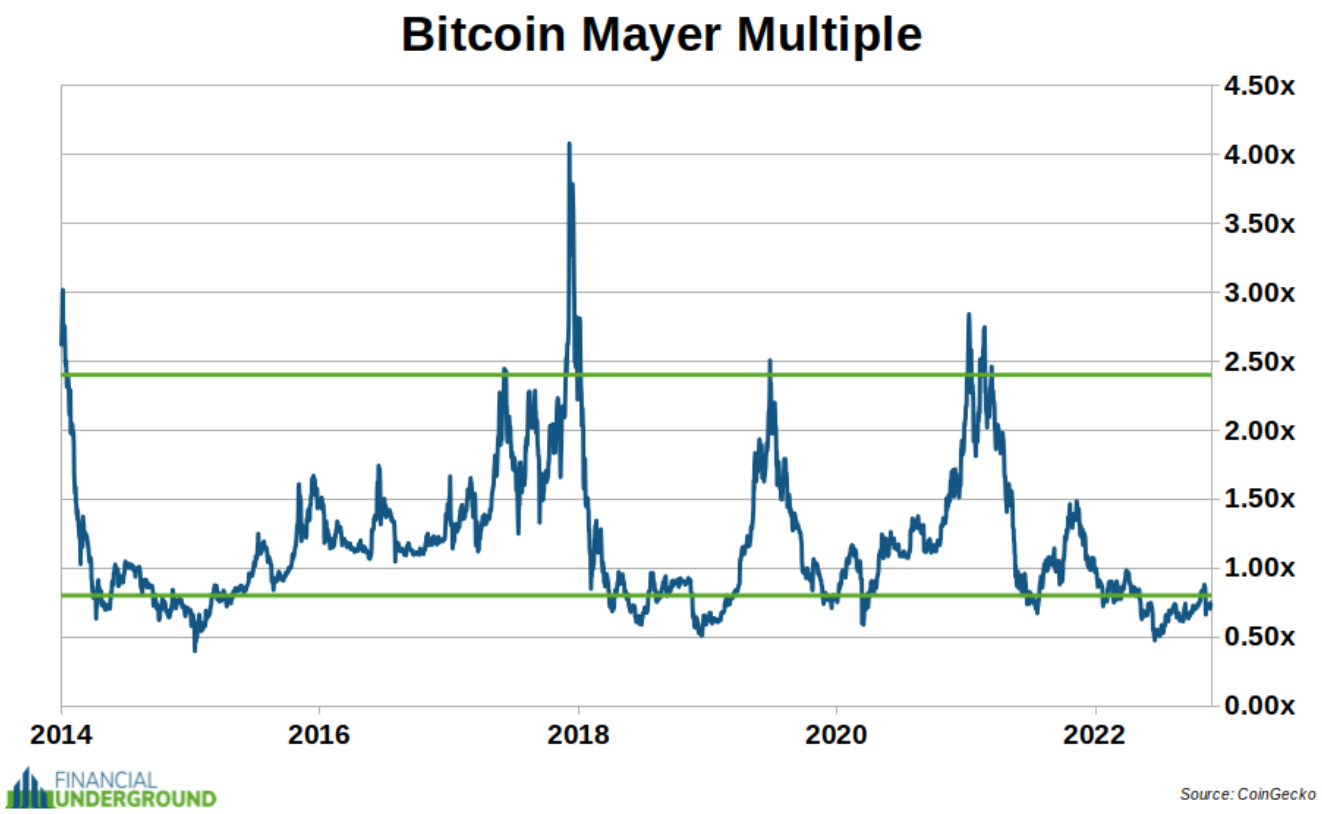
Trace Meyer—an early Bitcoin advocate—created this indicator.

The Mayer Multiple is calculated by dividing the current price by the 200-Day Moving Average (200 DMA). It shows how close the current price is to a long-term average price to evaluate whether Bitcoin is overbought or oversold.

A Mayer Multiple of 2.4x and higher indicates Bitcoin is overbought, and the market will likely not sustain the price.

A Mayer Multiple of 0.8x and lower indicates Bitcoin is oversold and represents a buying opportunity.

The chart below displays the overbought (2.4x) and oversold (0.8x) bands in green lines.



Conclusion

Bitcoin is absolutely scarce and easy to divide, verify, and transfer. It is already about as hard as gold and, in 2024, is set to become the hardest money the world has ever known—and will only get harder.

In short, Bitcoin represents a revolutionary improvement in money.

When you put it all together, you have an unstoppable, superior form of money conquering the world. It's not hard to see where this trend is going. Yet many people still don't understand Bitcoin or its implications.

Bitcoin can give monetary sovereignty to the individual. It allows anyone in the world to own and use incorruptible inflation-proof money without needing any other party.

In short, Bitcoin obviates central banks and their inflationary fiat currencies. That's no small accomplishment. It's the most important innovation in money in hundreds of years and alters the status quo profoundly. The implications of Bitcoin could shatter existing paradigms and be as disruptive as the invention of gunpowder, the printing press, and the Internet.

I have little doubt The Bitcoin Supremacy will be one of the biggest financial trends of the decade.

Think about it. You have the chance to front-run major investors, large multi-national corporations, and even governments by getting in on this trend before they do. It's an enormous once-in-a-lifetime opportunity and the biggest investment story I've ever seen.

Yet, the vast majority of humanity does not own or understand Bitcoin. That perception gap is a blessing, as it allows us to capitalize on this information asymmetry with investments that tap into this powerful trend.

However, I'd bet it won't be long until the rest of the world figures out Bitcoin's potential and acts upon that knowledge. And when they do, the opportunity to make transformative profits will probably be gone.

I do not doubt that those who buy and hold Bitcoin could make significant profits. But if that's all you do, you could miss out on the biggest and fastest gains.

For example, earlier in my investment research career, I recommended a publicly-traded Bitcoin mining stock that went up an incredible 2,123%—more than 22x—in just 77 days. But, of course, that is just a single trade and is not a full track record. And past performance is not an indication of future results.

How to Profit

Bitcoin miners are in the business of producing the hardest money mankind has ever known.

It's a cut-throat business, but the ones that get it right could be incredibly valuable businesses. That is especially true when the Bitcoin price rises, which I expect it to in the months ahead.

Think of investing in a Bitcoin miner like a leveraged play on Bitcoin. Even a tiny change in the Bitcoin price can have an enormous impact on the profits of a miner. It's similar to how junior mining stocks offer leveraged exposure to gold and silver… but potentially even more lucrative.

For example, suppose it costs $1,000 for a gold miner to produce an ounce of gold.

If gold prices fall 10% to $900, the company loses $100 on each ounce.

If the gold price instead rises 10% to $1,100, then the gold miner is making a $100 profit on each ounce.

Suppose the price of gold rises a further 9% to $1,200. The miner's profits don't just go up by 9%. They double—from $100 to $200 per ounce.

Suppose the price of gold doubles from $1,000 to $2,000 an ounce. The miner's profits don't just double. They go up 10 times.

That's how gold mining stocks offer leveraged exposure to the price of gold.

A similar dynamic is at work with Bitcoin and Bitcoin miners… but on steroids. That's because Bitcoin miners are producing something that is not just scarce but absolutely scarce. Bitcoin is the only commodity where higher prices cannot induce more supply, eventually bringing down prices.

That means the only way Bitcoin can respond to an increase in demand is for the price to go up. Unlike every other commodity, increasing the supply in response to increased demand is not an option.

That's why the business of Bitcoin mining can be even more profitable than that of other commodity producers.

When we see explosive moves in Bitcoin, we see even more explosive moves in Bitcoin mining stocks.

My proprietary **SCORE** system is how I avoid the junk companies—which could wipe you out—and find the winners with the biggest profit potential.

SCORE Is an acronym for a five-point analysis that looks at the most critical factors of a Bitcoin mining stock so that we can find the ones with the most upside.

Here is a summary of it:

Strategic partnerships—Does the company have a partnership to give them an edge?

Catalysts—What will move the needle in the next 3-6 months?

Orange Pilled—Does management really understand Bitcoin?

Retention—What does the company do with the Bitcoins it generates?

Electricity—Energy expenses can add up to over 90% of a miner's operating costs. Does the company have access to a reliable source of cheap electricity?

Here's the bottom line.
Bitcoin is misunderstood by almost everyone. But that's actually a huge blessing in disguise.

This information asymmetry gives us a rare chance to make smart speculations before the crowd figures out what is really happening.

However, historically, Bitcoin's biggest moves to the upside happen very quickly…

That's why many miss out on making fortunes from Bitcoin… and live to regret it.

The next big move could happen imminently.

Those who simply buy Bitcoin will do well.

But the real key to the huge—potentially life-changing—profits will be select Bitcoin mining stocks that anyone can access from an ordinary brokerage account.

These stocks tend to soar so high and fast that they make it look like Bitcoin's price is flat.

That's why I just released an urgent report that details what I believe to be the number one way to multiply your profits from Bitcoin's next upside explosion. It's easily accessible through any brokerage account.

The #1 Way To Multiply Your Profits From Bitcoin's Next Upside Explosion

Don't miss what could be your last chance to make potentially life-changing profits from this trend. Click here to get all the details now.

By Nick Giambruno

Nick is a renowned speculator and international investor. He's the Founder of the Financial Underground and Editor in Chief of *Contra Speculator*.

DISCLAIMER AND DISCLOSURES

To contact us by email, please click here.

The Financial Underground ("TFU", "we", "our" or "us") is an independent research provider and publisher.

Information contained herein has been prepared solely for informational purposes and does not represent investment advice. It is obtained from sources believed to be reliable, but its accuracy cannot be guaranteed and may contain errors. TFU shall not be liable for any errors or inaccuracies, regardless of cause, or the lack of timeliness. The opinions expressed herein are those of the publisher and are subject to change without notice. Information may become outdated and there is no obligation to update any such information.

Information contained herein is general in nature and is provided with the understanding that it may not be relied upon as, nor considered to be tax, legal, accounting, professional, or personalized advice. It is not designed to meet your personal situation. We are not financial advisors and are not rendering any personalized investment advice nor making any recommendations to you. Nothing you read here should be construed as a solicitation to effect (or attempt to effect) transactions in any security, financial product or instrument.

The securities discussed in our publications may be unsuitable for investors depending on their specific investment objectives and financial position. Investment decisions should only be made only after consulting with your registered professional financial, legal and tax advisors, only after reviewing the prospectus or financial statements of the company in question, and only after conducting your own due diligence. You shouldn't make any decision based solely on what you read here. Past performance is not an indication of future results. Securities discussed in our publications may lose value, are not insured by the Federal Deposit Insurance Corporation, and are subject to investment risks, including possible loss of the principal amount invested.

Our research is based on company public filings, current events, interviews, corporate press releases, and our own research. TFU is not compensated in any way for publishing information about the securities mentioned in our reports. All of the views expressed in our publications accurately reflect our personal views about any and all subject securities or issuers discussed. No member of TFU, nor any member's of their households, are an officer, director, or advisory board member of these companies.

All information contained herein is provided "as is" for use at your own risk. TFU shall not accept any liability for any losses or damages, monetary or otherwise, that result from the content of its publications. If you don't accept this responsibility for yourself, then you should not use our services. You agree that your use of our services is at your sole risk.

We eat our own cooking. Nick Giambruno may own positions in companies in the model portfolio of *Contra Speculator*, the premium investment research publication of TFU. Subscribers can click here for a disclosure of the current list. We will always disclose if and when we sell, and will give subscribers a full 24 hours notice before we sell. Electronic versions of Contra Speculator are made available to all subscribers simultaneously.

Full Terms and Conditions