

SEPTEMBER 2023

Bitcoin First Revisited

Why investors need to consider bitcoin
separately from other digital assets

Chris Kuiper, CFA[®] – Director of Research, Fidelity Digital AssetsSM

Jack Neureuter – Research Analyst, Fidelity Digital AssetsSM





Background

In January 2022, we outlined Bitcoin's unique characteristics, why they make Bitcoin fundamentally different from other digital assets, and why this is important for investors to consider. Over a year and a half later, Bitcoin continues to gain adoption and market share in the digital asset space, while other digital assets have faced separate headwinds. While we encourage those seeking a detailed understanding of Bitcoin's unique value propositions to read the [earlier overview](#), we aim to reiterate many of Bitcoin's fundamental advantages below while contextualizing Bitcoin's progress and position within today's current digital asset market.

Executive Summary

Once investors have decided to invest in digital assets, the next question becomes, "Which one?" Of course, bitcoin is the most recognized, first-ever digital asset, but there are hundreds—even thousands of other digital assets in the ecosystem.

One of the first concerns investors have regarding bitcoin is, as the first digital asset, it may be vulnerable to innovative destruction from competitors (such as the story of MySpace and Facebook). Another common consideration surrounding bitcoin is whether it offers the same potential reward or upside as some of the newer and smaller digital assets that have emerged.

In this paper, we propose:

- Bitcoin is best understood as a monetary good and one of the primary investment theses for bitcoin is as the store of value asset in an increasingly digital world.
- Bitcoin is fundamentally different from any other digital asset. No other digital asset is likely to improve upon bitcoin as a monetary good because bitcoin is the most (relative to other digital assets) secure, decentralized, sound digital money and any "improvement" will potentially face trade-offs.
- There is not necessarily mutual exclusivity between the success of the Bitcoin network and all other digital asset networks. Rather, the rest of the digital asset ecosystem can fulfill different needs or solve other problems that bitcoin simply does not.
- Other non-bitcoin projects should be evaluated from a different perspective than bitcoin.
- Bitcoin should be considered an entry point for traditional allocators looking to gain exposure to digital assets.
- Investors should hold two distinctly separate frameworks for considering investment in this digital asset ecosystem. The first framework examines the inclusion of bitcoin as an emerging monetary good, and the second considers the addition of other digital assets that exhibit venture capital-like properties.



What is Bitcoin?

It is beyond the scope of this paper to provide a detailed explanation of Bitcoin. However, we do think it is important to emphasize some of the basics that are necessary to understand how bitcoin has maintained a competitive advantage in the quest to represent the de facto non-sovereign monetary good of the digital asset ecosystem.

“Bitcoin” the Network vs. “bitcoin” the Asset

One of the most confusing concepts for those who are new to bitcoin is understanding that the word “bitcoin” can refer to two related, but distinctly different things. There is Bitcoin the network or payment system, and then there is bitcoin the token or asset. To help avoid confusion, we will adopt the standard of capitalizing Bitcoin when referring to the network and using a lowercase character for bitcoin the token or asset.

Bitcoin was initially just an idea that set out to solve the problem of creating a truly peer-to-peer electronic cash system. Although we can transact in the physical world without an intermediary using cash, this was not possible in the digital realm until Bitcoin was invented. This idea was put into practice by writing code. Therefore, Bitcoin is just code and Bitcoin the network is made up of thousands of computers all running this identical Bitcoin software. This code acts like a protocol and provides the rules that govern the Bitcoin network. This network operates a payment system, where users can send and receive a digital token, also called bitcoin.

The Bitcoin Network is Not Compatible with Other Networks

Anyone can join or leave the Bitcoin network as long as they follow the core rules. Anyone that tries to change the rules without the consensus of the majority of the other participants will be excluded from 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 the Bitcoin network and can not be removed or transported to another blockchain network. The importance of this will be revealed later in this paper as we discuss the power of network effects and why we see one network dominating the market.

Why We Believe Bitcoin is Best Understood as a Monetary Good

What is money? We believe money is a tool that allows exchange rather than barter. Throughout most of history, we have seen humans iterate in search of the “best” representation of money. A monetary good is a good that is valued for its tradability for other goods, not its consumption or use. Throughout history, various goods have been used as money, such as shells, beads, stones, fur, and wampum. This leads to the question: why do some things become treated as a monetary good, while others do not? Economists and













historians suggest that the answer lies in several characteristics that make “good money.”¹ The more characteristics a good possesses, the better it can serve as being money or the more likely it will emerge or be accepted as money.

Bitcoin clearly possesses a lot of good qualities of money, combining the scarcity and durability of gold with the ease of use, storage, and transportability of fiat (even improving on it).

It is also worth noting that, just like other monetary goods, bitcoin is not a company, it does not pay a dividend, nor does it have cash flows. Therefore, its value must be derived from its ability to better fulfill the characteristics of a monetary good compared to traditional alternatives.

Bitcoin’s Value is Driven by its Enforceable Scarcity

One of the greatest characteristics of bitcoin’s properties is its scarcity. Not only is bitcoin scarce (bitcoin’s current inflation rate of about 1.8% is roughly equal to gold’s inflation rate at the moment)³, but unlike gold, it is also provably finite. There will only ever be 21 million bitcoin. No other digital asset possesses an immutable monetary policy on the level of bitcoin. In other words, Bitcoin’s monetary policy may be viewed as the most credible.

	 GOLD	 BITCOIN	 FIAT CURRENCY	
 DURABLE	+	+	-	While all are physically durable, fiat currency has not maintained purchasing power durability over time
 DIVISIBLE	-	+	+	Physical gold is only divisible to small pieces; bitcoin is divisible to eight decimals
 FUNGIBLE	+	+	-	Gold and bitcoin are fungible, but fiat currency is not fungible with other fiat (i.e. U.S. dollar is not fungible with Canadian dollar)
 PORTABLE	-	+	+	Gold has a high value-to-weight ratio, but compared to the others, is still heavy and cumbersome to transport
 VERIFIABLE	-	+	-	Both gold and fiat currency have been counterfeited; gold can be verified, but only through cumbersome testing
 SCARCE	+	+	-	Gold is relatively scarce, bitcoin is scarce and finite; the only supply constraint on fiat currency is willingness of government or central bank
 TRACK RECORD	+	-	-	Gold has the longest track record as money and maintaining purchasing power; bitcoin’s history is the shortest; fiat currency has poor track record ²

1 See “On the Origins of Money,” Carl Menger, *Economic Journal* 2 (1892)

2 For example, post-Bretton woods there has been 201 currency crises from 1975 to 2007, or an average of more than five per year. See Glick, Reuven, and Michael Hutchison. “Currency Crisis.” Federal Reserve Bank of San Francisco Working Paper Series, Sept. 2011, <http://www.frbsf.org/publications/economics/papers/2011/wp11-22bk.pdf>.

3 World Gold Council, 2019, annual reports and <https://www.gold.org/about-gold/gold-supply/gold-mining/how-much-gold>



But how is bitcoin's scarcity (its 21 million supply cap) enforced? Two key characteristics underpin this credibility and are necessary to understand bitcoin's enforced supply cap and why it is distinct from every other digital asset.

The first is bitcoin's decentralization. No one person, corporation, or government owns or controls the Bitcoin network or the rules that govern it. As a completely decentralized network that is running open-source code, the network participants must adhere to the code's rules that govern the network. The 21 million supply cap was written in the original Bitcoin source code, which continues to run the Bitcoin network today.

But if the network is operated by mere code, can this code be changed? Yes, but only through consensus of the network participants (the node operators). A change in bitcoin's supply schedule is something that could happen in theory, but almost never will in actual practice.

First, gaining consensus is enormously hard to do because Bitcoin's network and market participants are so widely dispersed. There is not a large "consortium" to have sway or voting power. 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 because doing so would only serve to inflate the supply of bitcoin and dilute the value of their holdings, or in the case of miners, their mining rewards. Here, the powerful effects of game theory are at work as it is in the best interest of all participants to coordinate, cooperate, and not change the supply cap.

Second, the Bitcoin network is censorship-resistant. Because no person, corporation, or government owns or controls the Bitcoin network, it is very resistant to censorship. In addition, the Bitcoin network has no geographical boundaries, making it difficult for a nation-state to assume control or regulation of the network and the core Bitcoin code itself.

To review the step-by-step logic as to why we believe bitcoin is a monetary good that has value:

1. A monetary good is something that has value attributed to it above and beyond its utility or consumption value. Although Bitcoin's payment network certainly has utility value, people are also ascribing a monetary premium value to bitcoin tokens.
2. One of the primary reasons investors attribute value to bitcoin is its scarcity. Its fixed supply is the reason it can be a store of value.
3. Bitcoin's scarcity is underpinned by its decentralization and censorship-resistant characteristics.
4. These characteristics are hardcoded into bitcoin and almost certainly will never be changed because the same people that ascribe value to bitcoin and own it have no incentive to do so. In fact, network participants are incentivized to defend these very characteristics of a scarce asset and an immutable ledger.



Why We Believe Bitcoin Has the Potential to be the Primary Monetary Good

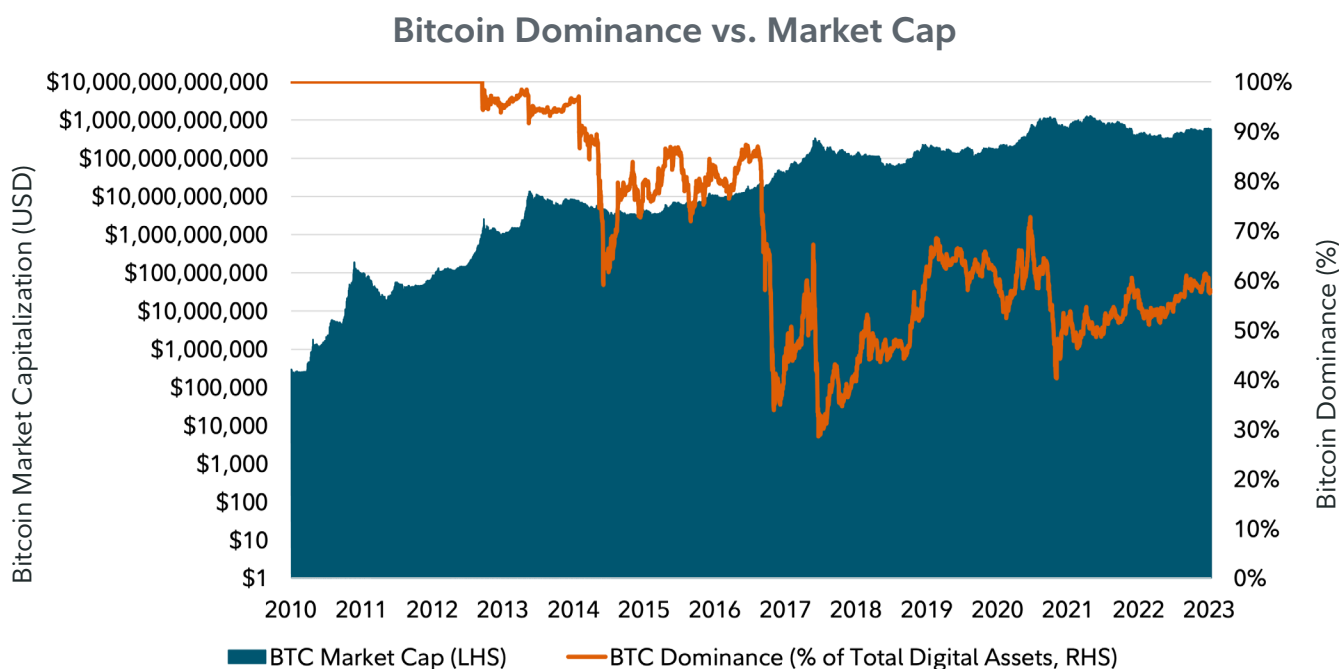
Investors may agree that bitcoin possesses many of the qualities that make for good money, but who is to say that only one monetary good can or will exist?

We will not be so bold as to predict there will only ever be one money, but we do believe that one monetary good will come to dominate the digital asset ecosystem due to the very powerful network effects.

Monetary Network Effects are Extremely Powerful

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, telephone network, etc.

If investors are looking for a digital asset as a monetary good, one with the ability to act as a store of value, then they will naturally choose the one with the largest, most secure, decentralized, and liquid network. Bitcoin as the first truly scarce digital asset ever invented received a first mover advantage and has maintained this advantage over time. Note that while bitcoin's dominance, or its market capitalization as a percentage of the entire digital asset ecosystem, has declined from 100% to approximately 50%, this is not due to it shrinking in size, but rather the rest of the ecosystem growing.

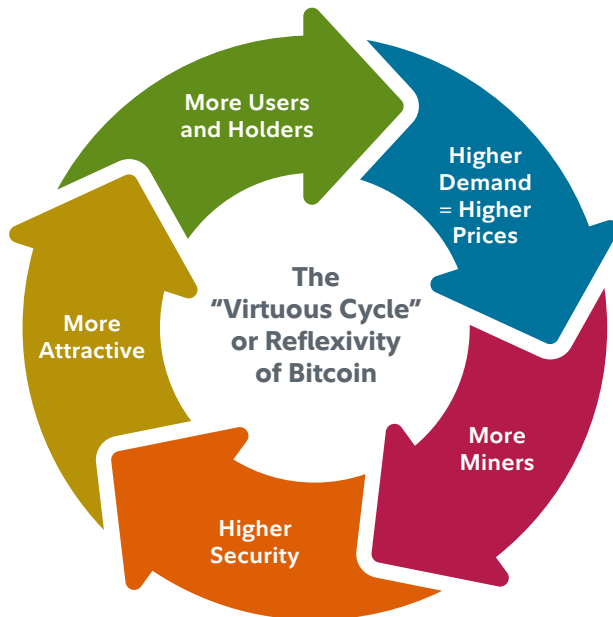


Source: Coin Metrics, 07/26/2023.



There is also a reflexive property to monetary networks. People observe others joining a monetary network, which incentivizes them to join as well because they also want to be on the network where their peers or business partners transact. This can be observed on a smaller scale with payment networks today as platforms, such as PayPal and Venmo, have grown at an accelerating rate.

In the case of bitcoin, the reflexive property is even more pronounced because it does not just include passive holders of the asset, it also includes miners that actively increase the network's security. As more people believe bitcoin has superior monetary properties and opt to store their wealth in it, demand increases. This, in turn, leads 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 lead to higher profit margins. More computing power devoted to bitcoin mining leads to higher network security, which, in turn, makes the asset more attractive, leading once again to more users and investors.



This network competition is likely to result in a winner-take-all scenario as the network grows and becomes more valuable because the choice of any other monetary network that does not become the dominant one will result in a loss of investment or opportunity cost. Every investor looking to store value in a monetary good is making a choice as to which monetary network they are opting into, whether they are acknowledging it or not.

Any Subsequent Monetary Good Would be "Reinventing the Wheel"

The invention of the wheel represented an entirely new technology that, once invented, could never be

reinvented. Similarly, never in human history had the problem of digital scarcity and true peer-to-peer electronic cash been solved until Bitcoin was invented. Solving this problem was not merely an incremental improvement, but a leap forward or an unlocking of the puzzle of how digital scarcity could exist.

Because Bitcoin is currently the most decentralized and secure monetary network (relative to all other digital assets), a newer blockchain network and digital asset that tries to improve upon bitcoin as a *monetary good* will potentially have to differentiate itself by sacrificing one or both of these properties, an idea we explore in more detail later (the "Blockchain Trilemma"). A competitor that tries to merely copy Bitcoin's entire code will also 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.



The Lindy Effect and Bitcoin's Antifragile Qualities

The Lindy Effect, also known as Lindy's Law, is a theory that the longer some non-perishable thing survives, the more likely it is to survive in the future. For example, a Broadway play that has run for 10 years is likely to run another 10 years compared to one that has run for only one year. We believe the same may apply to Bitcoin. Every minute, hour, day, and year that Bitcoin survives increases its chances of continuing into the future as it garners more trust and survives more shocks. This also goes hand-in-hand with the property of antifragility, where something becomes more robust or stronger with each attack or instance in which the system endures some form of stress.

In fact, if an investor were presented with the idea of Bitcoin and then asked to come up with a list of stressors, attacks, shocks, or failures that would likely be the demise of this nascent technology, they would probably underestimate all of the negative events that Bitcoin has already endured that have not proven to be the network's downfall.

A non-exhaustive list of some of the negative events that Bitcoin has endured:

Created by an anonymous person(s) whose true motive or any affiliation is unknown	Some bitcoin tokens have been confiscated by the FBI	Multiple exchange hacks	Multiple large exchanges and service companies going bankrupt
Used on the dark web for illicit purchases	Endured a "civil war" regarding the core code (see section on blocksize war)	Price has suffered multiple 50%+ drawdowns, many larger than 80%	Banned in multiple countries
Has been labeled a fraud, ponzi scheme, speculative gamble	Remains primary form of payment for ransomware attacks	Has endured multiple forks in its code	Copied by competitors thousands of times

Why Another Digital Asset is Unlikely to Supersede Bitcoin as a Monetary Good

Perhaps investors agree that bitcoin is currently the best monetary good in the digital asset marketplace and that it is likely that one digital monetary good will dominate the market because of network effects. However, could a superior or improved version of bitcoin be created and become the dominant monetary good? Bitcoin's code is open source so it is true that anyone can copy and try to improve upon it.

While it certainly is possible in a free market of emerging digital assets, we believe it is highly unlikely for bitcoin to be replaced by an "improved" digital asset for several reasons. One of the biggest reasons is that any improvement in one characteristic of bitcoin, such as improving its 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.

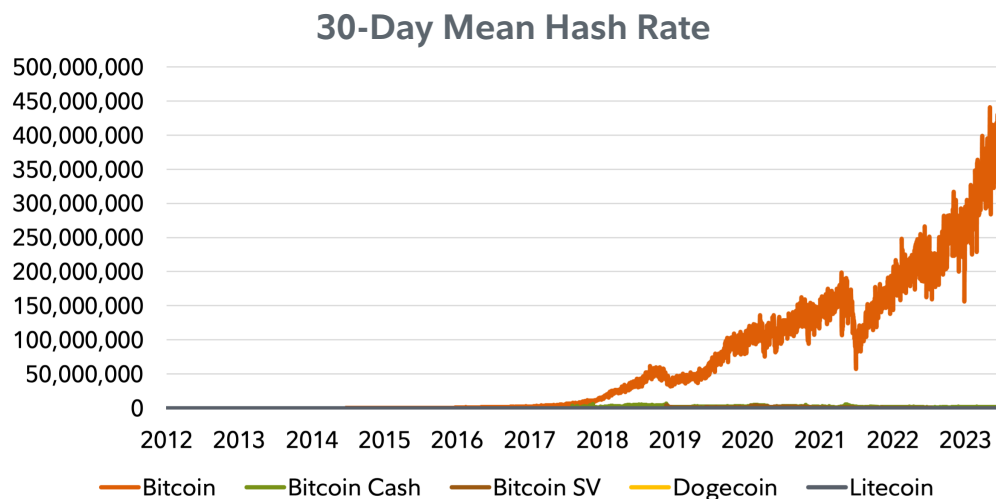


The Blockchain Trilemma

As far back as the early 1980s, computer scientists identified a kind of trilemma embedded in decentralized databases.⁴ More recently, a variation to this trilemma, known as the “Blockchain Trilemma,” was outlined by Ethereum creator Vitalik Buterin, who states that a decentralized database (of which Bitcoin is one type) can only deliver on two of three guarantees at one time: decentralization, security, or scalability.⁵

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 Bitcoin network’s computing power (known as hash rate). If this is achieved, the attacker could control the network or, more specifically, 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. As the Bitcoin network becomes larger, with more nodes and miners distributed among more people, entities, and geographic areas, it becomes harder and more expensive to attack.

Bitcoin is by far 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.



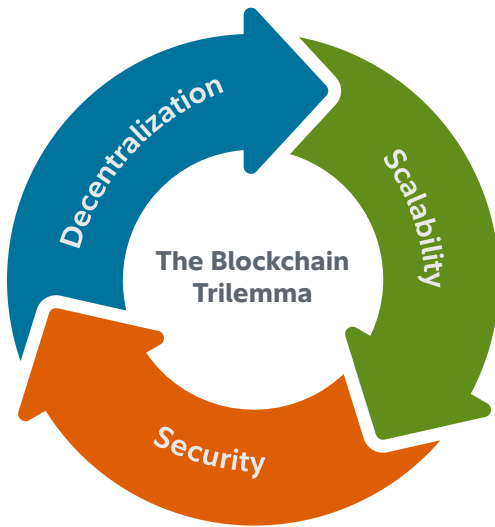
Unfortunately, because of the differences in hashing algorithms, bitcoin’s hash rate can not be directly compared to the hash rate of many other digital assets. Regardless, in terms of sheer computational power required to alter the network’s consensus, bitcoin far exceeds any remaining proof-of-work competitors.

Source: Coin Metrics, 07/26/2023.

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 kind of voting mechanism. In this system, no single entity can control or restrict the data. In an open decentralized network, anyone can join and no entity can exclude them if they follow the network’s rules or protocol. 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

4 See “The CAP Theorem” also known as Brewer’s Theorem for one of the first trade-offs identified between three properties in a decentralized database.

5 Specifically referred to as the “Scalability Trilemma” by Vitalik Buterin, <https://eth.wiki/sharding/Sharding-FAQs>



network would be a completely centralized network where one intermediary controls all aspects of the network. The advantage to this is incredible speed and throughput because there does not need to be a consensus, but the disadvantage is the need to trust this single intermediary.

Bitcoin is arguably the most decentralized digital asset based on many factors. For example, as a Coin Metric report noted⁶, Bitcoin continues to show increasing decentralization as the number of holders has become distributed, active addresses continue to increase, and bitcoin mining pools continue to become more fragmented and competitive. Furthermore, Bitcoin’s computing

power, known as hash rate, has recently undergone a great distribution. Only a few years ago, it was estimated that approximately 75% of the Bitcoin network’s hash rate was coming from operators located in China and only 4% from the U.S. More recently, China’s mining ban created an opportunity for mining to become more geographically distributed. The U.S. now holds the largest share of hash rate by country globally with roughly 38%, followed by China at 21%, and Kazakhstan with roughly 13%, according to the Cambridge Centre for Alternative Finance as of December 2021.⁷

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 the Bitcoin network’s Achilles heel because it maximizes decentralization and security, but as a result, is the network with one of the slowest transaction throughputs. The Bitcoin network adds a new block and validates transactions on average only every 10 minutes, and because Bitcoin’s block size is limited, only so many transactions can fit into each block. To put this into perspective, the Bitcoin network can process approximately three to seven transactions per second, versus a highly centralized payment network, such as Visa, which processes approximately 1,700 transactions per second with the ability to scale and process multiple times if needed.

None of the characteristics above are in and of themselves *better* than another; it depends on the use case. Some users may favor scalability over decentralization or vice versa. Our only point here is to understand that there is an inherent trade-off.

To summarize, we believe Bitcoin is currently the most secure and decentralized monetary network. Therefore, this excludes other networks that are competing in different use cases besides money. We also believe the Bitcoin network will continue to be the most secure and decentralized into the future due to the blockchain trilemma as outlined above and also as exemplified in a real-world example below (the block size war). We also believe that, because monetary networks have massive network effects, Bitcoin’s security and decentralization will only grow stronger over time. Could another network come along in the future that

⁶ <https://coinmetrics.io/measuring-bitcoins-decentralization/>

⁷ https://ccaf.io/cbeci/mining_map



somehow improves upon Bitcoin as a monetary network? We concede that there is a non-zero chance, but believe it is incredibly small—and decreasing—due to the arguments outlined here.

A Real-World Example of Trying to “Improve Bitcoin”: The Block Size War

As previously noted, Bitcoin’s transaction throughput is limited by both the time between when each block is added and transactions are validated (approximately every 10 minutes) and the block size (a little over one megabyte), which limits the number of transactions that can fit into each block.

Therefore, some users and developers proposed a seemingly simple and straightforward way to address this problem: increase the block size to greater than one megabyte. While this may seem to represent a non-controversial and simple change, it actually spawned a fierce war within the developer community that spanned years.⁸

The debate can be summarized by putting the opposing views into two camps: the “small blockers” vs. the “big blockers.” While the block size was the specific piece of code at the center of the debate, the issue at stake was a larger one regarding the principles of what Bitcoin is and how it should or should not evolve. Those that wanted the original block size, or smaller blocks, generally favored robust protocol rules that should be difficult to change with a long-term focus on Bitcoin’s stability. This ethos continues today with many proposed code changes, even upgrades that are considered improvements, failing to get implemented. In the small blockers’ view, any code change could potentially open the Bitcoin network to a new or unforeseen attack vector. The small blockers also believed the ability for individuals or average users to run a personal node was important to preserving Bitcoin’s security and decentralization. Bigger blocks would mean more history to archive in the blockchain and, therefore, make running a node (Bitcoin’s ledger) more difficult and expensive.

On the other hand, the big blockers wanted protocol rules that could be changed more easily and faster to focus on dismantling short-term obstacles or addressing arising opportunities with more of a “start-up” mentality. Larger blocks would allow for higher scalability and faster transactions.

However, increasing the block size does not come without trade-offs. First, larger blocks lead to larger blockchains. Currently, the entire blockchain (all transactions ever recorded on Bitcoin’s open-source ledger) is nearly 500 gigabytes in size.⁹ This makes it feasible for nearly anyone to download the entire blockchain and run a full node from their home computer or even a specially built simple computer that costs as little as \$100. If the blockchain is larger, it would become more expensive and difficult for individuals to run a node and could lead to less decentralization because only corporations or those with the more expensive equipment could realistically build and run nodes.

⁸ For more detail and a first-hand account of this, see “The Blocksize War: The battle over who controls Bitcoin’s protocol rules” by Jonathan Bier (2021)

⁹ <https://www.blockchain.com/charts/blocks-size>

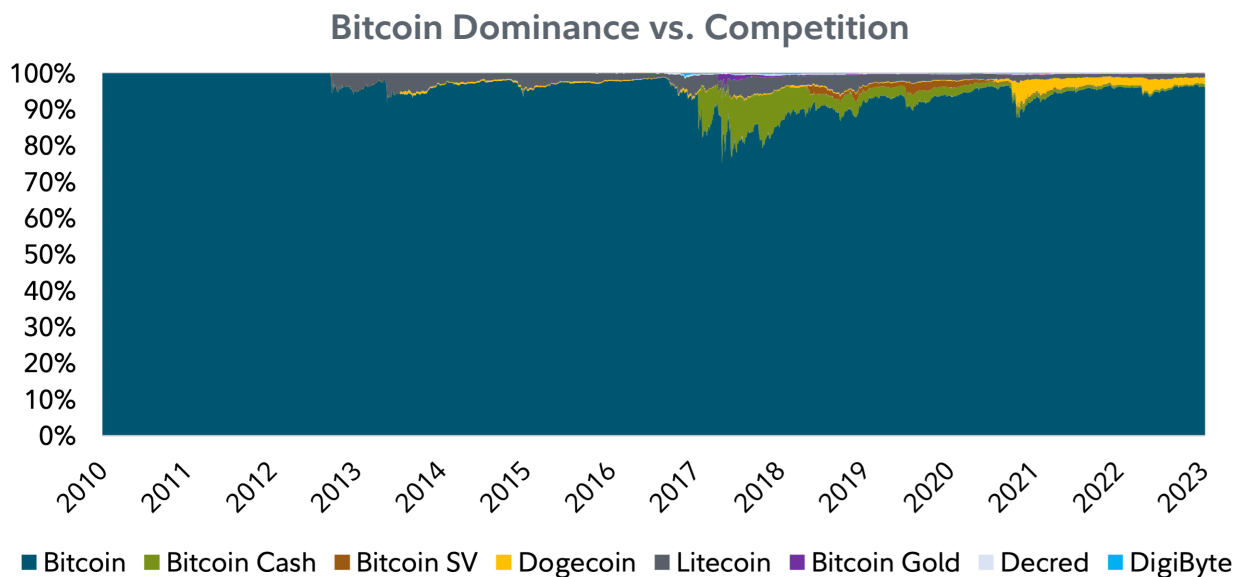


Larger blocks also mean there could be non-full blocks, which would lead to low transaction fees. While this certainly helps scalability, it could conversely lower the incentives for miners, particularly as the block subsidy (the reward bitcoin miners receive for their work) continues to get cut in half every 210,000 blocks, or roughly four years. If miners cease operation, this decreases the security of Bitcoin’s network.

In summary, the block size war demonstrates the Bitcoin network’s blockchain trilemma. Larger blocks could increase scale or throughput, but at the potential loss of decentralization and security.

The other important point about this history is that the changes proposed would (and did) result in a *hard fork*, meaning the change to the code would not be backwards compatible and all nodes would have to upgrade to avoid a split in the network. The various hard forks that have come about because of or in relation to the block size war have either failed completely (such as Bitcoin XT and Bitcoin Classic) or have struggled to gain any kind of market dominance (such as Bitcoin Cash (BCH) and Bitcoin SV (BSV) or “Satoshi’s Vision”).

Bitcoin continues to dominate the market capitalization of all competing currency tokens:



Source: Coin Metrics, 07/26/2023.

Bitcoin Cash (BCH) Case Study

One of the most notable hard forks that arose from the block size war was Bitcoin Cash. Advocates of this hard fork believe bitcoin should, first and foremost, be a literal “peer-to-peer electronic *cash* system,” or a system that can handle large amount of transactions. In other words, Bitcoin Cash advocates believe bitcoin should first focus on becoming a reliable medium of exchange rather than a store of value.

We emphasize that there is nothing inherently “wrong” with this approach, but it once again demonstrates the trade-offs made for scalability. There is also nothing stopping developers and the marketplace from



choosing Bitcoin Cash for faster or cheaper payments at the cost of security and decentralization. However, we can see that, in terms of overall value, with bitcoin's market cap over 100 times greater than Bitcoin Cash (BCH), investors have continued to choose Bitcoin (BTC) as the preferred monetary network and, therefore, appear to value a secure and sound store of value over faster or cheaper payments.

Bitcoin as a Superior Monetary Good is More Valuable than a Better Payment Network

This leads us to another point as to why we believe bitcoin should be considered primarily as a monetary good rather than a payment network. The fact that the market has shown a preference towards bitcoin, which is slower as a payment system compared to other digital assets and blockchains, signals the market currently values a highly secure and decentralized store of value rather than another payment network. As we previously noted, Bitcoin's revolutionary invention was solving the problem of digital scarcity and creating a digital store of value, not making an incremental improvement to a payment system.

Ethereum Case Study

It is beyond the scope of this paper to examine the [Ethereum](#) network and the ether (ETH) token in its entirety. However, it is instructive to observe some of the similarities and differences between bitcoin and ether, which is the second-largest digital asset by market capitalization.¹⁰

From its inception and as an idea published in a 2008 whitepaper¹¹, Bitcoin set out to solve the problem of a "purely peer-to-peer version of electronic cash."¹² Its network 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 supply cap of 21 million, giving bitcoin the ability to become a monetary good and store of value.

Ethereum also started as a whitepaper, originally published in 2013 by Co-Founder Vitalik Buterin.¹³ In summary, Ethereum set out to take the blockchain technology pioneered by Bitcoin and extend it to include more capabilities, most notably the ability to do more complex transactions. From the Ethereum whitepaper:

"What Ethereum intends to provide is a blockchain with a built-in fully fledged Turing-complete programming language that can be used to create "contracts" that can be used to encode arbitrary state transition functions..."

¹⁰ <https://coinmetrics.io/crypto-prices/>

¹¹ <https://bitcoin.org/bitcoin.pdf>

¹² Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. <https://bitcoin.org/bitcoin.pdf>

¹³ <https://ethereum.org/en/whitepaper/>



This allows the Ethereum blockchain network to host and run “smart contracts” that can be used to program different kinds of applications. It is for this reason that some like to refer to the Ethereum network as a “distributed world computer.” The network also allows different tokens to be issued on the Ethereum blockchain. This network acts as a kind of platform that others can use to build multiple applications on top of, including decentralized finance (DeFi) applications, games, social media tools, etc.

While Ethereum may be viewed by some as a superior or more advanced network than Bitcoin, the additional capabilities and flexibility come at a cost, most notably a more complex network that increases the chance for software bugs as well as less decentralization and potential decline in security.

Below is a summary of some of the differences and trade-offs between the Bitcoin and Ethereum networks:

BITCOIN NETWORK		ETHEREUM NETWORK
Decentralized, secure, monetary network	Primary Purpose	Distributed world computer, a multipurpose platform
Slow and deliberate	Speed of improvement implementation	Faster and more responsive to user demand
No	Programmable or Smart Contracts?	Yes
No, only bitcoin	Ability to host multiple tokens?	Yes
Fixed, pre-programmed, and has never changed	Monetary Policy	Has changed and is expected to change again ¹⁴
Yes, easy to audit at any time (can be done with consumer-grade computer)	Auditability (How many tokens exist?)	Can be audited but may be more difficult ¹⁵
Very decentralized	Level of Centralization	More centralized ¹⁶
Cheap (~\$100)	Cost of node	Expensive (32+ ETH)
Proof-of-Work	Consensus Mechanism	Proof-of-Stake ¹⁷

¹⁴ <https://decrypt.co/84520/ethereum-supply-pace-shrink-eth-2-upgrade>

¹⁵ <https://www.coindesk.com/tech/2020/08/11/how-much-ether-is-out-there-ethereum-developers-create-new-scripts-for-self-verification/>

¹⁶ A 2019 analysis suggested over 60% of all Ethereum nodes were hosted on a handful of major cloud provider services: <https://chainstack.com/the-ethereum-cloud-vs-on-premises-nodes-conundrum/>

¹⁷ <https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/>



How Bitcoin May Position Itself Against the Rest of the Digital Asset Ecosystem

As previously noted, Bitcoin's open-source nature enables individuals to easily copy, alter, and build off of the original Bitcoin base code for their own tokens and projects. This has allowed for the creation of a massive amount (literally thousands) of alternative coins (or "alt-coins"), leading to confusion for newcomers to the space, at times causing some to misstate that bitcoin is not scarce because there are hundreds of other digital assets.

However, from our discussion thus far, we have proposed:

- The Bitcoin network is not compatible with other blockchain networks and bitcoin tokens are not fungible with other tokens. Therefore, *bitcoin* tokens are scarce, while digital tokens broadly speaking are not scarce.
- The primary value driver of bitcoin tokens is scarcity and reliable supply cap.
- Bitcoin is best understood as a monetary good.
- Bitcoin is likely to be the primary monetary good and another digital asset is not likely to supersede bitcoin in this role.

In addition, we have seen that Bitcoin is currently the most secure and decentralized network but, at the base or native network layer, it is not the most scalable. Bitcoin's network also is *not designed to enable additional functionality or programmability*, as we have seen in our comparison to Ethereum.

Because of these inherent trade-offs, we have seen a boom in the digital asset ecosystem with thousands of different projects all looking to achieve some different level of usability to fulfill a market need.

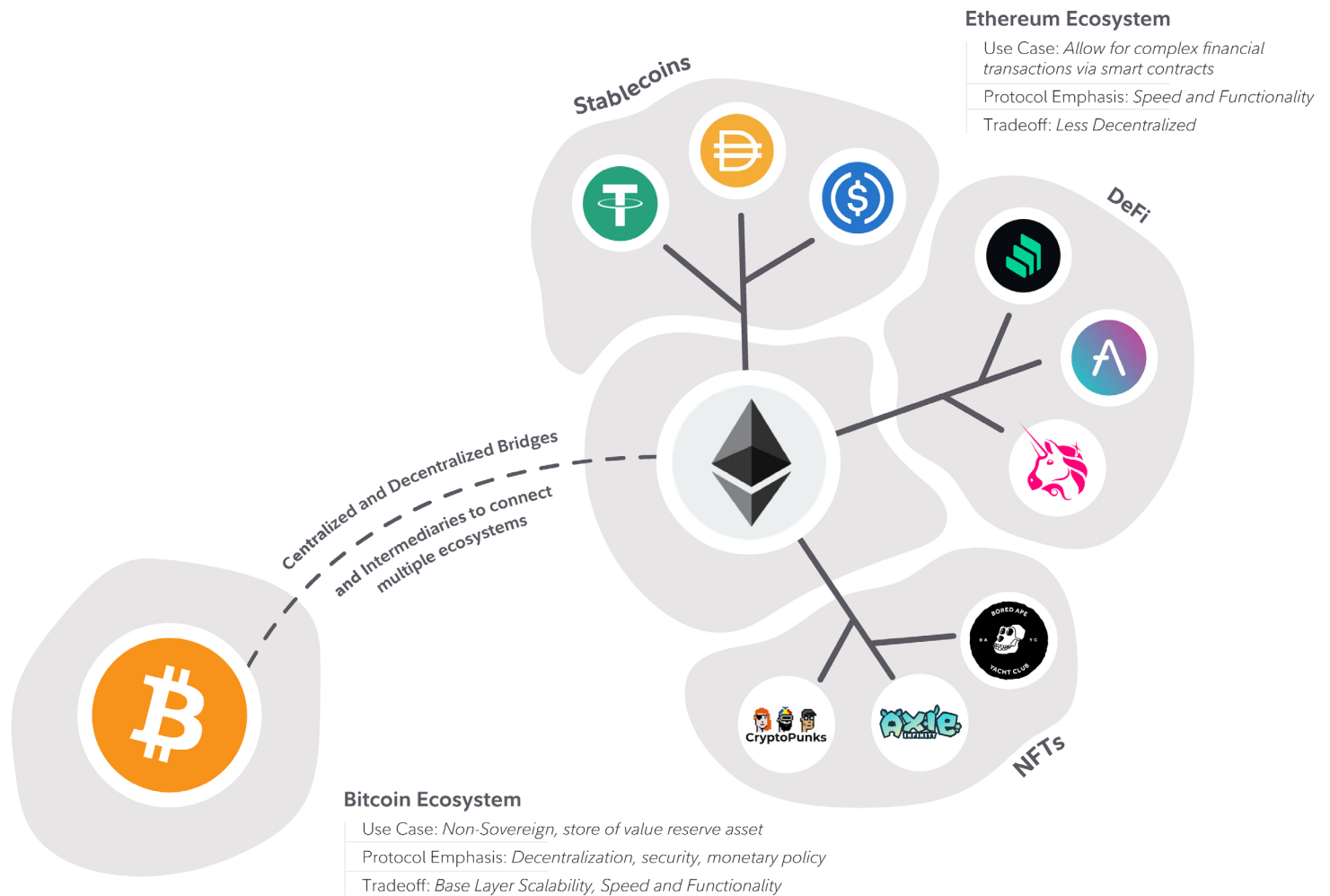
Naturally, investors wonder what the eventual end state of this innovation may look like. Although no one knows exactly what bitcoin may become, we think it is instructive to examine two dominant narratives that have grown popular for envisioning the future digital asset ecosystem. Particularly, we are interested in how Bitcoin may assert itself in each of these scenarios.

1. A Multi-Chain World

The current construction of various tokens has led to a relatively siloed digital asset universe with developers opting to work within a particular ecosystem. For instance, Bitcoin's construction is fundamentally different than that of Ethereum's. The result is that Ethereum and its entire ecosystem of tokens and non-fungible tokens (NFTs) are incompatible with native Bitcoin and unable to interact in an easy and trustless manner. To date, trusted third parties have been a critical requirement for swapping assets that live in different silos.



Bridges are being constructed to connect various blockchain ecosystems to one another, an important theme we have observed and expect will continue in the years ahead. Interoperability will be a key development for the success of the digital assets ecosystem if we are to assume that multiple chains will win because of various base layer trade-offs, use cases, and value propositions.



In a world of multiple winning chains, it still appears that Bitcoin is likely the best equipped to fulfill the role of the ecosystem's non-sovereign monetary good with relatively less competition than other digital assets attempting to fulfill alternative use cases. The explicit emphasis on security and maximum decentralization reinforces its ruleset and equally enforces all users' rights. Furthermore, because of its scarcity and supply limit, Bitcoin is the closest a digital protocol could be to enforcing absolute scarcity. In other words, any other project or blockchain network that requires its users to believe they are transacting with a token that has real monetary value likely needs to be directly or indirectly connected to bitcoin as the ultimate monetary good. For example, people use tokens at an arcade for ease of use and utility and attribute value to them because they know they represent a certain dollar amount or can be traded for other goods and prizes. However, outside of the native arcade environment, the tokens have little to no value.



This world leaves non-Bitcoin tokens battling to prove other viable use cases for their technology. They are aiming to find the right trade-off for some particular level of base layer scaling and encountering vast competition for development and functionality enhancements. This is not an indictment of those building on or investing in non-Bitcoin chains, but merely an observation that bitcoin's clear advantage as a store of value asset may reduce its risk, even in an ecosystem with many vibrant digital assets. Assuming this outcome, bitcoin is still a clear beneficiary of flows into the overall digital asset space because it is viewed as the ultimate monetary digital asset, making it arguably the greatest risk-adjusted and easiest investment to understand and allocate towards across the entire digital asset landscape.

2. A Winner-Take-All-or-Most World

Blockchains are undoubtedly an important technological creation. The ability to take an otherwise centralized database of information and remove a trusted third party was a radical, not incremental innovation. However, a *centralized* blockchain is relatively indistinguishable from a database that has existed for decades and reduces or negates the important qualities offered by a decentralized blockchain, including immutability, seizure resistance, censorship resistance, and trustless design.

Thus, we can envision a spectrum of decentralization that has taken place with tokens. This varies from as decentralized as possible (Bitcoin) to tokens whose protocols are decentralized in name only and give exorbitant power to developers or certain community members. Therefore, there is a possible scenario where users and investors prefer different tokens based on the trade-off of less decentralization for more features, similar to the multi-chain world described above.

However, there is another scenario that could arise due to the ability for applications and scaling solutions to be built on top of the "base layer" or "layer one" blockchains. If applications can be built on top of an existing blockchain network rather than be forced to start a new network, users would arguably want to build on top of the strongest, most secure network(s). Therefore, we could see a world in which one or very few of these chains accrues the majority of the value in the digital asset ecosystem and is chosen as the premier blockchain network. Given that Bitcoin is arguably the most decentralized and immutable blockchain in existence, it appears as a prime candidate to be one of, or perhaps even the sole winner, if this situation were to play out.



THE INTERNET OF INFORMATION TODAY...



THE INTERNET OF VALUE TODAY...



The internet and its base layer, TCP/IP, provides the perfect example of this. The internet protocol suite known as TCP/IP is an open-source base layer for communication to flow through and, subsequently, applications and content on top of which to be built. The TCP/IP protocol is not owned by anyone and, as it is open source, this internet of information does not allow ownership of the base layer. Rather, ownership is only possible for the applications and technology constructed

Source: Jesse Myers (@Croesus_BTC on X, formerly known as Twitter).¹⁸

on top of it. In contrast, ownership of the base layer is possible in the digital asset world. Like TCP/IP, applications can also be constructed using the base layer and then these technological upgrades enhance the value captured of the base layer. Innovations from Amazon, Facebook, Google, Netflix, and others made the Internet’s base layer far more valuable and important. Similarly, the innovation taking place in and around particular digital asset protocols makes their respective base layer ownership breadth increase and enhances its use cases and usability.

What is interesting about this architecture is that an investor can own part of the base layer of this new technology and can be relatively agnostic about what specific applications are built on top of it. It would be akin to being able to own the base layer of the Internet and getting exposure to all of the innovation built on top of it (e.g., Google, Amazon, etc.) without having to try to pick specific winners and losers.

The Bitcoin Lightning Network

One interesting “layer two” application we are already witnessing being built on top of the core Bitcoin network is the lightning network. This is a decentralized network that is built using smart contract functionality and allows off-chain transactions between persons but with the ability to make a final settlement transaction on the base layer Bitcoin network. A simple analogy of this would be participants opening a private tab between each other, transacting back and forth with greater speed and very low transaction fees. This increases Bitcoin’s scalability, but with the option to settle at any time on the base layer it still benefits from Bitcoin’s security.

¹⁸ https://twitter.com/Croesus_BTC/status/1367165017280237569



Bitcoin is Aiming to Satisfy a Clear Market Need

Of course, we do not know what the new digital asset system will look like as it continues to mature, whether we will see a multi-chain world of different tokens with varying degrees of centralization, or if we will see a winner-take-all approach where more applications are built on the most secure and decentralized chain. However, it appears at this point that Bitcoin has found a role in the digital asset ecosystem as a scarce, store of value asset at the very least. The ability for most of the other digital assets to fulfill some other necessary use case still remains to be seen in our opinion, although there has been significant progress over the past few years in terms of other assets finding their product-market fit. The same can not be said for Bitcoin. This creates far different risk-return investment profiles between Bitcoin and all other digital assets and ultimately should impact how allocators consider incorporating each into their investment portfolio.

Digital Assets' Place in a Portfolio

Investors working through their understanding of digital assets and creating a framework for considering investment in the space are likely to benefit from segmenting bitcoin and all other digital asset investments as separate decisions. This simplifies the portfolio construction process and allows for two simultaneous yet separate decisions to be made by allocators: the importance of holding exposure to the scarcest monetary asset (bitcoin) in this emerging digital asset category, while also considering the potential for exposure to the innovation and experimentation ongoing within the ecosystem outside of bitcoin.

To understand the proper place of bitcoin and non-bitcoin tokens in a traditional investment portfolio, investors must first derive the key risk and return drivers of their respective investment theses. This makes it possible to delineate the two and draw a conclusion upon the potential role each could play within an otherwise traditional portfolio.

Bitcoin's Risks, Potential Sources of Return, and Role in a Portfolio

The first-mover advantage led to a lack of true competition for bitcoin's primary use case as a monetary asset and a store of value and creates a drastically different return profile for bitcoin investors. Many of the risks and [criticisms](#) that could've been used to create a case for the demise of bitcoin are gone or diminishing and each day the network grows stronger with more users, miners, and infrastructure being built. Almost every risk that bitcoin still holds today can also be seen amongst every other digital asset, with nation-state attacks and protocols bugs being two of the most notable network risks.

Protocol Bugs: The potential for a vulnerability in any code is always a present threat. This problem can be mitigated by keeping the software simple and engaging in thorough review and scrutiny of the code. In Bitcoin's case, it is arguably the least likely protocol to encounter a major bug at this stage in its life because it has existed longer than any other project, holds an intentionally simplistic code, and has a roughly \$1 trillion bounty for anyone capable of exploiting it.



Nation-State Attacks: Another valid risk to the Bitcoin thesis is the potential for large countries to oppose the growth of digital assets. The geopolitical landscape to date has made proper regulation appear far more likely than outlawing these assets. In any case, Bitcoin is best positioned to defend itself against coordinated attacks due to its level of decentralization.

The risks bitcoin faces today appear lower in comparison to all other digital assets because of the lack of code complexity and emphasis on decentralization. Little to no true competition for its primary use case and 14+ years of operating as the de facto store of value token help to harden the case that bitcoin will continue to exist as the digital asset ecosystem's bedrock.

In other words, it is not that we think an allocation to bitcoin does not come without risks, but that we think some investors are overestimating the downside risks of bitcoin when compared to other digital assets.

We also think some investors may be doing the same with the return side of the equation, but in the opposite direction, as they may be underestimating the potential returns of bitcoin compared to other digital assets. There is some merit to this idea as bitcoin with a market capitalization of around \$1 trillion may have a harder time appreciating by a factor of 100 compared to its early history when it did grow by a factor of 100 (more than once), but from a much smaller market capitalization. However, these gains were accompanied by significantly more risk at the time. As described above, bitcoin's level of risk has dramatically reduced from its early days.

Bitcoin's return profile is driven by two strong tailwinds: the global growth of the broader digital asset ecosystem and the potential instability of traditional macroeconomic conditions. These bitcoin return tailwinds are likely to be captured in an easier way with less risk than via the majority of other digital assets.

Growth of the Digital Asset Ecosystem: As money flows throughout the entire asset class, the store of value standard gains more legitimacy and importance. Every project, token, or piece of infrastructure being built and funded expands the use case and value associated with having a neutral, scarce, digital reserve asset. While other tokens benefit from money that flows indirectly towards the space, bitcoin is the easiest beneficiary of this growth. As discussed earlier, bitcoin's lack of competition for being recognized as the preeminent store of value asset means that there is little threat to its current stronghold on being the ecosystem's "money." Much of the growth associated with the build-out of all digital assets is good for bitcoin.

Potential Instability of Traditional Macro Conditions: The increasing use of monetary and fiscal policy to support ongoing economic growth may give rise to concerns about the financial system's overall stability and the economy's ability to stand on its own. The build-up of these policies has led to never-before-seen global sovereign debt levels.¹⁹ Historically, leverage has driven financial systems towards fragility. One such potential outcome of the current sovereign debt situation is a path of financial repression (negative real interest rates).²⁰ Historically, these types of macro environments have tended to benefit scarce assets

¹⁹ <https://blogs.imf.org/2021/12/15/global-debt-reaches-a-record-226-trillion/>

²⁰ See for example "The Liquidation of Government Debt" by C. M. Reinhart and M. B. Sbrancia, IMF Working Paper (2015) <https://www.imf.org/external/pubs/ft/wp/2015/wp1507.pdf>



whose supply can not be altered. For example, gold performed extremely well for investors in the 1970s, a period known for its high levels of inflation and negative real interest rates.²¹ In the digital asset world, Bitcoin’s ruleset, historical precedents, and decentralization have created the greatest level 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.

Given the ability to hedge potential outcomes associated with traditional assets and capture overall ecosystem growth, bitcoin becomes a simple and efficient way to gain exposure to the digital asset ecosystem.

Non-Bitcoin Risks and Return Drivers

Many investors often cite the potential for extremely advantageous returns as their reason for overweighting alternative or non-bitcoin digital assets and, in some cases, omitting bitcoin entirely from their portfolio. While this potential return profile may exist for certain digital assets, these projects also often come with greater overall risks and a meaningful chance of the token becoming worthless if it fails to live up to expectations.

The risks with non-bitcoin tokens certainly ranges on a case-by-case basis and tends to become more extreme in longer-tail, more speculative tokens. However, many of these risks are still shared amongst the majority of these projects. A few key risks include:

Exhibiting Adequate Decentralization: Bitcoin’s proof-of-work algorithm, governance structure, and fair launch created the grounds for a decentralized project with minimal trust required. Other tokens have alternative consensus mechanisms, governance structures, and token launches, which often reduce their level of decentralization. Since it is one of the key value propositions promised by many of these protocols, investors should consider how decentralized each project actually is. A lack of adequate decentralization makes a particular protocol more susceptible to regulatory oversight and impairs users’ rights.

The Threat of Competition: Differentiation becomes difficult with open-source code when one platform can copy and build upon the shortcomings of another’s. Historically, many projects have failed and the turnover amongst the most valuable 10 or 20 coins has been extreme. Protocols must build a large enough network effect around their given use case in hopes that they can defend themselves against competitors since almost every non-bitcoin network is attempting to add some level of scalability or functionality to their base layer to prove their worth.

Top 10 Digital Assets by Market Capitalization

	2017	2023
1	Bitcoin	Bitcoin
2	Ethereum	Ethereum
3	XRP	Tether (Stablecoin)
4	Litecoin	XRP
5	Monero	BNB
6	Ethereum Classic	USD Coin (Stablecoin)
7	Dash	Dogecoin
8	Augur	Cardano
9	MaidSafeCoin	Solana
10	Steem	TRON

Source: CoinMarketCap, Date: 07/27/2023

21 <https://www.gold.org/goldhub/data/gold-prices>



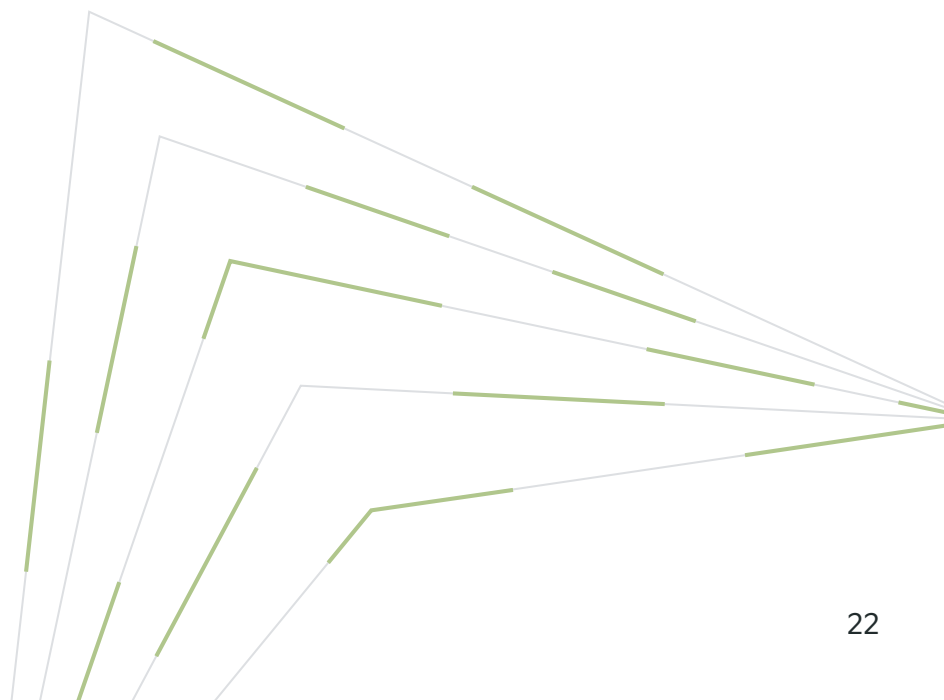
The return drivers of all non-bitcoin digital assets are also much different because protocols are forced to make certain trade-offs to enhance speed, functionality, and other characteristics to warrant a unique use case. Encompassed within all non-bitcoin digital assets is the most important driver of returns:

Attracting Developers and Creating Network Effects: Projects that have shown the ability to be successful and create something promising have done so by attracting the proper talent and retaining their userbase. Ethereum and Solana provide a great example of what is possible for a protocol that can attract a large amount of developers, build a usable platform, and gain a loyal network of users. When done right, there is clearly a lot of value that can be created for investors.

Given the increased amount of competition and potential paths of failure for many of these projects, allocating to non-bitcoin tokens is often done with a venture capital-like mindset. Instead of picking one particular project, investment allocators typically take small positions across many individual names. This typically results in seeking out an actively managed solution to deal with the increase in overall complexity. Again, this shows a stark contrast to a simple bitcoin-only approach to digital assets.

Conclusion

Traditional investors typically apply a technology investing framework to bitcoin, leading to the conclusion that bitcoin, as a first-mover technology, will easily be supplanted by a superior one or have lower returns. However, as we have argued here, bitcoin's first technological breakthrough was not as a superior payment technology, but as a superior form of money. As a monetary good, bitcoin is unique. Therefore, not only do we believe that investors should consider bitcoin first to understand digital assets, but that bitcoin should be considered first and separate from all other digital assets that have followed it.



Why investors need to consider bitcoin separately from other digital assets



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 or the solicitation of an offer to buy or sell securities or other assets. Please perform your own research and consult a qualified advisor to see if digital assets are an appropriate investment option.

Views expressed are as of 06/26/23, based on the information available at that time, and may change based on market and other conditions. Unless otherwise noted, the opinions provided are those of the authors and not necessarily those of Fidelity Investments or its affiliates. Fidelity does not assume any duty to update any of the information.

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, any person or entity in any jurisdiction or country where such distribution or use would be contrary to local law or regulation. Persons accessing this information are required to inform themselves about and observe such restrictions.

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 are not insured by the Federal Deposit Insurance Corporation (FDIC) or protected by the Securities Investor Protection Corporation (SIPC). Fidelity Digital Assets and the Fidelity Digital Assets Logo are service marks of FMR LLC.

The price of bitcoin is volatile, and market movements of bitcoin are difficult to predict. Supply and demand changes rapidly and is affected by a variety of factors, including regulation and general economic trends. All investments will risk the loss of capital. Therefore, an investment in bitcoin involves a high degree of risk, including the risk that the entire amount invested may be lost. No guarantee or representation is made that investing in bitcoin will be successful. Bitcoin exchanges may suffer from operational issues, such as delayed execution, that could have an adverse effect. Several factors may affect the price of Bitcoin, including, but not limited to: supply and demand, investors' expectations with respect to the rate of inflation, interest rates, currency exchange rates or future regulatory measures (if any) that restrict the trading of Bitcoin or the use of Bitcoin as a form of payment. There is no assurance that Bitcoin will maintain its long-term value in terms of purchasing power in the future, or that acceptance of Bitcoin payments by mainstream retail merchants and commercial businesses will continue to grow. Bitcoin is created, issued, transmitted, and stored according to protocols run by computers in the Bitcoin network. It is possible the Bitcoin protocol has undiscovered flaws which could result in the loss of some or all assets held. There may also be network-scale attacks against the Bitcoin protocol, which result in the loss of some or all of assets held. Advancements in quantum computing could break Bitcoin's cryptographic rules and consequently the reliability of the cryptography used to create, issue, or transmit bitcoin is not guaranteed.

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.

Fidelity Digital Assets and the Fidelity Digital Assets logo are service marks of FMR LLC.

This material may be distributed through the following Fidelity Institutional entities, none of whom offer digital assets nor provide clearing or custody of such assets: Fidelity Distributors Company LLC; National Financial Services LLC or Fidelity Brokerage Services LLC.

Fidelity and the third parties listed here are independent entities and not affiliated. Listing them does not suggest a recommendation or endorsement by Fidelity. © 2023 FMR LLC. All rights reserved.

1012662.6.0