ETC Group

The Investment Case for Bitcoin

Spring 2024

About the Authors

ETC Group — Exchange Traded Cryptocurrencies

ETC Group is bridging the gap between crypto and traditional financial services. Founded in 2019, the company is a first mover in European investment products that provide institutional-grade access to cryptocurrencies.

Blockchain technology and its applications continue to gain acceptance and traction. The world's largest banks, asset managers and transaction service providers are increasingly adopting cryptocurrencies and investing in the sector. Cryptocurrencies are the fungible payment units of blockchain ecosystems and therefore indispensable for blockchain and co.

ETC Group launched the world's first centrally cleared bitcoin ETP on Deutsche Börse XETRA, Europe's largest ETF trading venue. Since the product listing in June 2020, the company has become a leading European provider of physically-backed Crypto ETPs. With customer centric innovation at core of its product development approach, ETC Group continues to pioneer the field, having launched the first crypto basket ETP on an MSCI digital asset index in April 2023.

The company consists of an experienced team of financial services professionals and entrepreneurs. Years of experience in both the crypto sector and conventional investment products enable ETC Group to guide traditional investors and their risk and investment committees through the intricacies and novelty of the digital asset ecosystem.

André Dragosch, PhD
Head of Research, ETC Group

Table of Contents

Executive Summary

The comprehensive analysis within this report delves into the strategic investment potential of Bitcoin, elucidating its foundational role at the intersection of cutting-edge technology and finance. Bitcoin, emerging from the conceptual frameworks of cryptography and digital innovation, has swiftly ascended as a pivotal asset in the investment sphere, particularly appealing to professional investors seeking diversification and resilience in their portfolios.

This report further examines Bitcoin's historical performance, its resilience against potential sovereign defaults, and its burgeoning role as an alternative to conventional safe-haven assets. Through a critical analysis of various valuation models and on-chain metrics, we offer a comprehensive perspective on Bitcoin's market dynamics and its intrinsic long-term value.

Bitcoin presents a compelling narrative of technological innovation, market resilience, and incremental adoption that underscores its significance within the contemporary investment landscape. It emerges as a critical asset in the context of portfolio diversification, offering a blend of scarcity, security, and potential for significant returns. As institutional interest grows and Bitcoin's integration into financial systems deepens, its role as a disruptive force in traditional value storage and exchange mechanisms becomes increasingly pronounced.

Central to our investment thesis is Bitcoin's inherent scarcity, enhanced by mechanisms such as halving events and its proof-of-work consensus algorithm. These features not only distinguish Bitcoin from both traditional and digital counterparts but also position it as a formidable hedge against inflation and economic volatility. Our exploration into Bitcoin's adoption trends, augmented by its network effects and the Lindy Effect, reinforces its status as a viable store of value and medium of exchange, amidst growing global financial uncertainties.

Rooted in the pioneering contributions of Satoshi Nakamoto and subsequent advancements through Bitcoin Improvement Proposals (BIPs), Bitcoin's journey from an experimental digital currency to a globally recognized financial asset highlights its adaptability, security, and unique value proposition. This evolution is indicative of Bitcoin's capacity to address perennial issues of digital trust and transaction efficiency while ensuring robust security and decentralization.

The executive recommendation posits that Bitcoin, with its unique attributes and proven track record, constitutes an essential component of a well-rounded investment strategy. Emphasizing a balanced approach to Bitcoin investment, we highlight its capacity to augment portfolio performance, serve as a strategic hedge, and leverage the transformative potential of digital assets in the evolving financial ecosystem.

Investment Case for Bitcoin

> Bitcoin didn't appear out of thin air — it is the result of decades of work. Many digital currency projects failed before it succeeded. Understanding how we got here will help you understand where we're going.
>
> Jameson Lopp

Understanding Bitcoin

The History of Bitcoin

In fact, the scientific underpinnings of this technology date back to the developments of public key cryptography in the early 1970s.

Before the 1970s, cryptography was generally a military and intelligence domain. This changed with the development of the public internet and TCP/IP protocol put forth by Cerf & Khan (1974).

An important milestone with respect to public key cryptography that underpins the Bitcoin protocol today was the paper published by Diffie & Hellman (1976) that introduced key concepts such as digital signatures and asymmetric key distribution.

Satoshi Nakamoto's groundbreaking 2008 paper **"Bitcoin: A Peer-to-Peer Electronic Cash System"** itself is based on many previous academic works in cryptography like cryptographic timestamping and proof-of-work algorithms.

1974
Cerf and Kahn "A Protocol for Pocket Network Intercommunication" TCP/IP

1976
Whitefield Diffie & Martin Heilman "New Directions in Cryptography"

1978
RSA Pubic Key Cryptosystems

1980
Ralph Merkle "Protocols for Public Key Cryptosystems"

1983
David Chaum "Blind Signatures for Untraceable Payments"

1985
Eliptic Curve Cryptography

1988
Timothy C. May "The Crypto-Anarchist's Manifesto"

1989
David Chaum "Found Digicash"

1991
Phil Zimmerman "Pretty Good Privacy" PGP

1992
Cyberpunks founded in SF by Eric Hughes, Timothy C. May and John Gilmore

1993
E. Hughes "A Cyberpunk's Manifesto"

1994
Timothy C. May "The Cyphernomicon"

1996
NSA: "How to make a mint"

1996
E-Gold

1997
Nick Szabo "Formalizing and Securing Relationships on Public Networks"

1997
Adam Back "HashCash, DOS counter-measure w/proof-of-work"

1998
Nick Szabo "Securing Property Titles with Owner Authority"

1998
Bit-Gold

1998
Wei Da "B-money" – decentralized database to record txs and using a type of proof-of-work

1998—2001
Many online retailer currencies in the dotcom bubble (Beenz, Floor etc.)

1999
Max Keiser "Computer-Implemented securities trading system"

2001
Distributed Hash Tables

2001
Video game currencies and markets-era starts in 2001

2001
Bram Cohen, Bittorrent

2004
Hal Finney: "Reusable PoW"

2006
Liberty Reserve

2008
Satoshi Nakamoto
Bitcoin: A Peer-to-Peer Electronic Cash System

Before the invention of Bitcoin in 2008, there have been numerous attempts to create a digital peer-to-peer payment system cryptographically such as DigiCash (1990s), e-gold (1996), b-money (1998), Bit Gold (2005), and Liberty Reserve (2006).

However, these earlier attempts failed mainly because of centralization, lack of adoption, legal challenges, or vulnerabilities that Bitcoin sought to overcome with its decentralized model and robust security features. Bitcoin's design drew upon the ideas and lessons from these earlier attempts, combining them into a unique and revolutionary protocol.

More specifically, Satoshi Nakamoto's innovation in the field of cryptography was the solution for both the so-called "double-spending problem" and the "Byzantine General's problem" that were presented in his 2008 paper and which lay the ground work for Bitcoin (see highlight box on next page).

Moreover, the utilization of Proof-of-Work (PoW) in Bitcoin and other cryptocurrencies represents a significant advancement in the realm of cryptography and distributed systems, especially when compared to earlier models that did not incorporate the use of physical energy (in the form of computational power) as a fundamental component of the system's security and trust model.

Before the advent of PoW in cryptographic systems, most digital security and trust models were based on logical or mathematical principles without directly tying the security mechanism to the expenditure of physical resources.

These models relied on cryptographic algorithms for encryption, digital signatures, and secure communication. Trust within these systems was often managed through centralized authorities (like certificate authorities in SSL/TLS) or through pre-established trust relationships among parties.

Proof-of-Work, introduced into the broader public consciousness by Bitcoin, changed this paradigm by directly linking the security and integrity of the system to the expenditure of physical resources, specifically electricity and computing power.

This linkage creates a new form of trust model that does not rely solely on logical or mathematical assumptions but also on the economic principle that the cost of securing the network (through mining) is related to the consumption of a real-world resource (energy).

Thus, it is important to understand that the energy-intensive proof-of-work algorithm is an important security feature of the Bitcoin protocol and not a bug.

What's the innovation by Satoshi Nakamoto in cryptography?

Double spending

Imagine you have a 10 Euros. In the physical world, if you go into a store and use it to buy something, you no longer have that 10 Euros to spend again. However, in the digital world, before Bitcoin, it was hard to ensure that if you spent a digital 10 Euros, you couldn't just copy that digital file and spend it again somewhere else. This is the "double-spending" problem: the challenge of ensuring that digital money can only be spent once.

Nakamoto's Solution: Bitcoin's blockchain acts like a ledger or record book that keeps track of every transaction ever made. When you spend some Bitcoin, that transaction is broadcast to a network of computers (nodes). These nodes use a hashing algorithm to validate the transaction and add it to the blockchain. Since every transaction is linked to previous ones, trying to spend the same Bitcoin twice would be noticed immediately — it would be like trying to change a number in a long chain of calculations without anyone noticing.

Decentralization (Byzantine General's Problem)

This is a classic problem in computer science and describes a situation where involved parties must agree on a single strategy to avoid failure, but some of the parties might be traitors trying to cause failure. In the context of digital currencies, the problem is ensuring that all participants in the network agree on the current state of the blockchain (which transactions are valid, what the correct sequence of transactions is, etc.), even if some participants are trying to cheat or spread false information.

Nakamoto's Solution: Bitcoin solves this through a mechanism called "proof-of-work" and decentralized consensus. In proof-of-work, to add a block of transactions to the blockchain, a computer (miner) must find a hash. This requires real-world resources (electricity, computing power). The first miner to solve the puzzle gets to add the block and is rewarded with some Bitcoin. This makes cheating expensive and pointless because it would require an enormous amount of resources to outpace the honest nodes. As each block is added upon the previous one, the network reaches a consensus on the state of the blockchain. Even if some nodes are dishonest (like the traitorous generals), they can't overpower the honest ones without an impractical amount of computing power.

However, Bitcoin is still evolving and improving on a continuous basis. Today, anyone can propose a so-called "Bitcoin Improvement Proposal" (BIP) in order to introduce new features and capabilities of Bitcoin or remedy issues in the areas of scalability, security or decentralization. The fact that Bitcoin is open-source software allows for fast bug fixes and improvements over time. At the time of writing, there have already been 389 of those abovementioned BIPs[1].

So, the innovation of Bitcoin has not stopped with Nakamoto's work but continues to this day.

1 https://github.com/bitcoin/bips

Key features of the Bitcoin protocol

Bitcoin does not contain one single feature that makes it unique. It is rather a combination of key features that shape the main characteristics and economics of Bitcoin. However, many features of the Bitcoin algorithm are designed in such a way to maximize supply scarcity without disrupting the stability of the network. Consider the following characteristics of the Bitcoin network:

1

Decentralization

Decentralization is achieved via competition and economic incentives among miners to secure the Bitcoin blockchain. Contrary to the widespread belief that miners solve “complex mathematical problems” miners rather engage in a trial-and-error process in order to find the correct hash that connects the latest batch of transactions to the blockchain, which contains all other historical transactions of the Bitcoin blockchain.

Miners use powerful computers to make trillions of guesses per second to find the right hash. If a miner finds a correct hash, the miner is rewarded with the block reward which consists of the so-called block subsidy (currently 6.25 BTC) and the transaction fees included in the block of transactions (variable). Thus, miners have an economic incentive to process transactions and to secure the blockchain. Finding the right hash requires resources like hardware, time and energy which disincentivizes other dishonest miners to corrupt the system.

2

Halving

An important feature of the Bitcoin algorithm is the so-called Halving which occurs every 210000 blocks until it has occurred 32 times (and the supply of bitcoins reaches 21 million coins in circulation).

As every block is mined approximately every 10 minutes, Halvings occur once every 4 years. As the name suggests, a –50% reduction in the production rate/supply growth of bitcoins occurs at the Halving — production rate is “halved”. This is also a feature of the algorithm that increases supply scarcity over time.

Halvings function as an additional supply shock and have shown to be highly significant for Bitcoin’s price performance in the past. There already have been 3 Halvings in the past, in 2012, 2016, and 2020 and a 4th Halving is scheduled to occur in April 2024.

3

Difficulty adjustment

Another important feature of the Bitcoin algorithm is the so-called “difficulty adjustment”. Difficulty is the amount of computing power (in hashes) required to find the correct hash. The beauty is that the algorithm is fine-tuned in a way that this difficulty adjusts to 10 minutes block time dependent on the current prevailing hash rate of the network.

The difficulty is adjusted every 2016 blocks which is equivalent to approximately 2 weeks. If hash rate increased by +10% over the past 2016 blocks (average block time reduced by –10%), difficulty would also increase by +10% in order for blocks to be mined every 10 minutes again. It also works in reverse meaning if hash rate declined by –10% (average block time increased by +10%), difficulty would adjust downwards by –10%.

That way, the algorithm ensures that the amount of bitcoins produced converges toward the block time and block subsidy (currently 6.25 BTC) every 10 minutes. This implies that the supply of bitcoins that is being produced is almost completely price inelastic which increases scarcity even more.

4

Open-source public ledger

The open-source public ledger ensures that the network operates on a minimum amount of bilateral trust which is also a key prerequisite of a “trustless system”.

Open-source software ensures that the code is completely transparent and that any potential backdoors that could jeopardize the security of the network are impossible to implement.

Moreover, bugs can be detected faster by a potentially global community of developers. The open-source nature of the code also allows for any individual to run a full node without permission and verify transactions based on the common consensus rules of the algorithm.

Transactions and balances of any wallet can be checked via a simple online connection which also fosters trust in the system. Wallets are semi-anonymous which means that transactions and balances can be checked but it is generally unknown who controls those wallets.

The interplay between wallet users, full nodes and miners within the Bitcoin network

In the Bitcoin network, the interaction between wallet users, full nodes, and miners creates a secure and functioning ecosystem for transactions. Here's a simplified overview of how these components interact:

Interplay Summary

Transaction Initiation
It all starts with wallet users who create and broadcast transactions.

Verification and Relay
Full nodes verify these transactions and relay them through the network, ensuring they reach miners.

Confirmation
Once a block is added to the blockchain, the transaction is considered confirmed. Full nodes update their version of the blockchain, including the new block.

Mining
Miners include the transactions in new blocks, solving the proof-of-work puzzle to add these blocks to the blockchain.

This interplay ensures the Bitcoin network remains decentralized, secure, and up-to-date, allowing for peer-to-peer transactions without the need for a central authority.

The Innovation of Bitcoin in economics & finance

What's special about Bitcoin?

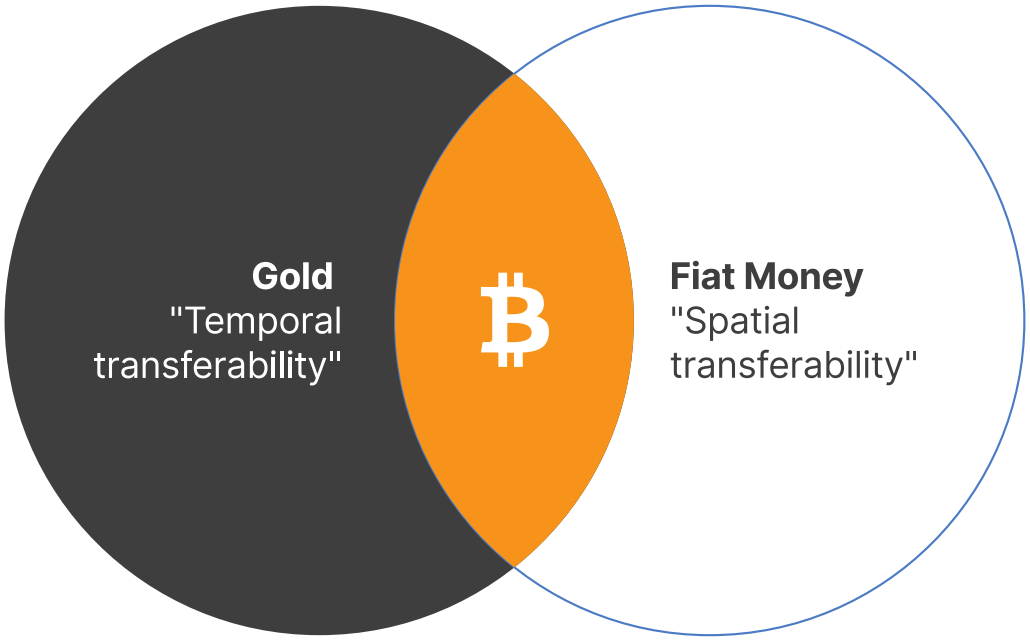
In order to understand the utility and use case of Bitcoin, one needs to understand its advantages over other types of monies. It is important to note that today's fiat monies such as the US Dollar or the Euro are not backed by gold since the demise of the Bretton-Woods agreement in 1971. In fact, fiat monies are created "out of nothing" in the banking system and are theoretically unlimited in supply. Therefore, gold as a finite resource is still different from today's fiat monies.

The following table compares Bitcoin to Gold and Fiat monies in terms of monetary characteristics:

Properties of Money	Bitcoin	Gold	Fiat (USD, EUR,...)
Scarcity limited asset	✓ Max. 21 mn coins	✓ Only ~1.5% p. a. supply growth	✗ Theoretically unlimited
Reliability outlasts time	✓ secured by global decentralized network	✓ 1000s of years	✗ dependent on soundness of fiscal & monetary policy
Transferability easy to transfer	✓ can be transferred by any device connected to the internet	✗ large quantities hard to transport	✓ easy to transter via different payment providers
Verifiability easy quality control	✓ blockchain enables immediate verification	✗ easy to counterfeit	~ cash: easy to counterfeit, eCash more difficult
Divisability divide into smaller units	✓ 1 BTC = 100 mn Satoshis	✗ hard to divide in equal parts	✓ divisable up to 100th of unit
Fungibility 1 unit = 1 unit	✓ 1 Bitcoin = 1 Bitcoin worldwide	✓ same value per ounce but depends on purity	~ Dependent on currency and gov't restrictions
Acceptability accepted for payments	✓ accepted everywhere where VISA & Mastercard are accepted; LN network	~ only accepted at jewleries, banks, gold traders	~ Dependent on currency

The key point to make here is that Bitcoin combines both the advantages of gold in terms of scarcity and reliability with the advantages of fiat monies in terms of transferability.

> In other words, Bitcoin offers a combination of so-called spatial transferability (across space) and temporal transferability (across time).



Gold ultimately failed as a modern store-of-value not only because it possessed an inferior transferability compared to fiat monies but because the physical nature of gold itself and custody of gold ultimately meant a high dependence on physical location which introduced additional custodial and ultimately counterparty risks.

Although Bitcoin tends to be custodied for institutional investors, the control of those funds is independent of physical location and can be exerted from anywhere in the world if one possesses the respective private keys.

At the same time, Bitcoin allows for instant and almost free transactions on a peer-to-peer basis with just a simple internet connection. Balances held on the bitcoin blockchain are free of counterparty risk and transactions are censorship-resistant, i. e. cannot be blocked by any central authority.

Compared to other cryptoassets, Bitcoin represents by far the most secure blockchain. One of the reasons is that the Bitcoin network already comprises of more than 18k full nodes which validate transactions based on the common consensus rules of the Bitcoin algorithm[1].

1 Source: https://bitnodes.io

Can Bitcoin be “hacked” and is Quantum Computing potentially a threat to Bitcoin?

As a starter, it is theoretically possible to compromise (“hack”) the Bitcoin network. One of the ways to do so is to acquire the majority of computational power (i. e. hash rate) within the network and perform what is called a “51% attack” on the network.

By controlling the majority of hash rate, an attacker could potentially double-spend bitcoins which undermines the integrity of the blockchain as the same coins are fraudulently used more than once. An attacker could also censor transactions, reorganise the blockchain, reduce network security, or create a mining monopoly.

Quantum computing is seen as a general threat to the cryptography of Bitcoin in this regard due to its ability to leverage the principles of quantum mechanics to perform calculations at speeds unattainable by classical computers.

However, it is quite likely that Bitcoin miners would be the first to adapt this new technology since they are economically incentivized to do so and have invested in cutting-edge chip technology in the past. More specifically, Bitcoin miners currently use the most advanced chip technology in the newest ASIC mining hardware which comprises of 7 nm chips[1].

According to the latest estimates by Coinmetrics, already ~80% of the ASIC miner fleet worldwide consists of the newest mining hardware which are the MicroBT M50 and Antminer models S19, S19JPro and S19XP which use 7nm chips. 3 So, the large majority of mining hardware already employs the newest available chip technology.

Moreover, in order to replicate the current hardware of the Bitcoin mining ASIC fleet, any malicious attacker would need to invest around 3.7 bn USD in mining hardware in order to acquire around 51% of the network hash rate which is a lower-bound estimate.[2] Other authors have come up with higher estimates, depending on how scarce mining hardware might increase due to the increase in demand by the attacker.[3]

Note that this investment would be worthless after a successful attack so the attacker has no economic incentive to do so in the first place.

Furthermore, the attacker would only have a short time period to attack since most of the mining hardware already becomes obsolete within approximately two years on account of “Moore’s Law”.

What is more is that due to long lead times in the chip manufacturing supply-chain, it is almost impossible to purchase most ASIC miners in advance to attain the required majority in hash rate. Generally, lead times can range from a few months to over a year.

All in all, these factors make an effective malicious attack on the Bitcoin network very unlikely.

What is more is that the combined amount of computational power of the Bitcoin mining network is comparable to server operations of big tech giants like Google.

More specifically, at the time of writing, the global Bitcoin network computes hashes at a rate of 661 Exahashes per second. “Exahashes” refers to a measurement of hash operations per second, specifically one quintillion (10^18) hashes per second.

For comparison, the most efficient supercomputer on earth called “Henri” computes 3579.13 Teraflops per second at peak according to the latest data by the Green500 List.[4]

One teraflop is equivalent to 1 billion floating-rate computations per second.

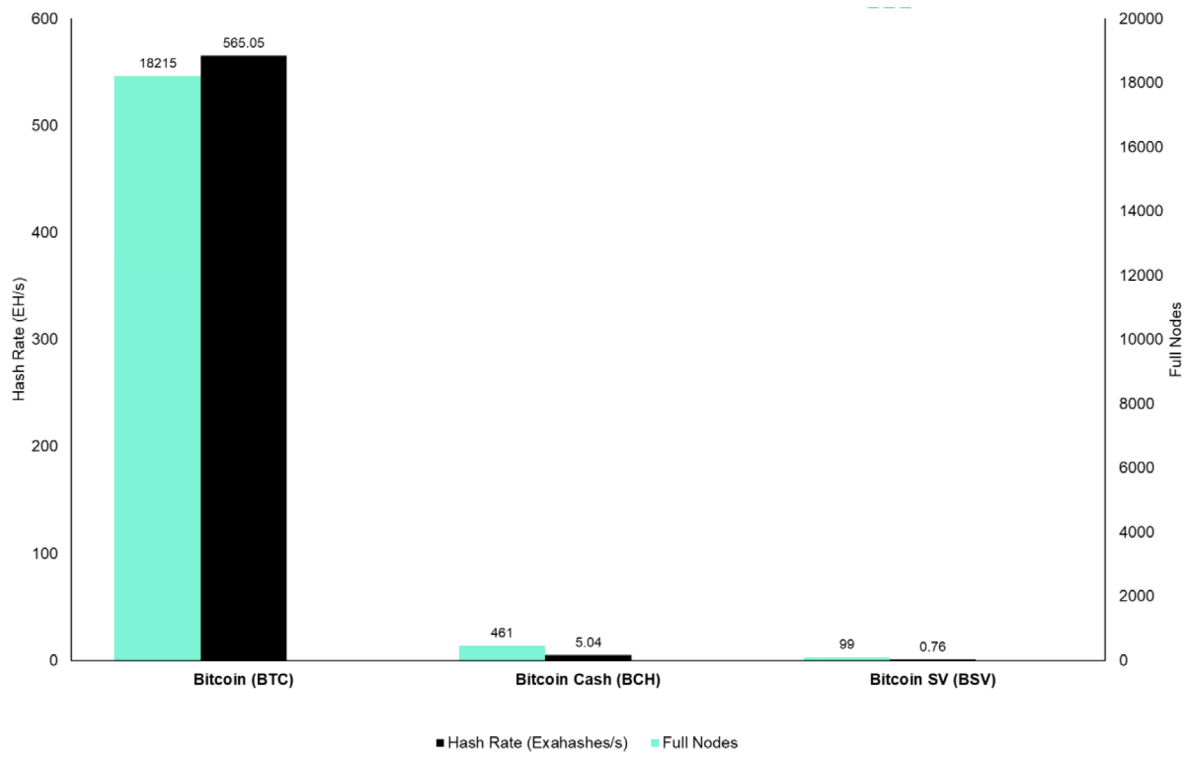
The degree of decentralization (>18k full nodes globally) as well as the amount of computational power that is securing the network (~661 Exahashes/second) is something that cannot be replicated in the short term.

1 https://labs.coinmetrics.io
2 Estimations based on the MINE-MATCH ASIC miner fleet estimate by Coinmetrics per January 2024. Hardware values based on cheapest-to-deliver prices via asicminervalue.com
3 Nuzzi et al. (2024)
4 https://www.top500.org/lists/green500/2023/11

Hard forks of the original Bitcoin (BTC) such as Bitcoin Cash (BCH) or Bitcoin Satoshi Vision (BSV) do not come even close to the amount of computational power of Bitcoin (BTC).

> This means that the global decentralized Bitcoin network computes hashes at a rate that is equivalent to 184,789 of the most efficient supercomputers on earth calculating at peak performance[1].

Bitcoin's (BTC) degree of decentralization & level of security are not easily replicable



Source: Bitinfocharts.com, bitnodes.io, cashnodes.io, nownodes.io; data as per 27/03/2024

1 Although you cannot directly compare FLOPS/second to Hashes/second, SHA-256 hashes contain 256 bits of information each while, e.g. a double-precision floating-rate operation usually combines only 64 bits of information. So, computing a single SHA-256 hash uses up more memory than, e.g. an addition of two 64 bits numbers. Hence, the abovementioned estimate of necessary supercomputers should be considered a lower-bound and conservative estimate.

Store-of-Value versus Medium-of-Exchange

The financial historian Adam Fergusson observed that in 1923, during the severe inflation of the Weimar Republic, the devaluation of the official currency led to its rejection as a medium of exchange for goods, prompting people to use any form of currency that had real value. A similar situation occurred in Zimbabwe in 2009 during the hyperinflationary period.

In situations of rampant inflation, people will opt for currencies that they perceive to have sustainable value and reject those that are perceived to have diminishing value. If they have no choice, they will hoard the currency that is perceived to have higher value and distribute the less valuable currency. This behaviour results in the circulation of the less valuable currency and the hoarding of more stable forms of money.

> “ Good and bad coin cannot circulate together.
>
> Thomas Gresham

This concept, in which the presence or absence of legal tender laws influences the acceptance of a currency, highlights that in the absence of such laws, a buyer will tend to use the currency with the lowest commodity value that creditors are forced to accept. Conversely, in the presence of such laws, sellers will demand currency of a certain value.

The economist Peter Bernholz named this principle “Thiers’ Law” after the French politician and historian Adolphe Thiers, describing the tendency of valuable currency to be hoarded and replaced by inferior currency in circulation as the latter loses value, also known as “Reverse Gresham’s Law”. This observation serves as a case study for the rapid adoption of stable currencies, including scarce cryptocurrencies, in times of high inflation.

It also showcases that the store-of-value function of money is ultimately more important than the medium-of-exchange function of money, since superior money is the one that is used as store-of-value while the inferior money is spent to get rid of it as medium-of-exchange.

Is Bitcoin primarily being used by criminals?

There is still a common misconception that Bitcoin is primarily being used for illicit transactions such as money laundering, drug trafficking or terrorism financing.

Although on-chain data are pseudononymous, i. e. one can see wallet balances but the holder cannot be identified, some companies have started tagging addresses in order to trace certain on-chain transactions back to their origin — a practice referred to as “on-chain forensics”.

This has also enabled on-chain analysts to identify potentially illicit transactions as well.

These on-chain forensics generally reveal that the share of illicit transactions in total Bitcoin transactions has been very low.

According to the latest data provided by Chainanalysis, the share of illicit transactions of all cryptocurrency transactions was at only 0.34% in 2023.[1]

The fact that transactions are not only recorded publicly in real-time but are also potentially stored forever, makes public blockchains like Bitcoin very unattractive for illicit transactions.

In fact, cryptoasset service providers are obliged by law to know the sources of funds, in this case bitcoins, and therefore also employ on-chain forensic data providers to safeguard investors from this risk.

Why do we need a hard money standard?

The modern monetary history of the world can essentially be divided into a long period of precious metals backed money and only a short period of unbacked fiat money. In fact, all of the previous global reserve currencies since the 15th century had some form of backing either in silver or gold that started with the Portuguese Real.

In fact, the more recent monetary history since 1971 appears to be an exception to the long period of commodity backed monetary standards across most of the civilized world with some exception during the 1st and 2nd World War when hard money standards were partially abandoned.

But it is generally a valid statement that throughout much of the past 500 years, reserve currencies were mostly backed by a scarce commodity like gold and the past 50 years of unbacked fiat monetary standard have rather been an economic experiment.

Under a fiat monetary standard, money can be created ex nihilo — out of nothing — by both the central bank and commercial banking sector via credit creation without any theoretical limit. The newly created money supply does not need to be backed by a scarce commodity.

One of the major advantages of a commodity backed monetary standard appear to be structurally lower rates of inflation compared to unbacked fiat monetary standard. This is supported by the fact that the US experienced significantly lower rates of inflation in the pre-1971 era.

Another major advantage is the fact that countries that both adhere to a hard money standard exhibit fixed exchange rates which facilitates trade in goods and services as well as cross-border payments.

Moreover, data by Reinhart & Rogoff (2009) show that the frequency of banking crises was significantly lower, especially during the Bretton-Woods era between 1945 and 1971. Systemic banking crises tend to be linked to an unsustainable expansion in the money supply which induces many social costs such as high unemployment, corporate bankruptcies etc.

All in all, a hard money standard was historically associated with structurally lower rates of inflation, lower frequency of systemic banking crises, and has facilitated international trade and cross-border payments via fixed exchange rates. Amongst others, Ammous (2018) has made the case that Bitcoin could serve as a new type of reserve asset for the digital age in a global monetary system based on a Bitcoin Standard.

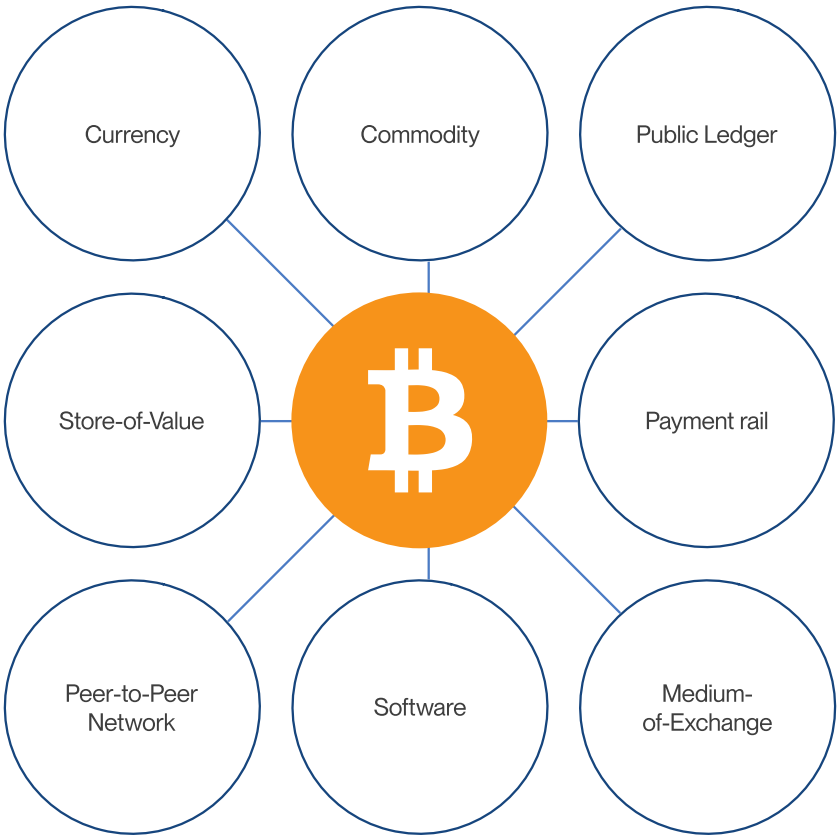
Valuing Bitcoin

> Bitcoin is not a stock, nor is it a startup or any investment fund... this is a completely different animal than other types of assets that people are trying to compare it to. You need to view it through a different lense.
>
> Marty Bent

Beauty and valuations have one thing in common — they are always dependent on the eye of the beholder.

In the same logic, there are multiple approaches to valuing Bitcoin which can differ from traditional asset class valuations. The reason is that Bitcoin can be regarded as both currency, commodity and monetary payment network at the same time. Bitcoin has many different characteristics which is why many different valuation approaches can potentially be applied.

However, most of the common valuation approaches centre around network utility, intrinsic value, and on-chain analysis.



Bitcoin as a network

Bitcoin can be regarded as a social network of participants that use Bitcoin as medium-of-exchange and payment rail. Similar to the way information is transferred between Email users, Bitcoin users send value across the Bitcoin network of users on a peer-to-peer basis. Utility for the users from the network can be derived from the medium-of-exchange function but also other usages such as censorship-resistance of transactions and the permissionless nature of the network itself.

Valuation methods for networks typically focus on the user base. The premise is that a network's utility and worth are directly linked to its total user count.

For example, Metcalfe's law suggests that the value of a telecommunications network increases with the square of its user count (n^2). This principle, attributed to Robert Metcalfe concerning Ethernet, was first introduced by George Gilder in 1993. Initially, it was applied to "compatible communicating devices" like fax machines and telephones in the early 1980s, not directly to users. Initially meant to describe Ethernet connections, its relevance expanded with the Internet's global spread, applying to broader user networks.

Various models have been proposed to link network value with user numbers.

Sarnoff's Law: Network Value = Number of users

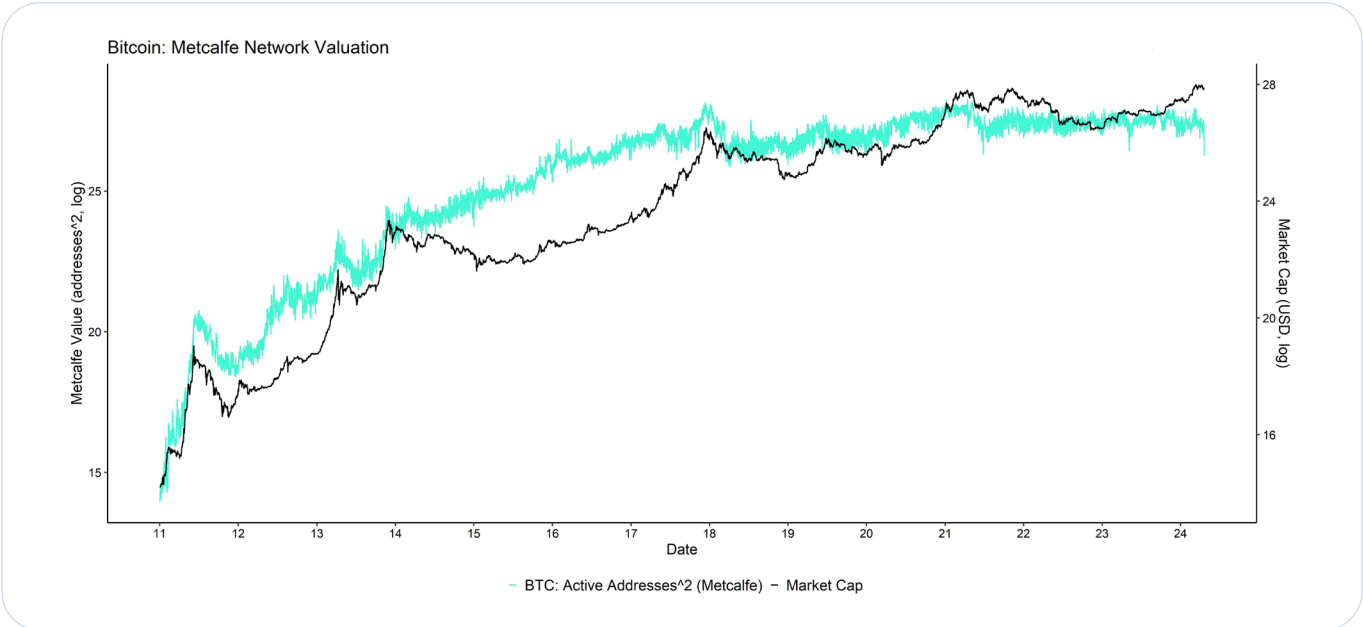
Zipf's Law: Network Value = Number of users * log (number of users)

Metcalfe's Law: Network Value = Number of users^2

Metcalfe's Law, which suggests a quadratic growth in network value with user numbers, remains one of the most prevalent valuation models today, in contrast to Sarnoff's Law, which indicates a linear growth.

The accompanying charts illustrate the correlation between market capitalization for Bitcoin and network activity (squared number of active addresses), demonstrating a strong link between network usage and valuation.

The higher the number of users, the higher the network's value



Source: Glassnode, Coinmetrics, ETC Group

Bitcoin as a scarce digital commodity

Bitcoin has many similarities with scarce commodities like gold which is why Bitcoin is often referred to as “digital gold”. In fact, the proof-of-work algorithm transfers physical scarcity of energy into the digital realm.

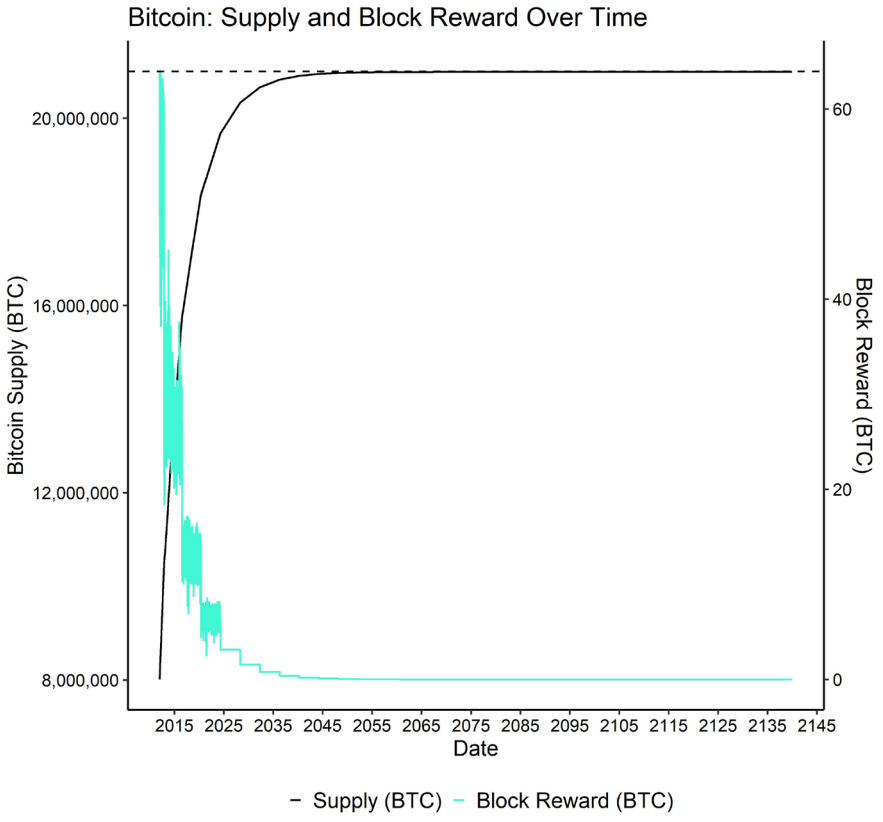
The process of mining in Bitcoin involves physical energy in the form of electricity and hashes are found randomly which is like the exploration of gold. That is why concepts from the commodity space have also been applied to Bitcoin.

One of these concepts is the stock-to-flow ratio which divides the current above-ground supply of the commodity by its annual production.

Stock-to-Flow (S2F) = Above-ground supply in circulation / annual production

In general, commodities that exhibit a higher stock-to-flow ratio are considered to be scarcer than others and tend to be more valuable. In fact, we can observe a similar phenomenon with respect to Bitcoin as higher stock-to-flow ratios have been associated with higher bitcoin prices in the past:

Bitcoin’s supply will converge towards 21M coins as reward converges towards 0



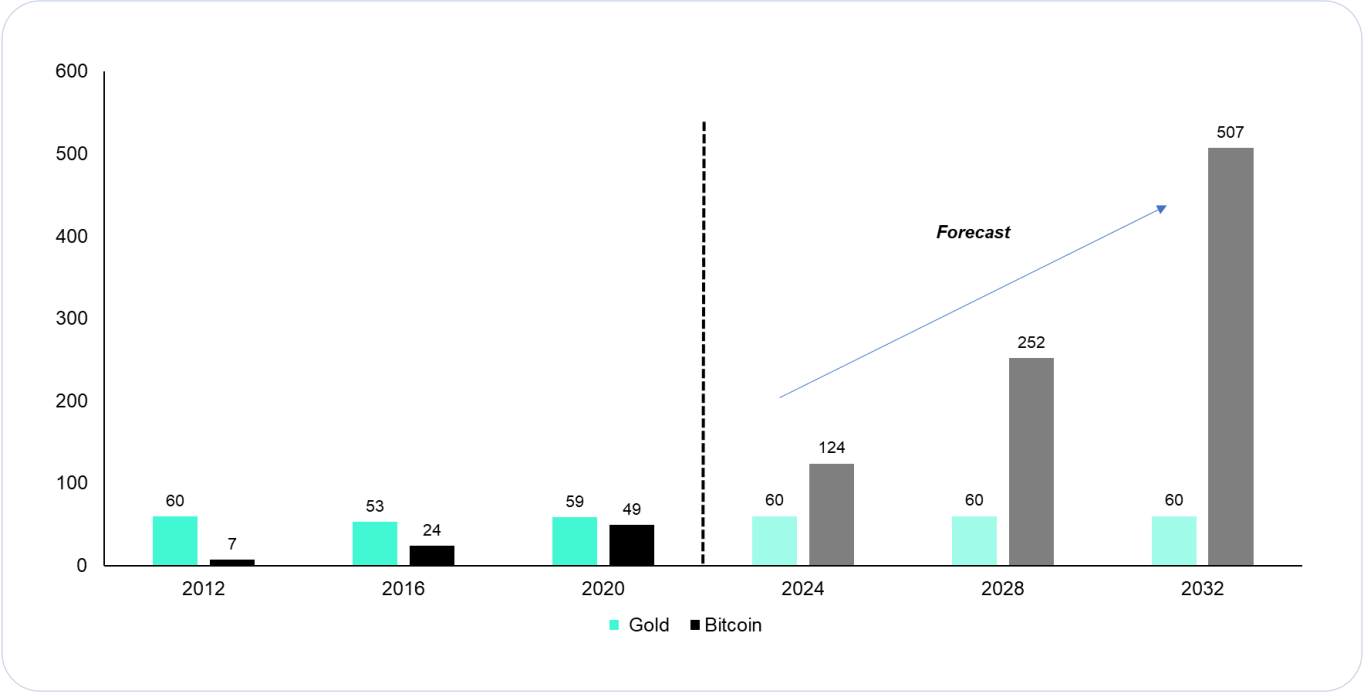
Source: Coinmetrics, ETC Group

The Stock-to-Flow of Bitcoin will double with every Halving as the annual production declines by –50% — the halving in annual production in the denominator mathematically leads to a doubling of the stock-to-flow ratio.

What is more is that gold's and Bitcoin's stock-to-flow ratio are very similar at the moment. However, Bitcoin's stock-to-flow will already leapfrog gold's stock-to-flow ratio in April 2024 by a very wide margin.

Bitcoin will become double as scarce as gold from supply growth perspective.

Stock-to-Flow Ratio: Bitcoin versus Gold



Source: ETC Group, Coinmetrics, World Gold Council

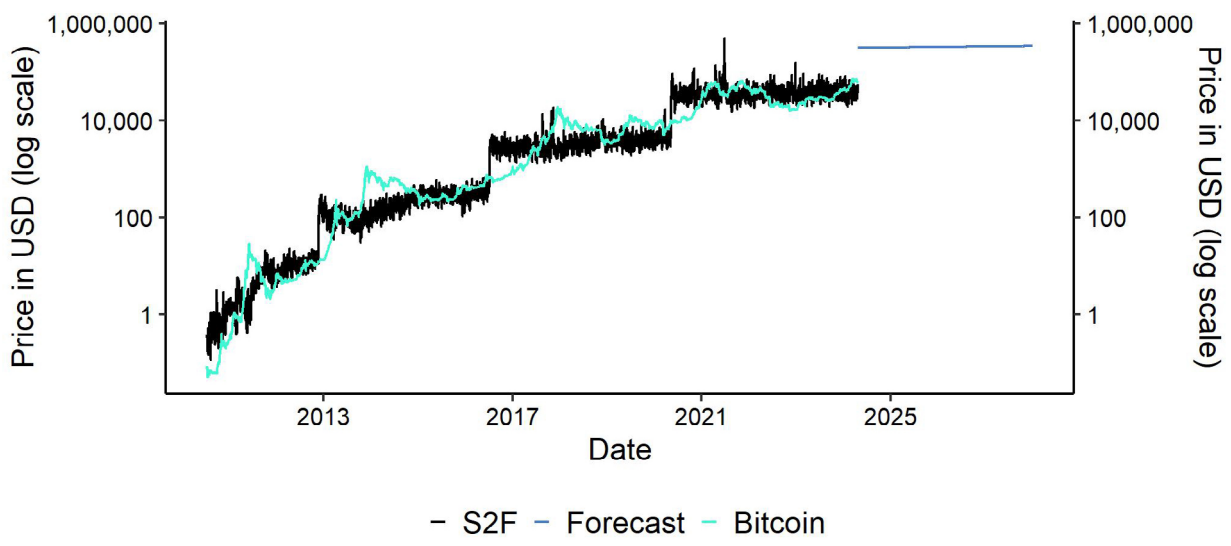
Moreover, this ratio will continue to increase over the coming decades and mathematically converge towards infinity as the block subsidy (currently 6.25 BTC per block every ~10 minutes) converges towards zero with the last (32nd) halving anticipated around the year 2140.[1]

The stock-to-flow ratio can also be used to make forecasts about bitcoin's performance about the future. The assumption would be that the price of bitcoin and the stock-to-flow were cointegrated, i. e. show a long-term equilibrium relationship.

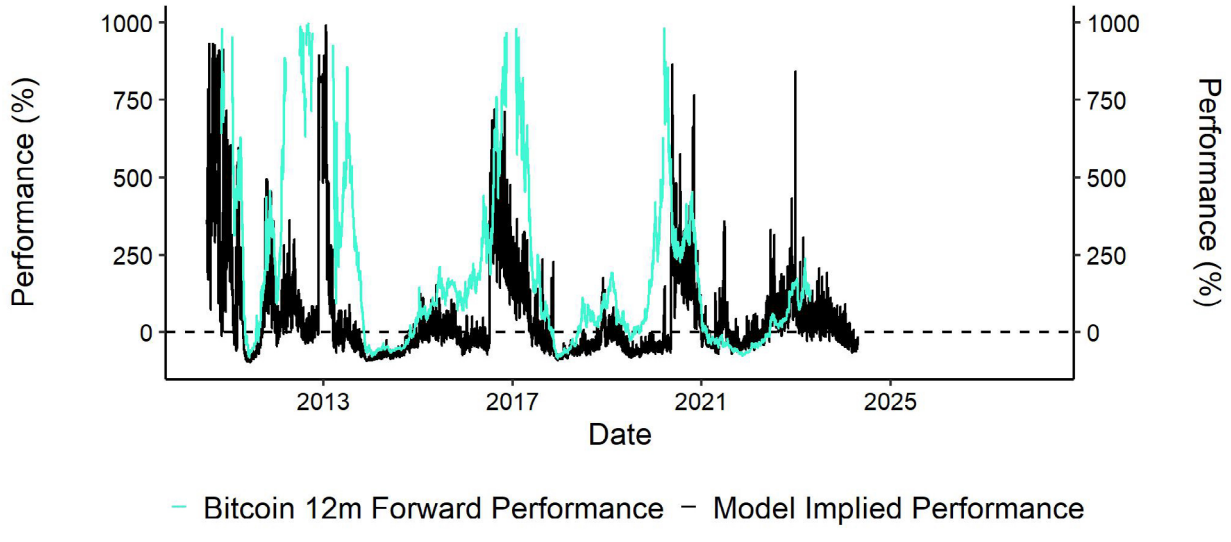
> "In fact, large deviations of the price of bitcoin relative to its stock-to-flow ratio have been associated with higher forward performances over the coming 12 months and vice versa.

1 A natural question that arises in the context of the discontinuation of the block subsidy beyond the year 2140 is how Bitcoin miners will be incentivized to secure the network. Beyond the date of the last block subsidy around the year 2140, miners will continue to be incentivized to secure the network through transaction fees that are also included in every block of transactions and which are also part of the overall block reward. In the very long term, increasing demand for block space on account of higher transaction throughput as well as demand for inscriptions is bound to lead to an increasing share of transaction fees of the overall block reward.

Bitcoin vs Stock-to-Flow (S2F) Model



Model implied performance vs 12m forward perfomance



Source: Coinmetrics, ETC Group; Past performance not indicative of future returns.

That being said, it is highly important to note that this model has been statistically invalidated on account of the fact that the stock-to-flow is a dependent variable that is dependent on (block) time itself. So, the stock-to-flow model suffers from statistical omitted variable bias (Kripfganz, 2020).

Production cost valuation approach to Bitcoin

Similar to a regular commodity, the production of bitcoins also inherits production costs which mainly consist of capital expenditures for Bitcoin mining hardware and operational costs for electricity.

However, most valuation approaches focus on the marginal cost of producing an additional bitcoin, hence focus on operational costs.

One of these approaches was put forth by Hayes (2016). Although his estimations are outdated, the general approach is still valid today. The general idea is to make assumptions about average hardware efficiency within the Bitcoin mining network and average electricity price paid by those miners.

Since the network's difficulty to find a Bitcoin block can be easily observed, the marginal electricity costs can be derived via the other two variables mentioned above. The approach is generally grounded in microeconomic theory that states that the equilibrium price should ultimately converge towards the marginal costs of production in a market with perfect competition.

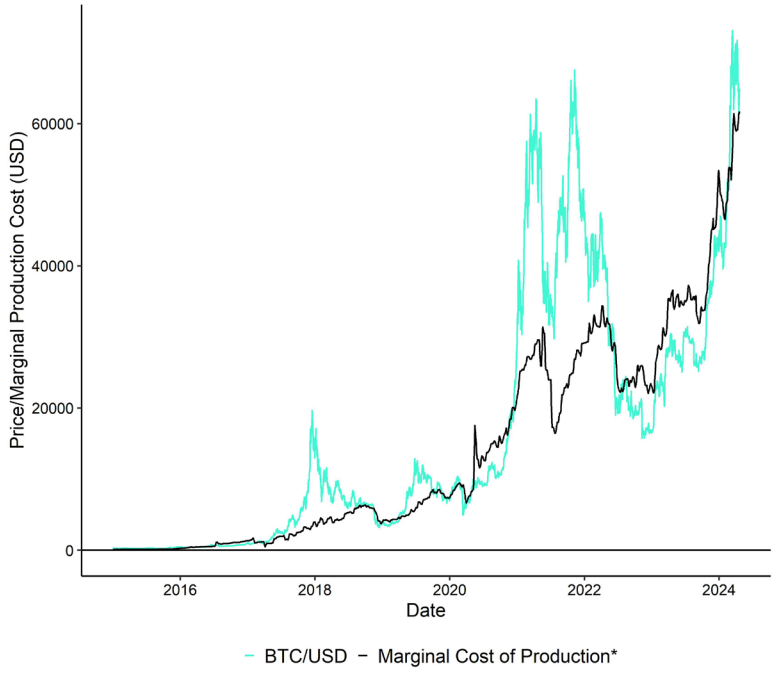
> At the time of writing, the marginal cost to produce a single Bitcoin amounts to around 59.9k USD based on an average electricity price of 0.079 USD/kWh.

As a caveat, the estimated model price is highly dependent on the assumed global average electricity costs (USD/kWh) which is cumbersome to estimate accurately on a global basis.

For instance, Hayes (2018) has assumed 0.135 USD/kWh. We have assumed a global average of 0.079 USD/kWh which is based on the average industrial price in the US in November 2023 according to the EIA.

Note that the global average retail electricity price is around 0.20 USD/kWh based on data by Statista so that the estimation above should serve as a rough (lower-bound) benchmark.

Bitcoin vs Marginal Cost of Production



Source: Coinmetrics, Cambridge Centre for Alternative Finance, ETC Group; *based on an average global electricity cost of 0.079 USD/kWh

On-Chain approaches to Bitcoin valuation

Puell Multiple

Another valuation approach related the economics of Bitcoin mining which leverages on-chain data is the so-called “Puell Multiple”.

The general idea is to identify periods of over- or undervaluation of Bitcoin based on the relative mining revenues that are dependent on transaction throughput, i. e. network activity, and also the price of Bitcoin (in USD) itself.

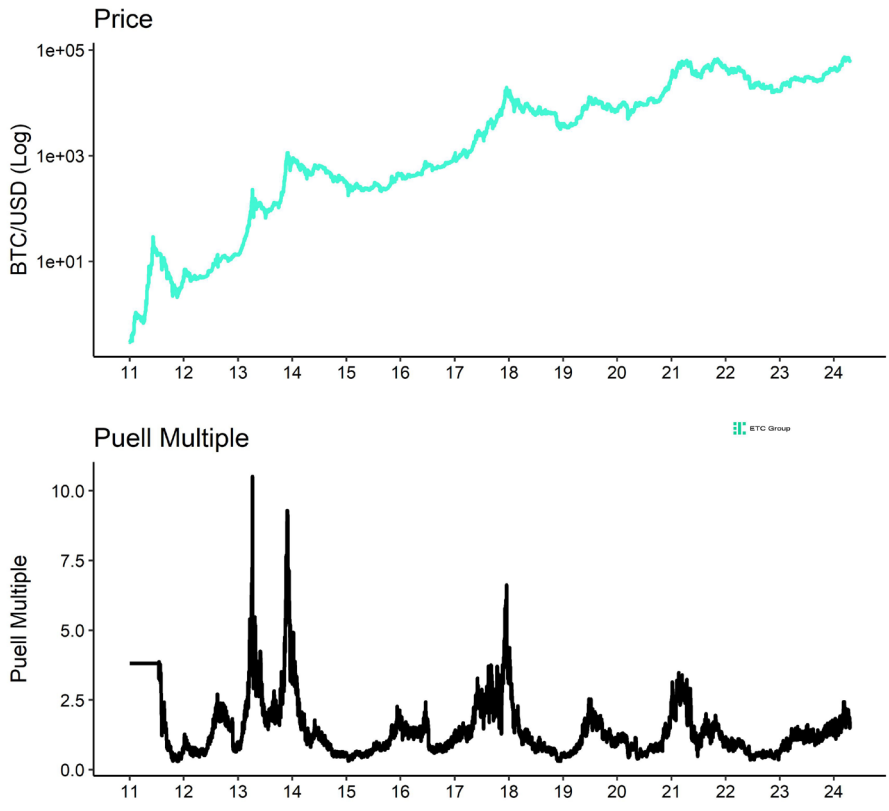
A detailed explanation can be found here.

If Bitcoin mining revenues diverge too far from the average over the past year, this could be a sign of excessive unsustainable transaction throughput which is likely to reverse. The same rationale can be applied to very low mining revenues relative to past year’s average which could be a sign for undervaluation.

More specifically, the Puell Multiple is defined as today’s value of coin issuance divided by the average value of coin issuance over the past 365 days.

Puell Multiple = Daily Coin IssuanceUSD / MA365 (Daily Coin IssuanceUSD)

Bitcoin: Price vs Puell Multiple



Source: Coinmetrics, ETC Group

Bitcoin on-chain cost basis (market value to realized value — MVRV)

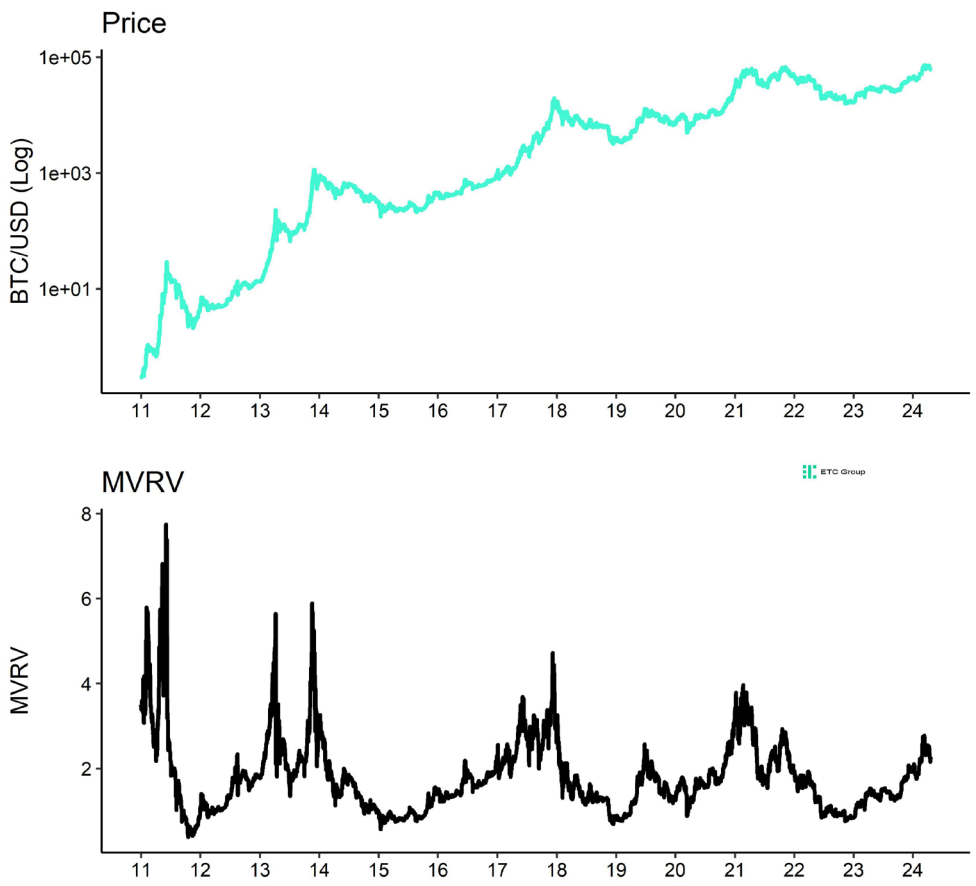
Similar to the way equities are valued, bitcoins can also be valued based on their on-chain cost basis or 'book value'. In this context, the on-chain cost basis is the price at which the respective bitcoins have been transferred last, which is usually different from the current market value which derives from most recent transaction prices on exchanges.

The former is also often referred to as "realized price" while the latter is simply referred to as "market price".

The ratio of market price to realized price or market value to realized value is also used a valuation indicator for Bitcoin which is similar to a price-to-book valuation approach applied in equities as book value is usually the acquisition cost at the time of initial purchase in the past.

Market value to realized value (MVRV) = current market price / realized price

Bitcoin: Price vs MVRV



Source: Coinmetrics, ETC Group

A composite valuation approach

As mentioned at the beginning of this chapter, beauty and valuations have one thing in common — they are always dependent on the eye of the beholder. As there is no conclusive answer whether Bitcoin is over- or undervalued from any single metric alone, it makes sense to draw conclusions from many different valuations approaches that value bitcoin from different angles.

A way to do so is to combine different valuation metrics into a single "composite valuation" metric. In our case, we have combined the following metrics:

- Bitcoin market value to realized value (MVRV)
- Stock-to-Flow deflection
- Thermocap Multiple
- Mayer Multiple
- Puell Multiple
- Market price to marginal cost of production
- Network valuation multiple

It is important to note that this is not an extensive list of valuation metrics. More and more valuation approaches are discovered every year which is why we have focused on the most-widely used ones in our opinion.

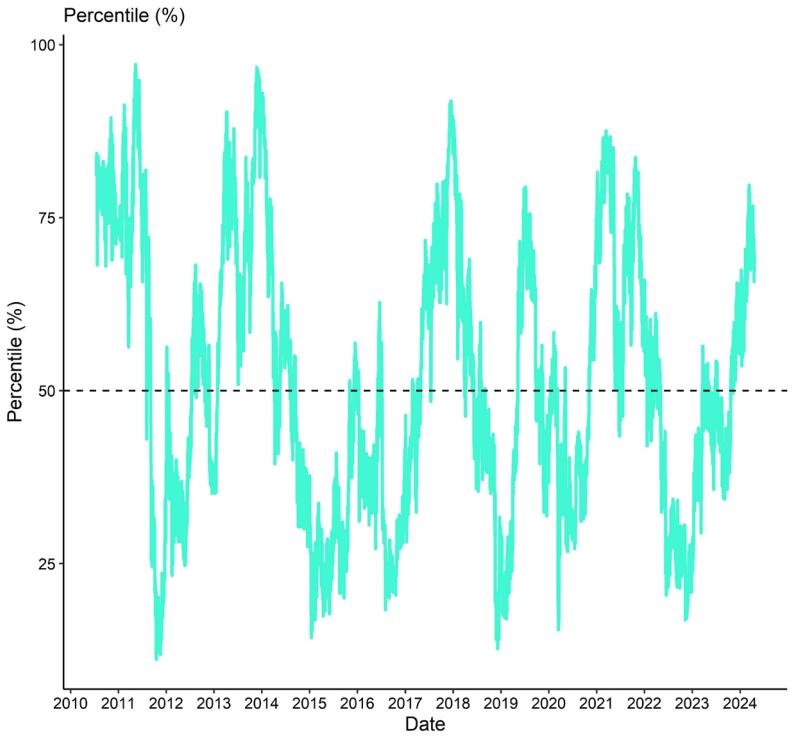
We used percentiles of the abovementioned valuation metrics in order to make them comparable to each other. Percentiles divide the observations into percentage values based on the relative frequency of the observations within the sample.

On the one hand, a 1% percentile implies that an observation was among the lowest 1% of the full sample of observations. On the other hand, a 100% percentile implies that an observation was among the highest observations within the full sample.

At the time of writing, Bitcoin appears to be moderately expensive based on the abovementioned array of indicators with an average percentile of 73%.

That being said, overall valuations are still far away from the highs observed during previous bull market tops in 2021, 2017, or 2013.

Bitcoin: Composite Valuation Indicator



Source: Coinmetrics, ETC Group

Is Bitcoin a hedge against sovereign default?

Unlike a centralized sovereign entity, Bitcoin is a decentralized global network. Moreover, transactions can be conducted permissionless and are not subject to censorship by a central authority. This renders assets held on the Bitcoin blockchain essentially unconfiscatable and counterparty risk-free.

The fiscal situation of major developed countries like the US or UK has come under more scrutiny more recently as debt-to-GDP ratios continue to be high while interest expenses are increasing rapidly on account of the recent tightening in monetary policy by the Fed and other major central banks.

As far as the US is concerned, annualized interest expenses have recently surpassed 1 trn USD which is more than the annual military spending, or the expenditures related to Medicaid. The Congressional Budget Office (CBO) forecasts that (gross) interest expenditures will likely reach 3 trn USD p. a. by the end of this decade while the annual budget deficit will continue to widen.[1]

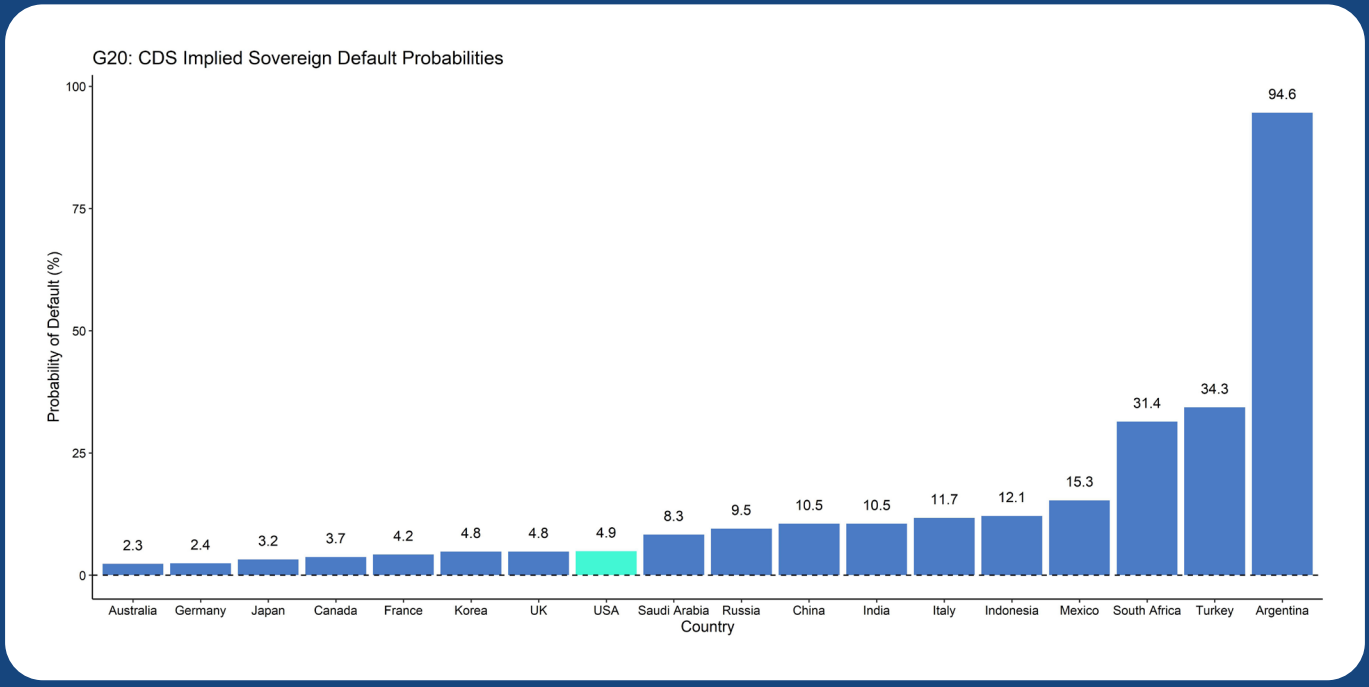
So, the probability of a sovereign default is likely going to increase.

In this context, Bitcoin can be viewed as an attractive hedge against a potential sovereign default as a censorship-resistant, permissionless and counterparty risk-free asset.

A modelling approach in this regard was also put forth by Foss (2021). The general idea is that, Bitcoin could act as a hedge against a basket of major sovereigns' debt/bonds. Theoretically speaking, if this was the case, Bitcoin's market cap should be equal to the current market value of this basket of sovereign debt multiplied by the weighted probability of default. In case of a cross default of all sovereign debt within the basket (100% default probability), Bitcoin's market cap should reach the same level as the market value of sovereigns it tries to hedge against.

The following chart shows the G20 sovereign's default probability implied by their 10-year CDS spreads.

Default probability over the next 10 years



Source: Bloomberg, ETC Group; assumed recovery rate of 0%; Data per 2024-03-28

1 https://www.cbo.gov/system/files/2024-02/59710-Outlook-2024.pdf

For instance, the market prices a default probability of around 4.9% for the US over the next 10 years. (We assume a 0% recovery rate, which tends to lead to even more conservative estimates in our case).

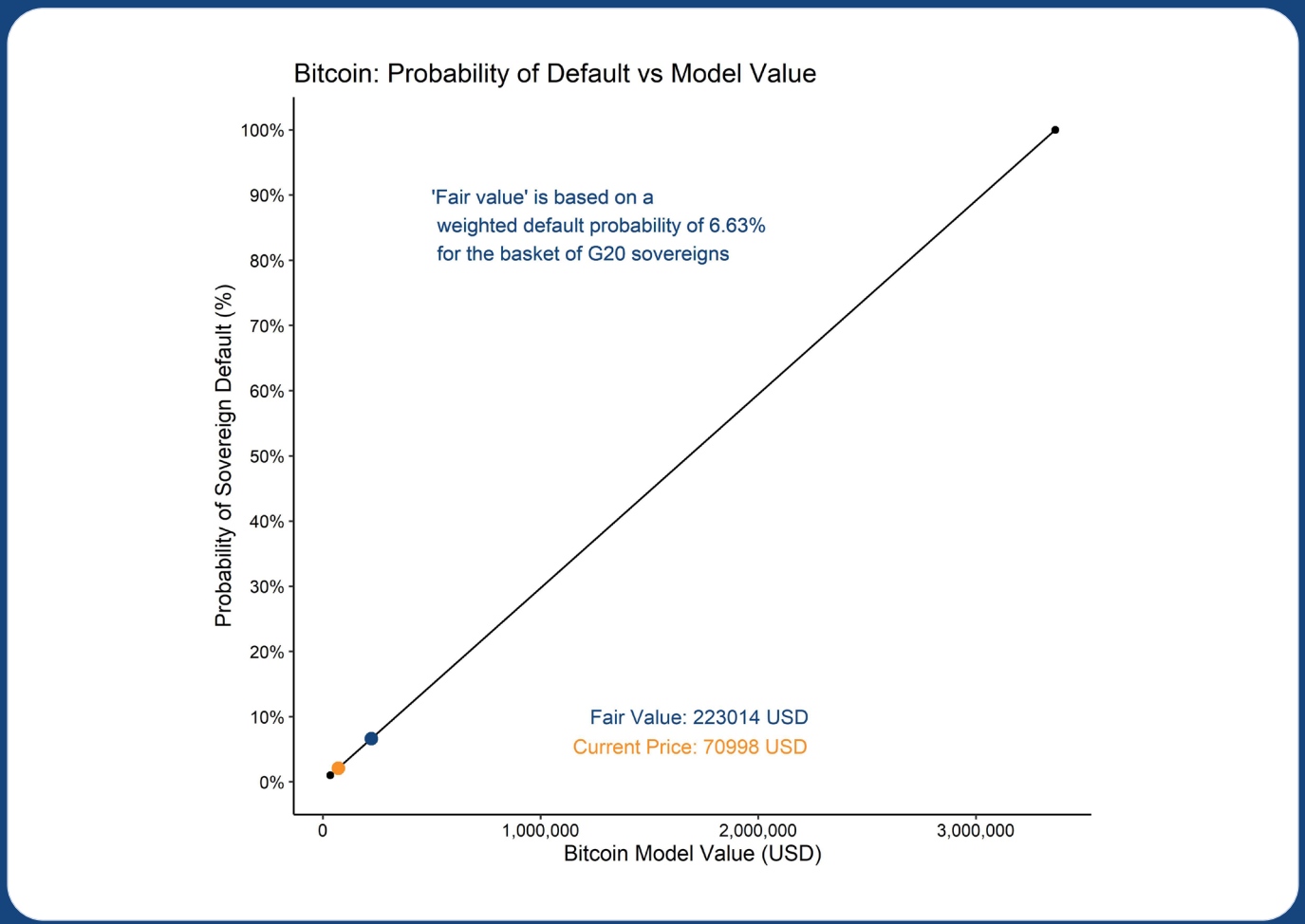
We multiply these probabilities by their respective market values of domestic and international sovereign debt, we get the theoretical market value of sovereign debt that is "at risk" and for which Bitcoin could serve as a hedge.

Based on this approach, the current "fair value" of Bitcoin would be around 223k USD per coin if it were to hedge the implied market value of G20 sovereign debt that is at risk.

The following chart shows the theoretical price of Bitcoin as a sovereign default hedge conditional on the weighted probability of default across all G20 sovereigns.

> "Hypothetically speaking, if all G20 sovereigns were to default simultaneously, Bitcoin's price could reach around 3.2 mn USD per coin based on this model.

Bitcoin's 'fair value' as sovereign default hedge is significantly higher than today



Source: Bloomberg, ETC Group; 'Fair value' based on a sovereign default model for G20 sovereigns; Greg Foss (2021); Data per 2024-03-28

The Investment Case for Bitcoin

From a pure investment point-of-view, Bitcoin has been one of the best performing “store-of-value” investments of the past 10+ years outperforming traditional assets like US equities or gold by a very wide margin.

Bitcoin has been one of the best performing assets of all time

Year	Bitcoin	S&P 500	Gold
2011	1316.7%	0%	10.1%
2012	217.9%	13.4%	7.1%
2013	5428.4%	29.6%	-28.3%
2014	-57.5%	11.4%	-1.4%
2015	36.2%	-0.7%	-10.4%
2016	120.3%	9.5%	8.1%
2017	1375.1%	19.4%	13.5%
2018	-73.8%	-6.2%	-1.6%
2019	94.8%	28.9%	18.3%
2020	305.1%	16.3%	25.1%
2021	59.8%	26.9%	-3.6%
2022	-64.3%	-19.4%	-0.3%
2023	157%	24.2%	13.1%
Year-to-Date	66.3%	10%	7.2%

Source: Bloomberg, ETC Group; Data available as of close 2024-03-28

This outstanding performance is mainly due to 2 main factors: Increasing global adoption and scarcity.

The following paragraphs will focus on these main drivers as well.

Global Adoption Trends

The adoption of cryptocurrency assets around the world shows a wide range of acceptance and regulatory stances by different countries. Some nations have welcomed digital assets, creating supportive regulatory environments, while others have taken a more cautious or even adversarial approach.

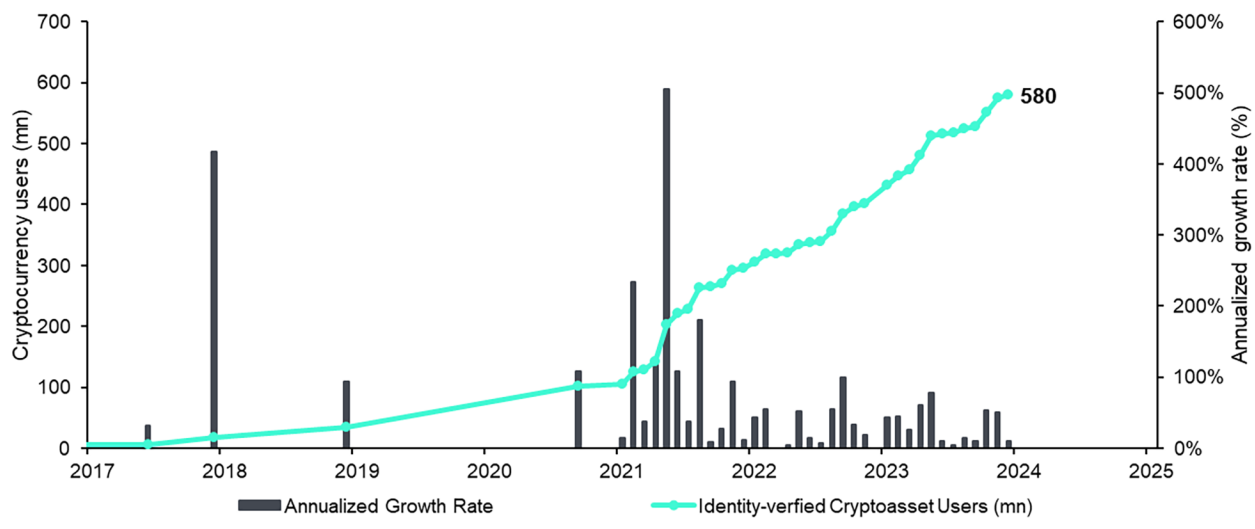
Countries like the United States, the United Kingdom, and Switzerland are seeing increased crypto asset adoption, supported by regulatory frameworks that foster the industry's growth. In the U. S., despite some uncertainty from the Securities and Exchange Commission (SEC) on unregistered securities offerings, efforts are being made to clarify crypto regulations, encouraging institutional investments. Switzerland is notable for its role as a centre for blockchain and crypto innovations, with its Crypto Valley recognized as a leading global entity in the sector.

Conversely, nations such as China and India have exhibited a more reserved stance towards crypto assets. China has prohibited initial coin offerings (ICOs) and has taken strict measures against cryptocurrency exchanges and mining, highlighting concerns over fraud and financial instability. In India, the Reserve Bank of India has banned banks from engaging with cryptocurrency businesses due to worries about money laundering and terrorism financing.

> The growth rate of global retail cryptocurrency adoption, focusing on ID-verified users, averages about 72% per annum. This adoption tends to accelerate in bullish market conditions and has peaked during the last two major bull markets in December 2017 and May 2021.

Despite these differences, the global trend leans towards an increasing adoption of cryptoassets.

Global ID-verified cryptocurrency users (mn)



Lower-bound estimate; Source: CJBS, Binance/CAF, Crypto.com, Triple-a io, ETC Group

There are an estimated 580 million ID-verified cryptocurrency users globally according to data estimated by Crypto.com, which is considered to be a conservative lower-bound estimate. Approximately 296 mn of those were Bitcoin users according to Crypto.com.

Previous research, such as that by the Cambridge Centre for Alternative Finance, suggests the actual number of users could be significantly higher, potentially around 870 million worldwide.

This discrepancy is due to many investors using methods that bypass Know-Your-Customer (KYC) and ID verification processes, such as anonymous wallets, receiving cryptocurrencies from other users, earning through mining or IT development, or peer-to-peer exchanges without a formal platform.

The current global retail adoption rate is approximately at 20.3% based on the latest estimates by Statista. This implies that around 1.2 bn people world-wide already hold some type of cryptoasset like Bitcoin.

Why adoption will increase over time — social dynamics of Bitcoin adoption

> “ People are impinging on other people and adapting to other people. What people do affects what other people do.
>
> Thomas Schelling

1 Network Effects

in economics where the usefulness or value that a user gains from a product or service increases with the number of other users utilizing similar goods or services. This effect, also referred to as network externality or demand-side economies of scale, usually results in a product becoming more valuable as more people join its network.

There are two kinds of network effects: direct and indirect. Direct network effects occur when the adoption of a product by a large number of users makes the product more valuable to each user. This is different from benefits derived from price reductions due to increased adoption. Examples of platforms exhibiting direct network effects include social media sites like Twitter and Facebook, as well as services like Airbnb, Uber, and LinkedIn, along with telecommunication tools such as telephones and instant messaging services.

Indirect (or cross-group) network effects arise when there are at least two distinct groups of customers that are interdependent, and the utility for at least one group increases as the other group (s) grow. An example of this is the increased value of hardware to consumers with the availability of more compatible software.

Thus, the spread of technology can be significantly influenced by network effects, making adoption self-reinforcing.

In the context of Bitcoin, the network effect implies that, as the Bitcoin network grows larger, adoption could accelerate as the size of the network could reinforce further adoption due to the higher utility that comes from using the network.

2 The Lindy Effect

The Lindy effect, or Lindy's Law, suggests that the future life expectancy of non-perishable entities, like ideas or technologies, is directly proportional to their current age. This means that the longer something has been around, the longer it is likely to continue existing. Longevity suggests a lower likelihood of becoming obsolete or being replaced. Originating from observations made at Lindy's Delicatessen in New York by comedians, the concept has been further explored by mathematicians and statisticians.

This effect does not apply to perishable entities, like humans, whose life expectancy does not increase with age. The Lindy effect is relevant to items without an inherent expiration date, indicating that the probability of a technology being adopted increases with its age.

In the context of Bitcoin, the Lindy Effect implies that the likelihood that Bitcoin will prevail increases with every day the network has been running successfully.

3 The Dunning-Kruger Effect

The Dunning-Kruger effect refers to the phenomenon where individuals with limited knowledge or skill in a particular area overestimate their competence. This cognitive bias demonstrates a systematic pattern of incorrect thinking or judgment. Biases are pervasive across various scenarios, and tendencies highlight specific patterns of thought or behavior observed among groups of individuals, although not necessarily manifested in every action.

In the context of technology adoption, the Dunning-Kruger effect can initially slow down the adoption process as people might underestimate new technology's capabilities and deem it irrelevant. However, as individuals invest time in understanding the technology, this effect can eventually lead to an accelerated adoption rate.

In the context of Bitcoin, the Dunning-Kruger Effect implies that, at the beginning of the adoption cycle, a high amount of (low-quality) critique and general aversion will be more likely than towards the end of the adoption cycle. A high amount of unfounded critique should be viewed as an indication for an early stage of the cycle.

Quantitative model of Bitcoin adoption

Some researchers have noticed that Bitcoin's price performance has been following a so-called power law very closely in the past.[1]

Power laws are particularly useful in explaining phenomena in which minor occurrences occur frequently but major ones are uncommon. Here are some common examples where power laws can be observed:

Cities

A power law can be used to characterise the distribution of city sizes when analysing the link between populations and cities. For example, the number of small towns and villages is far higher than that of large cities (such as megacities like Tokyo and New York). Nonetheless, a disproportionately large share of the population lives in these big cities. Here, the power law suggests that, according to a particular mathematical relationship, the frequency of cities declines as their size grows.

Large Corporations

A power law can also be used to describe how different business sizes are distributed inside organisations. There are far more small and medium-sized businesses (SMEs) than there are major organisations with a global presence and revenues greater than the GDPs of some nations. A power-law distribution is compatible with the size distribution of these firms, which tends to be composed of many smaller companies and fewer large ones based on factors like market capitalization, number of employees, or revenue.

Viruses

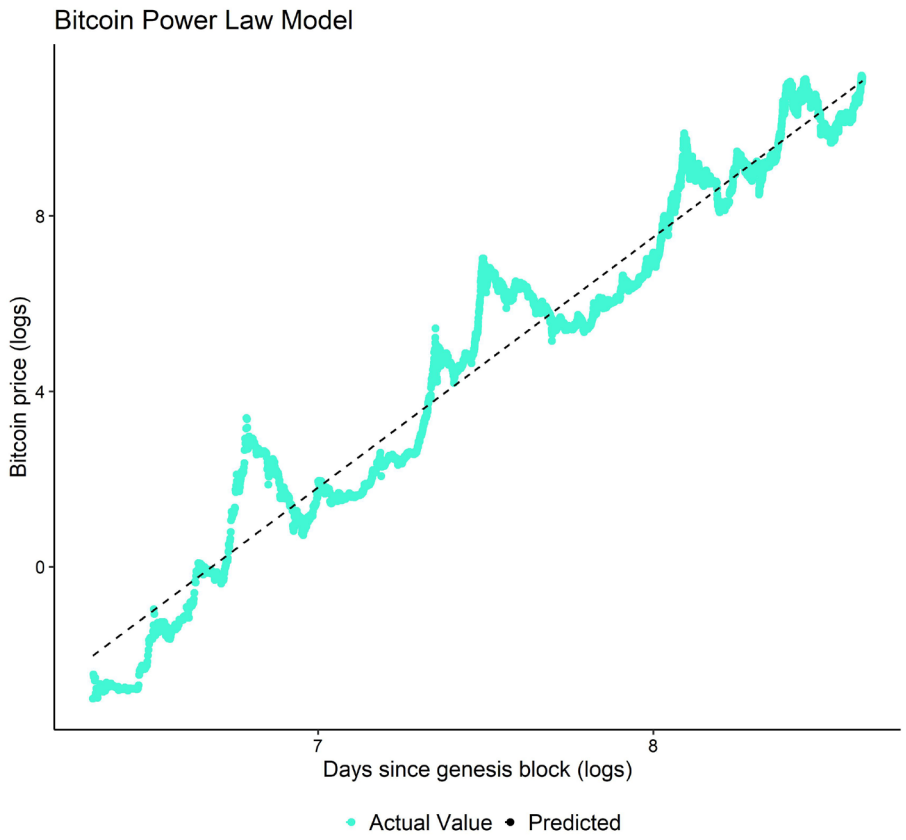
Power rules can be used to explain how viruses mutate or how epidemics spread. The theory is that while the majority of changes may not have much of an effect, a small number might drastically change the behaviour of the virus, making it more virulent or transmissible, for example. A power law can also be used to describe the distribution of outbreak sizes, with most outbreaks being little, localised episodes, but a small number having the potential to expand into broad pandemics that impact millions of people.

There has indeed been some research that implies that the adoption of Bitcoin as a monetary technology was spreading "like a virus".[2] In general, the propagation of a virus tends to follow a power law dependent on time passed since the first infection.

In fact, a closer look at the price evolution of Bitcoin reveals that the log of price has been increasing linearly with the log of time as expressed in terms of days since the Genesis block (3rd of January 2009).

1 Burger (2019)
2 Peterson (2019)

Bitcoin's price has followed a power law remarkably well

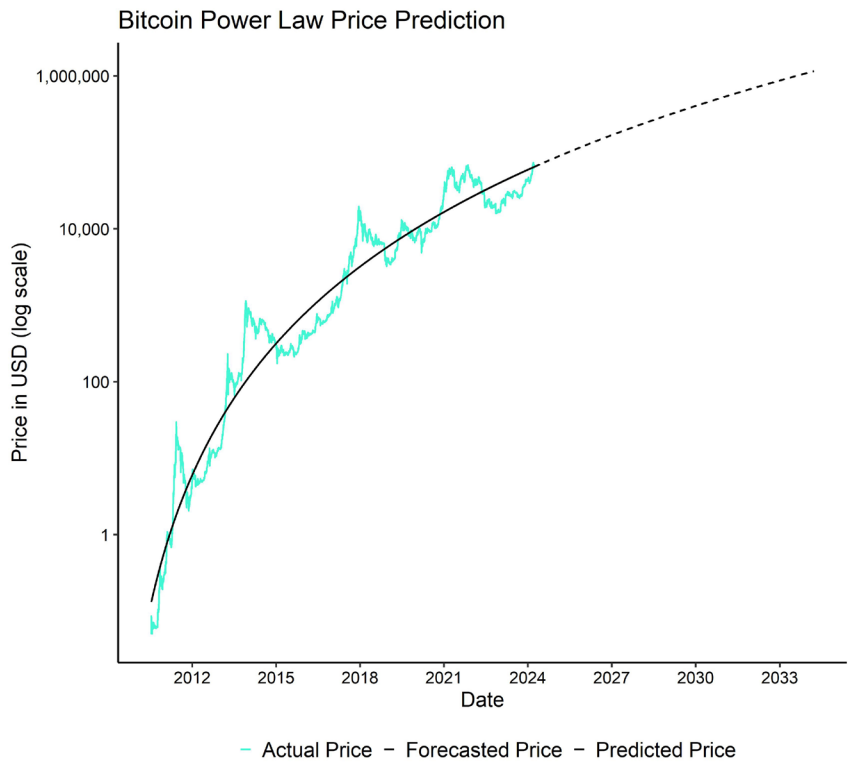


Source: Glassnode, ETC Group

What is more is that both the number of active addresses/users as well as the hash rate of the Bitcoin network also adhere to this power law.

If we assumed that Bitcoin adoption would continue to follow such a power law in the future, the next chart suggests that the price could reach 1 mn USD per one single Bitcoin over the next 10 years based on more wide-spread adoption of this technology.

If Bitcoin adoption continued to follow a power law, then the price could reach 1M USD early next decade



Source: Glassnode, ETC Group

The implication of Bitcoin following a power law is also that returns will decline marginally over time with increasing adoption and ultimately "saturation" of this adoption at some point in the future.

On a positive note, this also implies that risk/volatility will also tend to decline over the long term.

With increasing adoption, it is quite likely that Bitcoin's risk and volatility will also decline structurally over time.

The reason is that as market participants become more heterogenous over time, increasing dissent among buyers and sellers is bound to have a stabilizing effect on market prices and volatility.

Imagine a high-frequency trader that might sell a position on account of a short-term trading signal. In contrast, a longer-term buy-and-hold pension fund might see a short-term decline in price as a longer-term buying opportunity. Heterogeneity among investors has stabilized the price.

Increasing adoption and the Fractal Market Hypothesis — a case for lower volatility

In contrast, market instability usually occurs in environments with increasing consensus and homogeneity among investors, e. g. many investors selling at the same time on account of the same kind of information which can create price gaps/spikes.

This is also the logic of the so-called Fractal Market Hypothesis (FMH) put forth by Edgar Peters[1] which is considered to be an antithesis to the dominant Efficient Market Hypothesis. The FMH assumes investors to be heterogenous, to have imperfect information, and also different investment horizons.

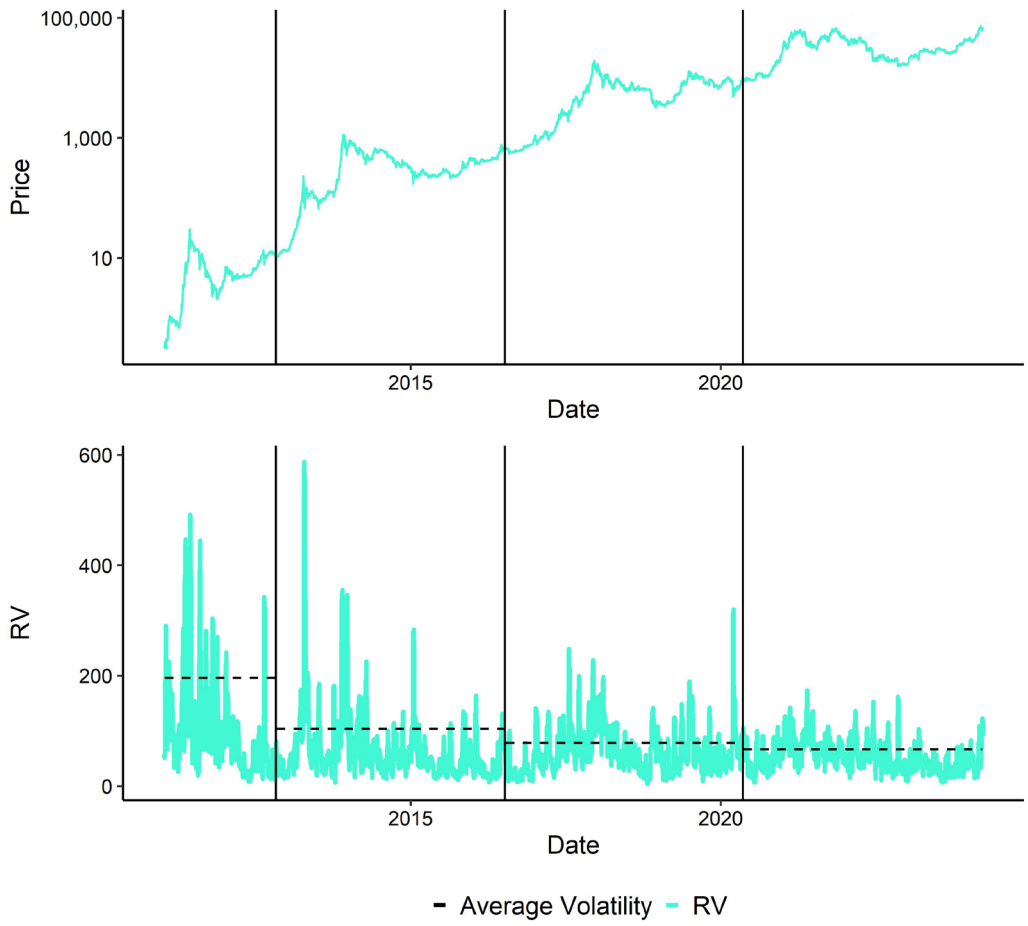
Peters (1994)

With respect to Bitcoin, increasing heterogeneity through wider adoption also implies structurally lower volatility over time.

The following chart shows Bitcoin's price performance (upper panel) and its realized volatility (lower panel) over time. The horizontal lines represent the dates of the Bitcoin Halvings.

As one can see, Bitcoin's volatility has been decreasing structurally over time with every Halving.

Bitcoin's average volatility has been decreasing structurally over time with every halving



Sample: 2011-01-14 until 2024-03-22; Source: Glassnode, ETC Group

Bitcoin Halvings, which were usually followed by significant price appreciations in the past, can also be a significant driver of adoption itself as adoption usually lags increases in price.[1]

The positive investment implication is that the risk characteristics of Bitcoin will continue to change over time.

As adoption rises, Bitcoin will likely evolve from a risky asset with high volatility to a safe-haven asset with low volatility over time.

The effect of those Halvings on Bitcoin's price performance will be analysed in the following chapter.

1 Auer et al. (2022)

Modelling Bitcoin's increasing scarcity over time

The Bitcoin Halving stands out as the most eagerly awaited occurrence in the realm of Bitcoin and other cryptocurrencies.

This event halves the block subsidy, meaning the reward that miners get for securing the blockchain by finding the correct hash. Consequently, this leads to a 50% reduction in the rate of new bitcoin creation.

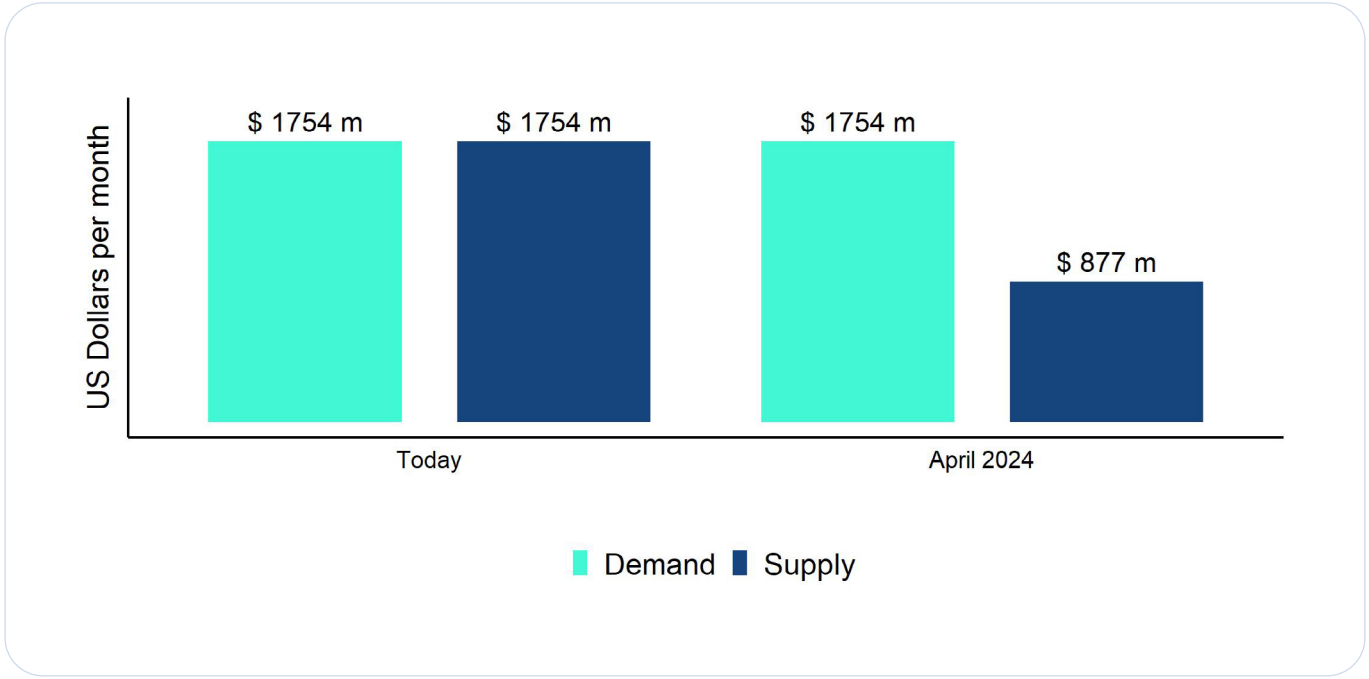
The Halving is a crucial aspect of Bitcoin's design, promoting a gradual decrease in the rate of new supply and guaranteeing that the total number of bitcoins will not exceed 21 million. The Halving is hard-coded into the Bitcoin algorithm to occur every 210,000 blocks which is around every 4 years.

Since Bitcoin's inception, there have been three such Halving events in 2012, 2016, and 2020, successively reducing the block subsidy from 50 BTC to 25 BTC, then to 12.5 BTC, and most recently to 6.25 BTC.

> "The Halving event is essentially a supply shock to the system.

As of this writing, the next Halving is anticipated to happen around April 20, 2024, at about 18:20 GMT, given the average block time remains at 10 minutes. This upcoming event will see the block reward diminish further to 3.125 BTC, leading to a daily output drop from approximately 900 BTC to about 450 BTC, assuming blocks continue to be mined every 10 minutes." with this "The Halving has occurred on the 20th of April at 02:09:27 UTC. This event has effectively halved the block reward again to 3.125 BTC per block, leading to a daily output drop from approximately 900 BTC to 450 BTC.

Bitcoin Halving event is best understood as a supply shock

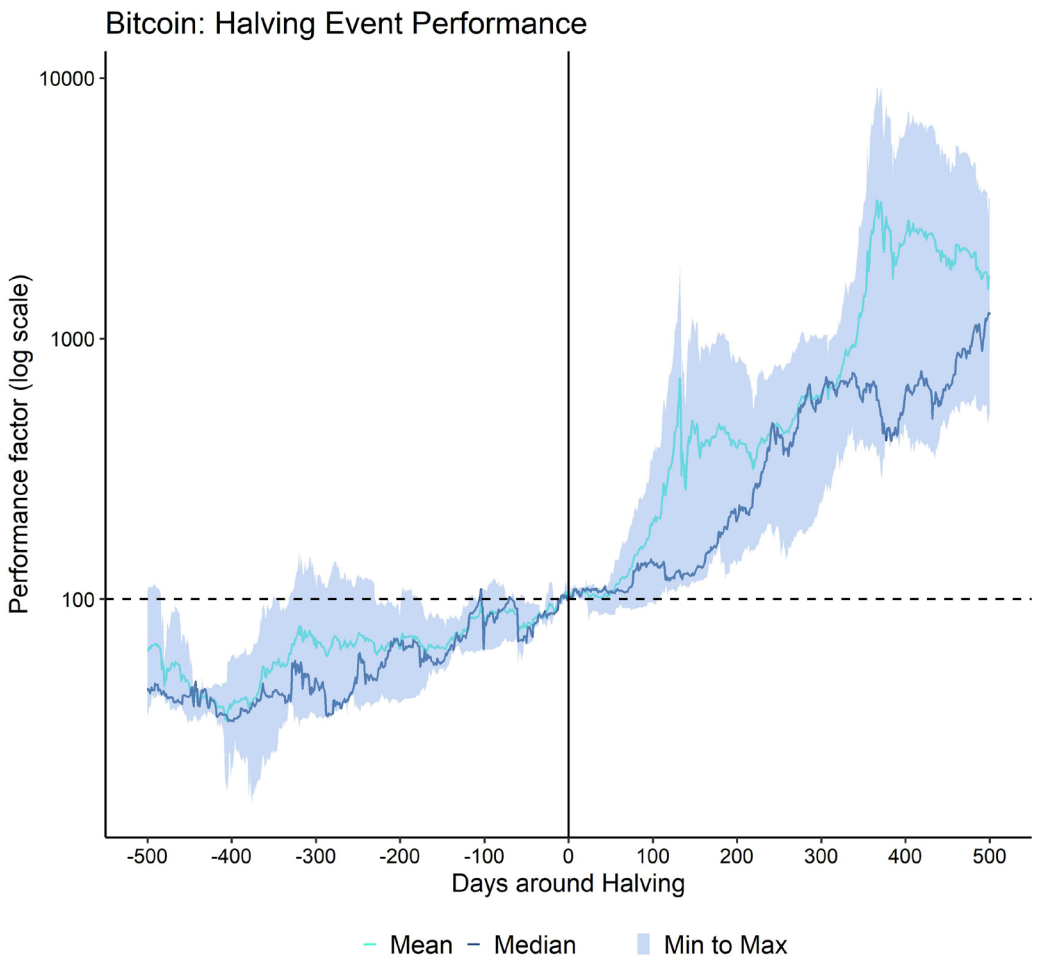


Source: Glassnode, ETC Group; Chart for illustrative purposes only; Data available as of close 2024-03-27

Should demand for bitcoins stay steady, the decrease in bitcoin supply is expected to push up its equilibrium price — the price must rise to balance the reduced supply.

Historical precedents show that Bitcoin's price surged significantly in the months following past Halvings. On average, Bitcoin's value increased approximately 17 times, or 1800%, 500 days post-Halving, based on the last three occurrences.

Halving events have led to significant price appreciations in the past



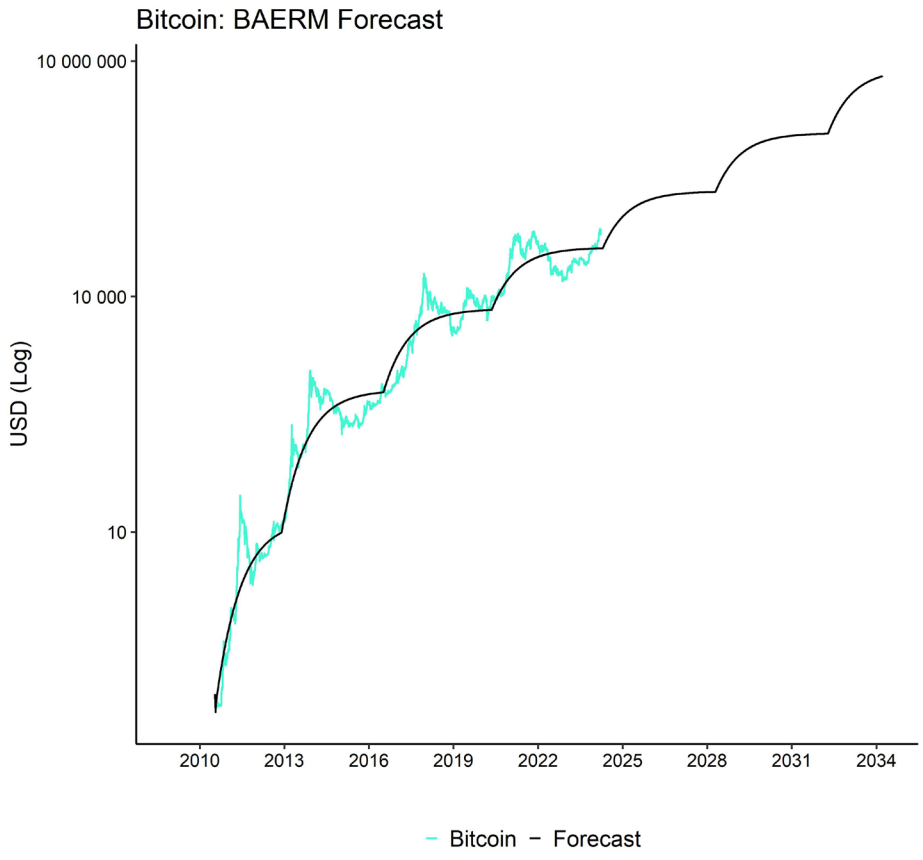
Source: Glassnode, ETC Group; Results based on the previous Halvings in 2012, 2016, and 2020

Although standard theories of capital market pricing and information theory would suggest that this event should already be priced in, our findings suggest that the very significant price performance that followed the Halvings are unlikely to be a random phenomenon (learn more in our recent research blogpost).

Overall, we anticipate that prices will trend towards a higher equilibrium value in the years following 2024, influenced by the Halving's positive impact and the ensuing increase in scarcity.

> According to our projections, Bitcoin's equilibrium price may rise to $ 103,000 by the close of 2024, reach $ 172,000 by the end of 2025, and potentially hit $ 215,000 by the culmination of the next Bitcoin cycle in 2028.

Bitcoin: Steady increase in scarcity will provide a tailwind for price appreciations



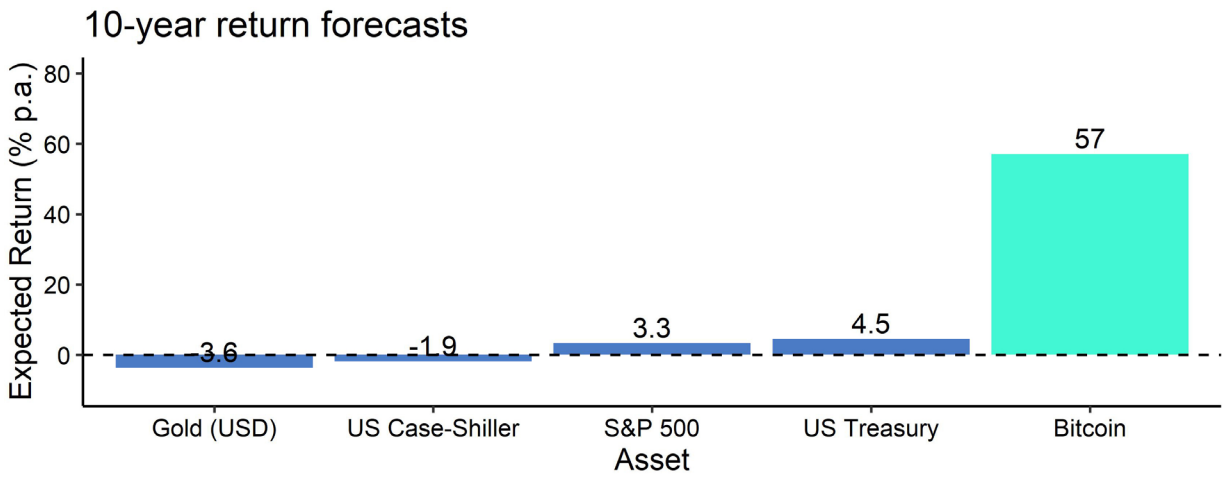
Source: Coinmetrics, ETC Group; BAERM = Bitcoin Autocorrelated Exchange Rate Model

Our analysis further suggests that the impact of the Halving will unfold progressively, reflecting over time as the supply shortfall created by the event gradually intensifies.

Based on the abovementioned model for Bitcoin's increasing scarcity, Bitcoin exhibits significantly higher long-term expected returns than traditional assets such as equities, bonds, gold, or real estate:

> Thus, we infer that the market has not yet fully incorporated the Bitcoin Halving into its pricing.

Bitcoin exhibits significantly higher long-term expected returns than traditional assets



Source: Various sources used for estimations; own calculations; ETC Group; data as of 2024-03-27

In the very long-term, we expect Bitcoin to dematerialize traditional stores-of-value like gold and US Treasuries on account of this increasing scarcity and supremacy as monetary asset.

Gold is likely to be technologically disrupted as store-of-value on account of the reasons outlined in the first chapter, i. e. the combination of spatial and temporal transferability of Bitcoin which is not applicable to gold.

US Treasuries, which have essentially leapfrogged gold as a store-of-value in the post-Bretton Woods fiat monetary system, will be disrupted on account of the likely worsening fiscal situation of the US that have historically led to financial repression and loss in the real value of Treasuries.

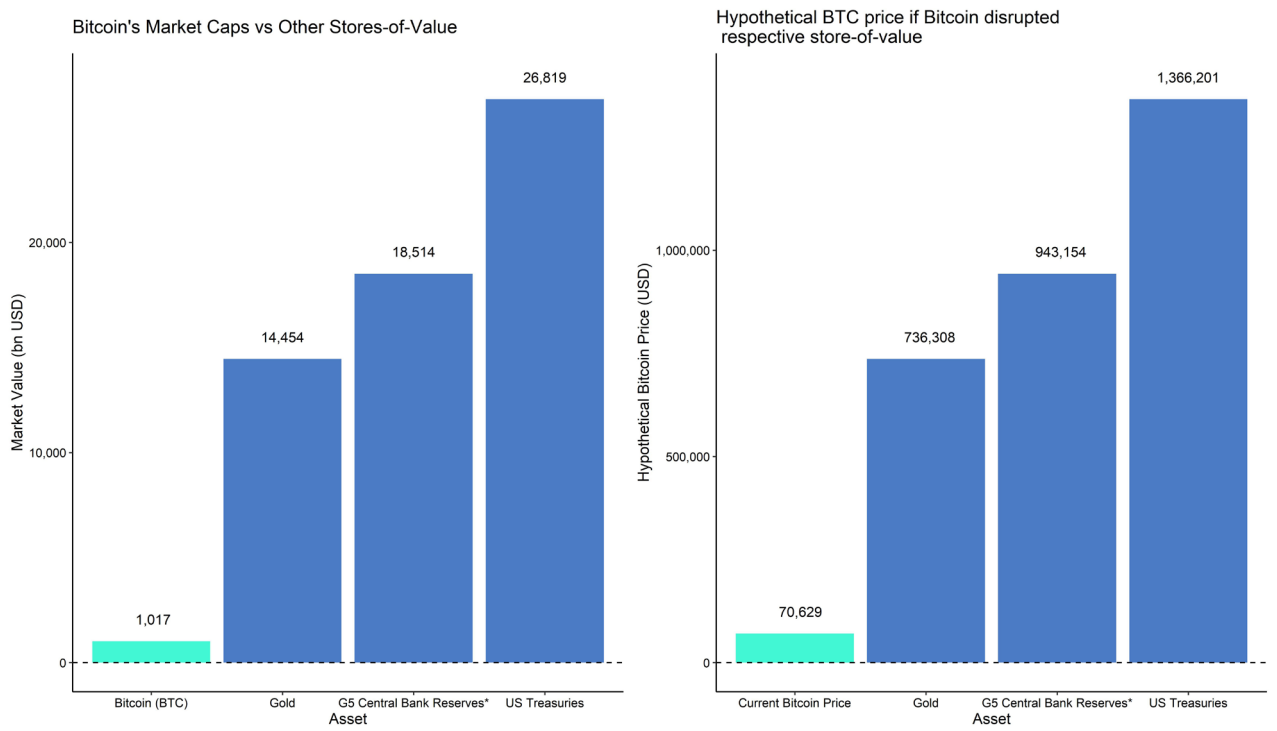
The potential investment implication of such a scenario for Bitcoin are vast:

Hypothetically speaking, if Bitcoin disrupted gold as the primary store-of-value and achieved a similar market cap like gold today, this would imply a theoretical price for 1 single Bitcoin of approximately 736k USD.

In addition, if Bitcoin disrupted US Treasuries as the primary store-of-value and achieved a similar market cap like US Treasuries today, this would imply a theoretical price for 1 single Bitcoin of approximately 1.4 mn USD.

This is not a far-fetched scenario. As has been demonstrated previously, Bitcoin will become almost 10 times as scarce as gold by the year 2032 based on the stock-to-flow ratio and will continue to become even scarcer over time in the future. We expect this increasing scarcity of Bitcoin to go hand in hand with an increasing monetary premium of Bitcoin at the expense of other traditional stores-of-value.

Bitcoin has significant performance potential if it catches up to traditional stores-of-value



Source: Bloomberg, ETC Group; *G5 = Fed, ECB, BoJ, BoE & PBoC; data as of 2024-03-28

In general, Bitcoin will likely continue to "cannibalize" on the monetary premium inherent in other traditional stores-of-value such as gold or real estate as outlined in one of our previous reports.

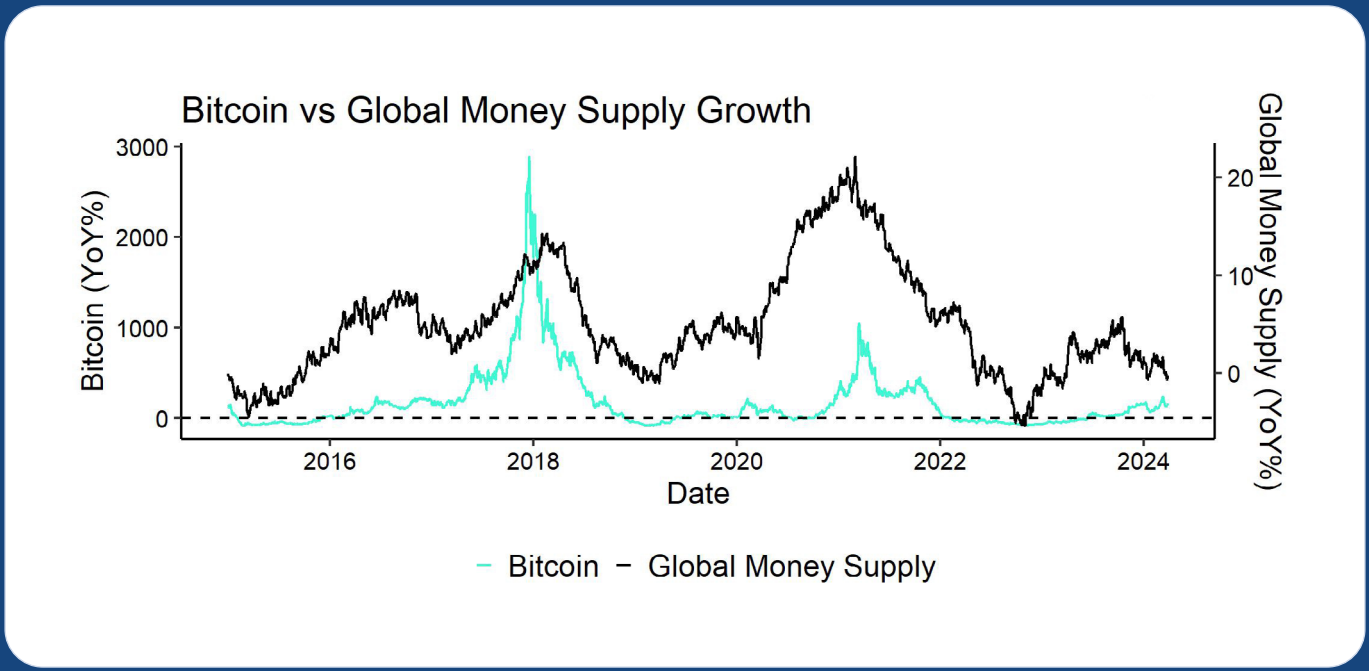
Is Bitcoin an Inflation hedge?

Bitcoin is a scarce digital asset. The algorithm dictates not only a gradual reduction in price-inelastic supply growth but also an ultimate limit of its circulating supply that will converge towards 21M coins in the long run.

The absolute scarcity of Bitcoin combined with its disinflationary supply growth schedule makes it a potential candidate as a hedge against inflation.

In fact, Bitcoin's performance has shown a closer correlation to global money supply growth, i.e. global monetary inflation over time.

Bitcoin's performance tends to be tightly correlated with global money supply growth



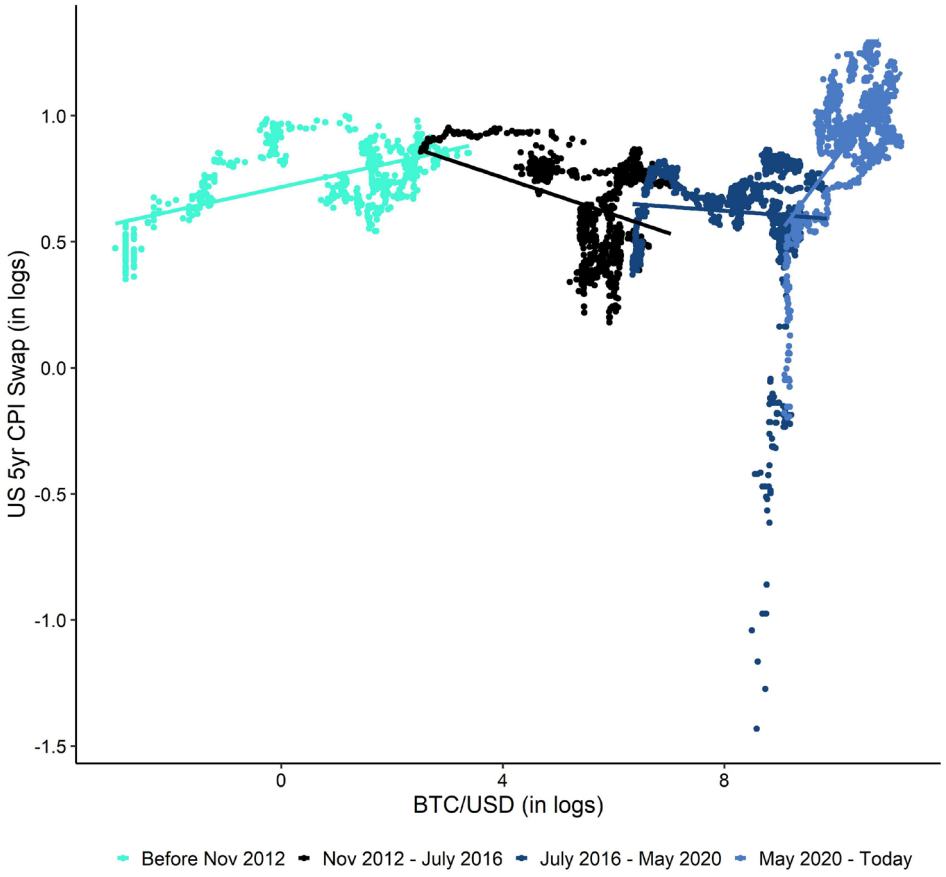
Source: Bloomberg, ETC Group

What is more is that Bitcoin has shown an increasing sensitivity to market-based inflation expectations such as medium-term US CPI swap rates or US TIPS break-even rates.

In this context, it is important to note that Bitcoin has not always shown this close correlation to inflation expectations: The earlier epochs of Bitcoin, i. e. from its inception in 2009 until around 2020, Bitcoin's price has shown little correlation to market-based inflation expectations.

This has significantly changed since the Covid crisis and the resulting monetary and fiscal stimuli which also coincided with the latest Halving event which happened in May 2020.

Bitcoin is becoming increasingly sensitive to US inflation expectations



Source: Bloomberg, ETC Group

We expect this sensitivity to inflation expectations to increase even further with an increasing supply scarcity of Bitcoin going forward.

In this context, easing US monetary policy amid high US fiscal deficits and increasing inflation expectations could provide an additional tailwind for Bitcoin going forward.

The reason is that countries with higher inflation rates tend to see an increasing adoption of Bitcoin as a store-of-value as well.[1] In general, countries with high inflation tend to show higher rates of cryptoasset adoption as well. The highest adoption rates tend to be observed in emerging markets which tend to have structurally higher rates of inflation rates as well.[2]

1 Bloomberg: Bitcoin Is Trumping Dollars for Many Inflation-Weary Argentines, March 19, 2024; Link: https://www.bloomberg.com/news/articles/2024-03-19/bitcoin-gains-dim-argentines-dollar-refuge-with-276-inflation?embedded-checkout=true
2 De Best (2024): Annual cryptocurrency adoption in 56 different countries worldwide 2019—2023; Link: https://www.statista.com/statistics/1202468/global-cryptocurrency-ownership/

“Get off zero”: A small Bitcoin portfolio allocation goes a long way

An increasing market cap of Bitcoin relative to other traditional assets is also bound to result from an increasing percentage of allocation by institutional investors.

Most recent institutional surveys among professional investors imply a portfolio allocation in digital assets of only 1.3% which includes Bitcoin but also other digital assets.[1]

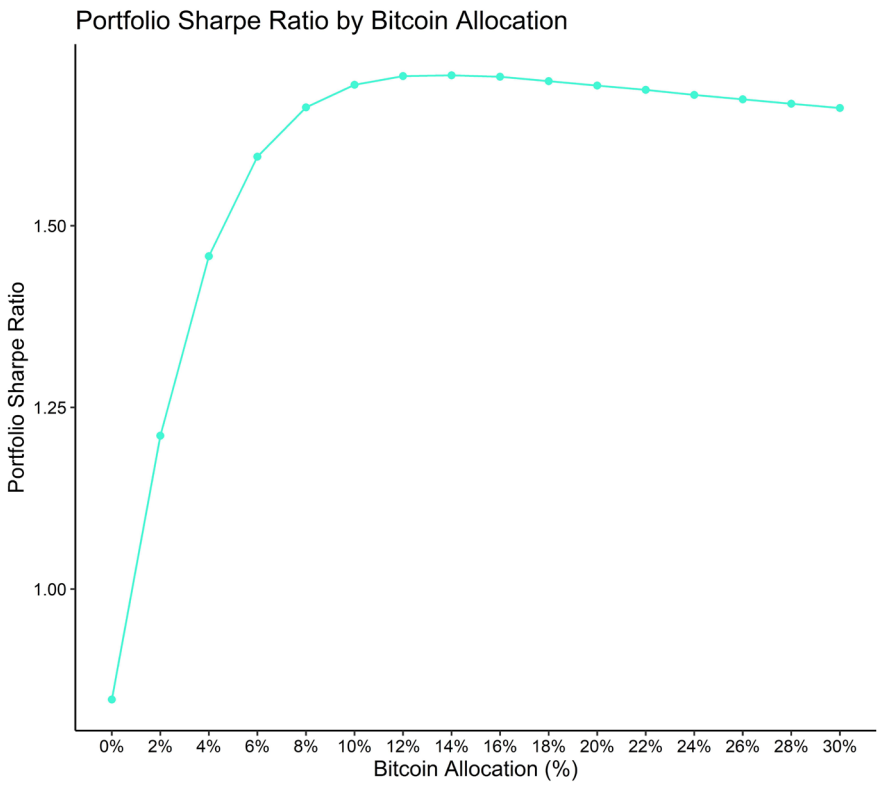
Utilizing the latest data provided by ICI, the data imply that approximately 8.1 trn USD in assets are currently invested into US passive ETFs alone.[2]

At the time of writing, approximately 57.8 bn USD is invested into US Bitcoin ETFs, both spot- and derivatives-based.

This currently implies a percentage of only 0.7% of US Bitcoin ETFs in total US ETFs.

However, we expect this percentage to increase significantly in the future. The reason is that the optimal allocation to Bitcoin in a multiasset stock-bond portfolio which maximized risk-adjusted returns (Sharpe Ratio) in the past, was between 12% to 16%.

The optimal Bitcoin allocation in a global stock-bond portfolio has been between 12% and 16%



Source: Bloomberg, ETC Group; Monthly rebalancing; Sharpe Ratio was calculated w/ 3M USD Cash Index as risk-free rate; BTC allocation is taken out of equity allocation of 60%, bond allocation remains at 40%; Sample: July 2010 - Today

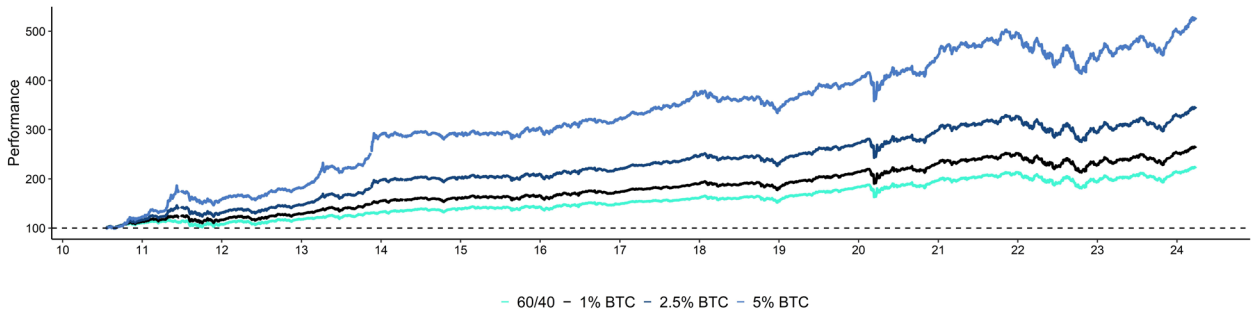
1 Coinshares Digital Asset Fund Manager Survey, Feb 2024
2 Data as of end of January 2024; source: Bloomberg

Note that these percentages may change conditional on sample period considered and/or rebalancing frequency of the multiasset portfolio.

However, the key takeaway is that the optimal allocation is probably well above 1% which is also corroborated by recent announcements from major US university foundations.

In fact, a small addition of Bitcoin to a multiasset consisting of global equities and bonds has led to a significant increase in portfolio returns with only a minor increase in portfolio volatility. As a result, risk-adjusted returns (Sharpe Ratio) were significantly increased by minor increases in Bitcoin allocation.

Multiasset Performance with Bitcoin (BTC)



	60/40 Portfolio	1% BTC	2.5% BTC	5% BTC
Cumulative Return (%)	224.9	266.2	346.5	527.9
Annual Return (% p.a.)	10.2	12.5	16.2	22.2
Volatility (% p.a.)	10.5	10.6	11.1	12.7
Sharpe Ratio	0.85	1.04	1.29	1.54
Max Drawdown (%)	15.2	15.7	16.4	21.4

Source: Bloomberg, ETC Group: Monthly rebalancing; Sharpe Ratio was calculated with 3M USD Cash Index as assumed risk-free rate; BTC allocation is taken out of equity allocation of 60%, bond allocation remains at 40%; Past performance not indicative of future returns.

> In other words, investors were more than compensated for the additional risk taken by investing into Bitcoin.

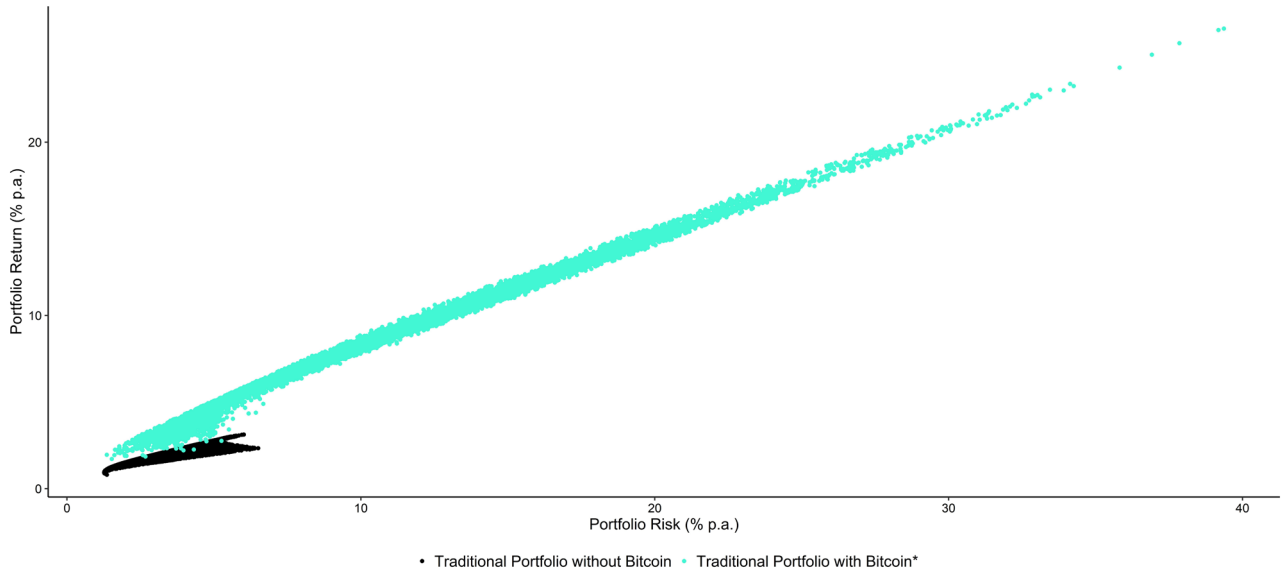
Generally speaking, allocations into Bitcoin not only increase risk-adjusted returns in multiasset portfolios. The addition of Bitcoin can also enhance the general set of possible investment portfolios by increasing the so-called “efficient frontier” significantly.

In this context, a multiasset portfolio is considered to be more “efficient” if it offers a higher return for the same amount of risk.

The inclusion of Bitcoin into multiasset portfolios has the potential to push the boundaries of the potential universe of efficient portfolios by allowing a vastly broader set of risk-return profiles.

All in all, we therefore conclude that no allocation to Bitcoin is probably suboptimal.

Efficient Frontiers: Multi-asset Portfolios with and without Bitcoin



Source: Bloombera. ETC Group: *Efficient frontier based on a simulation of 10000 multiasset portfolios consisting of global equities, bands, and commodities with varying allocations to Bitcoin (BTC). Sample: July 2010 - Today

Conclusion

In the comprehensive analysis presented in this report, we have explored the multifaceted investment case for Bitcoin, a groundbreaking digital asset that has redefined the boundaries of financial technology and investment opportunities. With its inception rooted in profound cryptographic advancements and a quest to solve enduring challenges in digital transactions, Bitcoin has emerged not merely as a technological triumph but as a pivotal player in the financial domain, offering unprecedented opportunities for investors.

The evolution of Bitcoin from a niche cryptographic experiment to a globally recognized and adopted digital asset underscores its resilience, innovation, and the growing acknowledgment of its unique value proposition among professional investors. This journey, marked by the pioneering work of Satoshi Nakamoto and the continuous enhancements through Bitcoin Improvement Proposals, highlights Bitcoin's adaptability and its capacity to address challenges of scalability, security, and decentralization, thus reinforcing its standing in the investment landscape.

Our exploration has shed light on Bitcoin's inherent characteristics — decentralization, scarcity, and security — augmented by the rigor of proof-of-work and the strategic implementation of halving events. These features not only differentiate Bitcoin from traditional and digital assets but also underline its potential as a hedge against inflation and financial instability. The analysis of Bitcoin's adoption trends, network effects, and its increasing relevance in the context of global economic uncertainties further cements its role as a compelling store of value and medium of exchange.

The investment thesis for Bitcoin is further bolstered by its impressive historical performance, resilience against sovereign default risks, and its emerging status as a viable alternative to traditional safe-haven assets like gold and US Treasuries. Through a meticulous examination of valuation models and on-chain analytics, this report presents a robust framework for understanding Bitcoin's market dynamics and its long-term value proposition.

In conclusion, the investment case for Bitcoin presents a compelling narrative of innovation, resilience, and growing acceptance. As Bitcoin continues to evolve and mature within the financial ecosystem, it offers a unique combination of scarcity, security, and potential for significant returns, making it an indispensable component of a diversified investment portfolio. The increasing adoption by institutional investors, coupled with the potential for Bitcoin to disrupt traditional stores of value, underscores the necessity of considering Bitcoin within the broader context of investment strategies.

In light of the evidence and analysis presented, we advocate for a prudent yet forward-looking approach to Bitcoin investment, recognizing its potential to enhance portfolio performance, hedge against systemic risks, and capitalize on the transformative possibilities of digital assets. As we navigate the evolving landscape of finance and technology, Bitcoin stands out as a beacon of innovation, offering both challenges and opportunities for the astute investor.

In case of questions about Bitcoin or any content in our report,
feel free to contact our research team via research@etc-group.com.

Bitcoin Investment Strategies

ETP Group offers a number of strategies to gain exposure to the investment opportunity of Bitcoin

Core Bitcoin

ETC Group Core Bitcoin is a first of its kind spot Bitcoin ETP specifically designed for benchmark conscious, long-term buy and hold investors and global institutional investors with extended liquidity and risk management needs.

Primary ticker	BTC1
ISIN	DE000A4AER62
WKN	EUR, USD
TER	0.30 % p.a.

Learn more →

Physical Bitcoin

ETC Group Physical Bitcoin is Europe's largest and most traded Bitcoin ETP*, ideal for investors with shorter time horizons. BTCE was the first crypto ETP to be listed on Deutsche Börse XETRA in June 2020.

Primary ticker	BTCE
ISIN	DE000A27Z304
WKN	EUR, USD, GBP, CHF
TER	2.00 % p.a.

Learn more →

*Bloomberg, data as of April 2024

All of ETC Group's Crypto ETPs are domiciled in Germany and provide transparency, security, and peace of mind to investors seeking exposure to digital assets.

References

- 100trillionUSD. (2019). Modeling Bitcoin's value with scarcity. Medium. Retrieved from https:// medium.com/@100trillionUSD/modeling-bitcoinsvalue-with-scarcity-91fa0fc03e25
- Ammous, S. (2018). The bitcoin standard: the decentralized alternative to central banking. John Wiley & Sons.
- Ammous, S. (2021). The Fiat Standard: The Debt Slavery Alternative to Human Civilization. United Kingsom: Scribe Media.
- Auer, R., Cornelli, G., Doerr, S. Frost, J. and Gambacorta, L. (2022). Crypto trading and Bitcoin prices: evidence from a new database of retail adoption (BIS Working Papers No. 1049). Bank for International Settlements. Link: https://www.bis.org/publ/work1049. htm
- Bloomberg: Bitcoin Is Trumping Dollars for Many Inflation-Weary Argentines, March 19, 2024; Link: https://www.bloomberg.com/news/articles/2024-03-19/bitcoin-gains-dim-argentines-dollar-refuge-with-276-inflation?embedded-checkout=true
- btconometrics. (2023). The Bitcoin autocorrelation exchange rate model: A novel two-step approach. Medium. Retrieved from https://archive. is/3XfkY
- Burger, H. C. (2019) Bitcoin's natural long-term power-law corridor of growth, Medium. Link: https://medium.com/quantodian-publications/bitcoins-natural-long-term-power-law-corridor-of-growth-649d0e9b3c94
- Cerf, V. G., & Kahn, R. E. (1974). A protocol for packet network intercommunication. IEEE Transactions on Communications, 22 (5), 637—648.
- Coinshares Digital Asset Fund Manager Survey, Feb 2024; Link: https://coinshares.com/de/research/digital-asset-quarterly-fund-manager-survey-feb-24
- Cryptopoiesis (2019, April 5). The Puell Multiple. A New Barometer of Bitcoin's Market Cycles. Medium. https://medium.com/unconfiscatable/the-puell-multiple-bed755cfe358
- De Best (2024): Annual cryptocurrency adoption in 56 different countries worldwide 2019—2023; Link: https://www.statista.com/statistics/1202468/global-cryptocurrency-ownership/
- Diffie, W., & Hellman, M. (1976). New directions in cryptography. IEEE Transactions on Information Theory, 22 (6), 644—654.
- Dragosch, A. (2020) "Which Macro Factors explain the price of Bitcoin?" Medium; Link: https://medium.com/@andre-dragosch/which-macro-factors-explain-the-price-of-bitcoin-f0538420c2c4
- Dragosch, A. (2021): "Modelling Bitcoin Value with Abundance" Medium; Link: https://medium.com/@andre-dragosch/modeling-bitcoin-value-with-abundance-20aa35fd4e5e
- Foss, G. (2021) Why Every Fixed Income Investor Needs to Consider Bitcoin as a Portfolio Insurance; Link: https://rockstarinnercircle.com/wp-content/uploads/2021/04/Why-Every-Fixed-Income-Investor-Needs-To-Consider-Bitcoin-As-Portfolio-Insurance. pdf

- Hayes, A. (2018). Bitcoin price and its marginal cost of production: Supporting evidence. ResearchGate. https://www.researchgate.net/publication/317601872_Bitcoin_price_and_its_marginal_cost_of_production_supporting_evidence
- Hayes, A. (2016) Cryptocurrency Value Formation: An empirical study leading to a cost of production model for valuing Bitcoin. Telematics and Informatics.
- Kripfganz, S. (2020, May 12). The Bitconometrics of the stock-to-flow model: An introduction and critical assessment [Video]. Retrieved from https://www.youtube.com/watch?v=u_VkwA5fkLA
- Nakamoto, S. (2009). Bitcoin: A peer-to-peer electronic cash system. Retrieved from https:// bitcoin.org/bitcoin. pdf
- Nuzzi, L., Waters, K. and Andrade, M. (2024) Breaking BFT: Quantifying the Cost to Attack Bitcoin and Ethereum. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4727999
- Peters, E. E. (1994). Fractal Market Analysis: Applying Chaos Theory to Investment and Economics. John Wiley & Sons, Inc.
- Peterson, Timothy, Bitcoin Spreads Like a Virus (March 20, 2019). Available at SSRN: https://ssrn.com/abstract=3356098
- Puell, D. (2018) Bitcoin Market-Value-to-Realized-Value (MVRV) Ratio. Medium; https://medium.com/@kenoshaking/bitcoin-market-value-to-realized-value-mvrv-ratio-3ebc914dbaee
- Reinhart, C. M., Rogoff, K. S. (2009). This Time Is Different: Eight Centuries of Financial Folly. United Kingdom: Princeton University Press.
- Rogers, E. M. (1962). Diffusion of Innovations. New York, NY: Free Press of Glencoe.

Contacts

etc-group.com

investors@etc-group.com

linkedin.com/company/
etcgroup-crypto

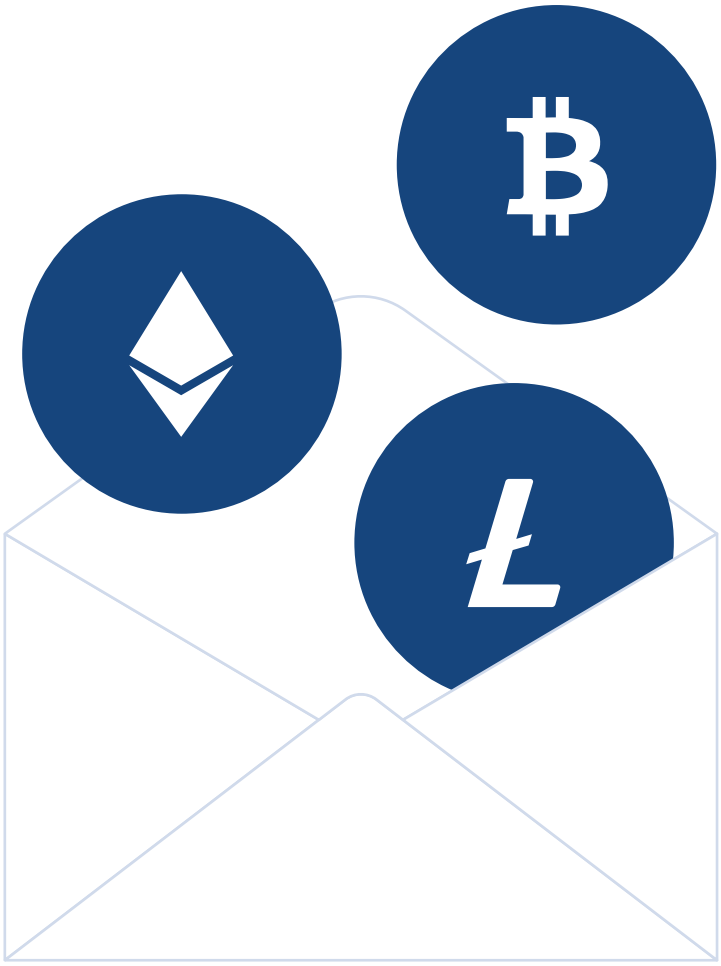
Product materials, analysis as well as due diligence collateral including SFDR information are available upon request.

Head office
ETC Management Ltd
3rd Floor Quality House,
5-9 Quality Court Chancery Lane,
WC2A 1HP, London, United Kingdom

Issuer
ETC Issuance GmbH
Thurn- und Taxis Platz 6,
60313 Frankfurt am Main
Deutschland

Be the first to get expert insights on the latest in crypto

Subscribe to our industry-leading newsletter and research content



Important Information

The information provided in this report is for informative purposes only and does not constitute investment advice, a recommendation or solicitation to conclude a transaction. This document (which may be in the form of a research report, marketing brochure, press release, social media post, blog post, broadcast communication or similar instrument — we refer to this category of communications generally as a "document" for purposes of this disclaimer) is issued by ETC Issuance GmbH (the "issuer"), a limited company incorporated under the laws of Germany, having its corporate domicile in Frankfurt, Germany. This document has been prepared in accordance with applicable laws and regulations (including those relating to financial promotions). If you are considering investing in any securities issued by ETC Group, including any securities described in this document, you should check with your broker or bank that securities issued by ETC Group are available in your jurisdiction and suitable for your investment profile.

Exchange-traded commodities/cryptocurrencies, or ETPs, are a highly volatile asset and performance is unpredictable. Past performance is not a reliable indicator of future performance. The market price of ETPs will vary and they do not offer a fixed income. The value of any investment in ETPs may be affected by exchange rate and underlying price movements. This document may contain forward-looking statements including statements regarding ETC Group's belief or current expectations with regards to the performance of certain asset classes. Forward-looking statements are subject to certain risks, uncertainties and assumptions, and there can be no assurance that such statements will be accurate and actual results could differ materially. Therefore, you must not place undue reliance on forward-looking statements. This document does not constitute investment advice nor an offer for sale nor a solicitation of an offer to buy any product or make any investment. An investment in an ETC that is linked to cryptocurrency, such as those offered by ETC Group, is dependent on the performance of the underlying cryptocurrency, less costs, but it is not expected to match that performance precisely. ETPs involve numerous risks including, among others, general market risks relating to underlying adverse price movements and currency, liquidity, operational, legal and regulatory risks.

ETC Issuance GmbH, incorporated under the laws of Germany, is the issuer of any securities described in this document, under the base prospectus dated 21 November 2023, supplemented from time to time, and approved by BaFin.

Any decision to invest in securities offered by ETC Group (including products and amounts) should take into consideration your specific circumstances after seeking independent investment, tax and legal advice. You should also read the latest version of the prospectus and/or base prospectus before investing and in particular, refer to the section entitled 'Risk Factors' for further details of risks associated with an investment. These prospectuses and other documents are available under the "Resources" section at etcgroup.com. When visiting this website, you will need to self-certify as to your jurisdiction and investor type in order to access these documents, and in so doing you may be subject to other disclaimers and important information.

IF YOU ARE IN THE UK, US, OR CANADA

Information contained in this document is not, and under no circumstances is to be construed as, an advertisement or any other step in furtherance of a public offering in the United States or Canada, or www.etc-group.com any state, province or territory thereof, where neither the issuer nor its products are authorised or registered for distribution or sale and where no prospectus of the issuer has been filed with any securities regulator. Neither this document nor information in it should be taken, transmitted or distributed (directly or indirectly) into the United States.

This document does not constitute an invitation or inducement to engage in investment activity. In the UK, this document is provided for information purposes and directed only at investment professionals (as defined under the Financial Services and Markets Act 200 (Financial Promotion) Order 2005 as amended from time to time). It is not intended for use by, or directed at, retail customers or any person who does not have professional experience in matters relating to investments. Neither the Issuer nor its products are authorised or regulated by the Financial Conduct Authority.

PUBLICATIONS & SOCIAL MEDIA DISCLOSURE

Social media posts (including, but not limited to, LinkedIn and Twitter) of ETC Group and its subsidiaries ("Social Media") are not, and should not be considered to be recommendations, solicitations or offers by ETC Group or its affiliates to buy or sell any securities, futures, options or other financial instruments or other assets or provide any investment advice or service. ETC Group makes all reasonable efforts to ensure that the information contained on social media is accurate and reliable; however, errors sometimes occur. You should note that the materials on social media are provided "as is" without any express or implied warranties. ETC Group does not warrant or represent that the materials on social media are accurate, valid, timely or complete.

RISKS OF CRYPTOCURRENCIES

Cryptocurrencies are highly volatile assets and are known for their extreme fluctuations in prices. While there is potential for significant gains, you are at risk of losing parts or your entire capital invested. The value of the ETCs is affected by the price of its underlying cryptocurrency. The price of cryptocurrencies can fluctuate widely and, for example, may be impacted by global and regional political, economic or financial events, regulatory events or statements by regulators, investment trading, hedging or other activities by a wide range of market participants, forks in underlying protocols, disruptions to the infrastructure or means by which crypto assets are produced, distributed, stored and traded. The price of cryptocurrencies may also change due to shifting investor confidence in future outlook of the asset class. Characteristics of cryptocurrencies and divergence of applicable regulatory standards create the potential for market abuse and could lead to high price volatility. Amounts received by Bondholders (i) upon redemption of the Bonds in USD, in cases where Bondholders are prevented from receiving cryptocurrency for legal or regulatory reasons; or (ii) upon sale on the stock exchange depend on the price performance of the relevant cryptocurrency and available liquidity.

For a detailed overview of risks associated with cryptocurrencies and specifically associated with the ETCs, please refer to the prospectus and base prospectus available at the issuer's website at www.etc-group.com.