



COIN REPORT:

Bitcoin (BTC)

An overview of Bitcoin and its potential use cases

By Fidelity Digital Assets[®]



ABNASIA.ORG

Asset Type:	Digital Currency
Consensus Mechanism:	Proof-of-Work
Launch Date:	January 3, 2009
Max Supply:	21,000,000

Key Takeaways

Facts

- Bitcoin was the first fully decentralized, peer-to-peer electronic cash system, marking a breakthrough in several fields including cryptography, computer science, and economics.
- The word "Bitcoin" can refer to two separate but related things: Bitcoin the network (a set of rules or protocols that operates a payment network) and bitcoin the token (an asset that resides on the network).
- Bitcoin maintains a programmatic issuance schedule, contributing to its scarce supply. There is a maximum supply of 21 million bitcoin that cannot be changed without a majority consensus of the network.
- Bitcoin's scarcity is underpinned by its decentralization and censorship-resistant characteristics, which are made possible through a consensus mechanism called proof-of-work.

Strengths

- Bitcoin is best understood as a monetary good, and one of the primary investment theses for bitcoin is as a store of value asset in an increasingly digital world.
- Bitcoin is often considered an entry point for traditional allocators looking to gain exposure to digital assets given its distinct characteristics as being the most decentralized, secure blockchain and its comparatively longer track record.
- Bitcoin is fundamentally different from any other digital asset. It is unlikely that another digital asset will improve upon bitcoin as a monetary good in the future because it is secure, decentralized, and sound digital money. Any potential "improvement" will face unavoidable trade-offs.
- Bitcoin's return profile is driven by strong tailwinds: increasing adoption given its characteristics as a store of value against a backdrop of unprecedented fiscal and monetary stimulus.

Weaknesses

- Bitcoin trades complexity and speed for a higher standard of security, decentralization, network integrity, and a self-correcting incentive structure.
- Given the above, it is more challenging to build on Bitcoin. It is slower and costlier to transact directly on the base layer (Layer 1) than newer Layer 1 blockchains.
- Bitcoin does not generate cash flow, and its utility lies in its perceived value as a monetary asset and its rate of adoption.
- Bitcoin is more volatile than other asset classes meaning its price can fluctuate significantly over short periods of time.
- Some governments are still working on regulatory frameworks and investor protection for the space, which could have an impact on price trajectory.

What Is Bitcoin and Its Value Proposition?

Bitcoin the Network vs. bitcoin the Asset

It is important to establish that the word “bitcoin” can refer to two related but distinctly different things: Bitcoin, the network and payment system, versus bitcoin, the token or asset. This report uses the standard of capitalizing Bitcoin when referring to the network and using a lowercase character for the bitcoin token.

Bitcoin was originally presented as a hypothetical solution for addressing the challenges associated with creating a truly peer-to-peer electronic cash system. Although people can transact in the physical world without an intermediary using cash, it was not possible to do so in the digital realm until Bitcoin’s invention.

Bitcoin is not governed by a singular person or organization. Instead, it is comprised of thousands of computers running the Bitcoin software. This network acts as a simple protocol that provides global rules that govern the network. Through this process, the network can be used as a payment system where users can send and receive a digital token called bitcoin.

History and Evolution of the Project

Bitcoin was created in 2009 by Satoshi Nakamoto, a pseudonymous individual or group, and is widely considered the first successful launch of a peer-to-peer digital cash system. Bitcoin differentiates itself from previous attempts at digital cash by introducing a hash-based proof-of-work consensus mechanism in combination with digital signatures and a decentralized framework to prevent double-spending. Proof-of-work is examined further in this report, however, the key takeaway is that this mechanism allows Bitcoin to maintain its decentralized nature and high settlement assurances.

Potential as a Store of Value and Medium of Exchange

Bitcoin maintains a programmatic issuance schedule, which contributes to its scarcity. There is a maximum supply of 21 million bitcoin that cannot be changed without a majority consensus of the network.

Bitcoin’s fixed maximum supply distinguishes it from many other digital assets. Unlike Bitcoin, numerous tokens either lack a predefined cap on total supply or employ dynamic supply adjustment mechanisms. These approaches may involve various economic factors that can make it difficult to predict future supply. Comparatively, investors can more accurately estimate the future supply of bitcoin because of its issuance schedule.






Bitcoin can be viewed as an alternative method to store long-term value. Its issuance schedule and maximum supply offer a unique digital asset with little to no maintenance costs commonly tied to traditional stores of value.

Additionally, its digital nature and purchasing power enable users to transact globally without an intermediary. This value proposition is further enhanced by the fact that Bitcoin is global, neutral, and censorship resistant. This applies to both the large- and small-scale use of bitcoin—individuals, banks, and even countries can use it as a medium of exchange and store of value.

An Aspiring Monetary Good

Given its two value propositions as a store of value and medium of exchange, bitcoin can be understood as a monetary good. A monetary good is defined as a good that is valued for its tradability rather than its consumption or use.

Why are some things treated as monetary goods while others are not? Economists and historians suggest the answer lies in several characteristics that make “good money.” The more of these characteristics an item possesses, the more likely it will emerge as an accepted form of currency or money.

 Fiat Currency	—	+	—	+	—	—	—
 Bitcoin	+	+	+	+	+	+	—
 Gold	+	—	+	—	—	+	+
	 Durable	 Divisible	 Fungible	 Portable	 Verifiable	 Scarce	 Track Record

Bitcoin possesses several “good” qualities of money, combining the scarcity and durability of a hard commodity with the ease of use, storage, and transportability of fiat money. It is also worth noting that like other monetary goods, bitcoin is not a company—it does not pay a dividend or have cash flows. Therefore, its value is derived from its ability to fulfill the characteristics of a monetary good compared to traditional alternatives.

There Is Only One Bitcoin Network

Bitcoin is inherently an “opt in” network, meaning anyone can join or leave the network at will. However, anyone that tries to change the rules without the consensus of a majority of participants will be ignored by the network. Therefore, while Bitcoin’s code is open-source and can be copied and modified, these copies or derivations of Bitcoin are entirely separate networks and are not “backward compatible” with the original Bitcoin network.

Furthermore, bitcoin tokens are native to Bitcoin and cannot be removed or transported to another blockchain network, contributing to Bitcoin’s network effects.

Bitcoin’s Value Is Driven by Its Enforceable Scarcity

One of bitcoin’s strongest properties is its scarcity. Not only is bitcoin scarce (as of August 2024, bitcoin’s inflation rate is at 0.8%), but it is also finite. There will only ever be 21 million bitcoin. No other digital asset possesses an immutable monetary policy on the level of bitcoin. Bitcoin’s enforced supply cap is underpinned by two key characteristics, both of which make bitcoin distinct from every other digital asset.

The first characteristic is bitcoin’s decentralization. No single entity owns or controls Bitcoin or its governing rules. As a completely decentralized network that is running open-source code, network participants must adhere to the code’s rules. The 21 million supply cap was written in the original bitcoin source code, which continues to run the network today.

This source code can only be changed through the consensus of network participants (the node operators). A change in bitcoin’s supply schedule is something that could happen in theory but likely never will in actual practice.

For one, gaining consensus is very difficult because Bitcoin’s network and market participants are so widely dispersed. More importantly, the network was designed with incentives to not change this supply cap. It would not be in the economic interest of the current network participants to raise or adjust the supply cap as doing so would inflate the supply of bitcoin and dilute the value of their holdings, or in the case of miners, their mining rewards. Here investors can see the powerful effects of game theory at work as it is in the best interest of all participants to coordinate, cooperate, and not change the supply cap.

The second characteristic is that Bitcoin is censorship-resistant because no singular body owns or controls it. Because the network has no geographical boundaries, it would be difficult for a nation state to assume control or regulation of the network and the core Bitcoin code itself.



Technology

Understanding Proof-of-Work

Bitcoin achieves decentralization and censorship-resistance through the proof-of-work consensus mechanism.

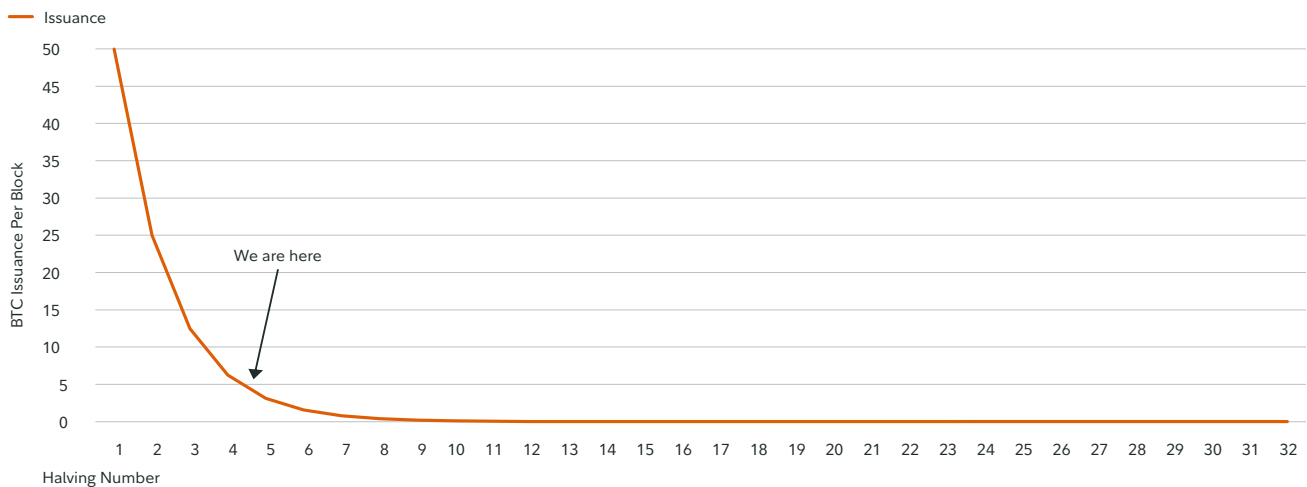
The blockchain is made up of thousands of computers all running the same software code. These computers, which anyone can run, keep a copy of a ledger that shows every transaction ever made on the network. Transactions are messages sent out to these computers telling them to update the ledger (e.g., “move X bitcoin from this address to this address”). Therefore, the network can act as a payment network.

Because Bitcoin is decentralized with no one entity in control, it needs a consensus mechanism to come to an agreement on the ledger’s true state. Proof-of-work acts as that consensus mechanism. Furthermore, the technological breakthrough also addressed the double-spend problem, ensuring a virtual token cannot be spent twice or copied. How Bitcoin achieves this mechanism of fraud prevention is especially important because it is accomplished without reliance on a third party or intermediary—something never previously done.

The Halving: Bitcoin’s Monetary Schedule

Every 210,000 blocks, or approximately every four years, the Bitcoin code halves the total compensation awarded to miners for successfully mining a valid block. Bitcoin’s issuance rate can be expected to halve roughly every four years until the 21 million supply is reached, which is estimated to happen in 2140.

Bitcoin Issuance Rate Over Time



Source: Fidelity Digital Assets Research, 10/16/24.

Competitive Analysis

Bitcoin's Potential to Be the Primary Monetary Good

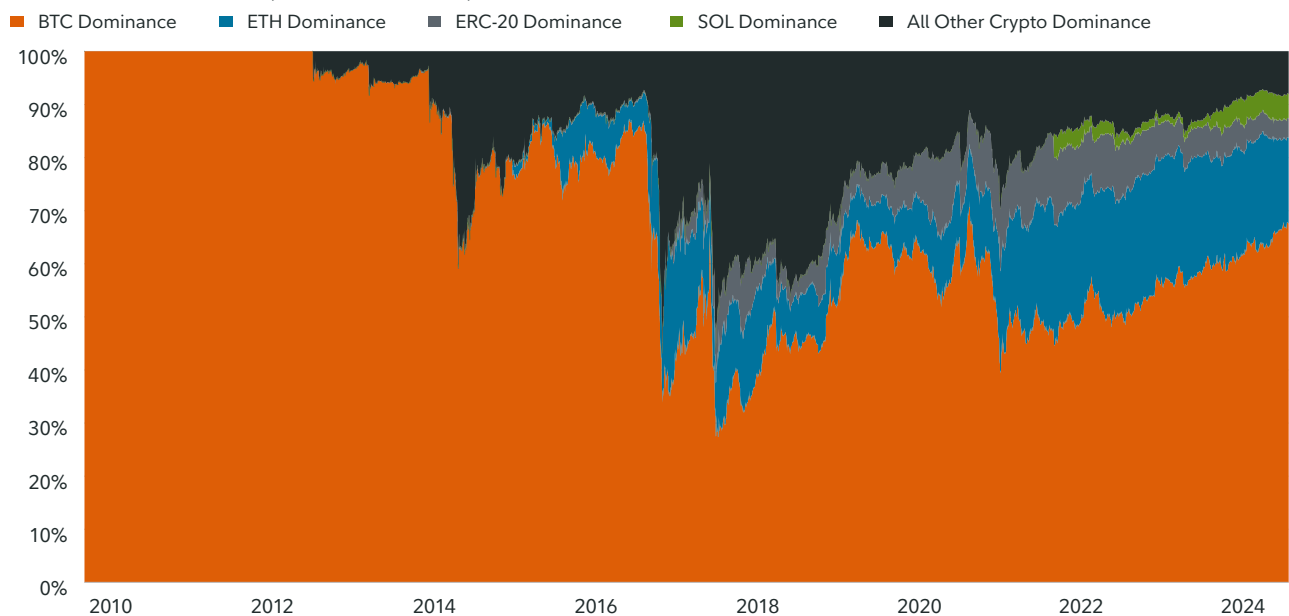
Investors may agree that bitcoin possesses many of the qualities that make for good money, but who is to say that only one monetary good can or will exist? Although it is highly unlikely that there will only ever be one money, this report takes the stance that one monetary good will come to dominate the digital asset ecosystem due to network effects.

The Power of Monetary Network Effects

Many investors are familiar with the power of network effects, where the value of a given network increases exponentially as the number of its users grows. Monetary networks are no different. However, they are even more powerful than other networks because the incentive to choose the right money is much stronger than any other choice of a network, such as a social network.

If investors are seeking a digital asset as a monetary good with the ability to act as a store of value, then they will likely choose the one with the largest and most secure, decentralized, and liquid network. As the first truly scarce digital asset, Bitcoin received a first mover advantage and has maintained it over time. Although bitcoin's dominance, or its market capitalization as a percentage of the entire digital asset ecosystem, has declined from 100% to approximately 55%, this is not due to it shrinking in size but rather the rest of the ecosystem growing.

Bitcoin Dominance (Ex-Stablecoins)



Source: Fidelity Digital Assets Research via Coin Metrics, 08/26/24.

There is also a reflexive property to monetary networks. People observe others joining a monetary network, incentivizing them to join as they also want to be on the network where peers or business partners reside. This can be seen on a smaller scale with existing payment networks as platforms such as PayPal and Venmo have grown at an accelerating rate.

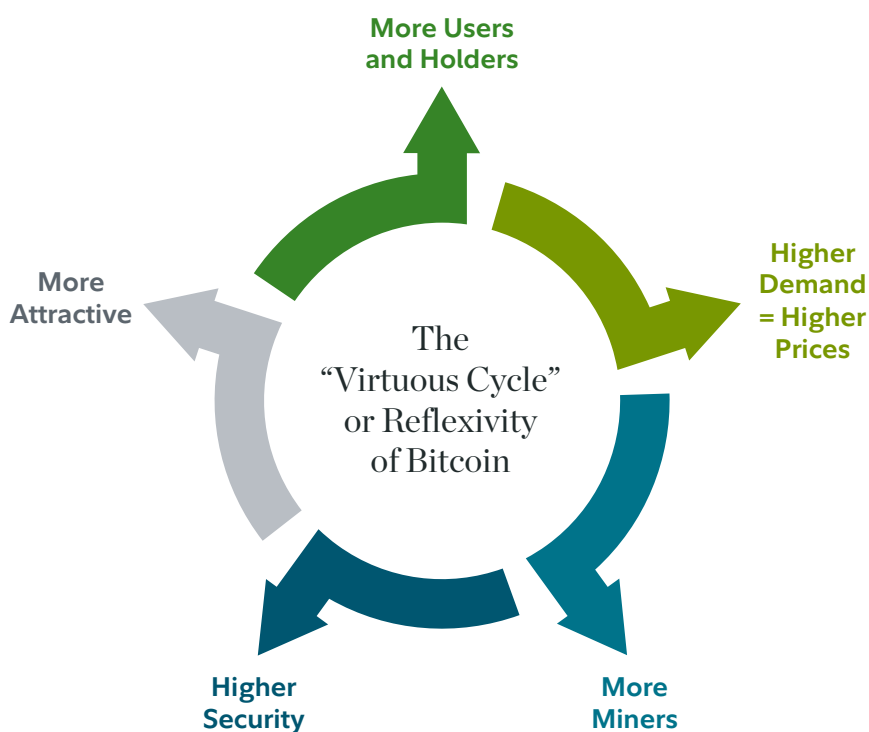
In bitcoin's case, the reflexive property is more pronounced because it does not just include passive holders of the asset, but also miners that actively increase the security of the network.

As more people believe bitcoin has superior monetary properties and opt to store their wealth in it, demand increases, potentially leading to higher prices (particularly as supply is inelastic or unresponsive to price). Miners are then incentivized to increase their capital expenditure and computing power as higher prices result in higher profit margins. More computing power devoted to bitcoin mining leads to higher security of the network, which in turn makes the asset more attractive, resulting in even more users and investors.

Bitcoin is currently the most decentralized and secure monetary network (relative to all other digital assets). Any newer blockchain network and digital asset that tries to improve upon bitcoin as a monetary good will have to differentiate itself by sacrificing one or both properties, an idea explored below (the "Blockchain Trilemma").

A competitor that tries to copy Bitcoin's entire code will also likely fail as there will be no reason to switch from the largest monetary network to one that is completely identical but a fraction of the size.

Moreover, the Lindy Effect, also known as Lindy's Law, is a theory that the longer a non-perishable thing such as a technology or idea survives, the more likely it is to persist in the future. The same may apply to Bitcoin.



Why We Believe Another Digital Asset Is Unlikely to Supersede Bitcoin as a Monetary Good

While it is theoretically possible in a free market, it is unlikely for bitcoin to be replaced by an "improved" digital asset for several reasons. One of the most significant reasons is that any improvement to one characteristic of bitcoin, such as speed or scalability, leads to a reduction in

another characteristic, such as bitcoin's level of decentralization or security. This trade-off is known as the blockchain trilemma.

The Blockchain Trilemma

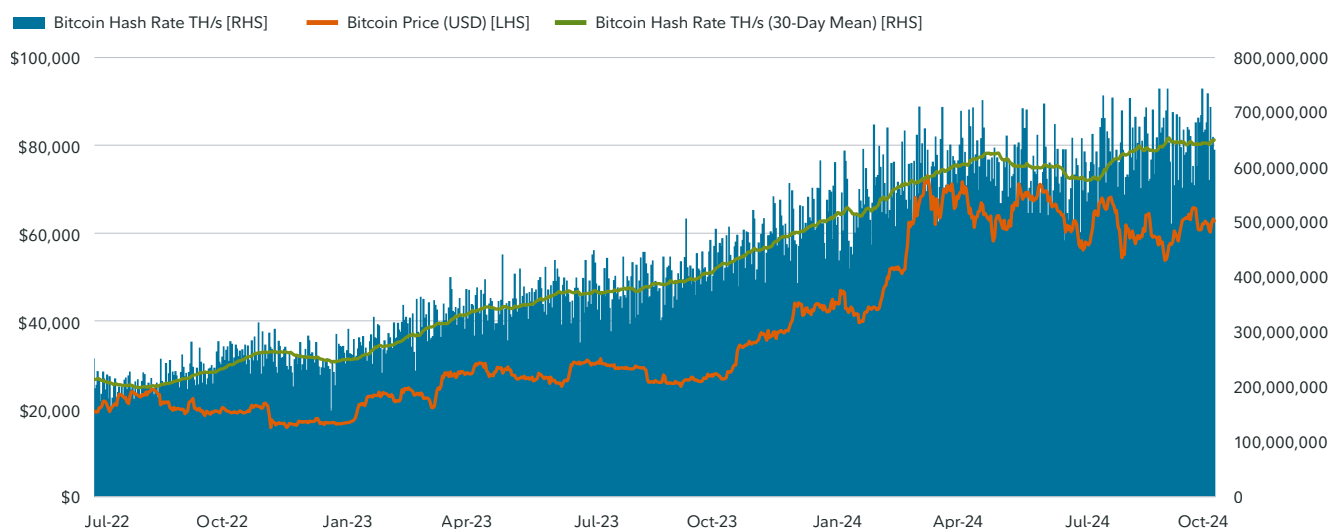
In the early 1980s, computer scientists identified a trilemma embedded in decentralized databases. More recently a variation to this trilemma—the blockchain trilemma—was outlined by Ethereum creator Vitalik Buterin. Buterin proposes that a decentralized database (of which Bitcoin is one type) can only fully deliver on two of three guarantees: decentralized, security, or scalability.

Security refers to how likely it is the network can be attacked or compromised. In the case of a decentralized network like Bitcoin, the main concern is a 51% attack, whereby a single person or entity controls more than half of the network's computing power (known as hash rate). If this is achieved, the attacker could control the network or make changes to the open ledger, such as performing double spending or reversing transactions. Trust in the network would be lost and could collapse the entire network. However, as Bitcoin becomes larger and is comprised of a growing number of nodes and miners, it becomes harder and more expensive to attack.

Bitcoin is the most secure digital asset when measured by the hash rate or computing power that is securing the network compared to other digital assets that use the same hashing algorithm. Total annual energy usage can be used as a proxy for security, with more energy usage as a measure of more mining resources dedicated to securing the network. Bitcoin is estimated to consume approximately 145 terawatt-hours annually, which is approximately 0.6% of global electricity consumption as of 2024.

The computing power or hash rate used to secure the network has grown over time.

Bitcoin Price vs. Hash Rate



Source: Fidelity Digital Assets Research via Coin Metrics, 08/14/24.

Decentralization refers to how much control any one person, entity, or group may have on a system or network. In a decentralized network, consensus is achieved through a voting mechanism so that no single entity can control or restrict the data. In an open decentralized network, anyone is also free to join, and no entity can exclude them if they follow the rules or protocol of the network. This allows the network to operate without intermediaries.

The cost of higher decentralization is lower network throughput, or the speed at which information can pass due to the need for a larger consensus. The opposite of a decentralized network would be a completely centralized network in which one intermediary controls all aspects. The advantage to this is speed and throughput as there does not need to be a consensus, but the disadvantage is the need to trust this single intermediary.

Scalability refers to how well the network can handle growth, such as growth in the number of users and how many transactions the network can handle in a limited amount of time. Scalability has notably been Bitcoin's greatest hurdle because it maximizes decentralization and security. Bitcoin is the network with one of the slowest transaction throughputs as a result.

The network adds a new block and validates transactions only every 10 minutes on average, and because Bitcoin's block size is limited, only so many transactions can fit into each block. To put this into perspective, Bitcoin can process approximately three to seven transactions per second. Comparatively, a highly centralized payment network such as Visa processes nearly 9,000 transactions per second.

None of these characteristics are innately better than another but this can depend on the use case.

Competitors

Ethereum

The Ethereum network and its token, ether, are not examined in this report. However, Ethereum is the second largest digital asset by market capitalization.¹ Therefore, it is relevant to note some of the key similarities and differences between Bitcoin and Ethereum.

From its inception, Bitcoin set out to fulfill the criteria of a "purely peer-to-peer version of electronic cash." It was designed to be decentralized and secure so that value could be sent without having to trust an intermediary. This was combined with a pre-programmed monetary schedule and enforced supply cap, giving bitcoin the ability to become a monetary good and store of value.

Ethereum also started as a white paper, originally published in 2013 by Vitalik Buterin. Ethereum's creators set out to take the blockchain technology pioneered by Bitcoin and extend it to include more capabilities, most notably the ability to do more computationally intensive transactions.



The Ethereum blockchain network can host and run smart contracts that can be used to program a variety of applications. It is for this reason some refer to Ethereum as a “distributed world computer.” The network also allows different tokens to be issued on the Ethereum blockchain, acting as a platform that others can use to build applications including decentralized finance applications, games, and social media tools.

While Ethereum can be viewed by some members of the digital asset community as a superior or more advanced network compared to Bitcoin, the additional capabilities and flexibility require trade-offs. Notably, a more complex network increases the chance for software bugs as well as increased centralization risks and a potential decline in security.

Litecoin

Another type of competitor to Bitcoin is Litecoin. Litecoin launched in 2011 and utilized much of Bitcoin’s original code, with a few minor changes to build its blockchain network. The goal of Litecoin is to be a “light” version of Bitcoin that is more efficient and cost effective to transact with.

Although it is relatively easy to re-purpose code from one blockchain to another, the value of bitcoin comes from its network effects, which are much harder to transfer over. As of 2024, the Litecoin market cap is under \$5 billion—less than 1% of Bitcoin’s. Litecoin is one example of many Bitcoin-adjacent networks that have struggled to compete with the original. For more details on Litecoin, please refer to [“Coin Report: Litecoin \(LTC\).”](#)

Key Differences Between Bitcoin, Ethereum, and Litecoin

	Initial Distribution	Supply	Market Cap (USD)	Annual Inflation / Issuance Rate	30-Day Avg Tx Fee	Daily Value Transacted in USD (1-Year SMA)	Number of Transactions Settled (1-Year SMA)
Bitcoin	0	19.79M	\$1,950B	0.83%	\$2.48	\$8.25B	538,456
Litecoin	150	75.22M	\$6.7B	1.68%	\$0.004	\$1.0B	283,417
Ethereum	72,000,000	120.43M	\$405B	0.20%	\$4.77	\$5.15B	1,157,850

Source: Fidelity Digital Assets Research via Coin Metrics, 11/22/24.

Fundamental Analysis and Investment Thesis

Bitcoin as a Macroeconomic Hedge

Bitcoin’s return profile is driven by two tailwinds: its scarcity and macroeconomic conditions.

Unprecedented levels of monetary and fiscal stimulus have led more investors and users to view bitcoin as an “insurance policy” that may provide protection against the unknown consequences. Leverage has historically driven financial systems towards fragility.

These types of macro environments have historically tended to benefit scarce assets whose supply cannot be altered. In the digital asset world, Bitcoin's ruleset, historical precedents, and decentralization have created the highest degree of scarcity of any digital asset protocol. This makes a compelling case as the greatest available hedge for some of the potential headwinds facing the legacy financial system.

Hard Commodity Competitor

In our 2023 Institutional Investor Digital Assets Study, 51% of respondents reported having a current investment in digital assets.² The rationale of institutional investors for establishing exposure now is that it will be a much larger market if it is widely used as a store of value in the future.

With a market capitalization estimated at over \$18.5 trillion as of October 2024, gold remains the premier store of value. However, bitcoin's market cap is growing. In 2020, it was 1.6% of gold's— as of late November 2024, that number is closer to 10%.

As bitcoin becomes more convenient to invest in through various traditional avenues, this gap may continue to narrow.

Valuation

Once investors understand the value proposition of bitcoin, the question of how to value it arises. There are many different valuation methods across a wide range of asset classes, whether the asset class generates cash flow or is a physical commodity. Investors may want to bring their own framework into the digital asset space. This report focuses on bitcoin's role as an aspirational store of value as the principal investment thesis. Based on its potential as a monetary good and the fact that it has no cash flow or industrial use case, this report takes the position that bitcoin is best analyzed through the lens of supply and demand.

Bitcoin's supply is predetermined and inelastic to demand. Its scarcity may be one of the value drivers and can increase as supply falls or demand rises. However, scarcity alone cannot drive value without a valid use case and market demand for said use. Both the supply- and demand-side valuation models are examined below.

The Supply Side: Increasing Scarcity

Bitcoin's halving events have historically been followed by large price runs in the subsequent months following the preprogrammed event. These halvings are the result of bitcoin's predetermined issuance schedule, automatically lowering its issuance rate roughly every four years.

In previous years, halvings appeared to cause a larger imbalance between the outstanding issued supply and total demand for bitcoin. Each subsequent halving has been followed by a reduction in newly issued supply that is likely less impactful to the imbalance between supply and demand and has historically been followed by price increases that are less dramatic.

Halving Event (Date)	Annual Inflation	Daily BTC Issuance	Two-Year Forward Returns
1 st Halving (2012)	8%	3,600	2,964%
2 nd Halving (2016)	4%	1,800	922%
3 rd Halving (2020)	1.8%	900	348%
4 th Halving (2024)	0.8%	450	?

Source: Fidelity Digital Assets Research via Coin Metrics, 08/23/24.

The Demand Side: Networking Effects

Network effects are a key component to many businesses' operating models. They represent the idea that the level of utility or perceived value from a particular good or service is a direct result of the number of users of that good or service.

Metcalfe's Law, a method used to explain network effects, states that the value of a telecommunications network is directly proportional to the square number of the users of that system. Each unique user is connected to all other users, resulting in compounding growth for the number of possible connections on that network and broader adoption amongst the general population.

Network effects tend to drive an adoption curve that looks similar across various successful technologies. This adoption curve, known as an "S-Curve," can be explained through the logic of adoption trends. Early adopters to a given technology often see current and potential future value in that network even though it is not yet widely used.

If a technology displays a large enough advantage relative to its incumbents over time, and switching costs are low enough, then adoption will begin to compound. This is when a technology begins to reach critical mass. As it becomes accepted as a superior and widely used technology, the product or service gradually demonstrates a decrease in its adoption rate, forming an asymptote near full maturity.

Metcalfe's Law can inform a possible bitcoin valuation based on projected address growth and its linkage to price. Historic adoption curves can be used as the basis for projecting potential future address growth, given bitcoin's adoption curve so far has progressed similarly to other technology adoption curves. However, this methodology can produce a wide range of outcomes, depending on which specific technology adoption curve Bitcoin ultimately resembles so it is far from precise. We can assume that Bitcoin is still early in terms of mass adoption with estimates of 52 million unique Bitcoin addresses with a non-zero balance, bearing in mind that one individual or entity can hold more than one wallet and that some may be dormant.³



Scenario Analysis

Bull case: Bitcoin experiences an inflection point where the value locked in the network and the number of users become so attractive to builders that they gravitate toward the blockchain as the default for creating additional use cases, such as financial applications. The network could experience technological upgrades that make Bitcoin more scalable without sacrificing decentralization and security.

In this case, the total addressable market for Bitcoin extends beyond being a digital asset to potentially becoming the backbone of the financial system, with bitcoin widely accepted as a valuable form of collateral. Other relevant factors could be a change to the tax treatment of bitcoin and a continued decline in its price volatility, which could enable wider use as a payment method.

Base case: Bitcoin continues to experience institutional and retail adoption and becomes accepted as a hedge against inflation and store of value. This would occur over a multiyear period given the market is still early in the process. Additionally, regulatory progress could evolve in a non-linear manner as it has done in the past, meaning access to standardized, regulated products could come in fits and starts. Finally, a more uncertain world where governments continue to run historically high fiscal deficits and cause continued currency debasement could accelerate the adoption curve even without better access or regulation.

Bear case: A bearish investment case for bitcoin could emerge from regulation that could stymie widespread access and adoption and reduce demand. Today, bitcoin is acknowledged by more jurisdictions around the world but there are some that remain unwelcoming or inconsistent in their approach given the asset class is perceived to be riskier. Moreover, a superior technology could emerge as could other alternatives and investors could become apathetic towards the key features of bitcoin such as its hard supply cap or decentralized nature.

Governance and Roadmap

Who “Governs” Bitcoin’s Code?

Bitcoin’s white paper was sent to a cypherpunk mailing list in late 2008 under the pseudonymous name, Satoshi Nakamoto. It is not clear whether that name belonged to a group of people or an individual. However, there were early adopters and contributors whose names were not hidden, including cryptographic activists that initiated contact with Satoshi after the white paper was released.

Satoshi was active in the development of Bitcoin from its release until the end of 2010 when they made the last commit to the project. Later, in April 2011, Satoshi announced they were moving on to other projects. Before leaving, Satoshi released control of the repository to Gavin Andresen, a developer and key figure in the Bitcoin community, and transferred Bitcoin-related domains to

various central community members. Satoshi has not moved or transferred the early tokens under their control since seemingly disappearing in 2011.

The Bitcoin Core software has grown into the hands of the wider community. Changes to the code are implemented through consensus among the developer community and adopted through the decentralized set of node operators. However, the project maintains stricter control of commit access and merge abilities to ensure the core project's integrity.

It is important to note that these select individuals do not have unilateral control of the repository and anyone can make contributions to the network today. Development of Bitcoin has been widely funded by grants and sponsorships from many individual contributors and organizations.

Initial Token Launch

Bitcoin was first announced with its white paper in 2008, allowing for an open and transparent launch of the network's rules. The protocol was officially launched in January 2009. The first block ever mined—the genesis block—produced the first 50 bitcoin which were presumed to have been awarded to Satoshi. It would take another three days before the next block was found.

In this time, anyone could opt into the network and compete for these bitcoin rewards. However, it is important to note that bitcoin was not launched with an exchange rate. Early adopters were effectively expending their time and energy on a then worthless "idea" of money.

Bitcoin did not launch with a pre-sale or pre-mine, which was widely considered a "fair launch" of the network. The proof-of-work reward mechanism continues to distribute new bitcoin to the miners expending the electricity.

Roadmap

Bitcoin's decentralized ruleset impedes the network from major consensus changes. These changes, known as hard forks, have historically created completely new and different blockchains. Some examples include Bitcoin Cash, Bitcoin SV, Bitcoin Classic, and Bitcoin Unlimited.⁴

However, Bitcoin has arguably never hard forked its own ruleset. In other words, in Bitcoin's 15-year history, the monetary policy and other major identifiable attributes have not been changed or "loosened" in a way that would cause a hard fork. This also means that nodes on Bitcoin are less likely to be arbitrarily ousted from the network due to negligence compared to protocols that commonly hard fork to enhance or alter fundamental rules of the network.

There are many upgrades and enhancements that are currently being researched and discussed within the community. These improvements are known as Bitcoin Improvement Proposals (BIPs).

It is worth noting that the Bitcoin community has chosen to value decentralization and security above all else. Therefore, most—if not all—proposed changes to the network come in the form

of a soft fork. Changes to Bitcoin are inherently slow, and there can be years between a BIP's introduction and final inclusion. The status of current BIPs can be found [here](#).

Risks and Uncertainties

Almost every bitcoin-related risk today can also be seen across every other digital asset, with nation-state attacks and protocol bugs being two of the most notable network threats. Meanwhile, evolving regulation can influence future price action as can perceived value given Bitcoin does not generate cash flow. It is also important to note declining but still high volatility, which can translate into large price swings relative to other investments.

Technical Risk

The hypothetical scenario for a vulnerability in its code is always a present threat because Bitcoin is a software running on computer hardware. In fact, Bitcoin did encounter two separate software bugs early on in its history, requiring patches to be implemented. This problem can be mitigated by keeping the software simple and engaging in thorough review and scrutiny of the code.

In Bitcoin's case, its protocol is less likely to encounter a major bug at this stage in its life. It has existed longer than any other project, holds an intentionally simplistic code, and has a bounty amounting to over \$1 trillion for anyone capable of exploiting it.

Any vulnerability could lead to a loss of confidence in the asset, negating its value as a secure way to build financial applications. Given bitcoin has no cash flow, or other use cases for now, its value could go to zero.

Regulatory Risk

Rather than attacks from nation-states, what has happened is a divergence in the way jurisdictions regulate bitcoin. A minority of nation-states have attempted outright bans, whereas others are creating regulatory frameworks. The uncertainty coming from a lack of regulatory clarity in some of the major economies has likely slowed adoption, particularly from institutional investors. The lack of a legal framework in some markets also means that investor protection may not be as robust as with other asset classes.

Competitor Risk

This report has made numerous arguments as to why the competitive risk to bitcoin appears to be low. However, there is always a risk that another asset (digital or otherwise) could gain (or retain) its advantage as a monetary good, fulfilling the use of store of value and/or medium of exchange.

Investor Apathy Risk

Finally, another possible risk to bitcoin as an investment is investor apathy. While many see Bitcoin as a breakthrough technology with many significant value propositions, its value is ultimately subjective. As with many investments, if investors lose interest, do not recognize the value proposition, and then adoption wanes, the value of bitcoin could significantly decrease.

Contributors

Martha Reyes-Hulme - Research Analyst, Fidelity Digital Assets®

Chris Kuiper - Director of Research, Fidelity Digital Assets®

Daniel Gray - Research Analyst, Fidelity Digital Assets®

Max Wadington - Research Analyst, Fidelity Digital Assets®

Zack Wainwright - Research Analyst, Fidelity Digital Assets®

Interested in learning more about Bitcoin and other digital assets?

Get in touch



The information herein was prepared by Fidelity Digital Asset Services, LLC ("FDAS LLC") and Fidelity Digital Assets, Ltd ("FDA LTD"). It is for informational purposes only and is not intended to constitute a recommendation, investment advice of any kind, or an offer to buy or sell any asset. Perform your own research and consult a qualified advisor to see if digital assets are an appropriate investment option.

Digital assets are speculative and highly volatile, can become illiquid at any time, and are for investors with a high-risk tolerance. Investors in digital assets could lose the entire value of their investment. Digital assets may also be more susceptible to market manipulation than securities. Digital assets are not insured by the Federal Deposit Insurance Corporation or protected by the Securities Investor Protection Corporation.

Digital assets are highly volatile, and their market movements are very difficult to predict. Various market forces may impact their value including, but not limited to, supply and demand, investors' faith and their willingness to purchase it using traditional currencies, investors' expectations with respect to the rate of inflation, interest rates, currency exchange rates, an evolving legislative and regulatory environment in the U.S. and abroad, and other economic trends. Investors also face other risks, including significant and negative price swings, flash crashes, and fraud and cybersecurity risks. Digital assets may also be more susceptible to market manipulation than securities.

Accounts for and custody and trading of digital assets are provided by Fidelity Digital Asset Services, LLC, which is chartered as a limited purpose trust company by the New York State Department of Financial Services to engage in virtual currency business (NMLS ID 1773897). FDA LTD relies on FDAS LLC for these services. FDA LTD is registered with the Financial Conduct Authority under the U.K.'s Money Laundering Regulations. The Financial Ombudsman Service and the Financial Services Compensation Scheme do not apply to the cryptoasset activities carried on by FDA LTD.

To the extent this communication constitutes a financial promotion in the U.K., it is issued only to, or directed only at, persons who are: (i) investment professionals within the meaning of Article 19 of the Financial Services and Markets Act 2000 (Financial Promotion) Order 2005 (the "FPO"); (ii) high net worth companies and certain other entities falling within Article 49 of the FPO; and (iii) any other persons to whom it may lawfully be communicated.

This information is not intended for distribution to, or use by, anyone in any jurisdiction where such distribution would be contrary to local law or regulation. Persons accessing this information are required to inform themselves about and observe such restrictions.

FDAS LLC and FDA LTD do not provide tax, legal, investment, or accounting advice. This material is not intended to provide, and should not be relied on, for tax, legal, or accounting advice. Tax laws and regulations are complex and subject to change. You should consult your own tax, legal, and accounting advisors before engaging in any transaction.

This material may be distributed by the following entities, none of whom offer direct exposure, nor provide clearing or custody for digital assets: Fidelity Distributors Company LLC ("FDC"), National Financial Services LLC ("NFS"), or Fidelity Brokerage Services LLC ("FBS"). FDC, NFS, and FBS, and their representatives, may have a conflict of interest in the products or services mentioned in these materials because they have a financial interest in them, and receive compensation, directly or indirectly, in connection with the management, distribution, and/or servicing of these products or services.

As with all your investments through Fidelity, you must make your own determination whether an investment in any particular digital asset/cryptocurrency is consistent with your investment objectives, risk tolerance, financial situation, and evaluation of the digital asset. Neither Fidelity nor any of its affiliates are recommending or endorsing these assets by making them available.

Coin Metrics is a trademark of Coin Metrics Inc. Copyright © Coin Metrics, 2024.

Fidelity Digital Assets is a registered mark and the Fidelity Digital Assets Logo is a service mark of FMR LLC.

1167499.2.0

¹ Coin Metrics, Crypto Prices, August 2024.

² The 2023 Institutional Investor Digital Assets Study was executed in association with Fidelity Consulting Strategic Insights. The survey included 1,042 institutional investors in the U.S. (406), Europe (370) and Asia (266), including financial advisors, family offices, crypto hedge and venture funds, traditional hedge funds, high-net-worth investors, pensions and defined benefit plans, and endowments and foundations.

³ Glassnode, BTC: A Number of Addresses with a Non-Zero Balance, August 2024.

⁴ Investopedia, A History of Bitcoin Hard Forks, March 2024.

