CFA INSTITUTE RESEARCH FOUNDATION / **BRIEF**

CRYPTOASSETS
THE GUIDE TO BITCOIN, BLOCKCHAIN, AND CRYPTOCURRENCY FOR INVESTMENT PROFESSIONALS

MATT HOUGAN
DAVID LAWANT

CFA Institute Research Foundation

CRYPTOASSETS

The Guide to Bitcoin, Blockchain, and Cryptocurrency for Investment Professionals

Matt Hougan and David Lawant

CFA Institute Research Foundation

Statement of Purpose

CFA Institute Research Foundation is a not-for-profit organization established to promote the development and dissemination of relevant research for investment practitioners worldwide.

Cover photo credit: Lingxiao Xie / Moment / Getty Images

ISBN 978-1-952927-08-9

CONTENTS

PL Qualified Activity CFA Institute

This publication qualifies for 1.75 PL credits under the guidelines of the CFA Institute Professional Learning Program.

CRYPTOASSETS: THE GUIDE TO BITCOIN, BLOCKCHAIN, AND CRYPTOCURRENCY FOR INVESTMENT PROFESSIONALS

Matt Hougan
Matt Hougan is the chief investment officer for Bitwise Asset Management.

David Lawant
David Lawant is a researcher at Bitwise Asset Management.

INTRODUCTION

Bitcoin, blockchain, and cryptocurrencies burst onto the world stage in 2008, when the online posting of a pseudonymous white paper envisioned a new way to transfer value over the internet.[1]

In the decade-plus since, the cryptoasset market has gone through all the classic phases of a disruptive technology: massive bull markets and crushing pullbacks, periods of euphoria and moments of despair, FOMO (fear of missing out), fear, and everything in between.

As the cryptomarket enters its second decade, one thing is clear: Crypto and blockchains are not going away. Today, cryptoassets boast a combined market cap in excess of $350 billion;[2] major financial institutions, such as Fidelity Investments and CME Group, are heavily involved; large endowments, such as those of Harvard University, Yale University, and Stanford University, are investing, alongside such hedge fund legends as Paul Tudor Jones II; the crypto efforts of leading companies, such as Facebook, PayPal, Visa, and Square, are front-page news; and central banks, from the US Federal Reserve to the People's Bank of China, are discussing how to develop blockchain-enabled digital currencies of their own.

Despite all the excitement, however, significant challenges remain for investors approaching the market.

For starters, the quality of information is poor. Even such basic data as accurate trading volume are hard to come by. Theories about the drivers of cryptoasset valuations are untested and often poorly designed, and they are rarely—if ever—published in peer-reviewed journals. Due diligence efforts from leading consultants are in their infancy, and few people have carefully thought through the role (if any) that cryptoassets should have in a professionally managed portfolio.

More fundamentally, few people even understand what crypto really is or why it might matter. Is it an alternative currency? A technology? A venture capital investment? A specious bubble?

[1]Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," white paper, Bitcoin.org (31 October 2008). https://bitcoin.org/bitcoin.pdf.
[2]Data as of 30 September 2020 from CoinMarketCap (https://coinmarketcap.com).

Increasingly, people are deciding that now is the time to start answering these questions. For financial advisers, the reason is that clients are asking. For fintech executives and central bankers, it is because crypto and blockchains threaten to disrupt their markets. And for professional investors, it is because the returns and low correlations that cryptoassets, such as bitcoin, offer to this point are becoming hard to ignore.

The goal of this document is to provide the inquisitive investor with a clear-eyed guide to crypto and blockchain: what they are, what they are not, and where they might go from here. We want you to walk away confident in your understanding and armed with information to decide how to best position yourself for what is ahead.

Let's dive in.

PART I: THE BASICS—HOW CRYPTO WORKS AND WHY IT MATTERS

The best place to start in understanding crypto and blockchain is with bitcoin.

Bitcoin was the first cryptoasset[3] and today is the largest, and the breakthroughs that allowed bitcoin to emerge underlie all other blockchain and crypto projects. As a result, understanding bitcoin—where it came from, how it works, and what new opportunities and challenges it creates—provides a firm foundation on which to consider the entire crypto and blockchain space.

[3]Although bitcoin was the first successful cryptoasset to reach a significant scale, it built on previous failed attempts. The first such attempt traces back to the 1980s and the development of the Chaum blind signature. Bitcoin's technical architecture also borrows heavily from additional attempts, such as 1997's Hashcash and 1998's Bit Gold and B-Money.

Bitcoin can be approached from two complementary perspectives: as a solution to a long-standing technical problem and as an economic phenomenon that allows people to do things they could not have done before.

This section will attempt to tackle the first perspective, describing at a high level bitcoin's core technical architecture. After building this understanding, we will explore what new market opportunities this novel technical architecture creates.

Understanding Bitcoin: From a White Paper to a New Asset Class

Bitcoin was created by a pseudonymous computer programmer, working under the alias "Satoshi Nakamoto," who published a white paper on 31 October 2008 titled "Bitcoin: A Peer-to-Peer Electronic Cash System"[4] to a then-obscure mailing list of cryptographers. The author described a vision for how individuals could hold, send, and receive items of value digitally, without any trusted intermediary (e.g., a bank or payment processor) in the middle.

On 3 January 2009, shortly after the white paper was published, the software was released, the first bitcoin was minted, and the bitcoin network was launched.

The Problem Bitcoin Was Designed to Solve

As an initial reason why bitcoin (and the broader blockchain space) is important, consider this strange fact about modern life: Although much of our lives have migrated online, money remains stuck in an analog age.

[4]Nakamoto, "Bitcoin."

We do not think about this reality much because we have slick fintech apps and online bank accounts, but the underlying plumbing of our "modern" financial system is archaic. You can feel this, for instance, in the facts that wiring money abroad takes two to four days and paying bills using your online bank account requires an equal amount of time.

Many people assume that the reason our financial system is slow is that banks are lazy and refuse to update old systems, but that is not true. The problem is that transferring items of value online is difficult, harder by far than transferring basic information, such as text messages, emails, and photos.

Consider a simple transaction wherein Alice wants to send Bob $1,000. They do not live close to one another, so Alice cannot give Bob cash. Instead, she sends Bob a check. If Bob and Alice use the same bank, that is great: Bob can cash Alice's check and go on his way. But if Alice banks at Bank A and Bob banks at Bank B, things slow down.

Bank B is not going to credit Bob's account until it knows that Alice's check is good. If it did so immediately, Bob withdrew that money, and Alice's check subsequently bounced, Bank B would be out of luck. Processing that check—making sure Alice's account is not overdrawn and that she has not written multiple checks on the same account—takes days.

The right way to conceive of this problem is as a database problem. Bank A has a database of its accounts, and Bank B has a database of its accounts. However, Bank B cannot see into Bank A's database to know whether an individual account has enough money to allow a check to clear. The process of coming to consensus over the status of accounts—of each bank trusting the other—takes time. If you try to short-circuit that process, the potential for loss is significant.

Modern payment applications, such as Venmo, solve this problem by creating a walled garden with a single database: You can settle transactions instantly in Venmo, but only with another Venmo customer. Try to move your money out of Venmo, and things bog down. (Also, you have to trust Venmo to hold your money.)

Allowing money or items of value to move the way text messages do between any two people and without any central intermediary requires a different solution.

A Distributed and Decentralized Database

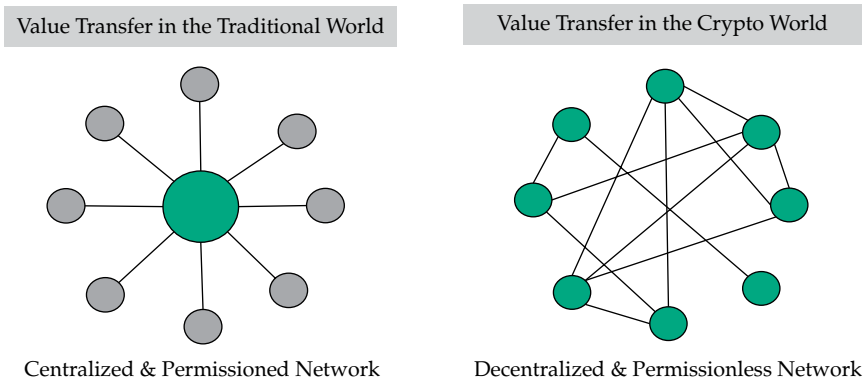
Nakamoto's solution to this problem (and the core idea behind all blockchain databases today) was to create a single distributed database that is accessible to everyone—where anyone in the world can view balances and submit transactions at any time—but where the ledger is not controlled by any single corporation, government, person, or entity. In other words, a "distributed ledger" that is "permissionless" and is maintained on a "decentralized" basis.

Figure 1 shows how this kind of distributed and decentralized database is structured and how it allows value to transfer directly on a peer-to-peer basis, without a trusted central intermediary.

The value of such a database is obvious. If every party can agree on the status of the database at any time, the delays required to allow Database A to sync with Database B can be massively reduced.

Although simple in concept, implementing this new database architecture involved surmounting several significant technical challenges that

FIGURE 1. CRYPTOASSETS DO TO VALUE WHAT THE INTERNET DID TO INFORMATION



had bedeviled computer scientists since the 1980s.[5] Chiefly, if you have copies of the same database floating around on a million different machines and no one is in charge, how do you make sure all copies are identical, are updated synchronously, and reflect only honest transactions?

In other words, how can one reliably create consensus about what is accurate and true?

This is the real breakthrough of blockchains: creating timely, bad-actor-proof consensus across all copies of a decentralized and distributed database. Doing so involves a cascading series of technological steps governed by clever incentives, cryptography, and other technological advancements. These steps lie at the heart of both the opportunities and the challenges created by blockchain applications, so understanding how they are structured and work is worthwhile.

How a Bitcoin Transaction Works

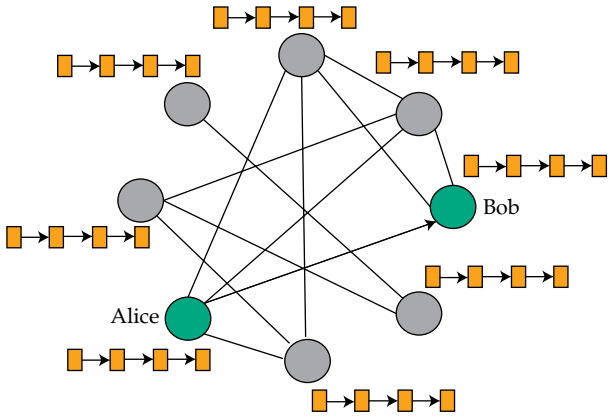
The best way to understand how the consensus formation process works is to follow a bitcoin transaction from start to finish.

Let's say that Alice has 10 bitcoin that she wants to send to Bob. Alice sends a message to all the computers that run a copy of the up-to-date database ("the Bitcoin network") that says, effectively, "I want to send 10 bitcoin to Bob." Alice has a unique password (called a "private key") that lets her sign the message so that the network knows the message is coming from her and not from anyone else. Computers in the bitcoin network can easily confirm that Alice has 10 bitcoin to send because they each have a copy of the current database.

Importantly, at this point the transaction has only been proposed; no computer has updated

[5]This problem of how to digitally transfer an item of value directly is a particular case of a problem described in the computer science literature in the seminal paper "The Byzantine Generals Problem," published in 1982 (Leslie Lamport, Robert Shostak, and Marshall Pease, *ACM Transactions on Programming Languages and Systems* 4 [3]: 382–401). The paper defined the challenge as how to reach consensus in an unreliable system where no one party can trust the next—exactly the problem outlined in our example of two databases trying to come to consensus. The paper is available at http://people.cs.uchicago.edu/~shanlu/teaching/33100_wi15/papers/byz.pdf.

FIGURE 2. SIMPLIFIED DIAGRAM OF NETWORK STATUS PART 1: ALICE PROPOSES A TRANSACTION TO THE NETWORK



its copy of the ledger yet. Transactions are initially placed into what amounts to a waiting room, where they sit waiting confirmation. Because the transaction is only being proposed and not settled, the system can rapidly relay the message to ensure every participant is aware of it.

The process is shown in **Figure 2**. Alice and Bob are represented as the green circles. The orange rectangles represent sequentially updated copies of the ledger at the time Alice proposes her transaction to the network.

Alice is not alone, of course: While she is sending her message, others are sending messages, too, wanting to send their bitcoin to various recipients.

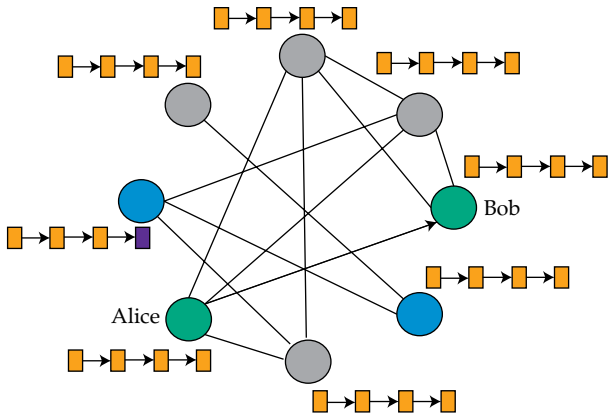
This is where a special participant in the network enters: "bitcoin miners." Miners are computers that are scattered around the world and form a critical part of the bitcoin network. Their job is to aggregate groups of valid new transactions, such as Alice's, and propose them for settlement. These groups of transactions are called "blocks," which is where the "block" in "blockchain" comes from. In Figure 3, the blue dots represent miners.

At any given time, thousands of these computers are competing with each other for the right to settle the next block. The competition involves solving a challenging mathematical puzzle, and miners can propose a new block only if they solve the current puzzle. Whoever finds the solution first is entitled to a reward, which consists of newly minted bitcoin and potentially transaction fees, which have been paid by the entity initiating the transaction.[6] The reward is significant: Each new block currently comes with a reward of 6.25 newly minted bitcoin, worth roughly $70,000 at the moment.[7] This payment is what incentivizes miners to perform the work necessary to verify transactions and maintain the database.

[6]Users who propose transactions, such as Alice, can append small fees to them to incentivize miners to settle their transaction ahead of other pending transactions. These fees are typically *de minimis*, though they can become significant if the network is busy.

[7]Data as of 30 September 2020, based on a closing price of $10,784, as reported at https://coinmarketcap.com.

FIGURE 3. SIMPLIFIED DIAGRAM OF NETWORK STATUS PART 2: A BITCOIN MINER BUILDS A BLOCK OF TRANSACTIONS THAT CONTAINS ALICE'S TRANSACTION



New blocks are settled on the bitcoin network roughly every 10 minutes, though the exact time depends on how quickly the puzzle is solved.[8]

This process is illustrated in **Figure 3**. Aside from Alice and Bob in green, the bitcoin miners are now represented as blue circles. The purple rectangle shows the updated ledger that includes a number of new transactions, including Alice's. For now, only one network participant (the miner who proposed the new block of transactions) can see the fully updated ledger; all other participants still only see the older blocks, which are depicted in orange.

Because the reward is significant, many miners compete to settle each block of transactions. Competing is expensive—by design, solving the puzzle takes significant computing power and burns a lot of energy—and knowing which of the thousands of miners will solve the puzzle first is impossible.

Once a miner *does* solve the puzzle, however, it can post the solution and propose a block of transactions to the network. The peculiar genius of the system is that although solving the mathematical puzzle is difficult and expensive, checking the result is trivially easy. And when a miner posts a solution and a block of transactions, other members of the network check the work. If the transactions are valid and the puzzle solution is correct, network participants update their copy of the database to reflect the new transactions. At that point, Alice's transaction is considered settled![9]

[8]The bitcoin blockchain's software automatically updates the difficulty of the puzzle roughly every two weeks, such that increases in the computer power focused on bitcoin mining does not alter the roughly every-10-minute cadence of new block production.

[9]In practice, many users wait for a small number of additional blocks (typically one to three, but sometimes as many as six) to settle before considering a transaction truly final.

One challenge a decentralized and distributed database, such as the bitcoin network, faces is that, because of communication delays, two miners could propose blocks of transactions at the same time without knowing about each other. You could imagine, for instance, a miner in Iceland and another in Japan proposing blocks at virtually the same time, before news of the other block could travel

Importantly, the competition to settle the next block of transactions depends on including the information from the previous block, which both provides the incentive for market participants to rapidly update their copy of the database and ensures that tampering with a settled block is very difficult. This "chaining together of blocks" is why this database architecture is called a "blockchain."

What if, you might be wondering, the unknown bitcoin miner submitting a block is a bad actor and proposes an invalid block of transactions that somehow benefits it? Or what if Alice herself is malicious, and she is trying to send the same 10 bitcoin to both Bob and Carol at the same time without anyone noticing?

Network participants examine each transaction in each proposed block and reject blocks with invalid transactions. Today, more than 40,000 computers[10] are independently verifying every single bitcoin transaction.[11] Because the work of validating transactions and ensuring that only valid transactions are settled is trivially easy for network participants and attempting to settle transactions is costly, the incentive to even try to defraud the system is minimal. This "consensus algorithm" is the heart of a blockchain network and arguably the most ingenious part of Satoshi Nakamoto's breakthrough.

This process is depicted in **Figure 4**. All network participants have now accepted the new block of transactions proposed (purple rectangle). As a result, their ledgers are updated and synchronized.

The most impressive feature of bitcoin's technical architecture is that it works. Ten years after this novel system design was first outlined by its anonymous author, the bitcoin blockchain has shown a track record of running and holding tens and even hundreds of billions of dollars of value securely and of processing only valid transactions, with nearly 100% uptime. The database has never been hacked and currently settles roughly the same value of transactions each year as PayPal,[12] all without a single employee or central organizing figure.

It is a true technical breakthrough—a significant advance in software and database design—and it is having a significant impact on the world.

around the world. In this situation, some miners might begin searching for additional blocks to add on to each of the chains, creating divergent databases.

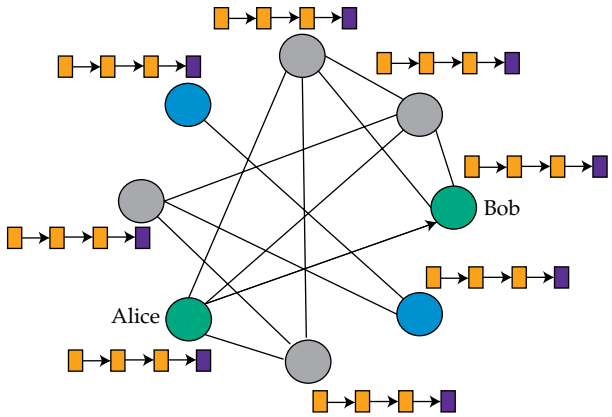
To solve this (rare) problem and ensure that databases return to a synchronous state, the bitcoin blockchain has a rule that the chain that has used the most computational power to solve for blocks is the valid chain. Because two divergent chains cannot continue to propose blocks at precisely the same pace, as multiple blocks pile up, one chain will inevitably emerge as the valid one, and all activity will focus on it. The likelihood of two divergent chains existing decreases with extreme rapidity as additional blocks are settled, such that after a very small number of blocks, users can be certain only one chain exists. A common analogy is to think of each block as a layer of amber around a fly: As time passes, the fly becomes buried deeper and deeper in computational effort and is, therefore, more difficult to tamper with.

[10]Luke Dashjr, a respected bitcoin core developer, regularly publishes an up-to-date and widely-cited estimate of the bitcoin network node count (i.e., the number of computers independently verifying each bitcoin transaction). As of 30 September 2020, this number was 46,056. The estimate can be retrieved at https://luke.dashjr.org/programs/bitcoin/files/charts/historical.html.

[11]For an excellent in-depth and technical view of how the bitcoin network shuns invalid transactions, we suggest the article "Bitcoin Miners Beware: Invalid Blocks Need Not Apply," written by pseudonymous crypto researcher StopAndDecrypt on 1 June 2018 and published on Medium (https://medium.com/hackernoon/bitcoin-miners-beware-invalid-blocks-need-not-apply-51c293ee278b).

[12]In the first half of 2020, the bitcoin network settled more than $358 billion in transactions (according to Coin Metrics), nearly comparable to PayPal's $412 billion (according to Statista).

FIGURE 4. SIMPLIFIED DIAGRAM OF NETWORK STATUS PART 3: ALL NETWORK PARTICIPANTS VALIDATE AND ACCEPT BLOCK PROPOSED BY MINER



Beyond the Technical Breakthrough: Bitcoin as a Novel Economic Phenomenon

Now that we have established how a blockchain works technically, the next question is, What impact might this new database architecture have on the world?

Answering that question is not easy. Attempting to do so is somewhat like trying to guess in the early 1990s how the internet would change the world. The internet clearly represented a new way to distribute information and could have major consequences, but moving from that to predicting that people would, for example, regularly use smartphones to rent out a stranger's house rather than staying in a hotel is a whole different matter.

Similarly, blockchains clearly represent a new way to transfer valuable assets and money, but moving from that to precise predictions of future applications is fraught.

Rather than attempting to answer this question with specificity, we will outline the fundamental, disruptive new capabilities blockchains offer and broadly define the three areas in which we believe those capabilities are likely to have an impact on the world.

Capability 1: Rapid, Low-Cost, 24/7 Settlement

The first disruptive capability has to do with settlement. As discussed, blockchains such as bitcoin provide a massive improvement over existing settlement paradigms.

Consider this transaction: On 12 April 2020, someone transferred 161,500 bitcoin—worth more than $1.1 billion at the time—in a single transaction. The transaction settled in 10 minutes, and the fee for processing the transaction was $0.68.[13]

Contrast that with an international money wire, which can be sent only during banking hours,

[13]Turner Wright, "Bitfinex Made a $1.1 Billion BTC Transaction for Only $0.68," Cointelegraph (13 April 2020). https://cointelegraph.com/news/bitfinex-made-a-11-billion-btc-transaction-for-only-068.

takes one to two days to settle, and has fees ranging from 1% to 8%.

The difference is startling.

An unmanaged software network with zero employees can settle a $1 billion-plus transaction in minutes, whereas the largest banks in the world take multiple days to move $5,000 abroad. In addition, bitcoin transactions can be sent at any time of day or night and from any location around the world to anywhere else.

This is true not just for isolated large transactions, either: Every day, users settle transactions on the bitcoin network with values as small as a penny, as well as ones measured in tens and even hundreds of millions of dollars. In the first half of 2020, the fees for bitcoin transactions amounted to just 0.019% of the volume transacted.[14]

These efficiency gains do not mean we are going to be buying coffee with crypto anytime soon; tax, price volatility, user experience, and basis-risk considerations make day-to-day consumer purchases with bitcoin unlikely today. But this kind of settlement speed represents a material improvement for many other types of transactions and use cases, including large transactions and transactions for which the current financial system charges very high fees (e.g., international remittance, wires). This is an area to watch.

Capability 2: The Creation of Scarcity and Property Rights in the Digital World

Perhaps the biggest breakthroughs that cryptoasset-powered blockchains have facilitated are the related concepts of digital scarcity and digital property rights.

Historically, the only way to "own" something online has been to have your ownership recorded by a trusted third party in a proprietary database. For instance, your broker keeps track of what stocks you own, your bank keeps track of what balances you own, video game companies keep track of in-game purchases, county clerk offices keep track of land titles, and so on.

Cryptoassets flip that system on its head.

Because the underlying blockchain database is available to everyone without being controlled by anyone, cryptoassets can provide ownership guarantees that were previously nonexistent in the digital world. In fact, one could argue that the ownership assurances blockchains offer are stronger than most of the ones we have in the physical world.

For instance, a key part of the software that created bitcoin guarantees that the total number of bitcoin will never be more than 21 million. Anyone can prove they own their bitcoin (or a fraction of a bitcoin) out of the eventual 21 million supply without any company or trusted intermediary having to say it is so. Also, the cryptography assures that no one can take that person's bitcoin away without his or her authorization.

Many people talk about bitcoin as "digital gold" specifically because it introduced the idea of digital scarcity to the world. A *New York Times* bestseller was even published with that name in 2016.[15]

Imagine someone trying to create digital gold before the bitcoin blockchain. This person

[14]Data from the public application programming interface provided by blockchain data provider Coin Metrics, accessed on 25 August 2020. Documentation is available at https://docs.coinmetrics.io/api/v2.

[15]Nathaniel Popper, *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money* (New York: Harper, 2015).

would have needed a company—let's call it the "digital gold company"—that offered the same service bitcoin does. It would have created a certain amount of digital gold and then maintained a database of who owns what.

Who would trust this mythical company with real money? What would stop it from deciding at some point, if the venture became large enough, to create extra digital gold for its account or to increase the overall supply of this digital gold? What would prevent it from taking digital gold from users or from simply walking away with people's money?

A decentralized database solves this problem.

Digital gold, however, is not the only potential application for digital scarcity. A bustling corner of the crypto industry is what is known as nonfungible tokens (NFTs), which the gaming industry is exploring.

Imagine a video game that allows players to own an item, such as a special sword. What if you wanted to sell that sword to someone on eBay? How would they know you own it? How would you transfer it to them? The NFT vision is that players can prove they own a specific asset, can trade that asset with other players whenever they see fit, and might even do so outside the confines of the game.

Another example of experimentation with scarcity is the digital equivalent of traditional sports trading cards. One startup is working with the National Basketball Association (NBA) and the National Basketball Players Association to produce digital playing cards.[16] Oddly, in 2020, even though much of our lives takes place online, kids and collectors have not yet embraced digital playing cards. But without a blockchain, the scarcity value of an online card disappears: You could just copy and paste the image of a card you wanted and say you had it. With a blockchain, ownership can easily be proven or disproven.

Anticipating what creative entrepreneurs will devise to leverage the technological breakthrough of digital scarcity and digital property rights is difficult. But this is a powerful concept that provides a way of doing things that was not possible before—and another place to watch for innovation.

Capability 3: Digital Contracts ("Programmable Money")

The final advance worth considering is that cryptoasset-powered blockchains allow users to effectively program money with certain rules and conditions, as you would program any software. These digital "smart contracts" can be created, reviewed, and enforced easily, instantaneously, and with virtually no cost.

With money programmable like software, you can create transactions with such conditions as the following:

- Alice transfers cryptoasset X to Bob, but only after Carol agrees—which looks a lot like an escrow account.
- Alice transfers cryptoasset X to Bob, but only after a certain amount of time—which looks a lot like a trust.
- Alice sends cryptoasset X to Bob, but only if Carol wins the race; if Carol loses, Bob sends cryptoasset Y to Alice—which looks a lot like a contract.

Blockchains allow these and many more-complex transactions to be executed without the need for trusted intermediaries. In so doing, smart contracts aim to replace or augment

[16]Fred Wilson, "NBA Top Shot," AVC (6 August 2020). https://avc.com/2020/08/nba-top-shot-2/.

many of the core functions provided today by banks, lawyers, accountants, escrow agents, and notaries, albeit in a way that is cheaper, faster, more transparent, open to all participants, and available 24/7/365.

Like that of digital cash, this idea of smart contracts is not new. Smart contracts were introduced as a theoretical concept by cryptocurrency pioneer Nick Szabo in 1997 but were made possible in practice only after the emergence of cryptoasset-powered blockchains.[17]

The ability to program money with conditions and digital contracts is the third new capability we expect to lead to significant applications and economic impact.

PART II: UNDERSTANDING THE CRYPTO LANDSCAPE

Bitcoin is not the only cryptoasset. According to the popular data aggregator CoinMarketCap, more than 6,000 different cryptoassets exist, and many new ones are created each month. Although most of these assets are small, many are valued at more than $1 billion.[18]

The Bitwise 10 Large Cap Crypto Index is a market-cap-weighted index of the 10 largest cryptoassets, screened for liquidity, security, and other risks. It captures approximately 85% of the total market capitalization of the crypto market. **Figure 5** showcases the relative market capitalization of these leading assets.

In this section, we will survey the current cryptoasset landscape and ask three critical questions:

- Why does more than one cryptoasset exist?
- Does the existence of thousands of cryptoassets damage the "scarcity" of an asset such as bitcoin?
- Do you need a cryptoasset to have a blockchain?

Why Does More Than One Cryptoasset Exist?

Multiple cryptoassets exist and are thriving because their underlying blockchains are optimized for different uses.

The blockchain technology tied to each cryptoasset is simply software. Any two blockchains are similar types of software, but they can be programmed to serve very different uses. Consider this analogy: Both Microsoft and Oracle are software companies, but their software products are designed to do different things.

The impact of these optimizations is best explored by comparing bitcoin's blockchain with that of the next-largest cryptoassets.

Bitcoin vs. Ethereum

Bitcoin's blockchain—the first ever launched—is in certain ways simple. As a piece of software, it allows for only a very narrow set of types of transactions: You can program it to send, receive, or hold bitcoin and to set up very simple escrow- and trust-style accounts.

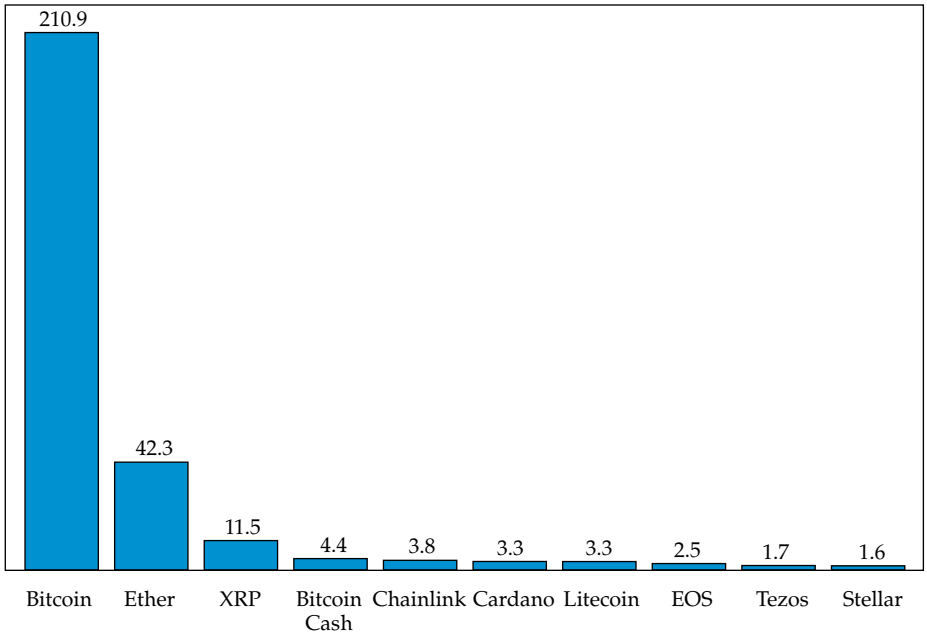
Ethereum, the second-largest cryptoasset by market cap,[19] was conceived in 2013 and launched in 2015 with the idea of expanding that list of capabilities. In fact, Ethereum's

[17]Nick Szabo, "Formalizing and Securing Relationships on Public Networks," *First Monday* 2 (1 September 1997). https://doi.org/10.5210/fm.v2i9.548.

[18]Data as of 30 September 2020 from CoinMarketCap.

[19]Data as of 30 September 2020 from Bitwise Asset Management.

FIGURE 5. CURRENT BITWISE 10 LARGE CAP CRYPTO INDEX CONSTITUENTS RANKED BY MARKET CAPITALIZATION (IN US$ BILLIONS)



Sources: Bitwise Asset Management with data from CoinMarketCap as of 11 October 2020.

developers designed it to be "Turing complete," a computer science term that means it can be programmed to do anything a general computer can do. By offering the ability to program any type of transaction, Ethereum has established itself as the platform of choice for the "programmable money" use case.[20] To date, people have replicated everything from collateralized loans to IPO-style fundraising efforts using Ethereum-based "smart contacts." People have even built fully functional decentralized asset exchanges, which rely on software-based automated-market-making programs to facilitate liquidity and have supported billions of dollars in crypto trades.

One might assume that this additional flexibility makes Ethereum a "better" blockchain than bitcoin, but this functionality comes at a cost. One core tenet of cybersecurity when programming software is to "limit the attack surface." In practice, for the crypto/blockchain space, this means that the simpler a blockchain is, the more secure the technology is. It is common sense: Just as a book is more likely to have a typo than a single sentence, a complex computer program is more likely to have a bug or vulnerability than a simple one.

Bitcoin's simplicity is part of what makes it extremely secure and what gives people confidence putting large sums of money into it—perfect for serving as "digital gold." Ethereum's flexibility and dynamism entail a level of technical risk that would be unacceptable for bitcoin

[20]Recently, Ethereum has gained particular traction in finance-specific applications, such as blockchain-enabled lending protocols, which has given rise to a new term: "decentralized finance," or "DeFi."

but that allows other interesting applications to flourish.

Bitcoin vs. XRP

XRP, also known as Ripple, is currently the third-largest cryptoasset.[21] It differentiates itself from bitcoin in an entirely different way from Ethereum.

Bitcoin is a fully decentralized blockchain, with instances of the database distributed around the world and maintained by thousands upon thousands of computers. The fully distributed nature of bitcoin offers great advantages: For instance, for any single government to disrupt, shut down, or harm the bitcoin blockchain would be very difficult because it is maintained in virtually every country around the world. Bitcoin is also truly censorship resistant and seizure resistant. No governmental or other entity can block bitcoin payments or seize bitcoin.

The flip side of this decentralization is that bitcoin is too slow for some use cases. The bitcoin blockchain can currently process only a handful of transactions per second, compared with more than 20,000 per second for a centralized payment network such as Visa's. Although researchers are working on ways to get around this limitation, it remains a significant restraint.

This restraint does not matter for bitcoin's primary use cases as a store of value or a tool to move large sums around the world with low fees, but it makes using bitcoin as a daily payment vehicle a challenge.

XRP and its underlying blockchain are designed specifically to support the payments use case. XRP's blockchain is maintained by a group of just 36 nodes, which work together to process transactions and maintain the blockchain's security. A single company, Ripple, controls the majority of the supply of the asset and maintains significant oversight of the ecosystem, including controlling 6 of the 36 nodes.

The advantage of this centralization is that the XRP blockchain is extremely fast, capable of processing transactions at a pace that matches Visa's. The downsides include that it is exposed to greater government oversight, that payments can be more easily censured or reversed, and that holdings of XRP are subject to possible seizure.

XRP would be a poor choice of blockchain for someone looking for digital gold. In contrast, XRP is a feasible blockchain if the goal is to process payments quickly, which means it might have applications in such fields as international remittances and corporate payments across borders, among others.

Other Assets

The aforementioned trade-offs—between security, programmability, and speed—are the three biggest trade-offs that blockchains must consider. And the aforementioned markets—digital gold, programmable money, and payments—are the three biggest markets that crypto is tackling today.

But other points of differentiation exist between blockchains and other use cases the industry is pursuing. These include the following:

- *Governance:* How should a blockchain handle software upgrades and settle disputes?
- *Development funding:* Should a centralized entity—such as a foundation—that is granted a large initial or ongoing share of a given cryptoasset be in place so that it can help develop the ecosystem surrounding that asset?

[21]Data as of 30 September 2020 from Bitwise Asset Management.

- *Privacy:* Should transactions on a blockchain be public, pseudonymous, or truly anonymous?
- *Consensus mechanism:* What is the best technical and incentive architecture to maintain a blockchain? And how should concerns about high energy use, database bloat, and similar issues be handled?
- *Specific use cases:* Should blockchains provide general capabilities, or should they focus on specific use cases?

Whatever the right priorities are, the natural tendency in the cryptoasset market is for the winners in each market to get bigger, because cryptoasset-powered blockchains are network effects systems. The larger the asset, the more liquid it is, the more development activity surrounds it, the more robust its regulatory framework will be, the more support it has from institutional custody and trading firms, the more feasible it is to use, and so on.

Despite this fact, however, the likelihood that a single cryptoasset will come to serve every market need seems low. Some degree of specialization typically exists even in network-effect businesses. For instance, in the realm of social networks, Facebook is used extensively for social connections, LinkedIn for work, WhatsApp for chatting, and so on. Something similar seems likely to emerge in the crypto space.

Does the Existence of Thousands of Cryptoassets Damage the "Scarcity" of an Asset Such as Bitcoin?

The other question people ask when learning about the great number of existing cryptoassets is whether their existence (and the potential future existence of an unlimited number of additional cryptoassets) threatens the scarcity value of a cryptoasset, such as bitcoin.

The answer is no. Just as a foreign country creating a currency does not affect the scarcity of the US dollar, given that the two currencies would not be fungible, a new cryptoasset is not fungible with existing ones simply because it is also a cryptoasset.

Consider that thousands of cryptoassets have launched since bitcoin's inception, but bitcoin's value has only increased. Dozens of "forks" of bitcoin have even been released—cryptoasset projects that copy and paste the original bitcoin code, change a relatively trivial feature, and issue a new version of the coin. These forks have such names as Bitcoin Cash, Bitcoin SV, Bitcoin 2, Bitcoin Nano, World Bitcoin, and Quantum Bitcoin. Although one or two forks have accrued meaningful value and seem to have staying power due to community interest and/or unique technical optimizations, most have amounted to virtually nothing.

What is important to understand is that the value of each cryptoasset-powered blockchain is less a patent-worthy secret technology and more the network that emerges around each one.

Bitcoin, for instance, is a well-known global brand that trades on exchanges in countries around the world. It is supported by a robust network of custodians, liquidity providers, and developers; is integrated with dozens of apps; and is coveted by millions of investors. The bitcoin blockchain is secured by the largest network of computing power in the world, a network that is many times more powerful than the world's largest supercomputer. This network is supported by an industry of "bitcoin mining companies" and chip manufacturers that exist

specifically to maintain and strengthen the network. There are bitcoin funds, efforts to launch bitcoin exchange-traded funds (ETFs), payment tools that focus on bitcoin, and so on.

In comparison, any new cryptoasset or blockchain has none of that: no liquidity, no computers securing the blockchain, no clear regulatory structure, and no global brand.

As an analogy, duplicating the software code that powers Facebook would be relatively easy, but recreating the network that makes it one of the most valuable companies in the world would be extremely difficult. Similarly, cryptoasset-powered blockchains are proprietary networks that form around nonproprietary software.

Do You Need a Cryptoasset to Have a Blockchain?

A final common question that arises when studying blockchains is, Why not just create a blockchain without a cryptoasset?

Many people understand the value that blockchains bring to the world, but they are uncomfortable with the idea of an independent cryptoasset, such as bitcoin, and its accompanying high levels of volatility or with the concept of a decentralized network that might be difficult to regulate or control.

Can you get the advantages of a blockchain without the cryptoasset?

At the heart of the question about blockchains versus cryptoassets is the issue of "public, decentralized blockchains" versus "private, centralized blockchains."

Public, decentralized blockchains, such as bitcoin, require a cryptoasset to function, in part because the issuance of that cryptoasset provides the economic incentive for miners to maintain the network.[22]

You can, however, have a "private blockchain" that uses much of the same distributed database architecture components as bitcoin but that has a company that sets up, maintains, and controls the network and provides the economic incentives for it to function. In a private blockchain, the company or entity in charge decides who gets to participate in the database, can block or reverse transactions, can determine what privileges different members get, can rewrite the rules, can shut the blockchain down, and so on.

In between these two extremes, you have shades of gray. For instance, some cryptoasset-driven networks are relatively centralized, such as Ripple, where transactions are processed by a limited set of entities, and most of the asset is owned by one company. Similarly, other blockchain networks are somewhat decentralized but still privately guided, such as the Facebook-associated Libra blockchain, which is managed by a consortium of dozens of members.

The variation in the level of centralization—from decentralized to more centralized to privately operated—is in many ways similar to the internet.

The internet we typically use today is an open, decentralized internet: No one owns it, and

[22]As discussed, many cryptoasset-enabled blockchains, including bitcoin, allow users who want to see transactions prioritized can append a "tip" or "fee" to their proposed transactions. In practice, however, transaction fees represent a tiny fraction of the mining reward. They would likely be insufficient at a network's inception to allow the network to function securely. Over very long periods of time, as a cryptoasset-enabled blockchain matures, it might be able to transition to a fee-powered model, but to date, the only large-scale successes have used new cryptoasset rewards to jump-start the network's growth and to incent miners to secure the network in its early days.

virtually anyone can create a website and interact with it. In this sense, the internet is like bitcoin or any other cryptoasset-driven blockchain database.

But privately run, corporate "intranets" that can be accessed only by certain people also exist. Your employer, for instance, might have an intranet whose content can be updated only by the firm's human resources department and viewed only by the company's employees.

In between are shades of gray: The Chinese internet, for instance, is one such system, with censorship and central control but a fair degree of discretion within those constraints.

So which system will win?

To date, by far the most exciting advances and new capabilities—such as digital gold and programmable money—have emerged from public blockchains powered by cryptoassets. Cryptoasset-powered blockchains, such as the bitcoin network, are the blockchains that have advanced such entirely new concepts as "digital scarcity" into the world and have garnered the attention of thousands of leading technologists, entrepreneurs, investors, and even innovative corporates. These cryptoasset-powered blockchains have grown from a proof of concept to an asset class valued at more than $350 billion in little more than a decade.

Surely, opportunities will arise for companies to create private blockchain-style databases to reduce back-office costs by a few percentage points or to increase transparency in supply chains, and significant ongoing efforts are being made by governments to iterate on fiat money by leveraging blockchain's advances to develop "central bank digital currencies." But these advances are incremental, rather than fundamental. They do not introduce entirely new capabilities into the world; rather, they enhance the functionality of existing systems in certain ways, while degrading them in others.

As in the early days of the internet, the public blockchain space can feel bizarre and even hazardous for the unversed. And again similar to the internet, the disruptive possibilities created by public blockchains have opened up windows for fraud and bad actors in its early years. But only public blockchains advance fundamental breakthroughs, such as digital scarcity, and in our opinion, this is likely the area where the largest leaps forward will happen.

We will focus on the investment opportunity provided by the cryptoassets that power public blockchains in the remainder of this document.

PART III: CRYPTO AS AN INVESTMENT OPPORTUNITY

As of 30 September 2020, bitcoin was trading for $10,784.[23] Considering the current circulating supply of approximately 18.5 million bitcoin,[24] this would imply a total market capitalization of $200 billion.

Is that a lot or a little?

The question of how to appropriately value cryptoassets is one of the most complex, challenging, and disagreed-on aspects of the crypto-market. This section will discuss why we believe the cryptoasset valuation question will remain open for a while and how investors can think about this issue.

We start with a brief but critical examination of the five most widely used cryptoasset valuation

[23]Data as of 30 September 2020 from CoinMarketCap.

[24]New bitcoins are issued each day. Although the total amount of bitcoin that will ever be issued is 21 million, roughly 18.5 million have been issued to date. New bitcoin issuance will continue until approximately 2140.

techniques and end with a proposal for how to consider the issue holistically.

Approach 1: Total Addressable Market

The most popular approach to value cryptoassets is to estimate their addressable markets and compare that estimate with their current market capitalization.

For instance, many people believe that bitcoin is competing with gold as a nonsovereign store of value. At current prices of roughly $2,000 per ounce, the total stock of gold held above ground amounts to approximately $13 trillion.

As we have noted, the maximum number of bitcoin that will ever be available is 21 million. And so, the thinking goes that if bitcoin matches gold as a nonsovereign store of value, each bitcoin would be worth roughly $620,000 (on a fully diluted basis); if bitcoin captures 10% of the gold market, each bitcoin would be worth roughly $62,000; and so on. With its current market capitalization of roughly $200 billion,[25] bitcoin captures less than 2% of the value stored in gold.

The clear advantage of this approach is its simplicity. It is easy to understand and provides a solid framework for considering order-of-magnitude comparisons between cryptoassets and the markets they address.

This approach also makes introducing additional use cases easy. For example, one can consider that bitcoin is going after not only the gold market but also the entire "store-of-value" market. In that case, one can add offshore assets, parts of the real estate market, art, negative-yielding bonds, and other potential markets to the mix. This would increase bitcoin's target market by multiple tens of trillions of dollars.

However, while directionally helpful, this type of back-of-the-napkin valuation exercise falls short in many ways. To start, it provides at best a rough estimate of the order of magnitude of value that a cryptoasset might attain. It also supposes that bitcoin will create a new store-of-value market, above and beyond the existing gold market.

Additionally, beyond bitcoin and other store-of-value use cases, comparative valuation metrics hold little meaning. If Ethereum is going after the programmable money use case and competing with the broader financial industry, how do you estimate the size of that market? Even for the payments use case, this calculation is significantly challenging.

Approach 2: The Equation of Exchange (*MV = PQ*)

A widely discussed alternative valuation model was proposed by Chris Burniske, a crypto researcher and partner at the venture capital firm Placeholder Ventures, and Jack Tatar, managing partner of Doyle Capital, in a book called *Cryptoassets: The Innovative Investor's Guide to Bitcoin and Beyond*.[26]

Burniske and Tatar's framework is widely referred to by the monetary equation of exchange that drives its calculation:

$$MV = PQ.$$

The equation is borrowed from traditional models of valuing currencies and is based on the assumption that a currency's value is related

[25]Data as of 30 September 2020 from Bitwise Asset Management.

[26]Chris Burniske and Jack Tatar, *Cryptoassets: The Innovative Investor's Guide to Bitcoin and Beyond* (New York: McGraw-Hill Education, 2017).

TABLE 1. EQUATION OF EXCHANGE TERMS IN MONETARY ECONOMICS AND CRYPTOASSET VALUATION

Term	Meaning in Monetary Economics	Meaning in Cryptoasset Valuation
M	Total money supply	Cryptoasset market capitalization
V	Velocity: Average frequency with which a unit of money is spent	Velocity: Average frequency with which a unit of the cryptoasset is spent
P	Price of goods and services	The average price of transactions executed in the period studied
Q	Quantity of goods and services	Number of transactions executed in the period studied

to the size of the market it supports and to its velocity as it moves through that market. The definitions of *M*, *V*, *P*, and *Q* in both traditional monetary economics and cryptoasset markets are shown in **Table 1**.

These numbers can be estimated for some point in the future for a mature market and then discounted into present value.

As an easy example using round numbers, let us assume bitcoin will process 100 billion transactions (*Q*) of $100 each (*P*) per year. Then $P \times Q$ = 100 billion × $100 = $10 trillion per year. If on top of that we assume that bitcoin has a velocity of 5 (in other words, on average, one bitcoin changes hands five times per year), we arrive at a potential market capitalization of $10 trillion per year/5 per year = $2 trillion. If we divide this number by the fully diluted amount of bitcoin outstanding (21 million), it yields a price target of $2 trillion/21 million, or $95,238 per bitcoin. If we assume further that this level will be achieved in five years, we can discount this amount by an appropriate rate and arrive at an estimated present value.

One important challenge with this approach is that it requires estimating velocity, which is notoriously hard to do—even for a stable currency such as the US dollar—and velocity has historically varied significantly over time. According to data from the Federal Reserve,[27] one key measure of money velocity (MZM)[28] has ranged between 0.9 and 3.5 over the past 30 years; cryptoasset velocity is likely to vary more. Small changes in this estimate can lead to very large changes in proposed valuations.

Approach 3: Valuing Cryptoassets as a Network

A third approach to valuing cryptoassets is borrowed from "Metcalfe's law," a popular theory in technology that states that the value of a network is proportional to the square of the number of participants. If you consider a social network, such as Facebook, Instagram, or LinkedIn, for instance, its value when it has a single user is zero. If, however, a second user is added, the network becomes valuable. As more users are added, the network's value grows.

A key part of Metcalfe's law is that the value of the network is not linearly related to the number

[27]Federal Reserve Bank of St. Louis, "Velocity of MZM Money Stock." https://fred.stlouisfed.org/series/MZMV.
[28]MZM stands for "money at zero maturity."

of users but is instead related by a square function. In other words, if the value of a network of two users is expressed as "4" (2 squared), the value of a network with four users is 16 (4 squared)—four times as large.

Metcalfe's law has been used to value social networks with some degree of accuracy.

Ken Alabi first proposed applying Metcalfe's law to the valuation of cryptoassets in his 2017 paper "Digital Blockchain Networks Appear to be Following Metcalfe's Law."[29] Using the number of active daily users participating in the network, Alabi showed that the valuation differences between certain cryptoassets (he used bitcoin, Ethereum, and Dash) can be explained with a high degree of accuracy.

The Metcalfe valuation method makes intuitive sense, given that daily active users are a proxy for interest in and adoption of a cryptocurrency. Among its key limitations is that it is appropriate only for relative valuations between cryptoassets or for proxying current valuations on the basis of historical analogs. Another potential drawback is that it gives equal weight to each participant, which is less true in financial settings than in advertising-driven social networks. For example, the decision by Paul Tudor Jones II in May 2020 to allocate 2% of his portfolio in bitcoin (and to promote that allocation heavily in his investor letter)[30] is exponentially more important for valuation purposes than a new retail client at Coinbase buying her first $100 of bitcoin.

On top of that, given the large historical volatility of cryptoassets—bitcoin, for instance, has had six bear markets of more than 70% in its history—the choice of the starting point can have a dramatic impact on the suggestion for current valuations.

Approach 4: Cost of Production Valuation

The "cost of production" valuation thesis was first proposed by Adam Hayes in 2015[31] and has been expanded upon by multiple researchers since.

The theory holds that crypto, just like any commodity, is subject to traditional pricing challenges on the supply side. Crypto miners—the computers that process transactions and are rewarded with the underlying cryptoasset—spend fiat money to produce each marginal cryptoasset, through both energy and hardware expenditures.

Hayes and others suggest that, viewing bitcoin as a commodity and according to traditional microeconomic theory, the cost of producing each marginal bitcoin should align with the price of that bitcoin. After all, if bitcoin mining were to become unprofitable, miners could simply turn their attention to another cryptoasset or exit the market altogether. As a result, the value of each bitcoin can be estimated by examining the marginal cost of mining (specifically, the electricity burned in running the computations as part of mining) versus the expected yield of new bitcoin.

Empirical backtesting shows a relatively strong alignment between bitcoin's price and the marginal cost of production, lending some

[29]Ken Alabi, "Digital Blockchain Networks Appear to be Following Metcalfe's Law," *Electronic Commerce Research and Applications* 24 (July/August 2017): 23–29. www.sciencedirect.com/science/article/abs/pii/S1567422317300480.

[30]Erik Schatzker, "Paul Tudor Jones Buys Bitcoin as a Hedge against Inflation," Bloomberg (7 May 2020). www.bloomberg.com/news/articles/2020-05-07/paul-tudor-jones-buys-bitcoin-says-he-s-reminded-of-gold-in-70s.

[31]Adam Hayes, "A Cost of Production Model for Bitcoin," working paper (New School for Social Research, March 2015). www.economicpolicyresearch.org/econ/2015/NSSR_WP_052015.pdf.

credence (though no directional causality) to this approach.

The "cost of production" analysis, however, involves some significant challenges. For one, it is circular in its reasoning because the decision made by miners to enter or exit the market is driven by the cryptoasset's price. Using two necessarily cointegrated variables to value one another has very little predictive or explanatory power.

The model also fails to account for or explain the massive short-term volatility of bitcoin's price or the fact that bitcoin's mining difficulty is programmatically adjusted on a biweekly basis depending on the level of effort miners have focused on it.

Beyond that, many cryptoassets use a consensus mechanism different from that of bitcoin, one that does not lend itself to this kind of analysis. In proof-of-stake systems, for instance, little or no energy is consumed in mining; instead, miners lock up assets in escrow in exchange for securing the network. For these markets, no direct concept of the cost of production exists.

In the end, although cost of production has aligned roughly with prices for some cryptoassets in the past, the cause-and-effect relationship is not clear and its predictive value for the future is very much in question.

Approach 5: Stock-to-Flow Model

A fifth approach, dubbed the "stock-to-flow" model, was first published in the 2019 paper "Modeling Bitcoin Value with Scarcity" by PlanB, a pseudonymous crypto quant researcher.[32]

The stock-to-flow model states that bitcoin's price is a reflection of its scarcity and that scarcity can be measured by the stock-to-flow ratio—the relationship between the extant value of bitcoin and the amount of new bitcoin being produced each year. The paper showed that the price of bitcoin has historically been tightly correlated with increasing scarcity expressed by the stock-to-flow model.

In 2020, PlanB published a new iteration of this model focused on the relationship of the stock-to-flow ratios of bitcoin and other stores of value, such as gold and silver.[33] This new version also accounted for state transitions, or different evolutionary stages in bitcoin's monetization process.

The stock-to-flow model is intended to apply only to bitcoin and is appealing to some who see scarcity as the dominating characteristic of hard monetary assets.[34]

We are skeptical of this approach because it appears to conflate correlation with causation. It is true that one of bitcoin's strengths is its strictly limited supply, but assuming that this is the only factor driving its price is an overreach. It is also overly convenient for crypto bulls because bitcoin's stock-to-flow ratio is programmatically increasing over time and, therefore, "predicts" in this model a perpetually rising price for the asset.

[32]PlanB, "Modeling Bitcoin Value with Scarcity," Medium (22 March 2019). https://medium.com/@100trillionUSD/modeling-bitcoins-value-with-scarcity-91fa0fc03e25.

[33]PlanB, "Bitcoin Stock-to-Flow Cross Asset Model," Medium (27 April 2019). https://medium.com/@100trillionUSD/bitcoin-stock-to-flow-cross-asset-model-50d260feed12.

[34]Economist Saifedean Ammous is among those who have advanced the idea that assets with a strictly capped supply ("hard money") will, over the long run, dominate other competing monetary assets. His book, *The Bitcoin Standard: The Decentralized Alternative to Central Banking* (Hoboken, NJ: John Wiley & Sons, 2018), is a strong introduction to bitcoin from a monetary perspective.

Also, given the programmatic nature of the model, many have pointed out that the market (even if only modestly efficient) should price in the impact of bitcoin's future stock-to-flow ratio, impounding future value today.[35] Though widely discussed in some crypto circles, the stock-to-flow ratio is not seriously considered by academic researchers.

Conclusion

The unfortunate reality is that none of the proposed valuation models are as sound or academically defensible as traditional discounted cash flow analysis is for equities or interest and credit models are for debt. This should not come as a surprise. Cryptoassets are more similar to commodities or currencies than to cash-flow-producing instruments, such as equities or debt, and valuation frameworks for commodities and currencies are challenging. Cryptoassets add another wrinkle in that they are still extremely early in their development, and we are still uncovering the utility that these assets can provide.

New York University professor of finance Aswath Damodaran has compared cryptoasset valuations with those traditional commodities and currencies. He has noted, "Not everything can be valued, but almost everything can be priced,"[36] pointing out that "cash generating assets can be both valued and priced, commodities can be priced much more easily than valued, and currencies and collectibles can only be priced."[37] Cryptoassets fit somewhere between the second and third buckets.

Commodities, of course, are analyzed from a supply-and-demand perspective, and this is where cryptoassets might have an edge. Imagine that an investor could have real-time access to a transparent ledger that contains a record of every instance in which a single barrel of oil changes hands. Although this is not feasible for oil, it is easily at hand for cryptoassets. In fact, a nascent but burgeoning field of analysis combines data from what is happening in the blockchain (on-chain data) with market data–like prices and volumes (off-chain data). We are optimistic that more-refined modeling techniques looking at these data wells will bear fruit in the years to come.[38]

In the end, most investors approach cryptoassets as some combination of commodity, currency, and early-stage venture capital investment, borrowing techniques from each approach and emphasizing long-term holding periods. This makes precision challenging but might be enough to justify or reject the idea of adding a cryptoasset allocation to a portfolio.

We examine the impact of such an allocation in the next section.

PART IV: CRYPTO IN A PORTFOLIO SETTING

Ultimately, investors arrive at this question: What role, if any, should cryptoassets play in an institutional portfolio?

In this section, we will attempt to answer that question in four steps:

[35]Nic Carter, "An Introduction to the Efficient Market Hypothesis for Bitcoiners," Medium (4 January 2020). https://medium.com/@nic__carter/an-introduction-to-the-efficient-market-hypothesis-for-bitcoiners-ed7e90be7c0d.

[36]Aswath Damodaran, "The Bitcoin Boom: Asset, Currency, Commodity or Collectible?" *Musings on Markets* (24 October 2017).

[37]Damodaran, "The Bitcoin Boom."

[38]An in-depth look at these (still incipient and imperfect) metrics is beyond the scope of this study. A good summary can be found in "Cryptoasset Valuation Research Primer, Part 2," produced by the blockchain data analytics firm Coin Metrics and available at https://coinmetrics.io/coin-metrics-state-of-the-network-issue-40-cryptoasset-valuation-research-primer-part-2/.

1. *Bitcoin's historical performance characteristics:* First, we will examine the historical performance of bitcoin, the cryptoasset with the longest track record (dating back to 2010).
2. *The performance characteristics of non-bitcoin cryptoassets:* Second, we will examine the performance of non-bitcoin cryptoassets and consider how those returns compare with bitcoin's.
3. *The impact of crypto on a diversified portfolio:* Third, we will examine the historical impact of adding crypto to a traditional diversified portfolio of stocks and bonds and consider key decision points, such as rebalancing frequency and position sizing.
4. *The future for cryptoasset returns:* Finally, we will consider whether crypto's historical performance is likely to persist.

Bitcoin's Historical Performance Characteristics

Bitcoin was the first cryptoasset, launching in 2009 and with public trading data available starting in mid-2010. Since bitcoin's launch, its performance has been characterized by three main attributes: high returns, high volatility (including sustained bull and bear markets), and low correlations with traditional assets.

High Returns

The first publicly available trading data for bitcoin dates back to 17 July 2010, when bitcoin was trading for just $0.05. As of 30 September 2020, bitcoin was trading at roughly $10,784, meaning a $10,000 investment in bitcoin on its first trading day would today be worth $2.2 billion.[39]

Long-term charts of bitcoin's price show this massive run-up and are often presented in log form so that the early returns can be differentiated, as shown in **Figure 6**.

Log charts can be difficult to interpret, so perhaps the easiest way to understand the evolution of bitcoin's returns is by considering them on a segmented calendar basis, as shown in **Table 2**.

As the data show, bitcoin has risen in 9 of the 11 calendar years since it has had traded prices and has posted triple-digit or greater returns in 6 of those years. These high returns make bitcoin the best-performing investment of the past decade and, to this point, arguably the best-performing publicly available investment opportunity of all time.

High Volatility

These high returns, however, have been accompanied by high volatility, whether measured on an intraday, daily, annual, or peak-to-trough basis. As Table 2 shows, bitcoin has experienced 15 negative-return quarters since its inception, along with two negative years, including 2018's 73.71% pullback.

Moving away from segmented calendar periods, bitcoin's price has gone through six different peak-to-trough drawdowns of more than 70%. The most major pullback occurred after bitcoin hit its all-time daily closing price of $19,396 on 16 December 2017. From that point, the price of bitcoin retreated rapidly until bottoming on 14 December 2018, when it traded for $3,177, an 84% drop.[40]

Beyond large bear markets, bitcoin has also experienced high intraday and day-to-day volatility. **Figure 7** compares the volatility

[39]Data as of 30 September 2020 from CoinMarketCap.

[40]Data from CoinMarketCap.

FIGURE 6. BITCOIN SPOT PRICE IN US DOLLARS (LOG SCALE), 17 JULY 2020–30 SEPTEMBER 2020

Source: Bitwise Asset Management.

(measured as rolling 90-day standard deviation of daily returns, on an annualized basis) of bitcoin against other major risky asset classes, including stocks (US large cap, US small cap, and emerging markets), corporate bonds (investment grade and high yield), commodities (a diversified basket and gold), and emerging market currencies. Although bitcoin's volatility is trending down and generally making lower peaks over time, it was still substantially above the volatility of all other assets presented here as of 30 September 2020.

Low Correlations with Traditional Assets

The final distinguishing characteristic of bitcoin's historical returns is that they have exhibited consistently low correlations with the returns of all other major assets. **Figure 8** compares the 90-day rolling correlations between bitcoin and the same major risky asset classes mentioned earlier, since 2017. The light green band highlights correlation levels between –0.25 and 0.25, which we consider small, and the dark green band highlights the range between –0.10 and 0.10, which we consider negligible.

As Figure 8 shows, correlations have historically been *de minimis*. They did increase, however, during the coronavirus-related market crisis in the spring of 2020, though they generally remained below 0.5 (with a resulting R^2 of 0.25 or less).

The general lack of correlation should not be surprising. Bitcoin remains an early-stage investment opportunity, and the core drivers of bitcoin's value are distinct from the core drivers of other assets. Equities, for example,

TABLE 2. BITCOIN'S QUARTERLY AND FULL-YEAR RETURNS, 17 JULY 2010–30 SEPTEMBER 2020

Year	Q1	Q2	Q3	Q4	FY
2010			25.03%	384.65%	505.94%
2011	161.54%	1,952.74%	−68.08	−8.16	1,473.76
2012	4.03	36.53	84.59	9.12	186.08
2013	604.58	2.23	43.02	447.24	5,537.40
2014	−40.31	41.03	−39.58	−16.92	−57.74
2015	−24.00	7.55	−10.18	82.17	33.74
2016	−3.33	61.73	−9.25	58.44	124.81
2017	11.48	127.63	77.29	222.10	1,349.04
2018	−50.67	−7.69	3.40	−44.17	−73.71
2019	11.14	174.40	−26.28	−13.74	93.95
2020	−9.36	41.12	17.21		49.93

Note: Returns shown only for full quarters.

Source: Bitwise Asset Management.

are primarily driven by corporate profits, economic growth, interest rates, and tax policy. Bitcoin is driven by market adoption, network security, liquidity, inflation risks, supply changes, regulatory developments, technological developments, and other factors.

Expecting bitcoin's correlation with traditional assets to increase over time is reasonable, particularly for those assets (such as gold) that might play a similar role in investor portfolios. Indeed, correlations today are higher than they have been in the past, but given the diverse drivers of returns, the likelihood of a significant increase in correlation seems low.

The Performance Characteristics of Non-Bitcoin Cryptoassets

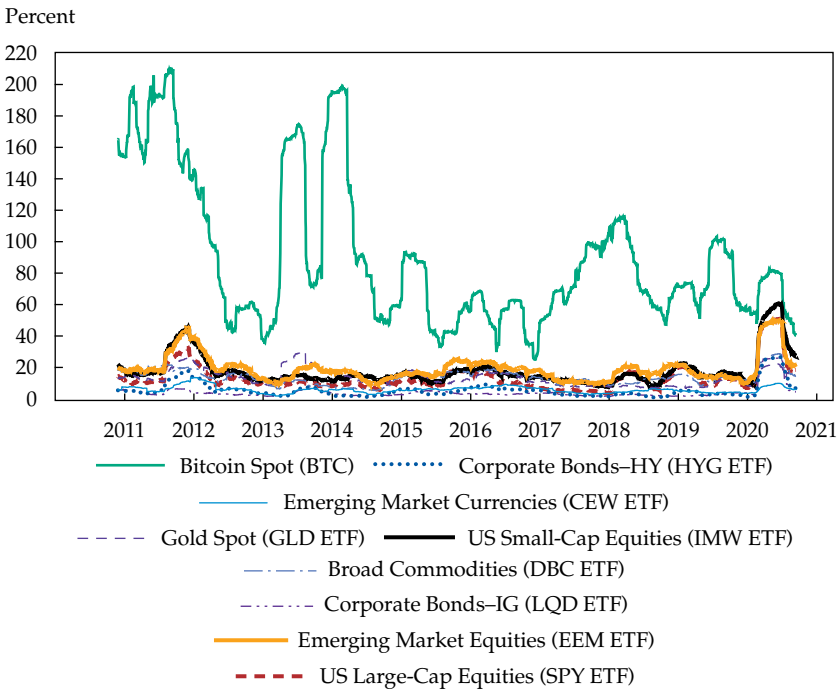
Bitcoin is just one of thousands of different cryptoassets that exist today. Although the market is very top-heavy—bitcoin alone accounts for almost 60% of the total market capitalization of the space, and the top 10 cryptoassets account for more than 80% of the total market capitalization[41]—many significant assets have market capitalizations measured in the billions or hundreds of millions of dollars.

Figure 9 shows how bitcoin's dominance of the total market capitalization of the space remains high, though it has generally trended down over time.

Although most cryptoassets rely on the same basic technology architecture as bitcoin, their blockchains are often optimized in different ways for different use cases, as discussed earlier. As a result, they have historically exhibited different returns, albeit with strong overall correlations.

[41]Data as of 30 September 2020 from Bitwise Asset Management and CoinMarketCap.

FIGURE 7. VOLATILITY OF BITCOIN VS. SELECT ASSET CLASSES (ANNUALIZED 90-DAY ROLLING STANDARD DEVIATION OF DAILY RETURNS), 20 JULY 2010–30 SEPTEMBER 2020



Notes: The price of bitcoin spot is calculated by Bitwise Asset Management from select exchanges considered to have real volume. "Broad Commodities" refers to the Invesco DB Commodity Index Tracking ETF (DBC). "Corporate Bonds–HY" refers to the iShares iBoxx $ High Yield Corporate Bond ETF (HYG). "Corporate Bonds–IG" refers to the iShares iBoxx $ Investment Grade Corporate Bond ETF (LQD). "Emerging Market Currencies" refers to the WisdomTree Emerging Currency Strategy Fund (CEW). "Emerging Market Equities" refers to the iShares MSCI Emerging Markets ETF (EEM). "Gold Spot" refers to the SPDR Gold Trust ETF (GLD). "US Large-Cap Equities" refers to the SPDR S&P 500 Trust ETF (SPY). "US Small-Cap Equities" refers to the iShares Russell 2000 ETF (IMW).

Sources: Bitwise Asset Management with data from IEXCloud.

The Correlation of Large-Cap Cryptoassets

Individual cryptoassets have historically exhibited correlations that are akin to the correlations exhibited by individual equities within the same market sector.

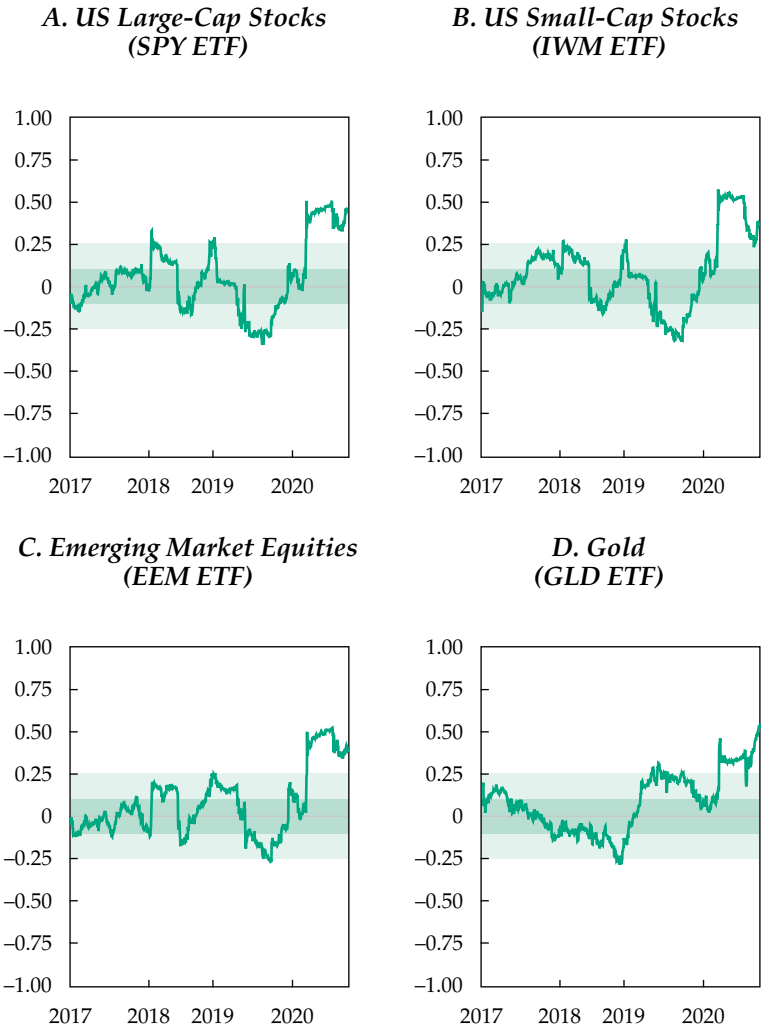
The charts in **Figure 10** compare the correlations (on a 90-day rolling basis) of bitcoin (the largest cryptoasset) with the next nine largest cryptoassets and of Berkshire Hathaway (the largest financial stock by market capitalization) with the next nine largest financial stocks held by the largest financials ETF, the Financial Select Sector SPDR Fund.

The similarity in correlations between competing large-cap cryptoassets and competing

large-cap financial stocks makes sense. Crypto, as an asset class, is affected by large factors, including evolving regulation, emerging education, liquidity, and new entrants, just as financial stocks are buffeted by their own macro factors, such as interest rates and economic growth.

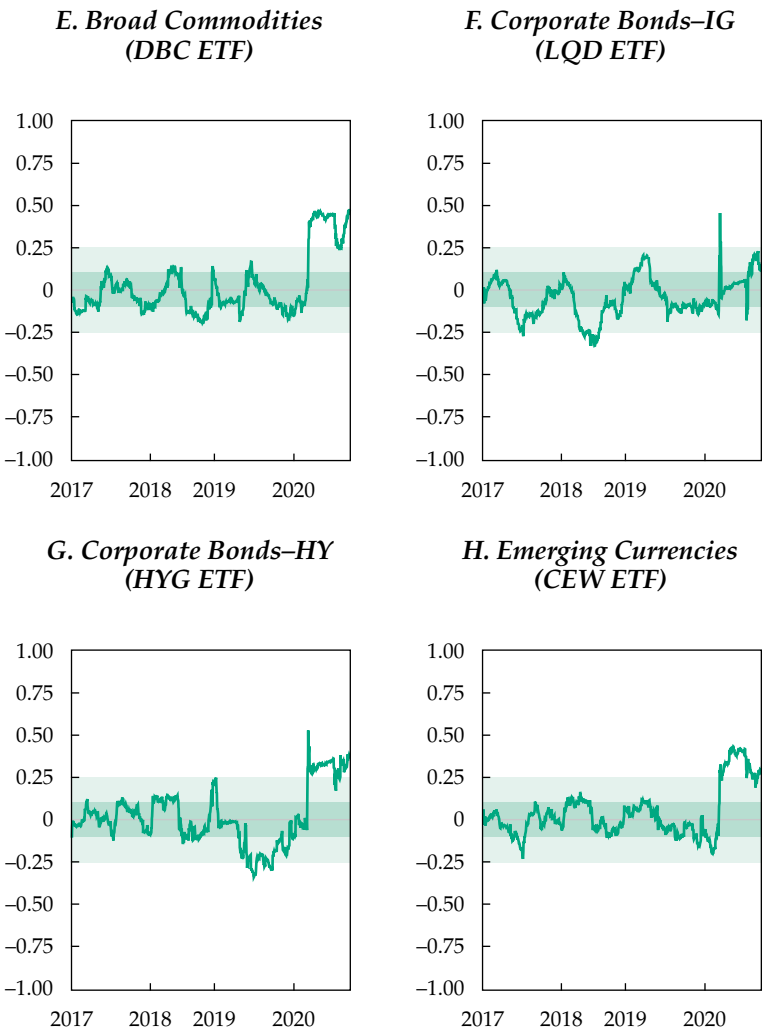
That said, the numerically high correlations between cryptoassets do not adequately depict the widely divergent long-term returns delivered by those assets over time.

FIGURE 8. ROLLING 90-DAY CORRELATION OF DAILY RETURNS BETWEEN BITCOIN AND OTHER MAJOR RISKY ASSET CLASSES, 1 JANUARY 2017–30 SEPTEMBER 2020



(continued)

FIGURE 8. ROLLING 90-DAY CORRELATION OF DAILY RETURNS BETWEEN BITCOIN AND OTHER MAJOR RISKY ASSET CLASSES, 1 JANUARY 2017–30 SEPTEMBER 2020 *(CONTINUED)*



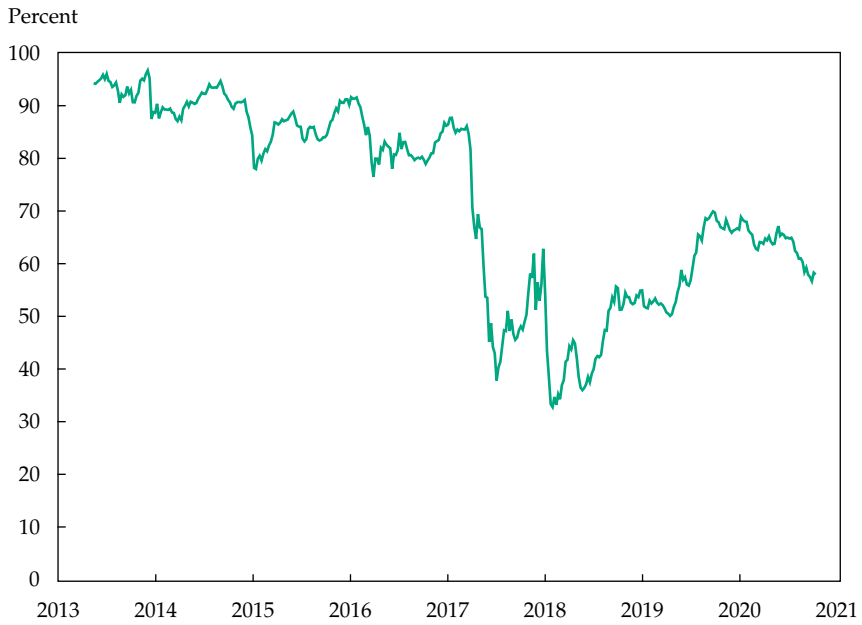
Note: See notes to Figure 7.

Sources: Bitwise Asset Management with data from IEXCloud.

The High Dispersion of Large-Cap Cryptoasset Returns over Time

Figure 11 borrows the familiar "Callan chart" format to show the monthly historical dispersion of returns for the 10 largest cryptoassets as of 30 September 2020. The difference between the best- and worst-performing cryptoassets among the top 10 in any given month averaged 59.3% over the past 12 months. Additionally, serial correlation between the stacked rank of

FIGURE 9. BITCOIN MARKET CAPITALIZATION AS A PERCENTAGE OF TOTAL CRYPTOMARKET MARKET CAPITALIZATION (WEEKLY DATA), 29 APRIL 2013–28 SEPTEMBER 2020



Sources: Bitwise Asset Management with data from CoinMarketCap.

performance of the various cryptoassets has been relatively low.

One way of considering the long-term impact of this dispersion of returns is by comparing the returns of a market-cap-weighted index of leading cryptoassets with the returns of bitcoin alone.

The Bitwise 10 Large Cap Crypto Index is a market-cap-weighted index of the 10 largest cryptoassets. The index was used by Cambridge Associates in its watershed report[42] on the space and is one of the most popular indexes for benchmarking the asset class.[43] From the index's base date of 1 January 2017 through 30 September 2020, the index had returns of 1,078%, versus 1,012% for bitcoin alone, as shown in **Figure 12**.[44] On a year-to-date basis through the same end date, the index returned 56.1%, versus 48.4% for bitcoin alone. Of course, periods of underperformance were seen, too:

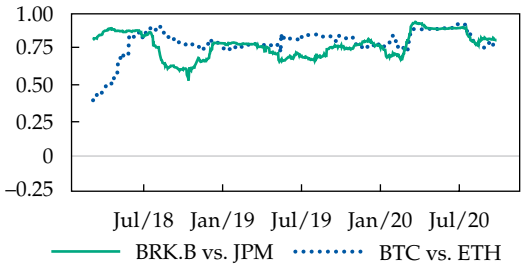
[42]Marcos Veremis, Alex Devnew, Michael Armstrong, and Dan Day, "Cryptoassets: Venture into the Unknown," Cambridge Associates (February 2019). www.cambridgeassociates.com/insight/cryptoassets-venture-into-the-unknown/.

[43]Matt Hougan and David Lawant serve on the Bitwise Crypto Index Committee, which governs the production of the index.

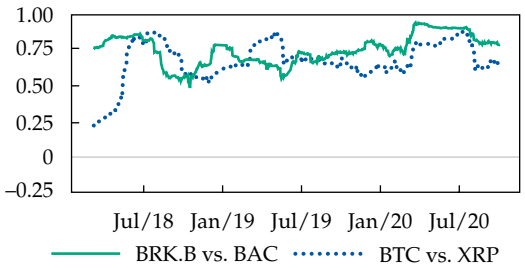
[44]The Bitwise 10 Large Cap Crypto Index's base date is 1 January 2017. Its inception date is 1 October 2017. Data from before 1 October 2017 are backtested data. Backtesting is performed by retroactively applying a financial model or index-weighting methodology to the historical data to obtain returns. Index returns are hypothetical returns that do not represent any particular investment and do not include transaction or tax-related costs.

FIGURE 10. ROLLING 90-DAY CORRELATIONS BETWEEN BITCOIN AND OTHER TOP 10 CONSTITUENTS IN THE BITWISE 10 INDEX AND BETWEEN BERKSHIRE HATHAWAY AND OTHER TOP 10 S&P 500 INDEX FINANCIAL STOCKS, 2 OCTOBER 2017–30 SEPTEMBER 2020

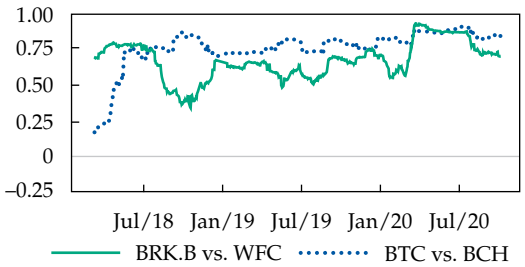
A. BRK.B vs. JPM and BTC vs. ETH



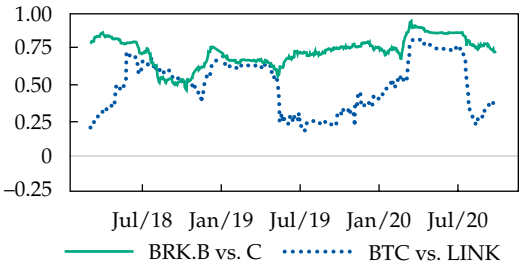
B. BRK.B vs. BAC and BTC vs. XRP



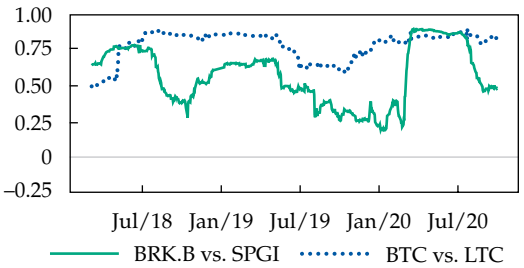
C. BRK.B vs. WFC and BTC vs. BCH



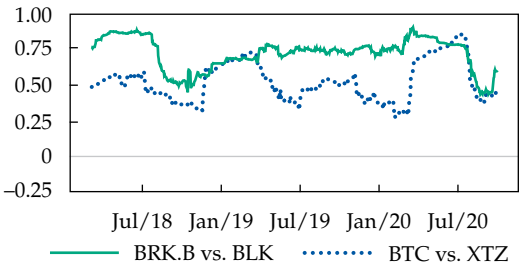
D. BRK.B vs. C and BTC vs. LINK



E. BRK.B vs. SPGI and BTC vs. LTC



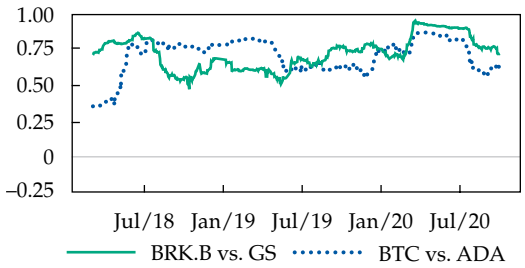
F. BRK.B vs. BLK and BTC vs. XTZ



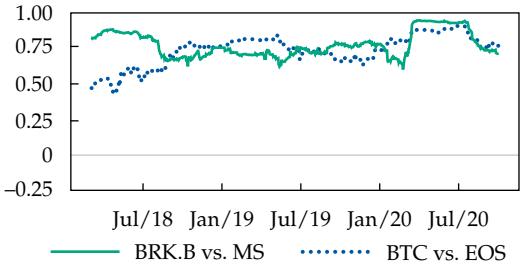
(continued)

FIGURE 10. ROLLING 90-DAY CORRELATIONS BETWEEN BITCOIN AND OTHER TOP 10 CONSTITUENTS IN THE BITWISE 10 INDEX AND BETWEEN BERKSHIRE HATHAWAY AND OTHER TOP 10 S&P 500 INDEX FINANCIAL STOCKS, 2 OCTOBER 2017–30 SEPTEMBER 2020 *(CONTINUED)*

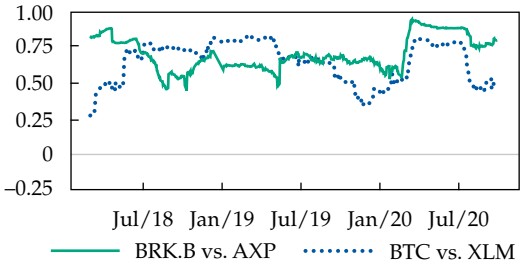
G. BRK.B vs. GS and BTC vs. ADA



H. BRK.B vs. MS and BTC vs. EOS



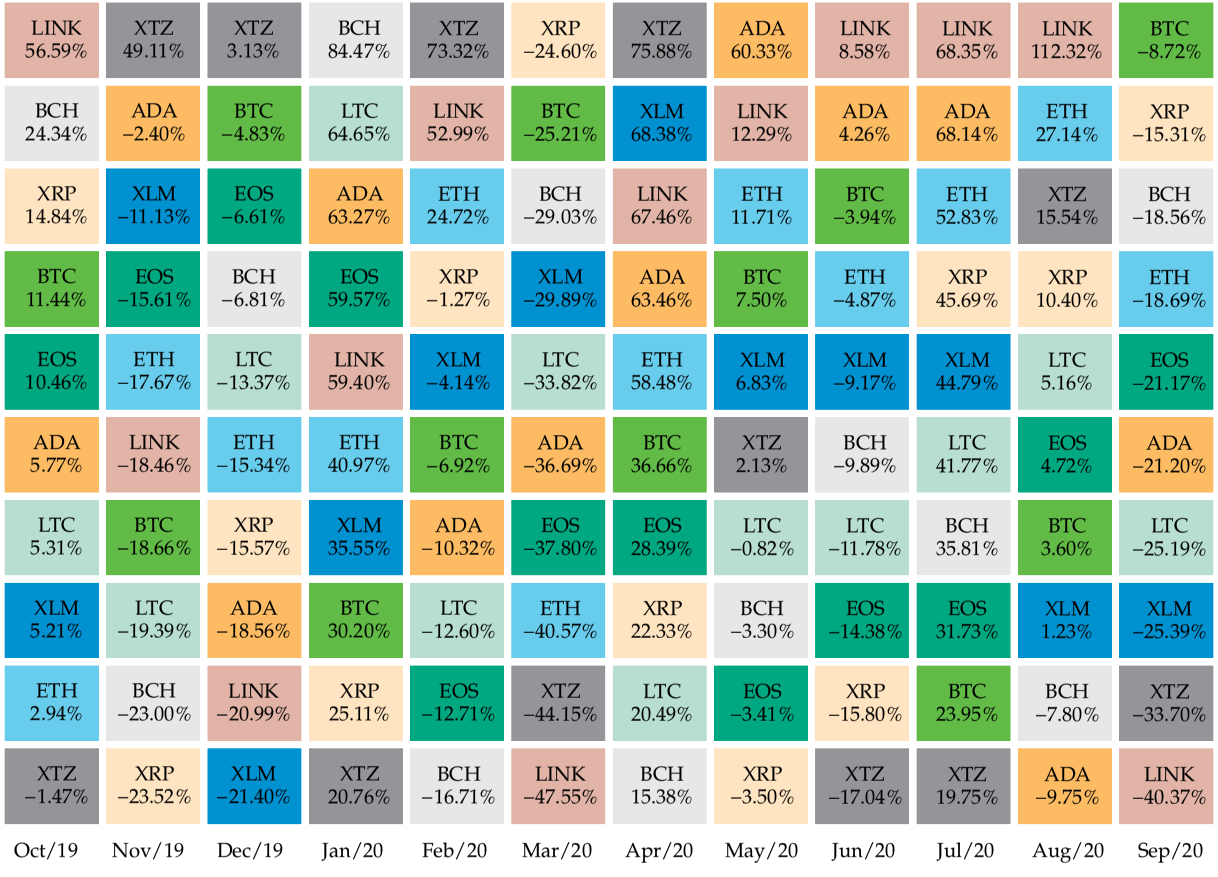
I. BRK.B vs. AXP and BTC vs. XLM



Notes: Prices of cryptoassets are calculated by Bitwise Asset Management from select exchanges considered to have real volume. S&P 500 financial stocks reflect the Financial Select Sector SPDR ETF. The Bitwise 10 Large Cap Crypto Index constituents, in descending index weight order, are bitcoin (BTC), ether (ETH), XRP, Bitcoin Cash (BCH), Chainlink (LINK), Litecoin (LTC), Tezos (XTZ), Cardano (ADA), EOS, and lumens (XLM). The Financial Select Sector SPDR ERF top 10 constituents are, in descending index weight order, Berkshire Hathaway Inc. Class B (BRK.B), JPMorgan Chase & Co. (JPM), Bank of America Corp. (BAC), Wells Fargo (WFC), Citigroup (C), S&P Global Inc. (SPGI), Blackrock Inc. (BLK), Goldman Sachs Group Inc. (GS), Morgan Stanley (MS), and American Express Company (AXP).

Sources: Bitwise Asset Management with data from IEX Cloud.

FIGURE 11. PERIODIC TABLE OF CRYPTOASSET RETURNS: MONTHLY PERFORMANCE OF CURRENT BITWISE 10 LARGE CAP CRYPTO INDEX (BITX) CONSTITUENTS, 30 SEPTEMBER 2019–30 SEPTEMBER 2020



Note: The BITX constituents, in alphabetical order by the ticker, are Cardano (ADA), Bitcoin Cash (BCH), bitcoin (BTC), ether (ETH), Chainlink (LINK), Litecoin (LTC), lumens (XLM), XRP, and Tezos (XTZ).

Source: Bitwise Asset Management.

In 2018, for instance, the index fell 77.7% while bitcoin fell 73.7%.

Figure 13 expands on these data by showing the year-to-date performance of all 10 assets that compose the index, showcasing the variable performance of various assets despite the overall high correlations. The index is up just 56.1% during this period, but three assets are up more than 100%, including one that is up more than 400%.

Looking ahead, as the cryptoasset space matures, the correlation between cryptoassets could quite possibly decline, as some of the fundamental parameters shaping the asset class harden (e.g., regulatory structure, tax structure, infrastructure for investing) and the distinctions between the use cases of various cryptoassets become more salient and understood. However, the dispersion of long-term returns among different cryptoassets will likely continue to be high.

Having discussed their individual performance, let's shift now to discussing the impact cryptoassets can have on a traditional portfolio.

The Impact of Crypto on a Diversified Portfolio

To evaluate the impact of bitcoin on a diversified portfolio, we consider the impact of adding various allocations of bitcoin to a portfolio with a 60% allocation to the Vanguard Total World Stock ETF (VT) and a 40% allocation to the Vanguard Total Bond Market ETF (BND)—the "traditional portfolio."[45] VT holds a market-cap-weighted portfolio of global stocks covering 98% of the world's market capitalization, and BND holds a market-value-weighted portfolio representing all taxable, investment-grade US bonds. This analysis assumes that all dividends are reinvested.

We use bitcoin because it has the longest track record of any cryptoasset and has been the easiest asset for professional investors to access during the study period. We examine the period from 1 January 2014 to 30 September 2020 because allocating to bitcoin was difficult for professional investors before 2014. We consider rolling one-, two-, and three-year holding periods during the 2014–20 time period. The use of a rolling-period analysis allows us to examine the results during bull, bear, and sideways markets for bitcoin and to minimize the impact of market timing.

Results

Our analysis shows that adding bitcoin to a portfolio has historically had a significant positive impact on long-term portfolio returns on both an absolute and a risk-adjusted basis.

For example, during the whole period under consideration (1 January 2014–30 September 2020), a quarterly rebalanced 2.5% allocation to bitcoin would have improved the traditional portfolio's returns by 23.9 percentage points. Importantly, volatility would have remained almost constant (10.5% versus 10.3%). As a result, the Sharpe ratio expanded from 0.54 to 0.75.

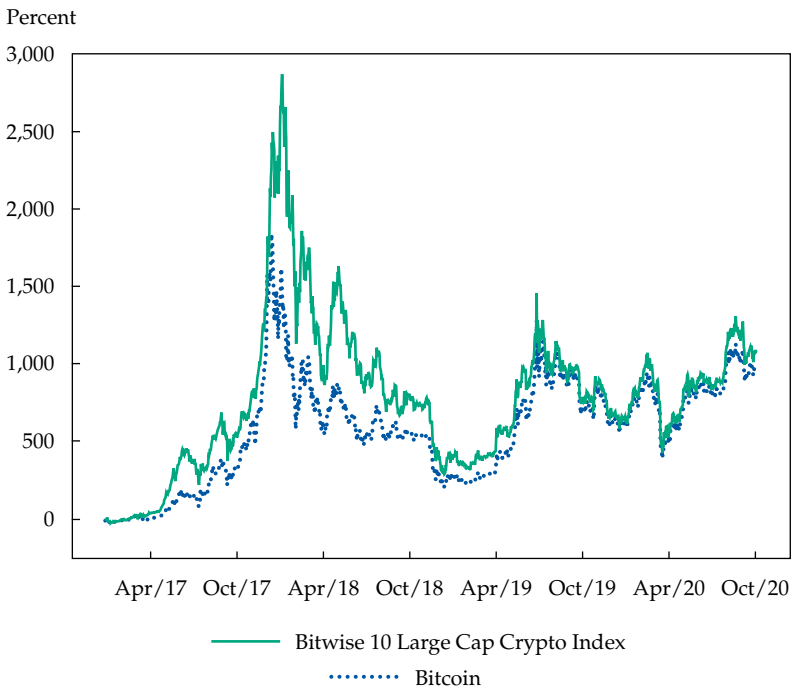
These results—as well as the full results for 0%, 1%, 2.5%, and 5% bitcoin allocations—are shown in **Figure 14** and **Table 3**.

Bitcoin's Portfolio Impact over Rolling Time Frames and Holding Periods

The positive impact over the 2014–20 period is notable, but it is also unsurprising: It captures a

[45]This section updates the analysis undertaken in the white paper "The Case for Bitcoin in an Institutional Portfolio," published by David Lawant and Matt Hougan in May 2020, by extending the cutoff date to 30 June 2020 from 31 March 2020. The full original paper is available at https://static.bitwiseinvestments.com/Research/Bitwise-The-Case-For-Bitcoin-In-An-Institutional-Portfolio.pdf.

FIGURE 12. CUMULATIVE RETURNS OF BITWISE 10 LARGE CAP CRYPTO INDEX VS. BITCOIN, 1 JANUARY 2017–30 SEPTEMBER 2020



Notes: Performance of an index is not illustrative of any particular investment. It is not possible to invest directly in an index. The darker green line for the Bitwise 10 index represents a hypothetical, backtested, and unaudited return stream that does not represent the returns of an actual account. Index performance does not include the fees and expenses that are charged by the fund. Actual returns may differ materially from hypothetical, backtested returns. Backtesting is calculated by retroactively applying a financial model or index-weighting methodology to the historical data to obtain returns. The inception date for the Bitwise 10 index is 1 October 2017; data before 1 October 2017 are backtested.

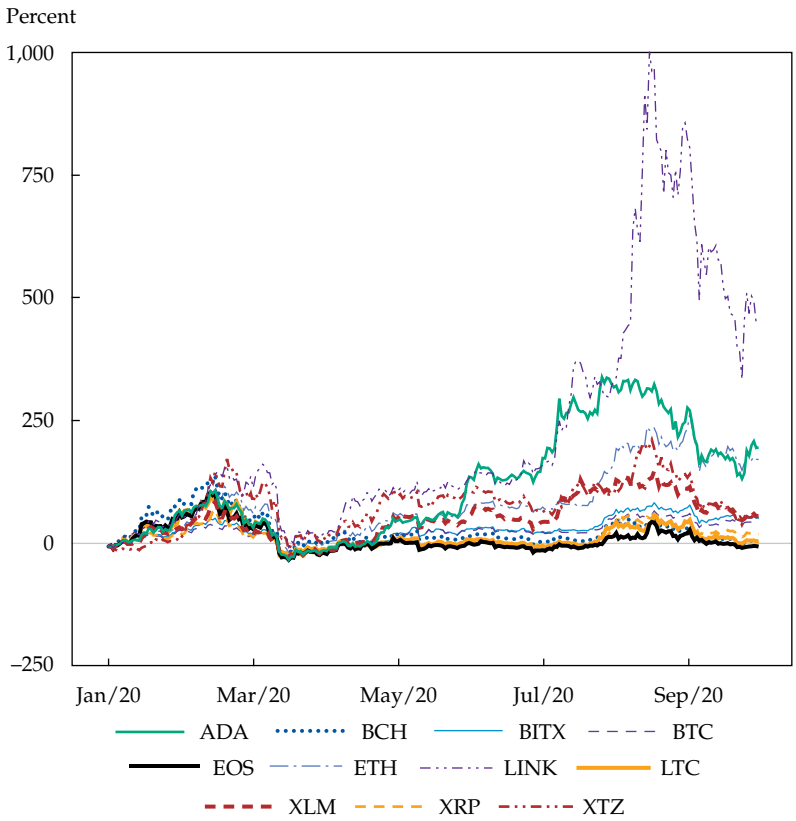
Source: Bitwise Asset Management.

period during which bitcoin's price appreciated substantially. To evaluate bitcoin's contribution to a portfolio over variable performance, we use a rolling-period analysis to simulate different holding periods over all possible time frames instead of point-in-time analysis.

Using a quarterly rebalancing frequency and allocating to bitcoin proportionally from the stock and bond side of the portfolios, a 2.5% allocation to bitcoin increases the returns of a diversified portfolio in 100% of three-year periods, 97% of two-year periods, and 74% of one-year periods since 2014. **Table 4** highlights those contributions (above and beyond the return of the overall portfolio) from both an absolute and a risk-adjusted return perspective.

Figure 15, **Figure 16**, and **Figure 17** illustrate this impact over one-, two-, and three-year

FIGURE 13. CUMULATIVE RETURNS: BITWISE 10 LARGE CAP CRYPTO INDEX AND CURRENT INDEX CONSTITUENTS, 31 DECEMBER 2019–30 SEPTEMBER 2020



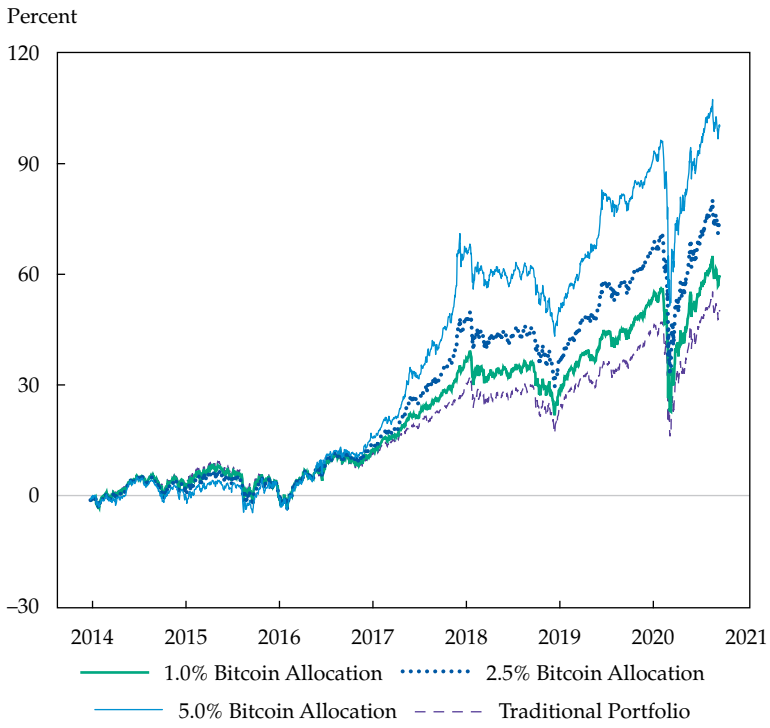
Note: Index composition is as of the last date in the covered period.

Source: Bitwise Asset Management.

rolling return periods. Positive contributions are shown in blue, and negative contributions are shown in orange. Figures 15, 16, and 17 have different start points because of the different lengths of the holding periods. For example, the first one-year holding period during the study stretched from 1 January 2014 to 1 January 2015, and the chart of one-year holding periods, therefore, shows results starting from 1 January 2015; in comparison, the first two-year holding period ended on 1 January 2016, and the two-year chart, therefore, begins at that date.

Over each of the three durations, the portfolio impact has been both significant and asymmetrically skewed on the positive side: For example, the median impact of a 2.5% allocation to bitcoin on a 60/40 portfolio over a three-year period has been to increase total returns by nearly 15%. Negative impacts, where they have occurred, have been limited.

FIGURE 14. CUMULATIVE RETURNS: TRADITIONAL PORTFOLIO WITH AND WITHOUT QUARTERLY REBALANCED BITCOIN ALLOCATIONS, 1 JANUARY 2014–30 SEPTEMBER 2020



Source: Bitwise Asset Management.

TABLE 3. PORTFOLIO PERFORMANCE METRICS (PORTFOLIO REBALANCED QUARTERLY), 1 JANUARY 2014–30 SEPTEMBER 2020

Portfolio	Cumulative Return	Annualized Return	Volatility (Annualized Std. Dev.)	Sharpe Ratio	Maximum Drawdown
Traditional portfolio, quarterly rebalanced	50.61%	6.26%	10.32%	0.54	21.07%
Traditional portfolio + 1.0% bitcoin	59.89	7.21	10.33	0.63	21.32
Traditional portfolio + 2.5% bitcoin	74.47	8.61	10.53	0.75	21.80
Traditional portfolio + 5.0% bitcoin	100.51	10.87	11.26	0.90	22.76

Source: Bitwise Asset Management.

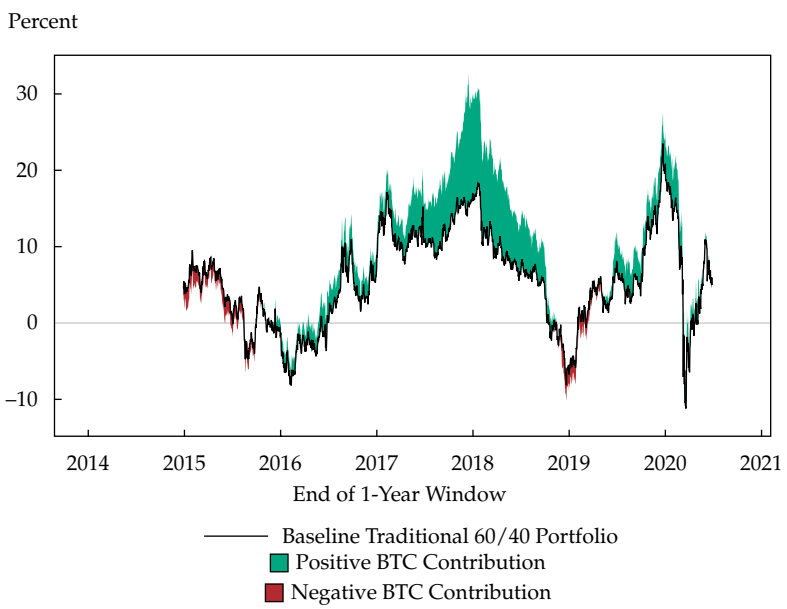
TABLE 4. CONTRIBUTION OF A 2.5% BITCOIN ALLOCATION TO A TRADITIONAL PORTFOLIO USING QUARTERLY REBALANCING, 1 JANUARY 2014–30 SEPTEMBER 2020

Holding Period	Rolling Cumulative Return Contribution					Rolling Sharpe Ratio Contribution				
	Maximum	Median	Minimum	Win Rate	Loss Rate	Maximum	Median	Minimum	Win Rate	Loss Rate
1 year	16.70 pp	2.80 pp	−3.00 pp	74.37%	25.63%	2.03	0.29	−0.45	73.61%	26.39%
2 years	20.27 pp	7.81 pp	−0.65 pp	96.89%	3.11%	1.10	0.41	−0.04	96.89%	3.11%
3 years	22.39 pp	14.65 pp	1.83 pp	100.00%	0.00%	0.74	0.48	0.07	100.00%	0.00%

Source: Bitwise Asset Management.

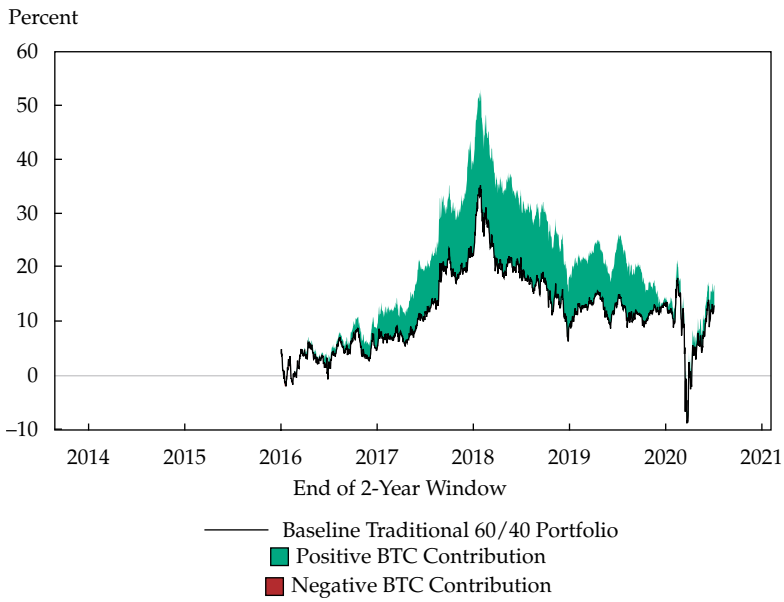
Importantly, just like in the point-in-time analysis, this positive impact came without a commensurate rise in portfolio volatility. Although bitcoin itself is volatile, its positive impact on returns has outweighed its negative contribution to risk, leading to significant increases in returns adjusted by volatility as measured by the Sharpe ratio. For instance, over three-year holding periods, the 2.5% allocation to bitcoin boosted the portfolio's Sharpe ratio by 41% on average

FIGURE 15. CONTRIBUTION OF A 2.5% BITCOIN ALLOCATION TO A 60/40 PORTFOLIO: ONE-YEAR ROLLING CUMULATIVE RETURNS



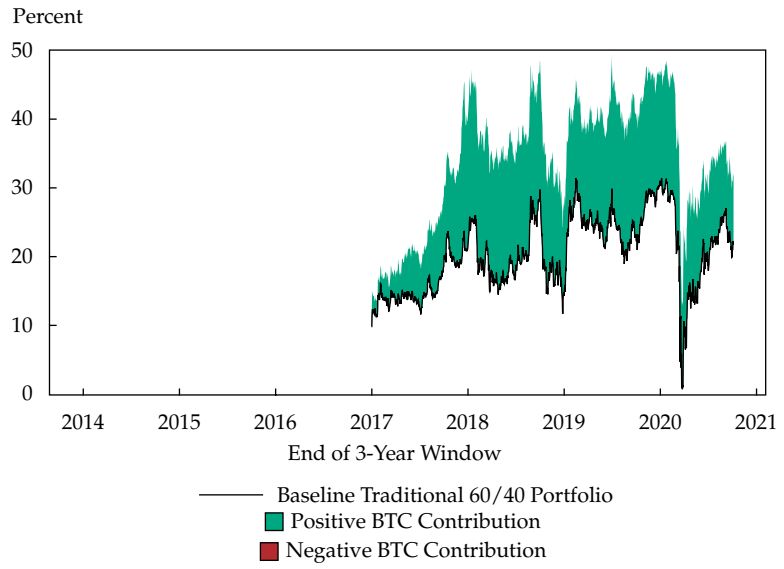
Source: Bitwise Asset Management.

FIGURE 16. CONTRIBUTION OF A 2.5% BITCOIN ALLOCATION TO A 60/40 PORTFOLIO: TWO-YEAR ROLLING CUMULATIVE RETURNS



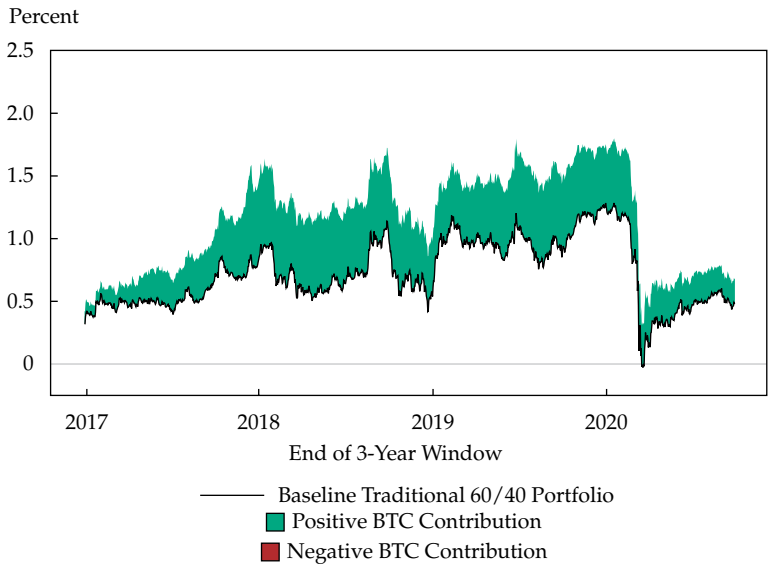
Source: Bitwise Asset Management.

FIGURE 17. CONTRIBUTION OF A 2.5% BITCOIN ALLOCATION TO A 60/40 PORTFOLIO: THREE-YEAR ROLLING CUMULATIVE RETURNS



Source: Bitwise Asset Management.

FIGURE 18. QUARTERLY REBALANCING: CONTRIBUTION OF A 2.5% BITCOIN ALLOCATION TO A 60/40 PORTFOLIO (THREE-YEAR ROLLING SHARPE RATIO)



Source: Bitwise Asset Management.

The Importance of Rebalancing

In containing risk, investors in bitcoin must assume some type of rebalancing program or the bitcoin allocation can come to overwhelm the portfolio and lead to a sizable increase in risk. **Figure 18** and **Figure 19** showcase the impact of rebalancing by comparing the rolling three-year impact that adding bitcoin to a portfolio had on the portfolio's Sharpe ratio both with and without a quarterly rebalancing program.

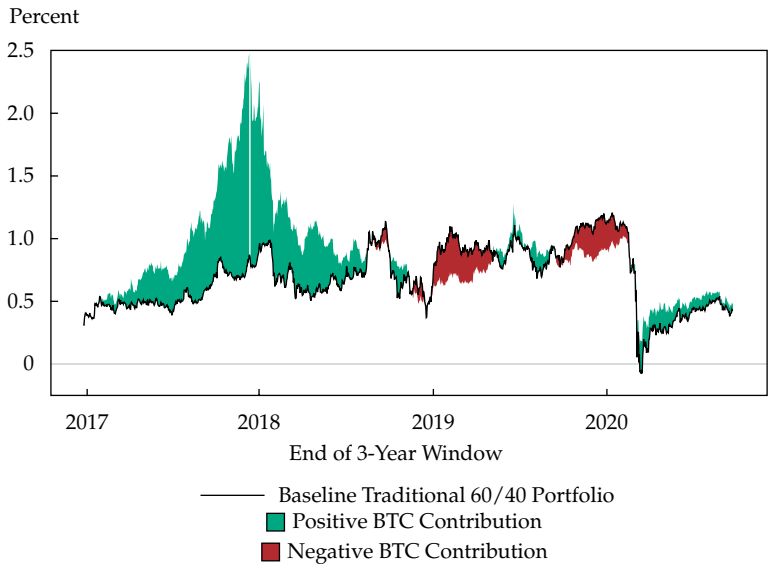
The non-rebalanced portfolio shows substantial periods when bitcoin hurt the Sharpe ratio, particularly for the three-year periods ending after January 2019. This finding is not surprising, given that bitcoin fell significantly in 2018; absent rebalancing, these negative returns dragged significantly on the risk-adjusted returns.

The importance of rebalancing is further emphasized when you consider the returns if investors allocated to bitcoin at its all-time high on 16 December 2017—the worst time to have bought—and held through the end of our study, 30 September 2020. Bitcoin fell 44.8% during this period.

Without rebalancing, this small allocation would have reduced overall returns by 1.4 percentage points, a significant amount. A quarterly rebalanced allocation to bitcoin, however, would have *boosted* returns by 1.8 percentage points.

How can an asset that declines 52.7% boost the returns of a portfolio? The answer comes from bitcoin's combination of high volatility, low correlation, and liquidity, which allows rebalancing. As discussed in an article by Bouchey,

FIGURE 19. NO REBALANCING: CONTRIBUTION OF A 2.5% BITCOIN ALLOCATION TO A 60/40 PORTFOLIO (THREE-YEAR ROLLING SHARPE RATIO)



Source: Bitwise Asset Management.

Nemtchinov, Paulsen, and Stein, applying a disciplined rebalancing strategy to a volatile, noncorrelated asset can yield positive portfolio impacts.[46]

Note, of course, that rebalancing raises the potential for loss as well: The most you can lose from a static allocation is the amount invested, whereas a rebalancing strategy can double down on a losing position if returns trend lower with no relief. Also note that the previous simulations do not account for transaction costs or taxes.

Bitcoin is a highly liquid asset, so transaction costs are relatively low. For context, the average inside spread on Coinbase Pro, the most liquid US bitcoin spot exchange, for the 30 days ending 19 October 2020 was 0.003%. Larger transactions will have higher costs: The average spread for an order-book-sweeping 10-bitcoin transaction (worth in excess of $100,000) on Coinbase Pro over that same time period was 0.061%.[47] Standard fees and/or commission costs might also apply, depending on the trading approach taken.

Taxes are highly subject to individual circumstances. Part V of this document addresses the taxation of cryptoassets.

[46]Paul Bouchey, Vassilii Nemtchinov, Alex Paulsen, and David M. Stein, "Volatility Harvesting: Why Does Diversifying and Rebalancing Create Portfolio Growth?" *Journal of Wealth Management* 15 (2 2012): 26–35.

[47]"Bitcoin Trading Volume," data.bitcoinity.org. Data are from 19 September 2020 through 19 October 2020, using hourly snapshots of the order book at Coinbase Pro. The inside spread is calculated by comparing the best bid with the best offer on an hourly basis. The 10-bitcoin spread is calculated by aggregating posted bids and offers that add up to 10 bitcoin or more on an hourly basis.

How Much Bitcoin Is the Right Amount?

Perhaps the most important question when allocating to crypto is, How big a position should you have? **Table 5** examines that question, looking at the impact of allocating between 0% and 10% of a portfolio to bitcoin over rolling three-year periods.

Table 5 suggests that for this set of rolling periods, increasing the allocation to bitcoin consistently led to higher average returns and higher average Sharpe ratios. For instance, a 1% allocation to bitcoin added 5.3%, on average, to the portfolio's return and boosted the Sharpe ratio by 0.19, whereas a 5% allocation to bitcoin added 28.1% to the portfolio's return and boosted the Sharpe ratio by 0.69, on average.

Note, however, that the impact on risk statistics is not linear. As shown, the average maximum drawdown of the portfolio remains largely flat for allocations to bitcoin between 0% and 4% because at this size allocation, bitcoin never competes with the equity allocation to drive the portfolio's maximum drawdown. Above 4%, however, the maximum drawdown rises rapidly, with each 1% additional allocation to bitcoin increasing the maximum drawdown by roughly 1%. This might provide a ceiling on appropriate allocations for risk-sensitive investors.

Summary

To date, bitcoin has been a rare asset, combining the return characteristics of a classic alternative asset with the liquidity characteristics of publicly traded equities. The key question is whether it will retain these key characteristics in the future.

The Future for Cryptoasset Returns

Looking at the historical returns of bitcoin or other cryptoassets and deciding that you should have allocated to them in the past is easy. But will these return characteristics continue in the future?

The best approach to tackling this question is to consider each of the three core characteristics of cryptoassets separately: high volatility, low correlation with traditional assets, and high potential returns.

High Volatility

High volatility has been a characteristic of the cryptomarket since its inception and is likely to continue in the future.

Cryptoassets and cryptoasset blockchains are still in a relatively nascent phase of their development, and although certain existential risks have been reduced over time, including those related to user interest, regulation, and banking access, big questions remain, including ones related to adoption, technical hurdles, and additional regulation.

Volatility has been declining over time: Bitcoin's standard deviation of daily returns was 5.4% between 2013 and 2015, 4.1% between 2015 and 2018, and 3.7% between 2019 and September 2020. Generally, we expect this pattern of high but declining volatility to continue.

Low Correlation with Traditional Assets

The low correlation between cryptoassets and traditional asset classes will likely persist because the underlying drivers of crypto

TABLE 5. KEY PORTFOLIO METRICS BY BITCOIN ALLOCATION (QUARTERLY REBALANCED PORTFOLIOS), 1 JANUARY 2014–30 SEPTEMBER 2020

Bitcoin Allocation	Cumulative Return			Sharpe Ratio			Standard Deviation			Maximum Drawdown		
	Min.	Average	Max.	Min.	Average	Max.	Min.	Average	Max.	Min.	Average	Max.
0%	1.05%	20.60%	31.64%	−0.032	0.718	1.279	6.90%	8.30%	12.97%	8.37%	12.62%	21.07%
1%	5.88	25.92	38.28	0.110	0.909	1.533	6.95	8.31	13.03	8.42	12.55	21.32
2%	10.66	31.39	45.47	0.241	1.075	1.724	7.23	8.47	13.19	8.34	12.49	21.61
3%	13.21	37.01	53.55	0.361	1.212	1.866	7.69	8.76	13.45	8.27	12.45	22.00
4%	14.20	42.79	61.91	0.464	1.322	1.988	7.99	9.15	13.80	8.20	12.65	22.38
5%	15.17	48.73	71.51	0.491	1.408	2.106	8.13	9.62	14.21	8.41	13.42	22.76
6%	16.13	54.82	82.02	0.514	1.475	2.254	8.31	10.16	14.70	8.32	14.32	23.13
7%	16.93	61.08	93.03	0.527	1.528	2.373	8.54	10.75	15.29	8.34	15.23	23.51
8%	17.56	67.50	104.63	0.531	1.569	2.471	8.81	11.38	15.93	8.36	16.14	23.88
9%	18.16	74.08	116.92	0.533	1.601	2.550	9.12	12.04	16.60	8.41	17.05	24.24
10%	18.75	80.83	129.72	0.532	1.627	2.617	9.45	12.73	17.29	8.59	17.97	24.61

EXHIBIT 1. EXPECTED FUTURE RETURN DRIVERS BY ASSET CLASS

Equities	Bonds	Cryptoassets
Corporate profits	Economic growth	Investor adoption
Economic growth	Interest rates	Millennial wealth
Interest rates	Issuance	Regulatory developments
Productivity		Weakening trust in authorities
		Institutionalization

Source: Bitwise Asset Management.

are significantly different from the underlying drivers of stocks and bonds, as highlighted in **Exhibit 1**.

These historically low correlations, however, might increase slightly in the years to come, given that certain drivers of crypto's historically uncorrelated returns are fading from the market. For instance, in the early days of crypto, the market could potentially collapse with a single regulatory decision, an unanticipated technological bug, or another such factor. As an example, at one point, only one banking institution (Silvergate Capital) was willing to provide basic cash banking services to crypto exchanges; the withdrawal of that support would have severely affected crypto liquidity and, therefore, prices.

Today, crypto exists on a stronger foundation. To follow that singular thread, the Office of the Comptroller of the Currency (OCC) recently issued a letter stating that all banks may provide banking services to the crypto industry.[48]

The removal of many existential concerns has boosted crypto's returns over the past decade in a manner disconnected from the broader capital economy, and those asynchronous drivers might be on the ebb.

Additionally, as cryptoassets penetrate further into their target markets, market-specific dynamics and investor flows might play a larger role in influencing returns, which will have an impact on correlations. As bitcoin penetrates further into the digital gold market, for instance, one would expect its correlation with gold (which is relatively low today) to rise.

Finally, if crypto transforms from an asset primarily owned by retail investors to one primarily owned by institutional investors (like most assets), the characteristics of its return profile might change as well.

Notwithstanding those factors, however, that correlations will rise substantially is unlikely, given the materially different core drivers of returns.

High Potential Returns

The question of crypto's future return potential is both the most interesting for investors and the most difficult to forecast.

Cryptoasset bulls argue that historical high returns will persist. They assert that crypto has yet to even begin to penetrate the mainstream,

[48]Office of the Comptroller of the Currency, "Interpretive Letter #1170" (22 July 2020). www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2020/int1170.pdf.

most institutional investors remain on the sidelines, use cases are just emerging, significant exogenous risks still exist and returns will follow when they are mitigated, no crypto ETF is available in the United States, and so on. These bulls paint a picture of a future world where cryptoassets are as familiar to individuals as cash and gold and where using a cryptoasset-powered blockchain to conduct such activities as lending, remittance, escrow, title transfer, automated market making, and settlement becomes as familiar as using a computer to write a paper. They point out that even the most established cryptoasset (bitcoin) has penetrated less than 2% of its most obvious comparable (gold) and suggest that prices could easily go 10–100 times higher.

Cryptoasset bears argue the opposite case, noting that the valuations of large-cap cryptoassets are already measured in the tens and even hundreds of billions of dollars, comparable to the valuations of some of the largest corporations in America. These bears argue that cryptoassets are highly overvalued and in some cases scams are destined to collapse and be remembered as the cyberequivalent of the tulip bulb market bubble. They note that cryptoassets have not yet returned to the all-time highs they hit in late 2017 and early 2018 and suggest that they might never retouch those lofty levels.

As with all assets, differing views make a market, and crypto is a new and volatile market indeed. Although nothing can be done about crypto's limited track record, the empirical truth is that crypto has survived multiple moments of panic and disaster and has each year set lows higher than the year before. Our view, aligned with the bulls, is that given crypto's still-early stage of development—with most professional investors yet to allocate to the space—it has significant room to run. If even small percentages of the tens of trillions of dollars invested in adjacent asset classes, such as commodities, alternatives, cash, and real estate, transfer into the crypto market, the impact and upside potential will be significant. Risks remain, but so does potential.

PART V: KEY CONSIDERATIONS AND RISKS FOR INVESTORS

In this part, we discuss certain framework considerations, compare various approaches to investing in crypto, and examine pertinent risk factors.

Framework Considerations: Custody, Taxation, and Regulation

As investors move down the path of exploring investment into crypto, they should be aware of several practical considerations, as with any asset class and certainly any alternative or real asset. This section briefly outlines the top three considerations for crypto: custody, taxation, and regulation.

Custody

One particular challenge for investors allocating to crypto is custody, which in this case refers to how one securely holds and stores a cryptoasset.

The ownership of a given cryptoasset is established by controlling a password, or "private key." If that password is lost or stolen, the related cryptoasset is lost forever. This finality is necessary to permit some of crypto's key advantages, such as rapid settlement, but it presents a significant risk if not handled appropriately.

Best practices in the space call for investors to hold cryptoasset private keys in "cold storage,"

otherwise known as "offline storage." To oversimplify, you can store that password either online (say, in a computer database connected to the internet) or offline—for example, written down on a piece of paper placed in a safe deposit box. Storing a password online exposes it to the risk of getting hacked and is, therefore, riskier than storing it offline, especially in an era of constant data breaches (e.g., Equifax, Yahoo).

Cold storage can be accessed in a variety of ways. Some investors with sophisticated computer science backgrounds can create their own. Another approach is to purchase a dedicated hardware "wallet," such as a Ledger or a Trezor, which uses hardware chip design to create an offline-like experience.

Most retail investors use investing apps such as Coinbase or Kraken, which provide all-in-one brokerage services for buying and selling cryptoassets and store the assets for users, often in a setting that is partially online and partially offline.

The most professional solution, however, is to work with a purpose-built, regulated, insured, enterprise-grade custodian. Today, regulated crypto custody providers include familiar financial names, such as Fidelity Digital Assets, and crypto-specialist firms, such as Coinbase Custody Trust Company, Anchorage, and BitGo. These firms have bank trust charters, often from New York or South Dakota, and undergo significant regulatory scrutiny. By and large, professional investors either work directly with such firms or access them by proxy through funds and investment products that use these custodians to hold assets.

Taxation

The tax treatment of cryptoassets is confusing to many people, largely because of the nomenclature that surrounds the crypto space.

Some people call cryptoassets "cryptocurrencies" and expect them to be taxed in the same way as other currency investments, with all gains (regardless of holding period) taxed as ordinary income. Other people consider cryptoassets to be commodities and assume they are taxed in the same way as commodity investments, which are often made using futures and are, therefore, subject to Section 1256 tax treatment, with mark-to-market annual taxation on gains. Still others anchor on the idea of bitcoin as "digital gold" and assume that all cryptoassets are taxed the same as gold, which is treated as a collectible by the IRS and taxed at 28% on any long-term capital gains.

In fact, the IRS has ruled that cryptoassets are taxed in the same way as property.[49] In general, that means that cryptoasset investments are taxed with traditional short- and long-term capital gains tax rates depending on the length of the holding period. (This does not apply to investments in cryptoasset futures, which are taxed as futures.)

Importantly, this study is not intended to be read as tax advice. Every situation is different, and investors should check with a tax professional before pursuing any tax strategy.

Regulation

The regulatory treatment of cryptoassets is evolving and varies from jurisdiction to jurisdiction. Investors should expect that kind of evolution and variation to continue.

Among the key regulatory developments that have defined the cryptoasset market in the United States since its creation are the following:

[49]The IRS has a comprehensive and readable FAQ on cryptoasset taxation available at www.irs.gov/individuals/international-taxpayers/frequently-asked-questions-on-virtual-currency-transactions.

- *2013: Financial crimes enforcement network issues guidance on crypto anti-money-laundering/know-your-client processes (FIN-2013-G001):*[50] In the first major regulatory development affecting the cryptoasset space in the United States, the Financial Crimes Enforcement Network clarified that crypto exchanges and other actors fall within its definition of "money transmitters" and must have appropriate anti-money-laundering (AML), know-your-client (KYC), and risk-monitoring programs in place.

- *2014: IRS issues initial guidance on crypto taxation:*[51] In its first guidance on cryptoassets, the IRS clarified the tax treatment of crypto as property and developed a clear FAQ list to help investors understand the treatment of these assets.

- *2015: In CoinFlip order, Commodity Futures Trading Commission asserts regulatory oversight of bitcoin as a commodity:*[52] This order defined bitcoin as a commodity and stated that online trading facilities that make markets in bitcoin derivatives must register as a designated "market maker" or "swap execution facility."

- *2015: New York State issues BitLicense:*[53] Many years in the making—and a requirement for firms conducting cryptocurrency business in the state—the New York State "BitLicense" instantly became the most developed state-level regulatory framework for the crypto space.

- *2017: SEC issues DAO Report, clarifies many initial coin offerings are securities offerings:*[54] In one of its first major actions surrounding cryptoassets, the SEC clarified that many initial coin offerings (ICOs)—a fundraising tool used extensively in 2015–2017 to raise assets to launch new cryptoasset-powered blockchains—were unregistered securities offerings. This finding cleared the way for substantial enforcement activity in the ICO market, removing some of the worst excesses of the 2017 bull market.

- *2017: Regulated bitcoin futures launch on Cboe, CME:*[55,56] In December 2017, both Cboe and the CME Group launched regulated bitcoin futures contracts. Though the Cboe contracts were subsequently

[50]Department of the Treasury Financial Crimes Enforcement Network, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies" (18 March 2013). www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering.

[51]Internal Revenue Service, "Virtual Currency: IRS Issues Additional Guidance on Tax Treatment and Reminds Taxpayers of Reporting Obligations" (9 October 2019). www.irs.gov/newsroom/virtual-currency-irs-issues-additional-guidance-on-tax-treatment-and-reminds-taxpayers-of-reporting-obligations.

[52]Commodity Futures Trading Commission, "In the Matter of CoinFlip, Inc., d/b/a Derivabit, and Francisco Riordan" (17 September 2015). www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoinfliprorder09172015.pdf.

[53]New York State Department of Financial Services, "Regulation of the Conduct of Virtual Currency Businesses" (25 February 2015). https://govt.westlaw.com/nyreg/Document/I41a4b512b7e311e493b50000845b8d3e?viewType=FullText&originationContext=documenttoc&transitionType=CategoryPageItem&contextData=%28sc.Default%29.

[54]Securities and Exchange Commission, "Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO" (25 July 2017). www.sec.gov/litigation/investreport/34-81207.pdf.

[55]Cboe Global Markets, "Cboe Plans December 10 Launch of Bitcoin Futures Trading" (4 December 2017). http://ir.cboe.com/~/media/Files/C/CBOE-IR-V2/press-release/2017/cboe-plans-december-10-launch-of-bitcoin-futures-trading.pdf.

[56]Chicago Mercantile Exchange, "CME Group Announces Launch of Bitcoin Futures" (31 October 2017). www.cmegroup.com/media-room/press-releases/2017/10/31/cme_group_announceslaunchofbitcoinfutures.html.

sunsetted, the CME market has become one of the largest bitcoin markets in the world.

- *2019: The Financial Action Task Force provides guidance on AML:*[57] In a major international regulatory development, the Financial Action Task Force—a multinational organization tasked with combating money laundering and terrorism financing—issued guidance requiring all crypto exchanges to conduct material KYC information gathering and to pass such information to one another when transferring funds.

- *2018–2019: SEC clarifies nonsecurity status of Ethereum:* In a series of steps—including a speech by the SEC director, William Hinman,[58] and a formal statement[59] and framework[60] from the SEC's FinHub division—the SEC clarified that Ethereum, despite having started as a security, no longer qualifies as one. This interpretation provided significant comfort around the security status of other large cryptoassets as well.

- *2020: OCC clarifies that all national banks can custody cryptoassets:*[61] In a significant interpretative letter, the OCC clarified that all federally chartered banks and thrifts may provide crypto custody services to clients. The letter also stated that banks may provide cash banking services to crypto-related companies as well.

The most appropriate way to view this series of developments is as a series of clarifications, normalizations, and tightening of regulations surrounding crypto, pulling its regulation closer in line with that of other asset classes and financial products. Although this progressive tightening of regulations runs counter to some of the perceived founding ethos behind cryptoassets, most view it as progress because it is necessary to allow for mainstream adoption and acceptance.

The current regulatory acceptance of crypto has limitations, of course. For instance, the SEC has repeatedly rejected applications to list a cryptoasset ETF, citing unsatisfied concerns about market manipulation, custodial risks, audit risks, and other factors. Efforts continue, however, and the lengthy process is similar to the experience of the initial approvals of ETFs in other asset classes and complex markets, including gold, commodities, and leveraged products.

Comparing Various Approaches to Investing in Cryptoassets

Investors looking to get exposure to cryptoassets have several options today. Each comes with certain features and trade-offs that must be weighed carefully before one invests. This section will walk through the six most common

[57]Financial Action Task Force, "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers" (21 June 2019). www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf.

[58]William Hinman, "Digital Asset Transactions: When Howey Met Gary (Plastic)," US Securities and Exchange Commission speech (14 June 2018). www.sec.gov/news/speech/speech-hinman-061418.

[59]William Hinman and Valerie Szczepanik, "Statement on 'Framework for "Investment Contract" Analysis of Digital Assets,'" US Securities and Exchange Commission public statement (3 April 2019). www.sec.gov/news/public-statement/statement-framework-investment-contract-analysis-digital-assets.

[60]US Securities and Exchange Commission, "Framework for 'Investment Contract' Analysis of Digital Assets." www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets.

[61]Office of the Comptroller of the Currency, "Interpretive Letter #1170."

investment approaches—brokerage apps, private funds, publicly traded shares, direct holdings with a custodian, CME futures, and venture capital funds—and enumerate the trade-offs therein.

Approach 1: Crypto Brokerage Apps or Other Brokerage-Like Windows

For traditional retail investors, the primary way to access crypto has historically been through crypto-specific brokerage websites and apps, such as Coinbase and Kraken. These apps allow users to buy and sell various cryptoassets in a fashion similar to how they would buy or sell equities through a brokerage solution, such as Charles Schwab. In fact, newer equity brokerage platforms, such as Robinhood, as well as many popular fintech applications, including Square's Cash App and PayPal, now offer crypto buying, selling, and trading as well.

The biggest crypto-specific brokerage companies today have tens of millions of users and process hundreds of millions of dollars in daily trading volume.

The primary advantage of these approaches is convenience. Often developed by well-funded companies and sporting high-quality user experience designs, these apps allow individual investors to easily transfer dollars in and to either purchase or sell multiple different cryptoassets.

With respect to security, the landscape of brokerage apps is large and varies widely. Some hold assets in robust (albeit often not 100% cold storage) custodial solutions, such as Coinbase, whereas others are negligent and have even lost client funds. You should be discerning about which particular service you use.

The challenges of this approach lie in the details, including relatively high fees on transactions (often greater than 1%–3% total for fees and spreads); non-competitive trade execution; the hassle of opening and funding a new account; the inability to invest via trusts, tax-advantaged accounts, and other entities; unclear compliance stature; delays and limits on withdrawals; and the personal security/custody risk that comes with holding assets in a mobile phone app. This last issue is particularly important: Even if the brokerage does not get hacked, your phone or email could. Users have been targeted in the past by cyberhackers using such techniques as SIM hacking and phishing to steal significant funds, with no recourse for recovery. Also note that for advisers and other professional investors, these holdings do not flow into standard reporting programs, which can present a significant challenge to standard workflows.

Nonetheless, brokerage apps and websites are the most popular way for individuals to invest and can be a great and easy solution for retail-level investing. However, being discerning about the specific service you use is important.

Approach 2: Passive and Active Private Placement Funds

As an alternative to investing apps, many private funds have emerged that offer certain investors access to cryptoassets in a familiar, fund-like setting. One of the first such funds to be widely recognized was the Pantera Bitcoin Fund, which launched in July 2013 and offered accredited investors an easy way to invest in bitcoin at a time when it was trading at roughly $60.

Since 2013, the landscape of private placement funds has expanded dramatically. Investors now have access to a wide variety of options, including single-asset funds, index funds, and active

hedge funds. These funds invest across an array of cryptoassets, including large caps, smaller assets, and everything in between. There are passive funds, holding single coins or an index of multiple coins, and active funds, running everything from long-only, long–short, market-neutral, event-driven, fundamental-driven, and special situation strategies. In general, passive funds offer liquidity daily or weekly, whereas active funds are more likely to offer quarterly or annual liquidity. In either rubric, high-quality fund providers custody assets with enterprise-grade regulated and insured custodians, though some firms trading smaller-cap assets have to hold those coins through other means because regulated custodians do not yet offer support.

The primary advantage of these funds is that they offer the ability to buy and sell managed exposure to cryptoassets in a familiar fund format. Funds handle custody, trading, reporting, tax, audit, and other features.

The challenges of these funds include that they are available only to accredited investors and have substantial paperwork burdens and that the hassle of funding and reporting can present significant logistical challenges, particularly for financial advisers or other professional investors who invest on behalf of multiple clients.

The choice between single-asset, index, and active funds in crypto is similar to the choice between single stocks, index funds, and active funds in equities. Single-asset funds require the investor to underwrite the decision to allocate to a specific asset and monitor developments on an ongoing basis. Active funds appeal to those who believe that market inefficiencies that are worth exploiting might exist and who are comfortable performing due diligence on a manager in the space, often based on a limited track record. Index funds allow for broad-based bets on the market and remove the need for investors to constantly monitor the shifting nature of the space, though they might leave alpha on the table.[62]

Today, private funds are most popular with high-net-worth individuals, registered investment advisers, family offices, and hedge funds.

Approach 3: Publicly Traded Shares

A third and increasingly popular approach among investors is to purchase the seasoned shares of private placement funds via traditional brokerage and custodial accounts, such as Charles Schwab, TD Ameritrade, and Fidelity. These shares are not listed on a national securities exchange, such as the New York Stock Exchange, but, rather, are traded via OTCQX, operated by OTC Markets Group. Shares listed on OTCQX include those of such large companies as Roche Pharmaceuticals and Adidas, as well as those of private placement funds that satisfy certain requirements, including a six- or 12-month seasoning period for shares.

The primary advantage of purchasing shares of a private fund via OTCQX is that investors can access crypto with the same ease and in the same manner that they purchase and sell shares of individual stocks or ETFs. For financial advisers, this has additional benefits, because shares can be held with traditional adviser custodians and reported and managed through traditional advisory reporting software. It also makes investing via an entity such as a trust, tax-advantaged account, or fund simple.

The ease of use allowed by OTCQX, however, comes with a cost: Because new shares created

[62]Bitwise Asset Management, the company for which both authors work, created the first crypto index fund, the Bitwise 10 Crypto Index Fund, in 2017.

through a private placement must season for 6 or 12 months before they can be traded on OTCQX, a disconnect can occur between the number of shares available for trading and the demand for those shares on the OTC markets. As a result, shares can trade at substantial and varying premiums and discounts to their true net asset value. The largest such fund, the Grayscale Bitcoin Trust, has historically experienced premiums and discounts ranging from approximately +140% to −1%. Bitwise Asset Management also recently announced that the Bitwise 10 Crypto Index Fund, the first and largest index fund in the space, is expected to begin trading on OTCQX and to be available in brokerage accounts by the end of 2020.

Today, publicly traded shares are most popular with retail investors, high-net-worth individuals, registered investment advisers, and other funds.

Approach 4: Direct Custodial Relationship

Large institutional investors can access cryptoassets by working directly with a crypto custodian and its trading operation to facilitate the purchase, sale, and custody of individual cryptoassets.

For the right investor, such a relationship can be a very low-cost way to gain exposure to the market, cutting out fund providers and their cost. The logistical challenges here include performing due diligence on the custodian and on the underlying assets and/or strategy, opening and funding accounts, and the existence of separate reporting flows.

Today this approach is most popular with crypto private and venture capital funds, family offices, and certain endowments. It is not available to smaller investors.

Approach 5: CME Futures

The CME bitcoin futures market, along with other nascent regulated futures markets, has emerged as a significant way for investors to access the market.

As with any futures-based investing strategy, maintaining a long-term position using futures involves costs, including the trading costs associated with rolling the position over time. Also, bitcoin futures have historically tended to trade at a modest level of contango, wherein futures contracts trade at a premium to the spot price, which presents a headwind to returns. Futures positions are also taxed differently from direct holdings of cryptoassets, with challenges to deferring the realization of capital gains.

Nonetheless, many investors find comfort in the facts that CME and other futures markets are fully regulated and the custody of futures positions is familiar. CME and other markets also allow individuals to access bitcoin futures using some degree of margin, which might add efficiency from a capital perspective.

Today this approach is most popular with hedge funds and proprietary trading firms.

Approach 6: Venture Capital Funds

Finally, many investors choose to allocate to the space through venture capital firms, which might invest in a mix of established cryptoassets, emerging cryptoassets, and the equity of companies building in the cryptoasset space.

A large number of well-established crypto venture firms from both venture generalists, such as Andreessen Horowitz, and crypto-specific firms, such as Blockchain Capital, have

multiple-year track records and often multiple funds.[63]

Many investors are more comfortable performing due diligence on a venture capital team, as opposed to an entirely novel asset class, and prefer to allow experts to select the best way to gain exposure to the cryptomarket rather than attempt to make those decisions themselves.

On the downside, accessing the top tier of venture capital funds can be difficult for many investors. Moreover, even the best funds have significant fees, and a lack of liquidity can make dynamically sizing the allocation to these funds difficult in a portfolio context. Finally, some people believe that the crypto venture capital space is oversupplied, with too many assets chasing too few opportunities, and that the best investment opportunities are in the past.

Today this approach is most popular with endowments, foundations, pensions, and certain family offices.

Future Approaches

None of the currently available approaches to investing in crypto is perfect. They variously come with high fees, liquidity restrictions, custodial concerns, access limitations, reporting challenges, variable premiums, and other issues.

A solution to these problems would be to package crypto inside an ETF or mutual fund, and a large number of asset managers have been pursuing this idea for years, including most recently Bitwise, VanEck, and Wilshire Phoenix. Exchange-traded products have been approved in certain jurisdictions, including Switzerland, Germany, and Sweden. As of yet and despite efforts dating back to 2013, however, no provider has won approval to launch a crypto ETF or an unfettered crypto mutual fund in the United States. Expectations are that the first such fund, if approved, would hold bitcoin only.

Risk Factors for Crypto Investors

The cryptoasset market is early in its development, and investors accessing the space face material risks. In this section, we examine those risks, classifying them into two groups: risks to crypto as an industry and risks that accrue specifically to crypto as an investment.

Risks to Crypto as an Industry

Eleven years after its creation, the cryptoasset industry is relatively well established, with sufficient critical mass in terms of asset size, institutional support, regulatory development, and other factors to appear to be sustainable in the future. But significant large-scale and even existential risks to crypto that are worth bearing in mind remain.

Technical Risks

Crypto continues to face large technological risks.

Even the most established blockchains, such as bitcoin, are potentially susceptible to bugs and other technical issues that could expose unknown security flaws. As recently as 2018, researchers uncovered a bug in the bitcoin code that, if left unchecked and exploited, could have led to significant (theoretically infinite) inflation in the issuance of new bitcoin.[64]

[63]Disclosure: Blockchain Capital is an investor in Bitwise Asset Management.

[64]Alyssa Hertig, "The Latest Bitcoin Bug Was So Bad, Developers Kept Its Full Details a Secret," CoinDesk (21 September 2018). www.coindesk.com/the-latest-bitcoin-bug-was-so-bad-developers-kept-its-full-details-a-secret.

In practice, that any such bug could have been exploited in a significant manner is highly unlikely. However, the fact that such a bug emerged recently is a reminder that technical flaws are a lingering threat to an asset built entirely on software. Moreover, the threat is likely larger for newer and more complex blockchains.

Beyond these sorts of existential technical risks are incremental performance challenges that could prevent various blockchains from realizing their full potential. Bitcoin, for instance, is currently able to handle only a handful of transactions per second. Although efforts are under way to improve or work around that limitation, it remains a significant bottleneck.

Competitive Risks

Another significant risk is that cryptoasset-powered blockchains will lose out to rising competition from other technological solutions. These solutions could come in the form of improved iterations on distributed databases, improvements to the traditional financial architecture, or other, unanticipated disruptions.

For instance, as discussed, the ability to settle transactions more quickly than the traditional financial services industry is one of the three key technological breakthroughs cryptoasset-powered blockchains offer. But traditional financial services are not standing still. For instance, in August 2019, the Federal Reserve announced plans to launch a real-time gross settlement program called "FedNow" that will significantly speed up financial transaction settlement in the United States.[65] Also, the Federal Reserve announced that it would explore the expansion of its Fedwire Funds Service to run 24/7/365, rather than during banking hours.[66] These and similar advances globally could challenge rapid settlement as a differentiating factor for crypto.

Malicious Noneconomic Actors

Cryptoasset consensus mechanisms rely in large part on economic game theory to exist. The "miners" that validate cryptoasset transactions are incentivized to behave honestly because doing otherwise would be uneconomical.

For instance, if someone wanted to execute fraudulent transactions on the bitcoin network, they could do so if they could amass more computer mining power than the rest of the network combined. This would eventually allow them to "control" the network and dictate the settlement of transactions through what is called a 51% attack (because it requires 51% of the total mining power directed at the asset).

Setting up a 51% attack on bitcoin would cost hundreds of millions of dollars (or more) in installed hardware, millions of dollars in electricity, and nearly impossible logistical processes. Even if it were possible, however, criminals intent on posting fraudulent transactions would never embark on such a scheme because its success would destroy the value of bitcoin, rendering the undertaking unprofitable.

A noneconomic actor, however, such as a state entity, could potentially engage in such an activity. Although the cost would be significant—and would scale if a cryptoasset's value increases—and potential defenses against this type of attack have been built into the code of many blockchains (including bitcoin), it remains a risk.

[65]Federal Reserve Board, "Federal Reserve Announces Plan to Develop a New Round-the-Clock Real-Time Payment and Settlement Service to Support Faster Payments," press release (5 August 2019). www.federalreserve.gov/newsevents/pressreleases/other20190805a.htm.

[66]Federal Reserve Board, "Federal Reserve Announces Plan."

Regulatory Threats

To a large degree, existential regulatory risks to crypto have subsided in recent years. But significant areas of regulatory uncertainty remain for investors to consider, including the following:

- *Asset seizure or bans:* Some worry that the government could ban the ownership of all or some cryptoassets. This concern is particularly acute for cryptoassets that have untraceable transactions, such as Monero and Zcash, because they might raise significant concerns about money-laundering activity.
- *Enhanced AML/KYC requirements:* All cryptoasset transactions are pseudonymous at a minimum. Therefore, to satisfy money-laundering regulations, the crypto industry has been enforcing enhanced AML and KYC requirements at crypto on-ramps, such as exchanges. The further strengthening of these protections could affect the liquidity of the marketplace.
- *Security status:* Cryptoasset exchanges can exist in their current format in part because cryptoassets are not deemed "securities" by US federal regulators. If they were to be deemed securities, the resulting restrictions could severely affect the current liquidity ecosystem. While the "nonsecurity status" of the largest cryptoassets is well established, smaller and newer cryptoassets might have additional risks in this regard.

Additional Threats

An exhaustive list of the threats to the crypto industry is beyond the scope of this paper. However, other areas of concern include the following:

- *Market manipulation:* Cryptoasset trading venues are not as regulated or mature as national securities exchanges or many other financial marketplaces. As a result, they are potentially more susceptible to market manipulation, and such manipulation might be more difficult to monitor and correct.
- *Fraudulent entities:* The history of the cryptoasset industry is beset with stories of fraudulent entities that stole investor money as a result of incompetence or malicious intent. That all investors work with best-in-class partners is critical to avoid the potential for fraud in this fast-moving industry. Investors have lost billions of dollars working with fraudulent or incompetent third parties.

Investment-Specific Risks

Although the aforementioned exogenous and existential risks are important to consider, by far the bigger and more real risks for investors come on the investment side.

Critically, investors must realize that any investment in crypto is likely to be volatile. Crypto is a nascent industry, and cryptoassets have exhibited extremely high levels of volatility, including multiple instances of substantial drawdowns. Although volatility has declined somewhat over time, it remains significantly higher than in traditional asset classes, such as stocks and bonds.

On a related note, this high volatility makes crypto a particularly challenging asset from a behavioral perspective. The temptation to chase runaway returns or sell against falling prices is a common trait in all asset classes, and it might be particularly difficult for investors to stick to a structured investment program in crypto given its exceptionally high volatility.

Additionally, performing due diligence in parts of the crypto space is difficult. Crypto expertise is still developing at consultants, few Wall Street firms provide extensive research on the space, valuation metrics are still under development, and data quality is uneven. Beyond that, many fund managers are new and have limited track records, and those track records might be heavily influenced by the cyclical bull and bear movements.

And, of course, crypto's strong historical returns are unlikely to repeat or could even reverse in the future. Many believe crypto is a bubble, and others, while recognizing its potential, question whether either the space or any particular asset can justify current valuations (much less higher valuations).

Finally, which cryptoassets will emerge as the most important is not clear, nor is how the market will be divided in the future.

The cryptoasset space is a new and evolving market, and its outlook is uncertain, with a wide range of possible outcomes. As with any disruptive, new, and early-stage environment, investors moving into crypto must be prepared for the potential of substantial loss.

CONCLUSION

The goal of this guide is to provide an introduction to cryptoassets: what they are, what they are not, and what they might become in the future.

Our view is that the key to understanding cryptoassets lies in understanding the fundamental idea behind blockchain databases. All the hopes, dreams, excitement, disbelief, and risk that accrue to the cryptoasset space exist because of the breakthroughs that this novel database design provides.

The designer of the first blockchain—Satoshi Nakamoto—created a system that birthed a significant new possibility into the world: the ability to have a distributed database that is controlled by no individual party but maintains a verifiable public record of "the truth." This breakthrough allowed money and other items of value to move onto the internet in a native fashion for the first time and created the possibility of digital scarcity, programmable money, and the rapid settlement of financial transactions between any two parties without the need for a trusted intermediary.

Making this leap introduced trade-offs. Blockchain databases are not as fast as traditional databases, they do not scale as well, they are more challenging to regulate, AML and KYC protections are difficult to enforce, system upgrades and payment protections are challenging to implement, and so on. And as with any new technology, the introduction of blockchains and cryptoassets to the world has been messy, with instances of fraud, overexuberance, scams, and criminal activity.

Despite these drawbacks, the space has grown by leaps and bounds. For early-adopter investors, cryptoassets have been a boon, providing a rare and impactful combination of high returns, low correlations with other assets, and intraday liquidity. Even a small allocation to crypto has had a significant positive impact on portfolio returns.

As we march further into the second decade of crypto's existence, the question becomes, What should we watch for on the horizon?

Will the incredible investment that has occurred in crypto infrastructure—including the development of regulated custodians, the launch of regulated futures contracts, and the creation of

cryptoasset funds—turn crypto into a popular allocation in institutional portfolios?

Will cryptoasset-powered blockchains continue to penetrate their unique use cases, whether that is digital gold, decentralized finance, payments, or other areas?

Will the accommodative stance of regulators continue to progress and develop?

Perhaps most importantly for investors, will crypto's historical pattern of returns persist into the future, or will returns flatten or even reverse?

These are the questions investors and observers must wrestle with in the years to come. We hope that this document has provided a foundation and a framework for doing that.

One thing is for certain: The emergence of a new asset class and financial ecosystem is a rare event, and the potential for cryptoasset-powered blockchains to move the world forward is exciting.

Named Endowments

CFA Institute Research Foundation acknowledges with sincere gratitude the generous contributions of the Named Endowment participants listed below.

Gifts of at least US$100,000 qualify donors for membership in the Named Endowment category, which recognizes in perpetuity the commitment toward unbiased, practitioner-oriented, relevant research that these firms and individuals have expressed through their generous support of the CFA Institute Research Foundation.

Ameritech
Anonymous
Robert D. Arnott
Theodore R. Aronson, CFA
Asahi Mutual Life Insurance Company
Batterymarch Financial Management
Boston Company
Boston Partners Asset Management, L.P.
Gary P. Brinson, CFA
Brinson Partners, Inc.
Capital Group International, Inc.
Concord Capital Management
Dai-Ichi Life Insurance Company
Daiwa Securities
Mr. and Mrs. Jeffrey Diermeier
Gifford Fong Associates
John A. Gunn, CFA
Investment Counsel Association of America, Inc.
Jacobs Levy Equity Management
Jon L. Hagler Foundation
Long-Term Credit Bank of Japan, Ltd.
Lynch, Jones & Ryan, LLC
Meiji Mutual Life Insurance Company
Miller Anderson & Sherrerd, LLP
John B. Neff, CFA
Nikko Securities Co., Ltd.
Nippon Life Insurance Company of Japan
Nomura Securities Co., Ltd.
Payden & Rygel
Provident National Bank
Frank K. Reilly, CFA
Salomon Brothers
Sassoon Holdings Pte. Ltd.
Scudder Stevens & Clark
Security Analysts Association of Japan
Shaw Data Securities, Inc.
Sit Investment Associates, Inc.
Standish, Ayer & Wood, Inc.
State Farm Insurance Company
Sumitomo Life America, Inc.
T. Rowe Price Associates, Inc.
Templeton Investment Counsel Inc.
Frank Trainer, CFA
Travelers Insurance Co.
USF&G Companies
Yamaichi Securities Co., Ltd.

Senior Research Fellows

Financial Services Analyst Association

CFA Institute
Research
Foundation

Available online at www.cfainstitute.org

ISBN 978-1-952927-08-9