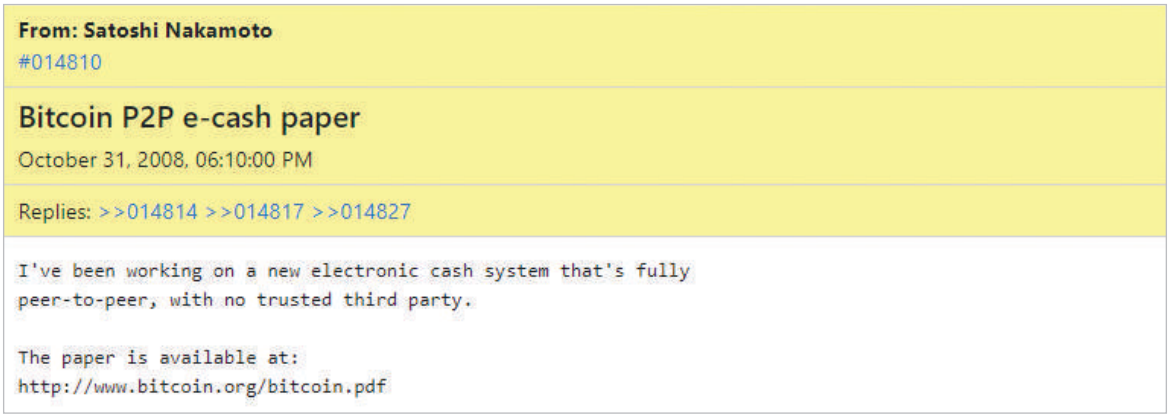
Key Wealth Institute

Cryptocurrency Basics: Blockchain, Bitcoin, and Betting on the Future

by Justin Tantalo, CFA, Senior Lead Research Analyst

Part 1: Bitcoin and blockchain basics

Bitcoin was introduced on October 31, 2008, in a short message from Satoshi Nakamoto[1] sent to an obscure mailing list of cryptography enthusiasts:



From: Satoshi Nakamoto
#014810

Bitcoin P2P e-cash paper

October 31, 2008, 06:10:00 PM

Replies: >>014814 >>014817 >>014827

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

The humble message linked readers to a nine-page white paper, where Satoshi outlined the Bitcoin peer-to-peer payment framework and introduced a set of solutions to overcome the shortcomings of previous attempts at decentralized digital cash. The message represented the birth of a revolutionary technology — the decentralized digital blockchain — and, on that blockchain bitcoin, the world's first cryptocurrency.

Who was Satoshi Nakamoto?

We still don't know. "Satoshi Nakamoto" was an alias used by the person (or persons) who developed Bitcoin. The mystery around Satoshi is an intriguing side story in Bitcoin that could remain unsolved indefinitely: It's been more than 10 years since Satoshi Nakamoto was last active online. The most credible theories of Satoshi's identity center on a small group of cryptography and computer science experts, some of whom have passed on since Bitcoin went live in January 2009.

What we do know from Satoshi's writings is that he/she/they were likely motivated by a distrust of the fractional reserve currency system that underpins modern monetary policy. The fractional reserve system places trust in a centralized monetary authority that ultimately controls money supply. Satoshi believed that sound money could be created using cryptography and transparent code rather than central banks and politicians who might be subject to whims of the moment. Coincidently (or not), the timing of Bitcoin's launch (January 2009) coincided with the depths of the Great Financial Crisis and the ultra-unorthodox monetary response to it. Satoshi embedded a message into the first block of Bitcoin: *"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks."*

[1] http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html

Defining Bitcoin

First, some terminology. The word Bitcoin — slightly confusingly — refers to two separate but related concepts. It refers to both the blockchain network and the cryptocurrency that trades on that network.[2] Other blockchain protocols such as Ethereum differentiate the network (Ethereum) from the currency (ether) with less ambiguity.

What is Bitcoin?

Bitcoin is a decentralized, digital blockchain network that allows peer-to-peer transfer of value (bitcoin) without the need for permission or trusted intermediary. A bitcoin is not simply a file that is sent from one user to another, since the sender could keep a copy while also spending it (i.e., double spend). Instead, the Bitcoin network keeps track of all historical transactions on a distributed ledger to accurately reflect who currently holds bitcoins.

Ledgers, ledgers everywhere!

Banks, central banks, security brokers, remittance services, and countless other intermediaries make up our modern-day centralized financial infrastructure. Collectively these entities maintain interconnected ledgers of who owns what and who owes what: They implicitly reflect historical transactions made between parties. It's a complicated web of centralized ledgers that is costly to maintain, but the plumbing works.

Digital blockchains like Bitcoin, on the other hand, operate as decentralized distributed ledgers where network participants propose, validate, and record transactions without a centralized, trusted intermediary.

In Bitcoin, all transaction data is stored on a blockchain. A blockchain is a ledger record of every historical transaction in the network, since day one, where "blocks" of data (transactions) are "chained" to previous blocks such that the blockchain tells a single, immutable story of how current balances came to be. The ledger is append-only, which means that data or transactions can only be added in subsequent blocks. Cryptographic verification is used to ensure that transactions in historical blocks cannot be altered without breaking the sanctity of the chain.

How it works.

The Bitcoin blockchain is software maintained concurrently on thousands of independent nodes (servers) distributed globally. Anyone can operate a node on something as basic as a personal laptop. This distributed architecture makes Bitcoin both hard to shut down and secure, since a rogue or malicious node with false transaction data will have its record disregarded by the consensus of the thousands of other nodes. Consensus is the ultimate truth.

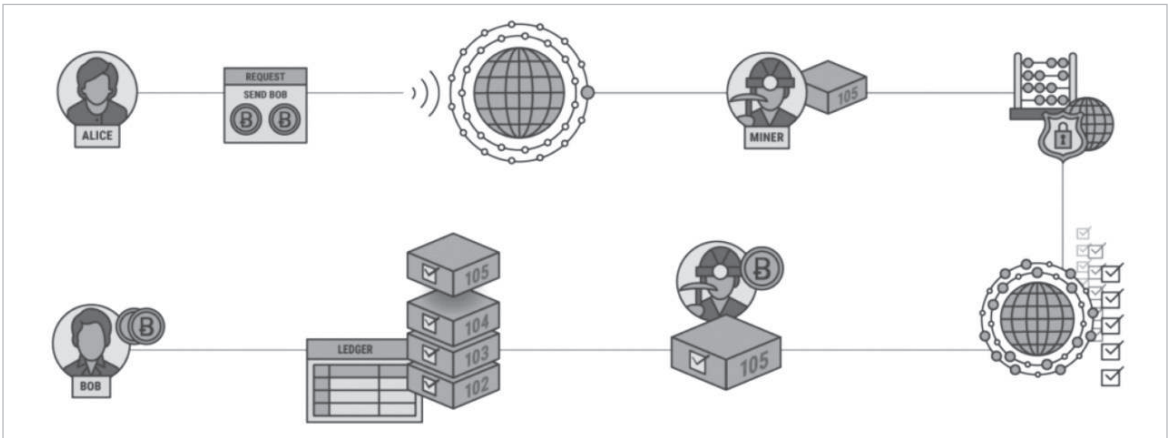
Each node maintains its own copy of the Bitcoin blockchain which is updated with a new block every 10 minutes or so. Let's walk through a simple example to better understand the process.

[2] A differentiation is sometimes made: "Bitcoin" with an upper-case "B" refers to the blockchain network protocol, while "bitcoin" lower-case "b" refers to the cryptocurrency itself. Think of a railroad analogy: the goods (bitcoin) travel on the rails (Bitcoin).

Suppose Alice would like to send two bitcoins to Bob. Alice creates a transaction request using Bob's public address, signs the request digitally using her private key that only she knows, and broadcasts her proposed transaction to the network of nodes. All newly proposed transactions like Alice's are distributed to each node. Cryptography is then used to verify that Alice sent the message and that the two bitcoins are in fact hers to send.

Alice's transaction only becomes "official" when it is included in the next block of the blockchain. This last step requires a consensus-building mechanism amongst nodes so that each of them has the same record with the same cadence. Consensus-building is undertaken by a specialized participant called a Bitcoin miner.

Understanding a bitcoin transaction



Source: CBInsights

Anyone can mine Bitcoin.

Miners race against each other to be first to solve a computationally challenging cryptographic puzzle, because with that solution (called "proof-of-work"), they win the right to package awaiting proposed transactions (including Alice's) into the next official block in the blockchain. The successful miner is entitled to newly minted bitcoin as a reward for solving the puzzle and formally creating the next block.[3] All nodes update their blockchain once a new block is mined by a miner; in the above schematic, Bob officially takes custody of his two bitcoins in block 105.

Bitcoin miners play an important role in building consensus and maintaining network integrity. The incentives they face steer the blockchain to include only the set of transactions which have been verified as legitimate (digitally signed and unspent coins). How so? A miner who solves the cryptographic solution but proposes a block with a fraudulent set of transactions will have their block rejected by the network of nodes (due to unrecognized transactions), which leads to failing to achieve consensus and forgoing their associated reward of newly minted bitcoin.

Every Bitcoin came into existence through the mining process just described. To close out our example, Alice may have originally acquired those two bitcoins she sent to Bob in one of three ways:

1. She mined them
2. She purchased them with fiat currency like US dollars or other cryptocurrency at a crypto exchange
3. She acquired them in exchange for goods or services (i.e., accepted payment in bitcoin).

These are the three ways one can acquire bitcoin: mine them, buy them, or trade for them.

[3] Mining rewards are currently 6.25 BTC per block. Rewards started at 50 BTC per block in 2009, but halve every four years.

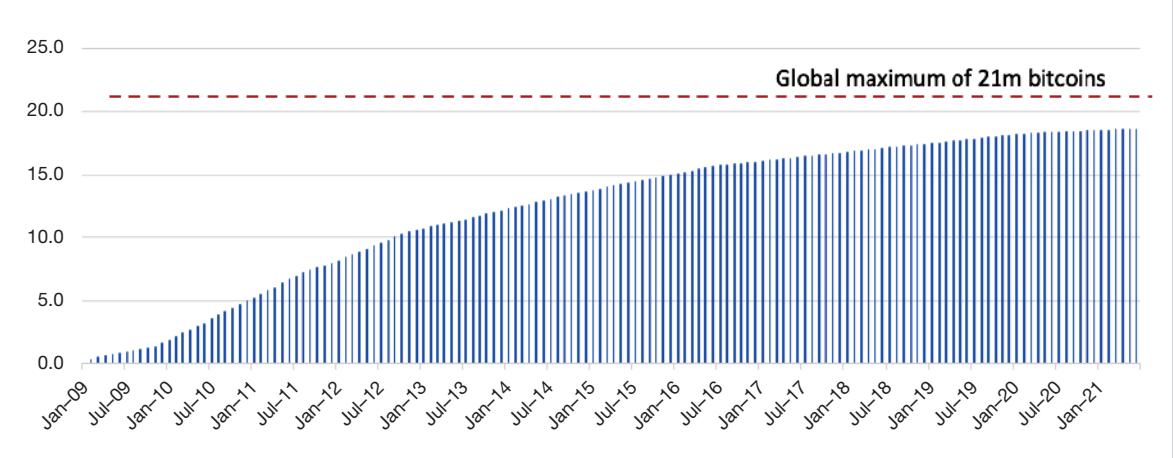
Digital scarcity

Satoshi Nakamoto appreciated that for users to adopt Bitcoin, it needed to be grounded in sound money principles. Establishing trust would be difficult if an unlimited supply of bitcoin could be conjured up in a discretionary manner, a weakness Satoshi believed to be inherent with fiat money. To address this, the protocol dictates that new bitcoin awarded to miners follows a known trajectory with ultimate supply capped at 21 million bitcoins.

The supply of bitcoin is scheduled to grow at a decelerating rate until sometime in the year 2140, when all 21 million bitcoins that will ever exist will have been mined.[4] As of mid-2021, approximately 18.7 million bitcoin have been mined.

Bitcoin introduced the world to the concept of digital scarcity — a digital good with verifiably limited supply.

History of Bitcoin Supply (Millions)



Source: Coinmetrics

Is bitcoin money?

Livestock, salt, shells, cloth, leather, coins of copper, silver, and gold have all been used as money at some point in history. Is bitcoin (or other cryptocurrencies) the future of money? Maybe.

Money is a complex, societal construct. Some of history's brightest economists have written treatises on money that span hundreds of pages. We won't take that liberty here. But to approach this question objectively, we remind ourselves of the three textbook roles of well-functioning money. Money should act as 1) a medium of exchange, 2) a unit of account, and 3) a store of value. It turns out that when viewed using this objective lens, bitcoin is a relatively weak form of money. Consider:

Bitcoin as a **Medium of Exchange:**

- Money should be widely accepted in exchange for goods and services. US dollars are widely accepted because those dollars are widely accepted elsewhere. That circle of trust is exceptionally important for a medium of exchange. Bitcoin, although growing, are not yet widely accepted as a form of payment.
- Scalability issues. The Visa payment network handles an average of 1,700 transactions per second. Bitcoin can accommodate approximately seven transactions per second. There are side-chain or "layer two" solutions that can improve scalability, but using bitcoin to purchase a cup of coffee is not likely anytime soon.

[4] Beyond 21 million bitcoins, miners will be incentivized by transaction fees paid by senders.

- Bitcoin settlement is final. A credit card transaction can be reversed through a chargeback. There is no such discretion in Bitcoin, and it is impossible for a payer to unilaterally reverse a transaction, even if justifiable because of error or fraud. With Bitcoin, all transfers are final, including mistakes.

Bitcoin as a **Unit of Account:**

- Money should be fungible and divisible into smaller units. Here, bitcoin scores well as 1) all coins are equal and fungible, and 2) a coin can be divisible into a hundred-millionth unit called a "satoshi" (0.00000001 BTC).
- A unit of account needs price stability. Bitcoin is still far too volatile to reliably price goods. There are some goods which can be purchased in bitcoin today, but these transactions are usually priced first in a hard currency like US dollars, then wrapped with the equivalent bitcoin price tag at the final transaction.

Bitcoin as a **Store of Value:**

- A store of value refers to money's ability to retain its purchasing power across both space and time.
- A good store of value over space (geographically) was first defined by neoclassical economist Stanley Jevons as "Something which is very valuable, although of little bulk and weight, and which will be recognized as very valuable in every part of the world...".[5] Since bitcoin lives on a decentralized global network, it scores exceptionally well as a portable asset that stores value, arguably the best in history.
- However, money should be a good store of value over time too. Bitcoin's volatility can easily be forgiven when prices are rising, but there have been three drawdowns of 80% in the past 10 years. The high volatility materially limits the attractiveness as a store of value. Historically, stores of value during economic and political duress (when they are needed the most) have been volatile given high levels of uncertainty and risks of punitive capital controls. Given Bitcoin's more limited history and much higher volatility, other assets such as gold may be more palatable for a broader range of people.

Bitcoin has scalability issues and a volatility profile that makes it a weak form of transactional money.

A better analogy for Bitcoin might be "digital gold." Gold and bitcoin are both liquid, volatile, bearer assets whose incremental supply is verifiably constrained. There are superficial parallels too: Both bitcoin and gold are mined into the market, and bitcoin is even popularly portrayed as a golden coin, with an engraved **B**.

	Gold	Bitcoin
Finite supply	Supply increases about 2% per year.	Supply increases less over time, with a terminal limit of 21,000,000 coins.
Liquid markets	Gold has a highly liquid market with a huge variety of participants and contracts.	Bitcoin, like gold, appears to have highly liquid markets, including futures contracts.*
Uncorrelated	Correlations with other assets are typically low, especially in times of economic distress.	Price behavior is still evolving, with correlations increasing more recently.
Inflation hedge	Past inflationary episodes have shown gold tends to perform well in such environments.	Finite supply is attractive, but the asset remains untested given its limited history.
Global acceptance	Gold is a globally recognized store of value, held as reserve assets by most central banks.	Bitcoin is banned in a number of countries and is widely regarded with skepticism by authorities.
Use in goods	Gold is commonly used in high-tech manufacturing and jewelry.	Bitcoin has no uses outside its value as an asset.

Source: Invesco
*Bitcoin trades 24/7, resulting in periods of relative liquidity. This appears to be especially true on Sundays, resulting in greater price volatility on these days.

[5] Money and the Mechanism of Exchange, (New York: D. Appleton and Co. 1876)

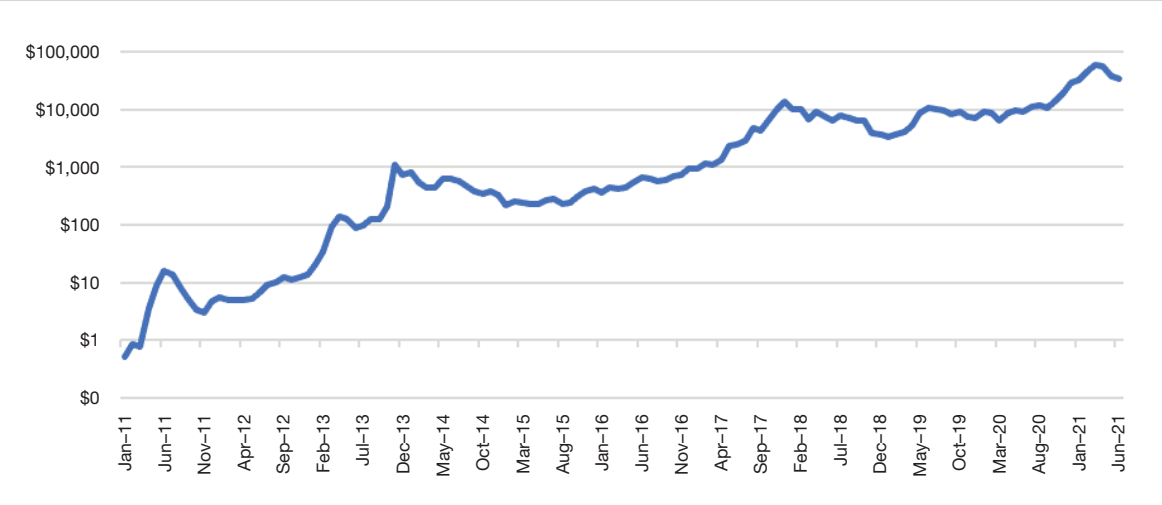
Part 2: Crypto assets in a portfolio

Bitcoin is a cleverly designed peer-to-peer payment network. But how does its technology and growing adoption translate to price? In other words, what is a bitcoin worth?

Bitcoin has no obvious intrinsic value. Any theoretical model or narrative on the fair value of bitcoin requires a good dose of abstraction. Unlike traditional assets like stocks, bonds, and real estate, bitcoins do not have a stream of cash flows that can be discounted. How then should one think about bitcoin's price and/or fair value?

Consider the uncertainty of this question through the lens of bitcoin's historical price range. It's enormous. At the bottom of the range, the 10,000 bitcoins that Laszlo Hanyecz paid for two Papa John's pizzas in 2010 implies a price of less than $0.01 per bitcoin. At the top end of the range, in early 2021, one bitcoin traded for approximately $65,000. From less than one cent to $65,000 with exceptional price volatility along the way, it's clear that even the wisdom of the masses struggle with bitcoin's fair value.

Bitcoin Price USD (Log Scale)



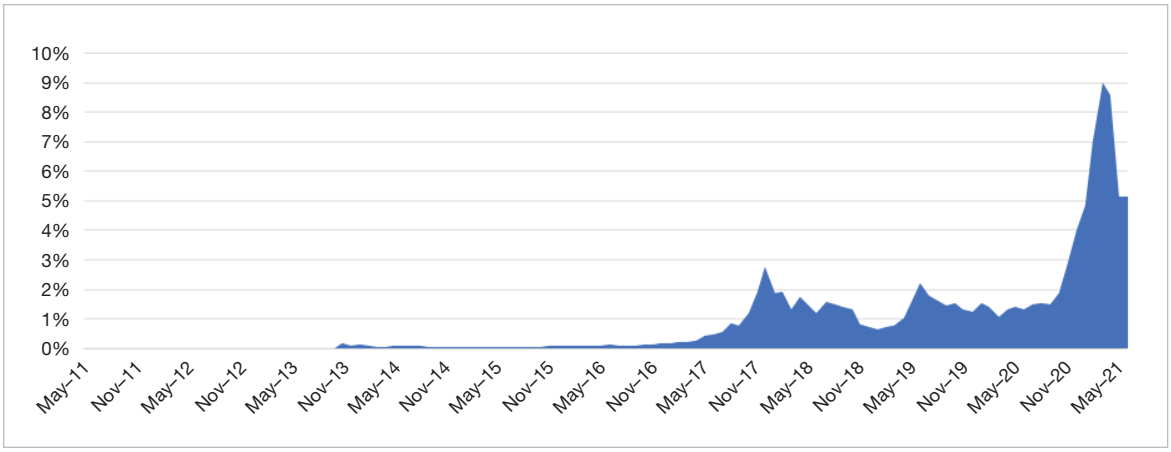
Source: Coinmetrics

Market participants have proposed various frameworks to understand bitcoin's price. We review a few of the most compelling here:

Relative to gold

Bitcoin's conceptual parallel to gold has been extended to valuation. If one considers gold as a financial asset and store of value and ignores its use in jewelry, electronics, and dental work, then comparing gold's total capitalization to bitcoin could be informative. The World Gold Council estimates that ~200k tonnes (or metric tons) of gold have been mined throughout history. Because gold is practically indestructible, we can assume that it is all still held somewhere. That gives gold a market capitalization of approximately $12 trillion (at $1,750/oz). Using June 30, 2021, price (approximately $35,000/BTC), Bitcoin's market cap of $650 billion values the asset at 5% of gold. Some gold-based valuation models also adjust for bitcoin's substantially higher volatility. If volatility is incorporated, then the relative market cap to gold is materially higher.

Bitcoin Relative to Gold (Total Market Cap)



Sources: Coinmetrics, World Gold Council

Bitcoin in relation to an exogenous market price like gold is one way to approach valuation. An alternative group of models attempt to understand bitcoin's price endogenously, or its price in relation to internal variables. Three of these models are presented below.

Model #1: Using Metcalfe's Law.

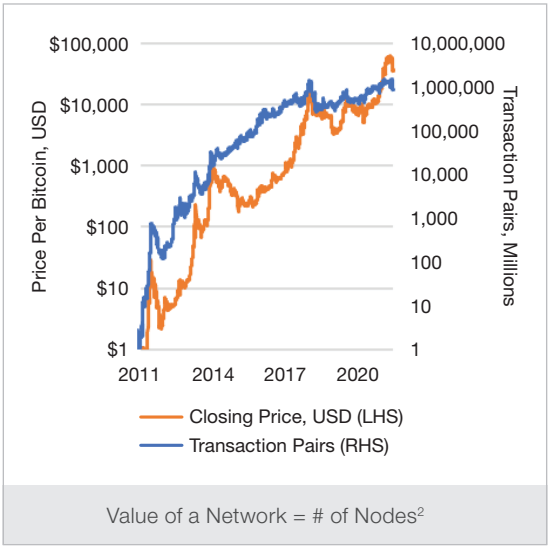
Metcalfe's Law suggests that the value of any network is nonlinearly proportional to the number of users on it (value = users^2). In other words, the value of a network is equal to the square of its user base.

Consider a simple telephone network with two users. It has some value, but with three users it has more than twice that value, since more than twice as many combinations of calls can be made on it.

Proponents of this framework see Bitcoin as a payment network with growing adoption. Invesco evaluated this model using transaction pairs to proxy Bitcoin's user base and plotted it against bitcoin prices over time.

The challenge with this model is that Metcalfe's Law is rather vague about the definition of value. Does it refer to the value (price) of a single bitcoin in dollars? Does it refer to the value (economic utility) of the Bitcoin blockchain network? The difference matters. Email as a network has exceptional value (utility), but it also has a comparatively low price.

Network Effects: Metcalfe's Law



Sources: Bitcoin price and its marginal cost of production: support for a fundamental value by Adam S. Hayes, CFA, and Metcalfe's Law as a Model for Bitcoin's Value by Timothy F. Peterson, CFA, CAIA. Model recreated using estimates from Cambridge University Centre for Alternative Finance and data from CoinMetrics.io. Data as of 31 May 2021. Past performance does not guarantee future results.

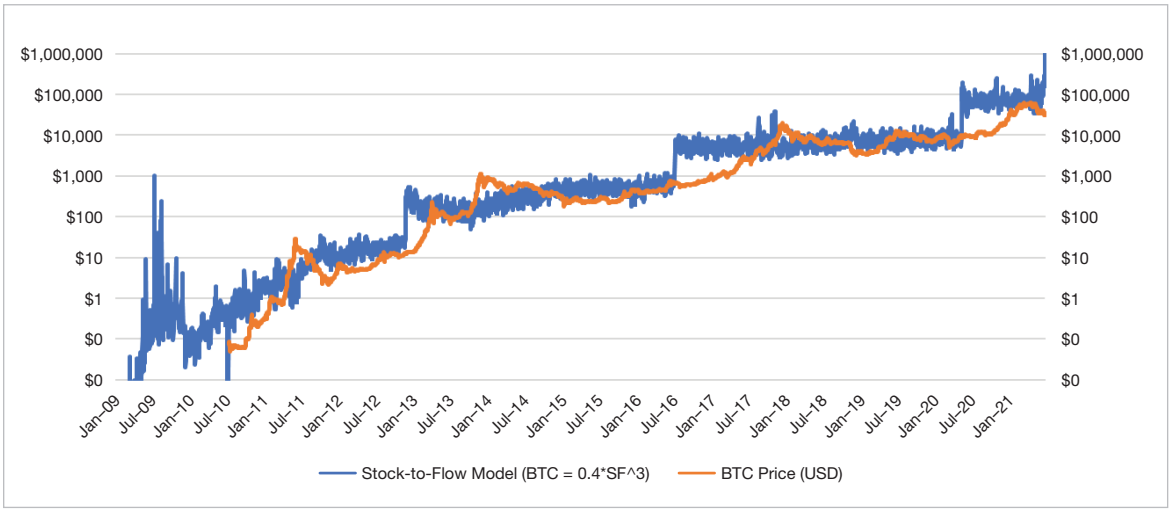
Charting produced by Invesco.

Model #2: Stock-to-Flow.

The Stock-to-Flow (S2F) model was first disseminated in 2019 by pseudonymous Bitcoin enthusiast "Plan B." The model hypothesizes that a scarcity factor (SF = stock/flow) explains price levels. Gold, for instance, has a scarcity factor of approximately 66x (existing stock of ~200 thousand tonnes, annual flow of three thousand tonnes), meaning that it takes approximately 66 years of current gold mining production to double outstanding gold supply.

Bitcoin has a dynamic scarcity factor that increases over time as the new supply of bitcoin created by the mining process halves every four years. An increasing scarcity factor was thought to drive prices higher. Plan B fit a predicted value estimate through statistical regression, which is presented below.

Stock-to-Flow Model (Log Scale)



Sources: PlanB, Coinmetrics

The Stock-to-Flow model hypothesizes that a scarcity factor (SF = stock/flow) explains price levels.

The S2F model had exceptional out-of-sample success early on, which thrust the model and the author firmly into the spotlight. More specifically, when the model was released in March 2019, bitcoin was trading at less than $4,000. The model predicted that post the May 2020 halving of mining rewards, from 12.5 per block to 6.25, the price of bitcoin would be close to $70,000, reflecting a higher scarcity factor. A nearly 20x implied return was a bold prediction indeed. And it was surprisingly prescient: The price of bitcoin rose more than 15x to $65,000 by early 2021.

Academics tend to dismiss the S2F model on the grounds of the efficient market hypothesis. They argue that the future supply trajectory of bitcoin is known in advance, and thus it should already be priced in. In fact, bitcoin supply has almost no uncertainty to it (it's transparent code). Fluctuations in demand, which are variable, should thus matter more than widely understood incremental supply. In short, academics dismiss the S2F model as a classic case of mistaking causation for correlation.

Model #3: Marginal Cost.

The final model to note was proposed by Adam Hayes, who borrows from neoclassical economics and suggests that the price of bitcoin might be related to its marginal cost of production, or at least provide a floor. The marginal cost of bitcoin comes in the form of energy and computing equipment that miners use, since that is the process by which new bitcoins enter the system. Haye's thesis is this: The higher the cost of mining bitcoin, the higher its price should be.

The challenge with this model is that unlike traditional commodities, incremental supply of bitcoin does not respond to expanded mining capacity. Bitcoin's protocol automatically adjusts the difficulty of the cryptographic mining puzzle such that regardless of network-wide hash-rate (i.e., mining capacity), a new block is created on average every 10 minutes. The math adjusts and the puzzle gets harder to solve. Since no amount of computing power can change the rate of incremental bitcoin supply, marginal cost arguably converges to price, not the other way around.

Embodied Costs of Production

$$\text{Cost of Production} = \frac{\text{Electricity Cost of Hash Rate}}{\text{Bitcoins Mined Per Day}}$$

Sources: Bitcoin price and its marginal cost of production: support for a fundamental value by Adam S. Hayes, CFA, and Metcalfe's Law as a Model for Bitcoin's Value by Timothy F. Peterson, CFA, CAIA. Model recreated using estimates from Cambridge University Centre for Alternative Finance and data from CoinMetrics.io. Data as of 31 May 2021. Past performance does not guarantee future results.

Charting produced by Invesco.

Haye's thesis says that the higher the cost of mining bitcoin, the higher its price should be.

Investors have long struggled to describe or predict the price of unproductive assets whose cash flows cannot be simply discounted. Warren Buffett, arguably the most-famous investor in history, is well known for being uninterested in gold precisely because it yields nothing, and suggests that the asset is not useful outside of "going long fear." In his 2011 letter to Berkshire Hathaway shareholders, he wrote: "What motivates most gold purchasers is their belief that the ranks of the fearful will grow."

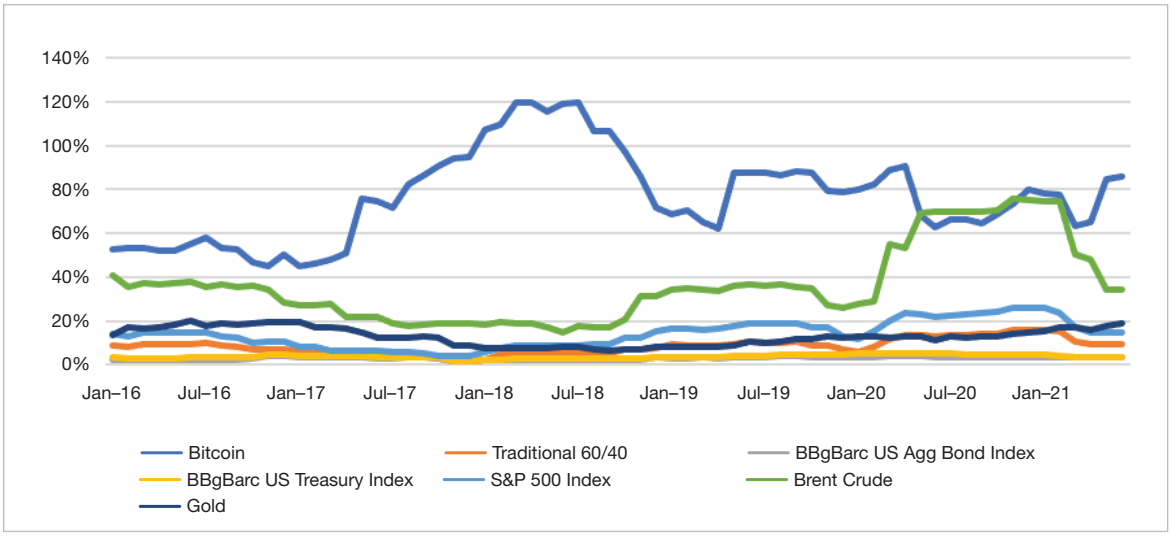
The reality is that there is no theoretical model that reliably captures bitcoin's price. No reliable model indicating whether its price is low, fair, or expensive. Bitcoin has value because humans ascribe it value. Like gold. And just like gold, there is no endgame with bitcoin's price discovery; it will continue to be a volatile reflection of speculation, fear of inflation, fear of missing out, risk of regulatory intervention, risk of technological obsolescence, and ultimately, buyer's sentiment.

Bitcoin in a portfolio

Institutional and private investors are increasingly incorporating bitcoin and other crypto assets into their investible opportunity set. The asset class is relatively new and volatile, but high risk-adjusted returns have commanded attention. In this segment we'll review the characteristics of bitcoin in an investment portfolio.

We'll start by stating the obvious: Bitcoin is an exceptionally volatile asset. The standard deviation of returns for bitcoin averaged 75% over the past five years. That is more than twice the volatility of crude oil, 5x the volatility of gold and US equities (S&P 500 Index), and more than 20x the volatility of US investment-grade bonds (Barclay's Aggregate Bond Index).

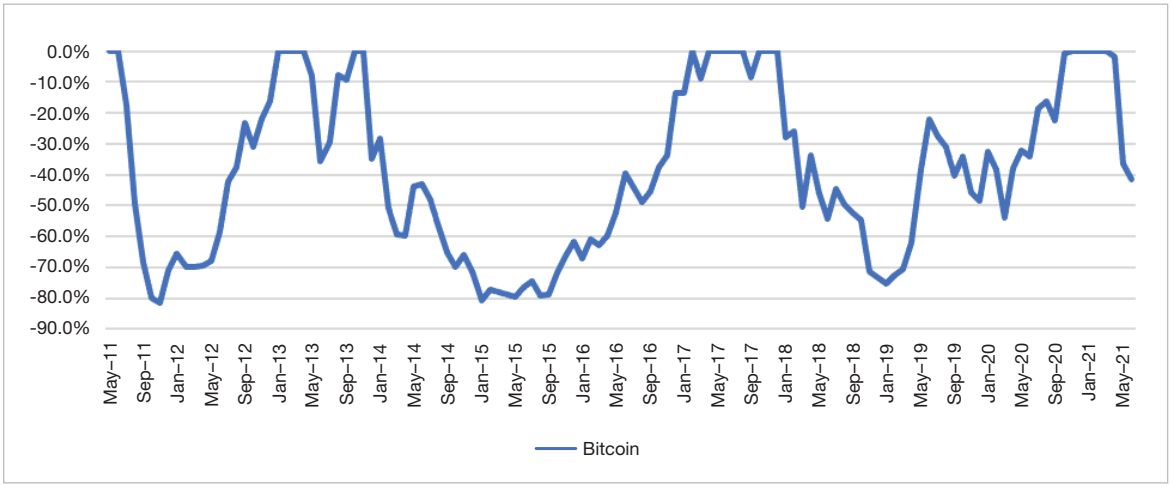
Annualized Return Volatility (Trailing 12m)



Sources: Coinmetrics, Morningstar

Drawdowns in bitcoin prices are shown in the figure below. Over the past 10 years, bitcoin has lost nearly 80% of its value on three separate occasions. Enthusiasts have even coined an acronym for it: HODL — hold on for dear life. In each of those drawdowns prices rebounded to record new highs over the coming years.

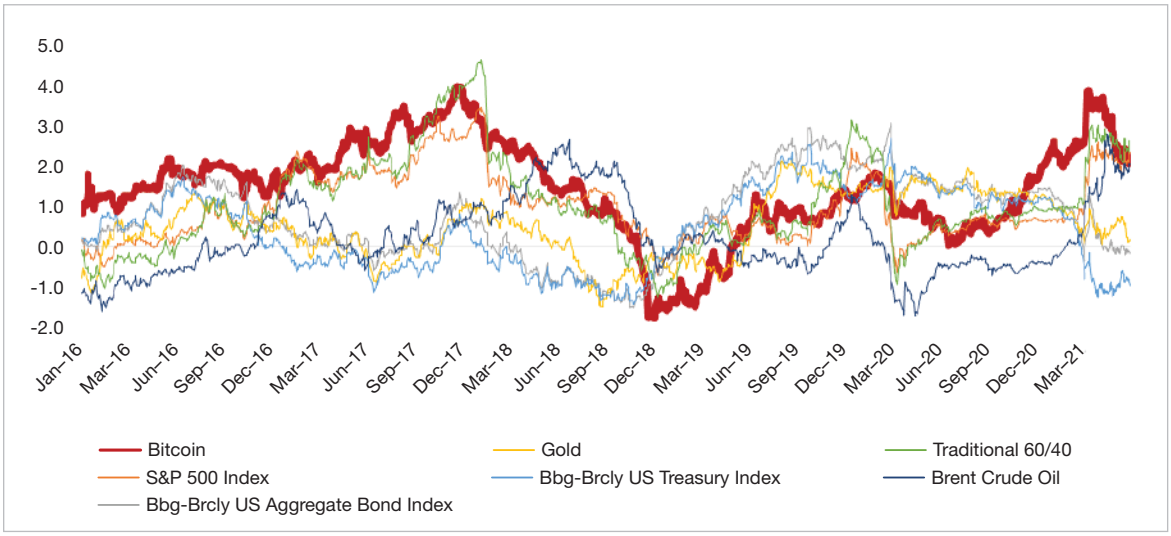
Bitcoin Price Drawdowns



Source: Coinmetrics

Despite this history of volatility and aggressive drawdowns, bitcoin's returns have more than compensated, resulting in a stream of historically high risk-adjusted returns. The trailing one-year Sharpe ratios are shown below. As a reminder, the Sharpe ratio compares an asset's excess returns (over the risk-free rate) to its volatility (standard deviation of returns). Higher is better.

Sharpe Ratio (Trailing 12m)



Sources: Coinmetrics, Morningstar

Bitcoin return correlations with traditional assets for the past decade are shown in the matrix below.

	Bitcoin USD	60% FTSE All World + 40% US Bonds (IG)	BBgBarc US Agg Bond	BBgBarc US Corporate High Yield	BBgBarc US Treasury	S&P 500	Russell 2000	FTSE Dvlp Mrkts (ex US)	FTSE Emerging Markets	FTSE Nareit All Equity REITs	Bloomberg Commodity	S&P GSCI Brent Crude	S&P GSCI Gold	S&P GSCI Industrial Metals	S&P GSCI Softs
Bitcoin USD	1.00														
60% FTSE All World + 40% US Bonds (IG)	0.11	1.00													
BBgBarc US Agg Bond	0.00	0.11	1.00												
BBgBarc US Corporate High Yield	0.12	0.85	0.20	1.00											
BBgBarc US Treasury	(0.04)	(0.27)	0.88	(0.23)	1.00										
S&P 500	0.14	0.95	(0.07)	0.77	(0.41)	1.00									
Russell 2000	0.12	0.84	(0.15)	0.75	(0.47)	0.89	1.00								
FTSE Dvlp Mrkts (ex US)	0.11	0.96	(0.03)	0.80	(0.39)	0.88	0.80	1.00							
FTSE Emerging Markets	0.04	0.87	0.09	0.78	(0.27)	0.74	0.68	0.85	1.00						
FTSE Nareit All Equity REITs	0.00	0.73	0.35	0.69	0.03	0.69	0.65	0.63	0.59	1.00					
Bloomberg Commodity	0.03	0.58	(0.09)	0.61	(0.33)	0.52	0.52	0.60	0.63	0.37	1.00				
S&P GSCI Brent Crude	0.06	0.55	(0.15)	0.66	(0.42)	0.53	0.56	0.59	0.48	0.28	0.73	1.00			
S&P GSCI Gold	(0.11)	0.19	0.41	0.19	0.34	0.06	0.01	0.15	0.29	0.14	0.40	0.08	1.00		
S&P GSCI Industrial Metals	(0.02)	0.53	(0.07)	0.47	(0.27)	0.46	0.48	0.55	0.65	0.32	0.71	0.48	0.35	1.00	
S&P GSCI Softs	0.03	0.43	0.04	0.42	(0.17)	0.35	0.35	0.44	0.50	0.37	0.65	0.44	0.24	0.45	1.00

Sources: Coinmetrics, Morningstar

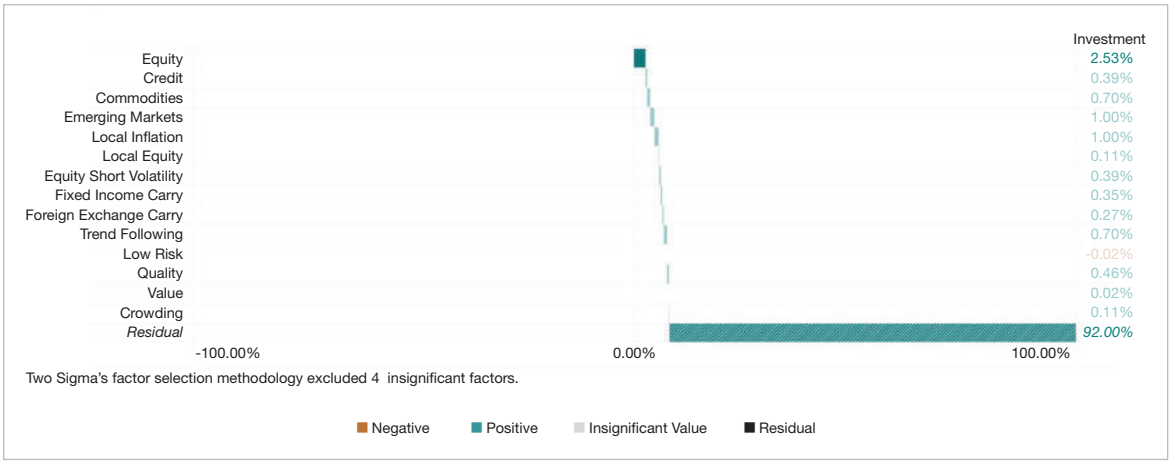
The slightly negative correlation with gold is worth noting. If the narrative is that bitcoin is "digital gold," shouldn't the correlation be higher? Or positive? One potential explanation is that as an investment substitute for gold, bitcoin may be drawing incremental demand and capital away from bullion.

Overall, bitcoin has negligible return correlations with traditional assets.

Analyzing bitcoin's price volatility using the Venn risk model designed by Two Sigma confirms the idiosyncratic nature of bitcoin's volatility. Less than 10% of volatility can be explained by common factors. The remaining 90%+ is residual and unexplained, which is consistent with the low correlations shown in the matrix on the preceding page.

Factor Contributions to Risk

What percent of total risk is driven by each factor?



Sources: Two Sigma Venn, Coinmetrics

Assets with high risk-adjusted returns and low correlations with stocks and bonds are the holy grail in modern portfolio theory. Including these assets in a diversified portfolio pushes out the efficient frontier and increases the benefits from diversification. The challenge, of course, is determining whether the high and uncorrelated historical returns of bitcoin persist.

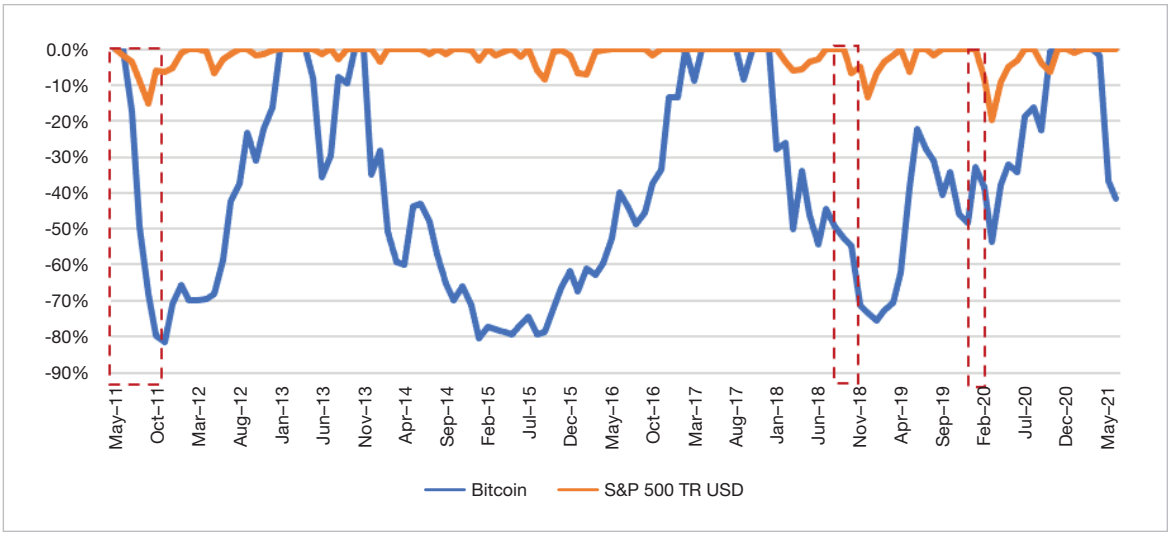
The "easier" forecast to make is that one should expect correlations with traditional assets to rise over time as institutional adoption of bitcoin and crypto assets increase.

Allocation sizing

Digital assets are new to most portfolios. Investors should consider the risks involved, which we discuss in the next section, but recognize that these assets represent the next layer of a digital transformation that's been taking place over the past 30 years. It's been a costly theme for investors to ignore.

An investment in bitcoin (or any digital asset) should be sized appropriately in a portfolio. Bitcoin's low correlations with traditional assets help, but ultimately the only real mitigant to 75% volatility is to size the allocation accordingly. And for the avoidance of doubt, while bitcoin is statistically uncorrelated to most assets, it is not a portfolio hedge. During meaningful drawdowns in risk assets, bitcoin declines too.

Bitcoin During S&P500 Drawdowns (10%+)



Sources: Coinmetrics, Morningstar

For investors who manage risk using benchmark tracking error, we examined the impact of adding bitcoin to a portfolio of traditional assets. We start with a traditional "60/40" portfolio benchmark composed of 60% MSCI ACWI Index and 40% Bloomberg Barclays US Aggregate Bond Index.

	Stocks	Bonds	Bitcoin	Tracking Error
Traditional 60/40 portfolio	60.0%	40.0%	0.0%	–
Traditional plus 1% BTC	59.4%	39.6%	1.0%	1.1%
Traditional plus 2% BTC	58.8%	39.2%	2.0%	2.2%
Traditional plus 3% BTC	58.2%	38.8%	3.0%	3.3%

The five-year backtest suggests that bitcoin adds tracking error in roughly equal parts to its allocation. In other words, a 2.0% allocation to bitcoin added 2.2% tracking error to the neutral 60/40 portfolio. This relationship may be somewhat overstated due to skewed historical upside volatility, but it helps frame the sizing question using relative risk.

A second approach to portfolio sizing is cap weighting. Consider that global listed equities were valued in aggregate at roughly $75 trillion in June 2021. Digital assets like bitcoin and ether were valued at roughly $1 trillion during the same period. If an investor were to use relative market prices as a crutch to determine neutral weight, then they might consider $1 of digital assets for every $75 of equities in their portfolio. A neutral weight to digital assets for a 60/40 investor would then be 0.8%.

Sizing an allocation to bitcoin with a focus on risk management allows investors to gain exposure to digital assets without overly relying on future price forecasts. In our view, most investors would be well served to limit their overall exposure, and any allocation of 5% or more should be reserved for those with outsized risk tolerance and deeply rooted conviction in the future of digital assets. The table on the next page describes the various approaches to gaining exposure to the asset class.

Asset Approach	Notes
Crypto Exchange	For traditional retail investors. Web and mobile apps can be used to buy and sell various crypto assets. Convenient, but security varies depending on the custody protocol which varies by exchange platform.
Private Fund	For accredited investors or qualified investors. Most popular with HNWI. Typically passive exposure to underlying digital assets. Can be active.
Public Fund (ETFs)	In certain jurisdications, like Canada, bitcoin and ether ETFs are available. The SEC in the United States is currently evaluating applications for crypto asset ETFs traded on American exchanges.
Direct Custody	Large institutional investors may choose to bypass collective investment vehicles by establishing a direct custody relationship with specialist crypto custodians.
CME Futures	Bitcoin futures trade on the Chicago Mercantile Exchange. The synthetic exposure bypasses potential issues with digital asset custody, but adds trading and roll costs. Capital gains tend to be difficult to defer when rolling futures.
Venture Capital Funds	Typically for qualified investors. Venture capital firms will invest in newer digital assets and/or start-ups in crypto infrastructure.

Sources: Bitwise, CFA Institute

Many investors with exposure to digital assets simply hold the most prominent coins, like bitcoin and ether. Some might complement this with exposure to smaller, less-established coins and tokens, which are more volatile but have the potential for excess returns should they gain more prominence.

Beyond coins and tokens, some qualified investors gain exposure to blockchain opportunities through venture capital (VC) funds. VC funds provide seed capital or early stage equity to entrepreneurs to help scale their businesses. Some of the most prominent VC firms have had tremendous success backing crypto businesses and have established dedicated crypto investment teams and funds. The investor demand is there too: In June 2021 one well-known VC firm raised a $2.2 billion crypto-dedicated fund, which is an impressive vote of confidence given the nascency of the sector.

Part 3: Risks

Bitcoin is risky.

We've referenced bitcoin's annual price volatility north of 75%, more than 3 – 5x as volatile as other traditional risk assets like equities and commodities. If one accepts that price volatility represents risk, an argument could even be made that bitcoin and similar digital assets are the riskiest of all investments.

Some investors disagree that price volatility represents risk. For them, risk is the potential for permanent loss of capital. Bitcoin has that too.

The risk for permanent loss in bitcoin centers on custody and typically comes from errors in self-custody or crypto exchange hacks.

Recall that bitcoins are secured by private keys that control a Bitcoin address. For bitcoins that are self-custodied (i.e., held outside an exchange), the private keys are the sole responsibility of the asset owner and are often stored in digital wallets. Those wallets containing private keys can be lost or passwords forgotten. Chainalysis, a blockchain-analysis firm based in New York, estimates that up to a fifth of all bitcoins are stranded due to lost private keys. A vast majority of these coins have not been transferred since the days when bitcoin was sub-$10, which partially explains the carelessness.[6]

Most small holders of bitcoin store their private keys in a digital wallet hosted by a crypto exchange. Each exchange differs in protocol, but typically a user has recourse should they lose access to their wallet or forget their password by contacting the exchange. This access redundancy has obvious value, but it also introduces another point of failure since exchanges can be run by malicious actors or hacked by them. Users have lost access to their bitcoin through exchange hacks in the past.

Exchange	Date	Bitcoin Lost	Value, at Time of Theft	Value ($35,000/BTC)
Mt. Gox	February 2014	840,000	$460.0 MM	$28.6 B
Bitfinex	August 2016	120,000	$68.0 MM	$4.0 B
AfriCrypt	June 2021	69,000	$3.6 B (reported)	$2.8 B
Thodex	April 2021	unknown	$2.0 B (reported)	$2.0 B
Bitfloor	September 2012	24,000	$250.0 MM	$816.0 MM

Source: Various

In the institutional and fiduciary space, specialist digital custodians have entered the market. They store bitcoin for large investors in “air-gapped” or “cold-storage” hardware wallets, which are physically disconnected from the internet or any wireless device in buildings with high degrees of access control. Keeping bitcoin keys stored in this fashion reduces the threat from hackers.

51% attack

A 51% attack refers to the risk in proof-of-work blockchains (such as Bitcoin) that a miner or group of miners gains enough hash power to take control of 51% or more of a blockchain mining network, thereby allowing it a mechanism to double-spend coins. The risk is acute for smaller blockchains with few miners supporting the network. An attack has not happened in Bitcoin since network inception, likely because the network’s collective hashing power has been far too large to attack. Hardware costs (est. $5-10 billion), chip shortages, and enough electricity to power a small country stands in front of would-be attackers. That said, state-sponsored commandeering of existing mining capacity cannot be ruled out.

An attack has not happened in Bitcoin since network inception, likely because the network’s collective hashing power has been far too large to attack.

[6] Consider the case of James Howells, who stored private keys to 7,500 bitcoins on a hard drive that was accidently thrown out in 2013. He offered 25% of the $300m bounty to the city council in Newport, Wales, for permission to search the since shuttered landfill site. The city declined.

Regulatory risk

Destabilizing regulation is the biggest risk faced by Bitcoin and the broader digital asset ecosystem. It would be a mistake to conclude that since blockchains are permissionless, decentralized, and global, they operate with regulatory immunity. Regulation is very much possible; the largest on-ramps and off-ramps to crypto assets are centralized exchanges, and they require banking relationships, which in turn are heavily regulated in each country.

The focus of regulators so far has centered on:

- **Taxes/AML/Terrorism Funding:** Law enforcement agencies globally have increased their attention on crypto assets, including Bitcoin, to stem its use to evade taxes, launder proceeds from criminal activities, or fund terrorists. Blockchain technology represents an interesting combination of attributes for those who "follow the money." Bitcoin is pseudonymous in that all transactions ever made on the blockchain are available for anyone to review or scrutinize. The challenge for law enforcement is understanding the beneficial ownership of sending/receiving addresses. KYC (know-your-customer) procedures at crypto exchanges helps connect the dots.
- **Securities Laws:** Bitcoin is interpreted as property in the United States, but other tokenized assets can look and act very similar to traditional securities. Tokens can be created to represent fractional ownership like stocks and REITs, to represent loans, or even contract-for-differences derivatives (CFDs). The Securities and Exchange Commission has used public advisory statements, testimony, and enforcement actions to remind participants that regardless of the platform, securities law applies.

Investors should expect the regulatory environment surrounding crypto assets to broaden. Regulation tends to lag technology. Recall that the first law related to the internet in the US was enacted in 1996, well past its early adoption. In the Telecommunications Act of 1996, lawmakers emphasized the role of private investment and markets as the best route to promoting innovation. If the same philosophy is embraced with digital assets and blockchain technology, one should expect the balance of regulation to support innovation.

On the other hand, if advances in decentralized blockchain technology create a risk of financial market destabilization, then one should expect a stronger response from regulators. It is unlikely that governments will tolerate decentralized digital assets to meaningfully compete with fiat currencies. If digital assets such as stable coins begin taking market share from fiat currencies for everyday transactions, then regulatory risk would likely increase. Ultimately, regulatory risk is path dependent.

Investors should expect the regulatory environment surrounding crypto assets to broaden.

Environmental impact

Blockchains like Bitcoin that run on proof-of-work protocol consume significant amounts of electricity. The electricity is used by miners in their race to solve the cryptographic puzzle, which is rewarded with fresh issuance of bitcoin. Network electricity demand is useful in making it costly for a malicious actor to mount a 51% attack, but in a world focused on reducing carbon emissions it represents a real problem. Bitcoin enthusiasts argue that the economics incentivize miners to go where there is stranded electricity, which is usually renewable (e.g., hydro), but the environmental impact of proof-of-work blockchains is undeniable.

The Cambridge Centre for Alternative Finance (CCAF) estimates that Bitcoin consumes approximately 0.5% of global electricity, or nearly the equivalent of the energy consumed in the Philippines or the Netherlands.

Unknown unknowns

Bitcoin and blockchain are new technologies with new terminology and a steep learning curve. Investors considering adding an allocation to bitcoin or any other digital asset should remember that public equities have been around since the Dutch East India Company was founded more than 400 years ago. Bonds are even older. The asset price behavior and range of possibilities in traditional assets are understood far better than nascent digital assets, which have been around for less than 15 years.

While the future possibilities for digital assets are virtually endless, a fully informed investor should realize that there is equally impressive downside risk. We advise investors to tread carefully, understand the possible risks, and for active strategies, partner only with the highest-quality managers.

Appendix:
Beyond Bitcoin: Ethereum, and the second layer of digital assets

Blockchain is a decentralizing technology that can be used for any application which relies on time-stamped, verifiably trusted data. Bitcoin focuses exclusively on transfer of value, but that is just one of the many use cases that blockchain can support. Vitalik Buterin and Gavin Wood recognized this early, and in 2013 they began working on Ethereum, which was envisioned to be a blockchain platform that could be used for applications beyond money.

Ethereum is a more-complex protocol than Bitcoin. It too includes a native token (ether) like bitcoin, but it also includes a decentralized Ethereum Virtual Machine (EVM), which is in essence a shared computer that can execute code. The combination of the two components allows developers to create malleable "smart contracts."

Smart contracts are code that can execute conditional actions using the blockchain to maintain integrity and transparency. For example, a smart contract might be programmed to execute simple travel insurance:

- If Alice's flight is delayed by more than 30 minutes, escrowed ether (Ethereum's native coin) is automatically disbursed to her as insurance proceeds.
- If Alice's flight departs on time, her escrowed insurance premium is automatically transferred to the insurer.

Ethereum is a platform that can bring Alice and an insurer together in a decentralized way, where trust is placed in the blockchain and smart contract instead of traditional counterparties and brokers. The code, along with an oracle (external data source), determines to which party the locked money will be released.

The technology has benefits for both sides of the transaction. Alice may be happier that a wider array of insurance is available at potentially lower premiums as more of the process is automated. And our hypothetical insurer, who may be a start-up or even an individual investor looking for uncorrelated returns, is happy that it can participate in the market now that blockchain lowered the barriers to entry. Ethereum provides the trust, decision-making protocol, and payment network to settle smart contract transactions.

With the flexibility of smart contracts, a developer can use blockchain technology in a myriad of use cases. Ethereum is the mortar, and the developers bring the bricks.

Our hypothetical insurance example above is an example of **Decentralized Finance (DeFi)**. As of H1-21 there are more than 100 functional DeFi tokens disrupting traditional finance in asset-backed loans, decentralized exchanges, and derivatives, with over $50 billion of value locked (i.e., smart contracts engaged).

DeFi Token	Category	Total Value Locked (B)
Aave	Loans	$10.8
Curve Finance	Decentralized Exchange	$7.9
Maker	Loans	$6.9
Compound	Loans	$6.8
InstaDApp	Asset Management	$5.9
Uniswap	Decentralized Exchange	$5.7

DeFi Token	Category	Total Value Locked (B)
yearn.finance	Asset Management	$3.8
Liquity	Loans	$2.9
SushiSwap	Decentralized Exchange	$2.7
Flexa	Payments Network	$1.4

Source: DeFi Pulse, https://defipulse.com/

The DeFi Tokens listed above operate entirely on the blockchain. Interestingly, almost all these applications used the blockchain to undertake an "initial coin offering" to finance their start-up. **Initial coin offerings (ICOs)** can be used to "tokenize" corporate equity, and trade on a blockchain just as bitcoin does, mimicking the public listing of a stock. More than 1,500 token offerings have taken place in the past five years, raising north of $20 billion. The table below details some of the similarities and differences between an ICO and an IPO.

	ICO	IPO
Owner-related motivations	Diversification of the ownership, facilitation of acquisitions, and increasing valuation	
Company-related motivations	General investment needs (currency for acquisitions, stock liquidity), monitoring and certification requirements by analysts, marketing, image, and public relations	
		Monitoring and certification requirements by the Securities and Exchange Commission markets (SEC)
Degree of regulation	Low	High
Disclosure of information for the campaign	Entirely voluntary	Large amount of disclosure required for listed, public companies
Information asymmetry between emitters and investors	Rather high	Rather low
External auditor	Unregulated, audit by self-proclaimed experts	Strongly regulated, audit by certified auditors
Transaction cost	Rather low, strongly self-determined by the emitter	Very high, strongly determined by regulations and mandatory processes
Issue price	Self-determined	Set by investment banks
Investors securities	Coins or tokens are classified as securities and represent a share of the emitting company	Companies must meet requirements by exchanges and the Securities and Exchange Commission (SEC)
Investment decision	Based on very high uncertainties (ICO whitepaper)	Based on lower uncertainties (IPO prospectus)
Type of emitters	Smaller and younger companies	Often rather large and mature companies
Rights of co-determination	Co-determination possible, depending on number of shares	
Role of social media	Important (emitter communicates exclusively through these channels with its investors)	Additonal (Use of social media can increase awareness before the launch of IPOs)
State of research	Initial stage	Very mature stage

Sources: Thies, F., Wallbach, S., Wessel, M., et al.

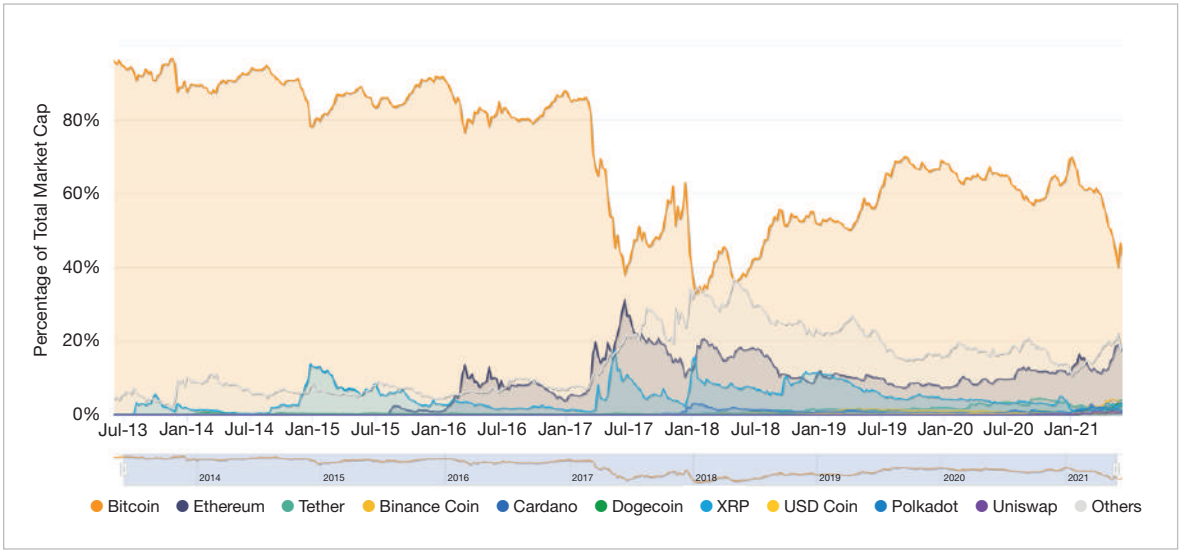
Non-Fungible Tokens (NFTs) are a relatively abstract use of blockchain. Digital art, photos, music, famous tweets, or other digital files can be made the subject of a unique non-fungible token, which represents its ownership, and can be traded in a way which was until now impossible. NFTs aim to attribute scarcity to any digital asset that can be replicated infinitely but has only one true owner. In some ways they are analogous to certificates of authenticity that typically accompany scarce collectibles. In other ways they're unprecedented.

Stable Coins are digital tokens pegged to a national currency, most often the US dollar. Tether, USD Coin, and Binance USD are the top three stable coins and trade at $1/coin. Each protocol differs, but stable coins are typically backed 1:1 with USD and high-quality, short-term paper, and provide some form of Independent Reserve verification mechanism.

It is important that holders understand how the stable coins are collateralized and/or pegged to the underlying fiat currency. The coins have been popular as a crypto dollar deposit, especially in some emerging markets with capital controls (e.g., Nigeria, Argentina, Iran, Venezuela). As of mid-2021, the largest stable coins were worth approximately $100 billion.

DeFi applications, stable coins, security tokens, and NFTs represent the growing "Layer 2" of the blockchain ecosystem. They largely operate on top of an existing blockchain like Ethereum. Even though these applications and tokens make up more than 90% of the number of digital assets today, they continue to account for less than 30% of ecosystem value as measured by market capitalization. The bulk of the value remains in Layer 1 coins, namely bitcoin and ether, which together account for 60-80% of aggregate crypto market cap.

Major Crypto Assets by Percentage of Total Market Capitalization (Bitcoin Dominance Chart)



Source: Coinmarketcap

For more information about how cryptocurrency may impact your portfolio, contact your Key Private Bank advisor.

About the Author

Justin Tantalo has 15 years of experience in investment management, both in Asset Allocation and Fund Management. As a Senior Vice President with Key Private Bank, Justin applies his expertise in Asset Allocation and helps oversee the equities and alternatives third-party manager research effort.

Justin received an MA in Economics from the University of Waterloo (Canada) and BA in Economics from the University of Western Ontario (Canada). Justin is a CFA Charterholder.