BITCOIN FIRST:

Why investors need to consider bitcoin separately from other digital assets

PREPARED BY FIDELITY DIGITAL ASSETS FOR USE BY FIDELITY INVESTMENTS

UPDATED APRIL 2022 (ORIGINALLY PUBLISHED JANUARY 2022)

CHRIS KUIPER, CFA, DIRECTOR OF RESEARCH & JACK NEUREUTER, RESEARCH ANALYST

Fidelity DIGITAL ASSETS℠

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 and 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 necessarily face tradeoffs.
- 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.
- Investors could 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 first 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, until Bitcoin was invented this was not possible in the digital realm. This idea was put into practice by writing code. Therefore, Bitcoin is just code and Bitcoin the network is made up of millions 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 enough 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 cannot 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. Which leads to the question, why do some things become treated as a monetary good while others do not? Economists and historians suggest the answer lies in a number of characteristics that make "good money,"[1] such as being durable, divisible, fungible, portable, verifiable, and scarse with a historical track record. 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 currently 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). Bitcoin does have the shortest history compared to that of gold and fiat currency. Gold has the longest track record as money and purchasing power, while fiat currency has a poor track record.[2]

It is also worth noting that just like other monetary goods, bitcoin is not a company, it doesn't pay a dividend or 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 1.8% is roughly equal to gold's inflation rate at the moment)[3], it is also provably *finite*. There will only ever be 21 million bitcoin. No other digital asset currently possesses an immutable monetary policy on the level of bitcoin.

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 as well as why it is distinct

[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, https://www.frbsf.org/economic-research/files/wp11-22bk.pdf

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

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 the network. As a completely decentralized network that is running open-source code, the participants in the network 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't 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 as 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 we 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.

Second, the Bitcoin network is censorship resistant. Because no person, corporation, or government owns or controls the Bitcoin network, it is believed to be 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 the bitcoin tokens.

2. One of the primary reasons investors attribute value to bitcoin is its scarcity. Its fixed supply is the reason it has the ability to 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 likely 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

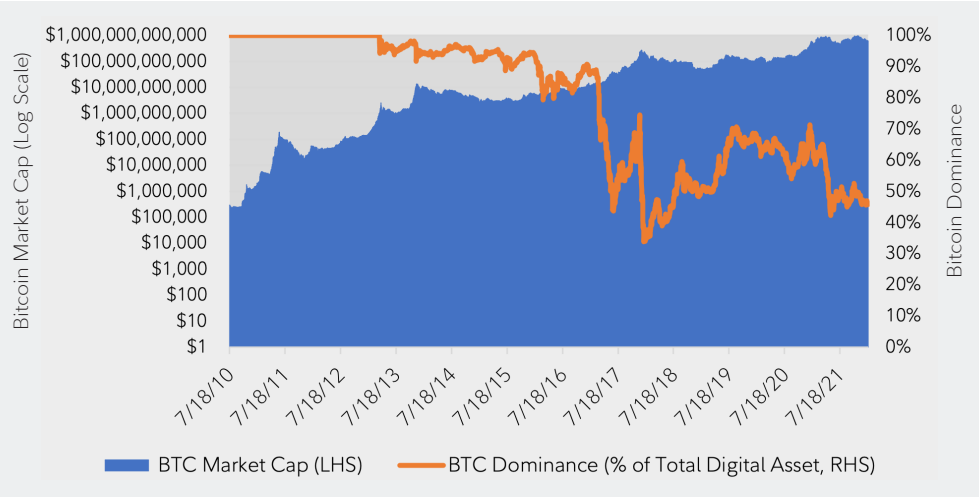
Investors may agree that bitcoin possesses many of the qualities that make for good money, but who is to say that only one monetary good can or will exist?

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, without any other outside influences, then they will naturally choose the one with the largest, most secure, most decentralized, and most 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.

BITCOIN DOMINANCE



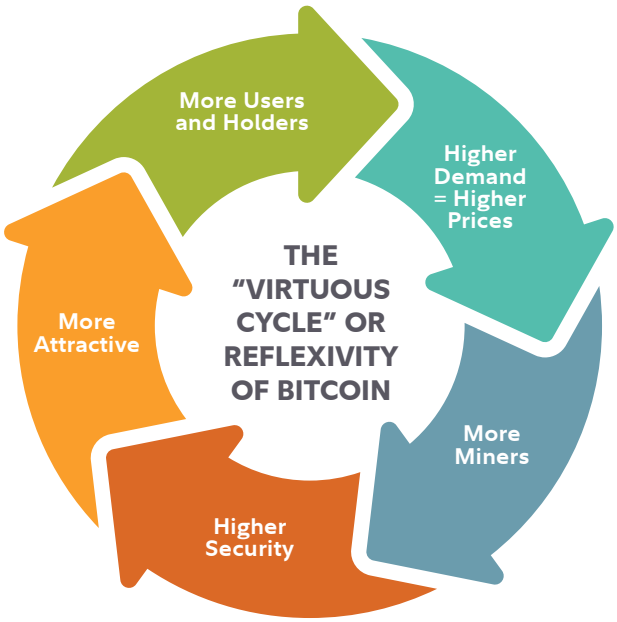
Data Source: Coin Metrics, Date: 1/18/2022

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

In the case of bitcoin, the reflexive property is even more pronounced because it doesn't just include passive holders of the asset, but it also includes 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. Miners are then incentivized to increase their capital expenditure and computing power. More computing power devoted to bitcoin mining leads to higher security of the network, 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. 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 phrase "don't reinvent the wheel" is so common it has become a cliché. Nevertheless, we think this applies to bitcoin as a digital monetary good. The invention of the wheel represented an entirely new technology that once invented could never be reinvented. Similarly, never before in human history had the problem of digital scarcity and a 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 necessarily have to differentiate itself by sacrificing one or both of these properties, an idea we explore in more detail below (the "Blockchain Trilemma"). A competitor that tries to merely copy Bitcoin's entire code will likely 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 ten years is likely to run another ten 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. It is also worth noting this goes hand-in-hand with the property of antifragility, where something becomes more robust or stronger with each attack or time the system is under 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 the negative events that Bitcoin has already endured that have not proven to be the death knell of the network.

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	Has been declared "dead" hundreds of times by major news outlets and famous investors, CEOs etc.
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 due to network effects. However, couldn't a superior or improved version of bitcoin be created and become the dominant monetary good? Isn't bitcoin's code open source so that anyone can copy it and 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 tradeoff 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, where he 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]

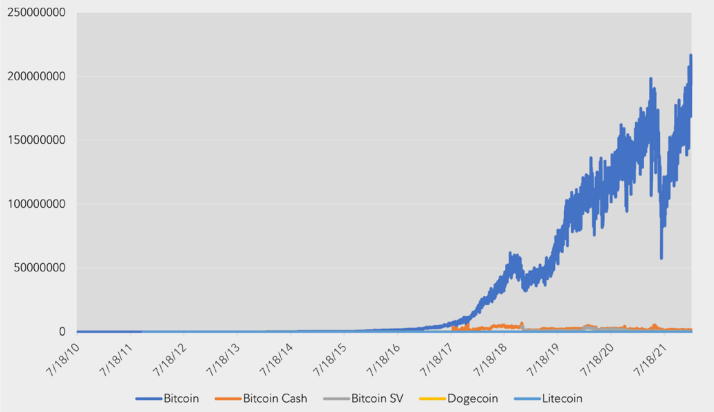
Security refers to how likely it is the network can be attacked or compromised. In the case of a decentralized network like Bitcoin, the main concern is a 51% attack, whereby a single person or entity controls more than half of the Bitcoin network's computing power (known as hash rate). If this is achieved, 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 as can be

[4] See "The CAP Theorem" also known as Brewer's Theorem for one of the first tradeoffs 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

seen in the following graph:

MEAN HASH RATE



Data Source: Coin Metrics, Date: 1/18/2022

Unfortunately, because of the differences in hashing algorithms, bitcoin's hash rate cannot be directly compared to the hash rate of other digital assets, most notably ether, the second largest digital asset by market capitalization. However, we can compare total annual energy usage as a proxy for security, with more energy usage as a measure of more mining resources dedicated to securing the network. On this measure, bitcoin is estimated to consume approximately 137 terawatt-hours (TWh)[6] annualized compared to approximately 25 TWh for Ethereum.[7]

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 is also free to join and no entity can exclude them as long as they follow the rules or protocol of the network. This allows the network to operate without intermediaries. The cost of higher decentralization is lower throughput of the network, 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 where one intermediary controls all aspects of the network. The advantage to this is incredible speed and throughput as there does not need to be a consensus, but the disadvantage is the need to then trust this single intermediary.

Bitcoin is the most decentralized digital asset based on many factors. For example, as a recent Coin Metric report noted[8], 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

[6] Cambridge Bitcoin Electricity Consumption Index (CBECI) (ccaf.io), accessed 1/21/2022
[7] Ethereum Emissions (kylemcdonald.github.io), accessed 1/21/2022
[8] https://coinmetrics.io/measuring-bitcoins-decentralization

recently undergone a great distribution. Only a few years ago it was estimated approximately 75% of the Bitcoin network's hash rate was coming from operators located in China and only 4% from the United States. Most recently, due to China's ban on these activities, virtually none is located in China and now the U.S. holds the top spot at approximately 35%.[9]

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 Achilles heel of the Bitcoin network as 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 is able to process approximately three to seven transactions per second, versus a highly centralized payment network, like Visa, which processes approximately 1,700 transactions per second with the ability to scale and process multiple times if needed.

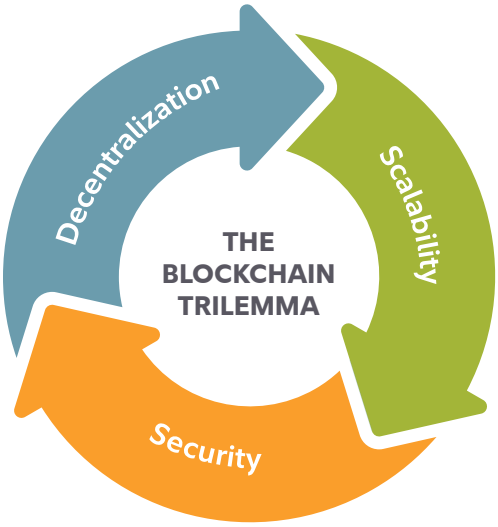
None of the characteristics above are in and of themselves *better* than another. It depends on the use case. Some users may favor scalability over decentralization or vice-versa. Our only point here is to understand there is an inherent trade-off.

To summarize, we believe bitcoin is *currently* the most secure and decentralized monetary network. Therefore, this excludes other networks that are competing on 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 blocksize war). We also believe 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 somehow improves upon bitcoin as a monetary network? We concede there is a non-zero chance, but believe it is incredibly small due to our arguments outlined here.

A real-world example of trying to "improve bitcoin": The blocksize war

As we 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) as well as the

[9] https://ccaf.io/cbeci/mining_map



block size (a little over one megabyte), which limits the number of transactions that can fit into each block.

Some users and developers therefore 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.[10]

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 actually a larger one regarding the principles of what Bitcoin is and how it should or shouldn't evolve. Those that wanted the original block size, or smaller blocks, generally favored robust protocol rules that should be very hard 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 change in the code could potentially open up 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 in order 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 tradeoffs. First, larger blocks lead to larger blockchains. Currently, the entire blockchain (all transactions ever recorded on Bitcoin's open-source ledger) is approximately 400 gigabytes in size.[11] This makes it feasible for nearly anyone to download

[10] 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)
[11] https://www.blockchain.com/charts/blocks-size

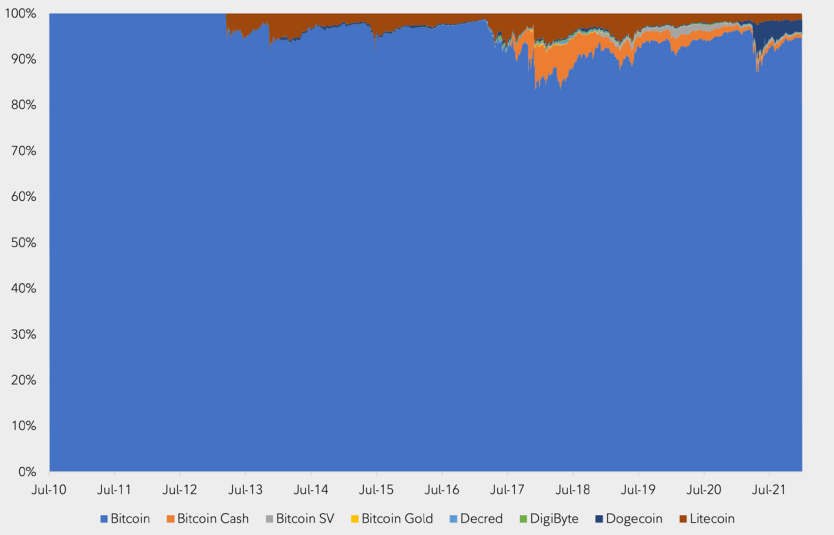
the entire blockchain and run a full node from their home computer or even a specially built simple computer that costs approximately $100. If the blockchain is larger, it would become more expensive and harder for individuals to run a node and could lead to less decentralization as only corporations or those with the more expensive equipment could build and run nodes.

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 due to lower transaction fees, particularly as the block subsidy (the other portion of the rewards miners receive) continues to get cut in half every four years. If miners discontinue operation, this decreases the security of Bitcoin's network.

In summary, the blocksize war demonstrates the blockchain trilemma inherent to Bitcoin's network. 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 in order to avoid a split in the network. The various hard forks that have come about because of or in relation to the blocksize 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 DOMINANCE VS COMPETITION



Data Source: Coin Metrics, Date: 1/18/2022

Bitcoin continues to dominant the market capitalization of all competing currency tokens as can be seen on the graph:

Bitcoin Cash case study

One of the most notable hard forks that came out of the block size war was Bitcoin Cash (BCH). 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 a 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 there is nothing inherently "wrong" with this approach, but it once again demonstrates the tradeoffs made for more 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 100 times that of 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 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 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.[12]

From its inception and as an idea published as a whitepaper, Bitcoin set out to solve the problem of a "purely peer-to-peer version of electronic cash."[13] 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 credibly enforced 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 Vitalik Buterin.[14] In summary, Ethereum set out to take the blockchain technology pioneered by Bitcoin and extend it to include

[12] https://coinmetrics.io/crypto-prices
[13] Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf
[14] https://ethereum.org/en/whitepaper

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..."*

This allows the Ethereum blockchain network to host and run "smart contracts" that can be used to program all kinds of applications. It is for this reason 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 applications, games, social media tools etc.

While Ethereum may be viewed by some as a superior or more advanced network compared to 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 tradeoffs between the Bitcoin and Ethereum networks:

	BITCOIN NETWORK	ETHEREUM NETWORK
Primary Purpose	Decentralized, secure, monetary network	Distributed world computer
Speed of improvement implementation	Very slow and deliberate	Fast and responsive to user demand
Programmable or Smart Contracts?	No	Yes
Ability to host multiple tokens?	No, only bitcoin	Yes
Monetary Policy	Fixed, pre-programmed and has never changed	Has changed and is expected to change again[15]
Auditability (How many tokens exist?)	Yes, very easy to audit at any time	Can be audited but may be more difficult[16]
Level of Centralization	Very decentralized	More centralized[17]
Cost of node	Cheap (~$100)	Expensive
Consensus mechanism	Proof-of-Work	Currently proof-of-work; plans underway to move to proof-of-stake[18]

[15] https://decrypt.co/84520/ethereum-supply-pace-shrink-eth-2-upgrade
[16] https://www.coindesk.com/tech/2020/08/11/how-much-ether-is-out-there-ethereum-developers-create-new-scripts-for-self-verification/
[17] 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/
[18] See "Sustainability" section at https://ethereum.org/en/eth2/vision/

How bitcoin may position itself against the rest of the digital asset ecosystem

As we previously noted, the open-source nature of Bitcoin creates the ability for individuals to easily copy, alter, and build off 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 coins.

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 the scarcity and credibly enforced supply cap.
- Bitcoin is best understood as a monetary good.
- Bitcoin has the potential 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 does not allow for additional functionality or programmability as we have seen in our comparison to Ethereum.

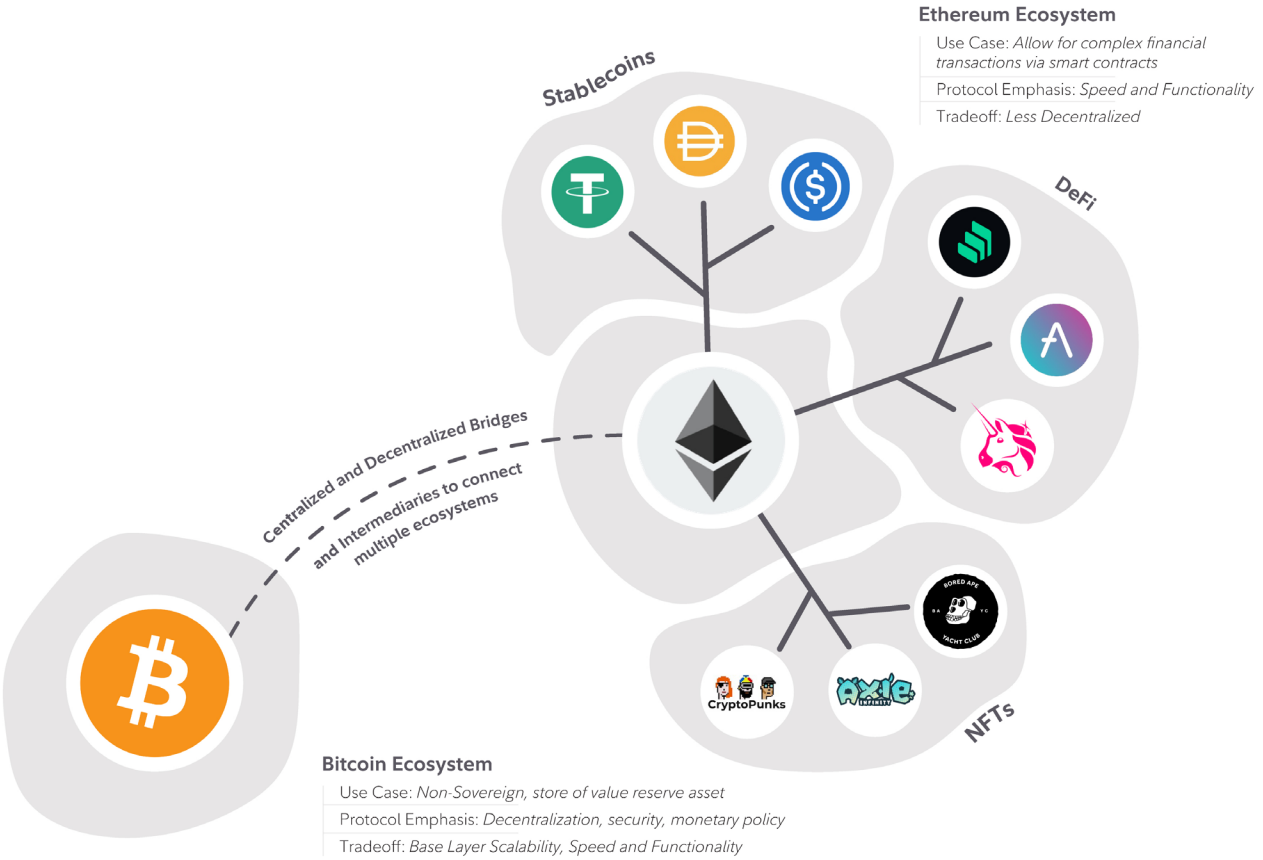
Because of these inherent trade-offs, we have seen a boom in the digital asset ecosystem with hundreds if not thousands of different projects all looking to achieve some different level of usability to fulfill a market need.

Investors of course naturally wonder what the eventual end state of this innovation looks like. Although no one knows exactly what this 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. The result is that Ethereum and its entire ecosystem of tokens and 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 coming months and 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 due to various base layer tradeoffs, 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 enforces all users' rights equally. Furthermore, as a result of its scarcity and enforced supply limit, Bitcoin is the closest a digital protocol could be to enforcing absolute scarcity. In other words, any project or other 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're aiming to find the right tradeoff 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 reduces its risk even in a world that contains an ecosystem of many vibrant digital assets. Assuming this outcome, bitcoin is still a clear beneficiary of flows into the overall digital asset space given that 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 all of the digital asset landscape.

2. A winner-take-all or most world

Blockchains are undoubtably 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 and reduces 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 will prefer different tokens based on the tradeoff of less decentralization for more features. This is 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 networks. 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.

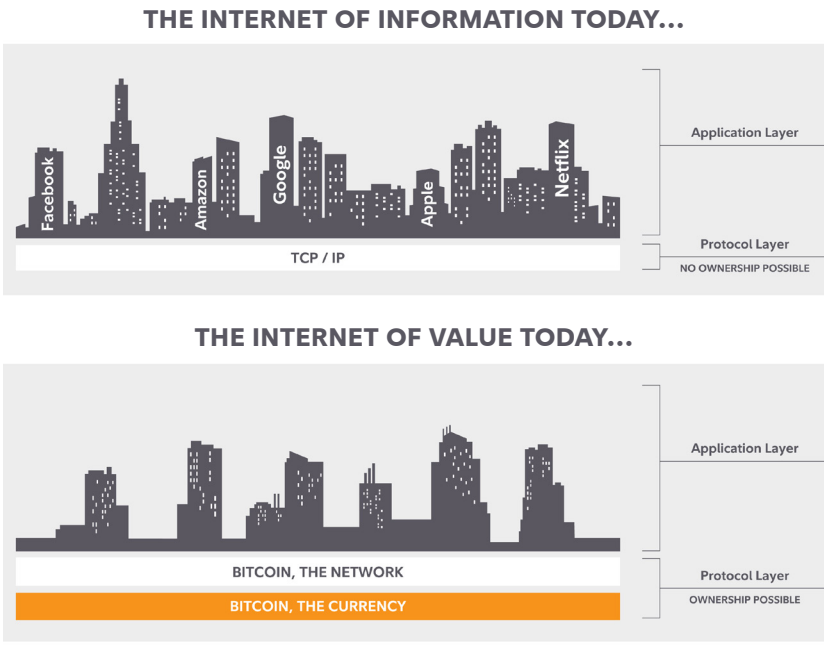
THE BITCOIN LIGHTNING NETWORK

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.

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 to be built on top of. 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 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. The 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 on top (e.g., Google, Amazon etc.).



Source: @Croesus_BTC on Twitter[19]

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, or 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 all of the other digital assets to fulfill some other necessary use case remains to be seen in our opinion. The same cannot be said for Bitcoin.

Digital assets' place in a portfolio

Investors working through their understanding of the digital asset ecosystem 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

[19] https://twitter.com/Croesus_BTC/status/1367165017280237569

holding exposure to the scarcest monetary asset in this emerging digital asset category (bitcoin), while also considering the potential for exposure to the innovation and experimentation ongoing within the ecosystem outside of bitcoin.

In order 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 that could've been used to create a case for the demise of bitcoin are now gone 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. As bitcoin's track record lengthens, it's possible that these risks will take on new importance or that new risks will emerge.

Protocol Bugs: The potential for a vulnerability in any code is always a present threat. This problem can be mitigated by keeping the particular 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 given it has existed longer than any other project, holds an intentionally simplistic code and has a now $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 the digital asset ecosystem. 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 prioritization of decentralization.

The risks bitcoin faces today appear lower in comparison with all other digital assets given the lack of code complexity and emphasis on decentralization. Little to no true competition for its primary use case and 13 years of operating as the store of value token help to harden the case that bitcoin will continue to exist as the bedrock of the digital asset ecosystem.

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 to 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 go up by a factor of 100 (more than once) but from a much smaller market capitalization base. However, these rewards were accompanied by a lot more risk at the time.

Bitcoin's return profile is driven by two strong tailwinds: the growth of the digital asset ecosystem and the potential instability of traditional macroeconomic conditions. These 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 further legitimacy and importance. Every project, token, or piece of infrastructure being built and funded is expanding 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 way to benefit from this growth. As discussed earlier, bitcoin's lack of competition for being recognized as the preeminent store of value asset means there is little threat to its current stronghold on being the digital assets 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 as a way to provide support for ongoing economic growth may give rise to concerns about the overall stability of the financial system and the ability for the economy to stand on its own. The buildup of these policies has led to never-before-seen global sovereign debt levels.[20] Leverage has historically driven financial systems towards fragility. One such potential outcome as a result of the current situation is a path of financial repression (negative real interest rates).[21] These types of macro environments have historically tended to benefit scarce assets whose supply cannot be altered. For

[20] https://blogs.imf.org/2021/12/15/global-debt-reaches-a-record-226-trillion

[21] 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

example, gold's outperformance in the most recent episode of high inflation and therefore negative real interest rates in the late 1970s. 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 a potential hedge for some of the headwinds facing the legacy financial system.

Non-bitcoin risks & 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, it's important to consider that 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 are noted below:

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 being promised by the majority of these protocols, investors should consider how decentralized their particular 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 is able to copy and build upon the shortcomings of another's. Historically, we have witnessed many failed projects 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.

The return drivers of all non-bitcoin digital assets are also much different, given that protocols are forced to make certain tradeoffs to enhance speed, functionality, and other characteristics to warrant a use case.

Encompassed within all non-bitcoin digital assets is the most important driver of returns:

Attracting Developers and Creating Network Effects: Projects which have shown the ability to be successful and create something promising have done so by bringing the proper talent onboard 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, showing a stark contrast to a simple bitcoin-only approach to this digital asset space.

TOP 10 DIGITAL ASSETS BY MARKET CAPITALIZATION

	2017	2022
1	***Bitcoin***	***Bitcoin***
2	***Ethereum***	***Ethereum***
3	***XRP***	Tether (Stablecoin)
4	Litecoin	BNB
5	Monero	Cardano
6	Ethereum Classic	USD Coin (Stablecoin)
7	Dash	Solana
8	Augur	***XRP***
9	MaidSafeCoin	Terra
10	Steem	Polkadot

Source: CoinMarketCap, Date: 1/18/2022

CONCLUSION

Traditional investors typically apply a technology investing framework to bitcoin, leading to the conclusion 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 investors should consider bitcoin first in order to understand digital assets, but that bitcoin should be considered first and separate from all other digital assets that have come after it.

1012662.2.0