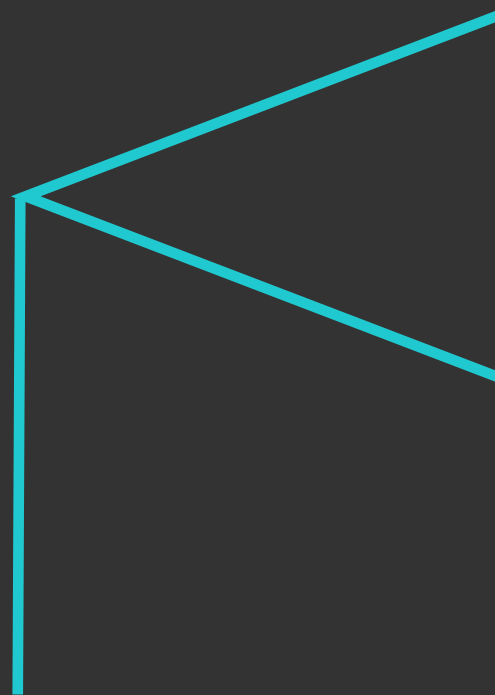
PALLĀDIEM

iDX

IDX Insights Presents:

A Fiduciary's Guide To Bitcoin and Blockchain

A resource for fiduciaries and their clients to help navigate the burgeoning asset class



A Fiduciary's Guide

To Bitcoin and Blockchain

Table of Contents:

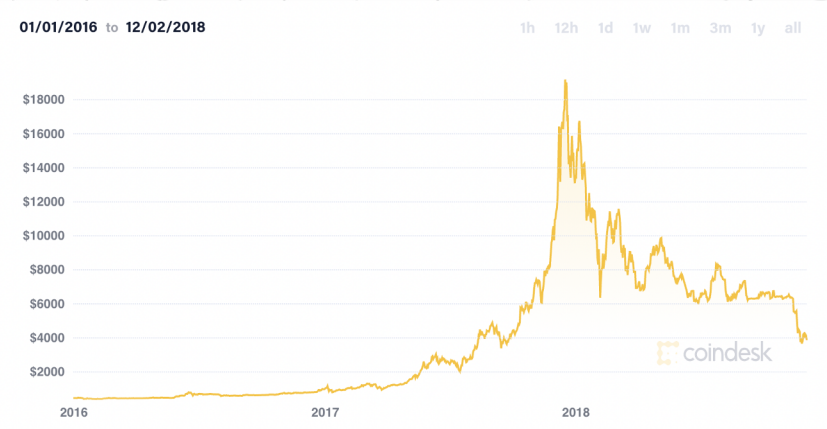
I. An Introduction to Bitcoin

Since its inception, fiduciaries have grappled with how to approach Bitcoin. The challenges are manifold. First, how to describe it: Is it a currency? A commodity? An equity or bond alternative? Some combination of these? Second: how does it work, and where are the risks? Third, and perhaps most challenging: how to discuss the asset class with clients?

Bitcoin burst into public view in 2017 seemingly from nowhere. As its price relative to the US Dollar climbed to remarkable heights, the business media complex went manic when CNBC added Bitcoin updates to its already crowded broadcast to provide real-time pricing data; even late night talk show hosts became investors, followers, and speculators of Bitcoin. 2017 also provided a public introduction to Bitcoin's and the Blockchain's fervent evangelists. Their zeal often bordered on the religious, including their enthusiasm for proselytizing Bitcoin's many virtues to any audience who'd lend an ear, willing or otherwise.

2017 was the first look at Bitcoin for many fiduciaries. Just glancing at it – the dizzying chart, the rabid media coverage, the relentlessly vocal followers – was enough to warrant skepticism. The fact that the traditional intermediaries like banks and fund companies played zero part in the development of Bitcoin, did little to assuage these concerns. And Bitcoin's apparent popularity with those conducting illegal activity also tipped the scales towards mainstream avoidance.

When Bitcoin's price collapsed in early 2018, the decision to avoid the cryptocurrencies seemed provident. But while the focus temporarily shifted away from Bitcoin, the investing landscape remained little changed. Central banks continue to pump liquidity into the system, depressing interest rates to near zero and elevating equity valuations to record highs. The United States' largest demographic, 'baby-boomers', continue retiring at a rapid clip, and many of them with scant savings beyond the equity in their primary residence. The US's deteriorating infrastructure is long overdue for an upgrade. And the political polarization has gridlocked progress. When brewed together, these forces create a potent mix for runaway inflation and rapid currency devaluation that may impair a traditional asset allocation approach for decades.



Bitcoin's Price Collapse in early 2018

Bitcoin's market dynamics changed in 2020.

The change in regulatory attitude, global adoption of digital payments options, and the prevailing financial conditions created by central banks led several institutional investors to incorporate Bitcoin into their asset management strategy. MicroStrategy CEO Michael Saylor announced that his firm had invested most of its cash reserves into 'digital assets' during a Q2 earnings call. The announcement had a ripple effect.

Soon, other institutional investors announced their Bitcoin positions including Tesla, PayPal, Square, and Metlife. Hedge funders Eric Peters and Alan Howard joined forces to purchase near $1 billion of Bitcoin in December 2020; famous investors Stanley Druckenmiller and Paul Tudor Jones also announced positions, and legendary quant shop Two Sigma has begun trading cryptocurrencies.

As for justification, each offers a variation on the same theme: unchecked money printing tends to devalue a currency and create runaway inflation. Bitcoin is a way to hedge inflation, hedge currency devaluation and generate higher yields than government bonds through price appreciation. Therefore, these institutional investors will continue to use Bitcoin and other digital assets until the central bank circumstances change.

As observers of the market, we are inclined to agree with the assessment of current conditions. Central bank money printing has warped market conditions to such a degree that a traditional view of asset allocation – whether through mean-variance optimization or some other approach – should be rigorously re-examined. In our view, the prevailing central bank trends have existed long enough to create an opportunity for alternative assets to play a role in a portfolio, specifically digital assets like Bitcoin. This paper will seek to help fiduciaries have a conversation with their clients about incorporating Bitcoin into their asset allocation.

In this resource, we'll seek to cover three areas:

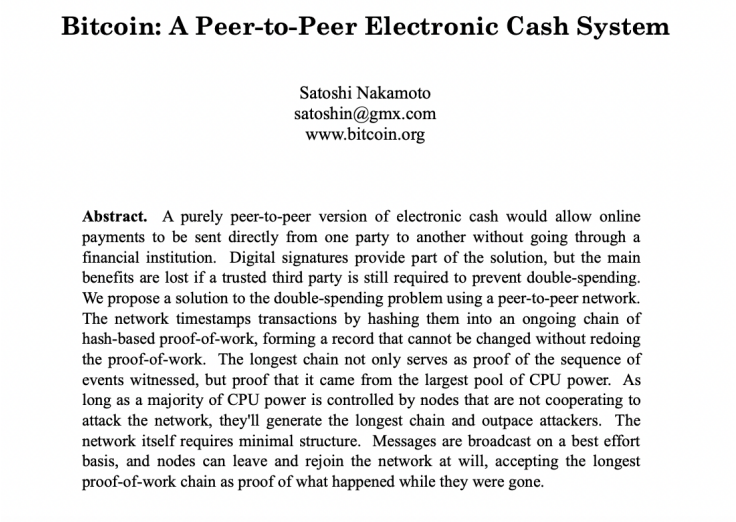
1. Why did Bitcoin come into existence?
2. What is the investment case for Bitcoin?
3. How to discuss digital assets with clients?

We hope that by the end, you'll be comfortable enough with cryptocurrencies and Bitcoin to have a prudent discussion with your clients and make an informed decision about the asset class.

II. Why Was Bitcoin Created?

Two words best summarize Bitcoin's origin story: **privacy and verification.**

The pseudonymous Satoshi Nakamoto invented Bitcoin. He published the original white paper on October 31, 2008, where he details how "a purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution." A clear shot across the bow to traditional financial institutions.



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Satoshi's 8-page white paper

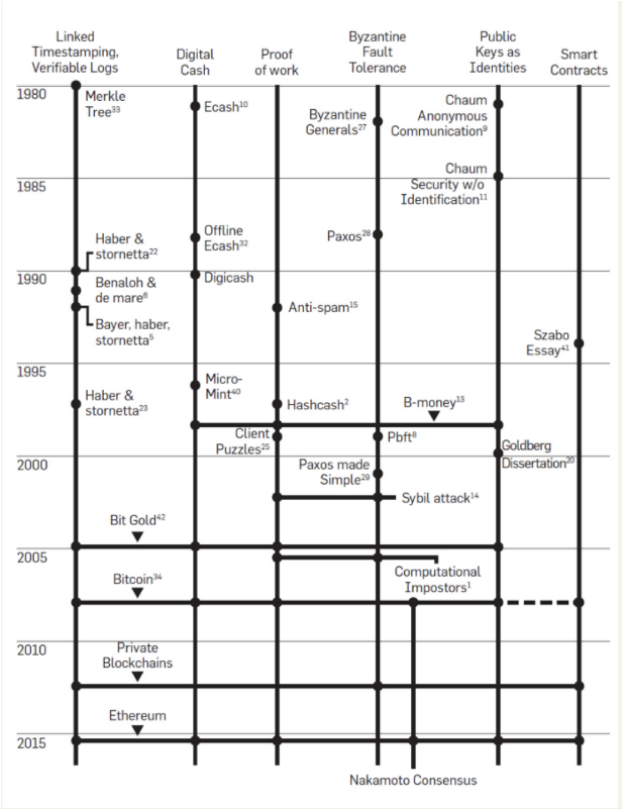
The timing seems hardly coincidental as Lehman Brothers had collapsed the month prior. Money market funds 'broke the buck.' Financial institutions around the world shuttered, unable to cover mushrooming losses. The entire financial ecosystem buckled under the weight of what would become known as the Global Financial Crisis. In other words, it seemed like a good idea to have the ability to circumvent traditional financial institutions, considering they were doing a lackluster job of managing their assets from time to time.

The concept of digital cash is not new. Beginning with David Chaum's eCash in the 1980s, digital cash and trustless transactions have been a significant part of the body of research in the field of cryptography. However, no one could solve for the verification required to cut out the banks' out of their third-party role. Further, no banks wanted to sign up as the intermediary for cashless transactions, so the idea remained purely academic.

Satoshi's achievement created a specific, complex way to assemble all of the component pieces and thus established Bitcoin.By standing on the shoulders of giants, he made the last innovative leap to form something truly unique. Bitcoin's intellectual history can help us understand the motivations behind the movement and paint a vision for its future.

Let's take a look at Bitcoin's six distinct innovations:

1. Linked timestamping
2. Digital cash
3. Proof of work
4. Byzantine fault tolerance
5. Public keys as identities
6. Smart contracts



Source:https://cacm.acm.org/magazines/2017/12/223058-bitcoins-academic-pedigree/fulltext

Cryptography is the study and practice of techniques that provide for secure communication. Cryptography focuses on constructing and analyzing protocols that prevent third parties, or the public from reading private messages. Modern cryptology originated among the Arabs, the first people to systematically document cryptanalytic methods. Al-Khalil (717–786) wrote *the Book of Cryptographic Messages*, which contains the first use of permutations and combinations to list all possible Arabic words with and without vowels.

Perhaps the most well-known example from modern history is Nazi Germany's Enigma machine, used during World War II to protect commercial, diplomatic, and military communication. The Allies eventually cracked the Engima machine's code, but not without years of work. Before the 1970's, cryptography was principally the practice of the military and intelligence agencies.

That changed when the US government published the Data Encryption Standard on January 15, 1977. IBM originally designed this early algorithm to encrypt unclassified but still sensitive electronic government data. Cryptographer Bruce Schneier characterized the publication of DES to have "jump-started" the nonmilitary study and development of encryption algorithms.

It wasn't long after the DES was published that the first piece of the Bitcoin puzzle emerged. Ralph Merkle patented the Merkle tree in 1982. A Merkle tree is a data structure that encodes blockchain data more efficiently and securely. That same year, cryptographer Dr. David Chaum published his paper "Blind Signatures for Untracable Payments". This seminal work served as the basis for digital cash, which proposed that someone could obtain digital currency from a bank and spend it in a manner untraceable by either the bank or any other third party.

These academic advancements served as the basis for the "Cypherpunks," a small group of cryptography enthusiasts that began corresponding in the early 1990's. This lead to the publication of "A Cypherpunk's Manifesto", wherein they made an important distinction between privacy and secrecy that's at the heart of Bitcoin:

"Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world."

It's best to think of privacy like curtains or shades for your home. Just because you have curtains doesn't automatically mean you're doing anything immoral or illegal. Instead, you simply have the right to control your privacy.

Cryptography, Over the Years

In 1993, cryptographic encryption was considered a military technology. Consequently, regulations prevented "exporting" key lengths longer than 40 bits which could be cracked in a few days with a personal computer. Following an expose of the NSA's so-called Clipper chip in the New York Times the government backed off.

In 1997, email spam and denial of service attacks were getting out of control. As a solution, British cryptographer Dr. Adam Back proposed a proof-of-work system to limit email spam. The purpose was to create a cost (in terms of time) to send an email by forcing servers to complete a small amount of work. Dr. Back hypothesized that spammers, whose business model relies on sending a large volume of emails at low cost, would have their revenue interrupted by the proof-of-work demand. He called it HashCash.

The Cypherpunks discussed how HashCash could improve Chaum's digicash because it didn't require you to create an account, thereby preserving some anonymity.

In 1998, computer engineer Wei Dai published his proposal to enforce contractual agreements between anonymous actors, called "b-money." His proposal includes a protocol in which every participant maintains a separate database accounting for how much money belongs to the user. Satoshi uses this ledger system in the Bitcoin proposal.

Bitcoin's proof-of-work can be derived from 2004 when developer Hal Finney created a reusable proof of work (RPOW) from protocols in Back's HashCash. Finney described his system this way:

"RPOWs can then be transferred from person to person and exchanged for new RPOWs at each step.Each RPOW or POW token can only be used once but since it gives birth to a new one, it is as though the same token can be handed from person to person. Because RPOWs are only created from equal-value POWs or RPOWs, they are as rare and "valuable" as the hashcash that was used to create them. But they are reusable, unlike hashcash."

Finney's proof-of-work concept figures prominently in Bitcoin's protocols. Hal Finney was the first recipient of a bitcoin from Satoshi Nakamoto once he got bitcoin operational. Finney's RPOW system still relied on validation from a central server, however.

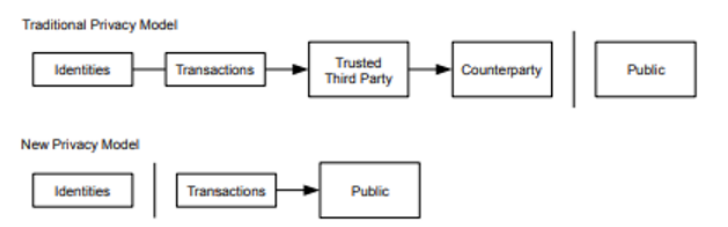
Bitcoin mining, the process of completing the hash to obtain the bitcoin reward, has its roots in "bit gold," a concept created by cryptographer and contract lawyer Nick Szabo in 2005. Szabo attempted to combine Wei's b-money with Finney's RPOW and Back's HashCash to "mimic as closely as possible in cyberspace the security and trust characteristics of gold."

Satoshi integrated three decades of cryptographic work into Bitcoin. By standing on the shoulders of these giants, specifically Back's hashcash and Wei's b-money, he was able to create a working system that solved the greatest puzzle in cryptography: verification. A required trusted intermediary dogged cryptographers for decades until Satoshi's innovation in 2008.

Satoshi uses section 10 of his paper to comment directly on the nature of privacy:

> ***"The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were."***

He then illustrates the new privacy model made possible by Bitcoin:



Satoshi demonstrates a nuanced understanding of cryptographic principles as well as the primal motivations of human beings. As Mirabeau, one of the French Revolution leaders, so aptly stated, "The two greatest inventions of the human mind are Writing and Money — the common language of intelligence and the common language of self-interest.

III. Bitcoin's Investment Case

Based on price appreciation alone, Bitcoin has been one of the most profitable investments one could have made in the last decade. **So why is it only now attracting institutional investment?**

A look at Bitcoin vs. Major Asset Classes over the past decade

@CharlieBilello		Asset Class Returns over Last 10 Years (as of 12/11/20)										Data Source: YCharts	
ETF	Asset Class	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020 YTD	2011-20 Cumulative	2011-20 Annualized
N/A	Bitcoin ($BTC)	1473%	186%	5507%	-58%	35%	125%	1331%	-73%	95%	162%	6271233%	203.5%
QQQ	US Nasdaq 100	3.4%	18.1%	36.6%	19.2%	9.5%	7.1%	32.7%	-0.1%	39.0%	42.7%	512.5%	20.0%
SPY	US Large Caps	1.9%	16.0%	32.2%	13.5%	1.2%	12.0%	21.7%	-4.5%	31.2%	15.5%	254.0%	13.5%
IWM	US Small Caps	-4.4%	16.7%	38.7%	5.0%	-4.5%	21.6%	14.6%	-11.1%	25.4%	16.1%	179.9%	10.9%
VNQ	US REITs	8.6%	17.6%	2.3%	30.4%	2.4%	8.6%	4.9%	-6.0%	28.9%	-6.8%	124.6%	8.5%
TLT	Long Duration Treasuries	34.0%	2.6%	-13.4%	27.3%	-1.8%	1.2%	9.2%	-1.6%	14.1%	18.8%	119.4%	8.2%
LQD	Investment Grade Bonds	9.7%	10.6%	-2.0%	8.2%	-1.3%	6.2%	7.1%	-3.8%	17.4%	10.1%	79.6%	6.1%
PFF	Preferred Stocks	-2.0%	17.8%	-1.0%	14.1%	4.3%	1.3%	8.1%	-4.7%	15.9%	6.0%	74.3%	5.7%
EMB	EM Bonds (USD)	7.7%	16.9%	-7.8%	6.1%	1.0%	9.3%	10.3%	-5.5%	15.5%	4.2%	70.4%	5.5%
HYG	High Yield Bonds	6.8%	11.7%	5.8%	1.9%	-5.0%	13.4%	6.1%	-2.0%	14.1%	3.3%	69.5%	5.4%
EFA	EAFE Stocks	-12.2%	18.8%	21.4%	-6.2%	-1.0%	1.4%	25.1%	-13.8%	22.0%	5.4%	65.2%	5.2%
BND	US Total Bond Market	7.7%	3.9%	-2.1%	5.8%	0.6%	2.5%	3.6%	-0.1%	8.8%	7.4%	44.4%	3.8%
TIP	TIPS	13.3%	6.4%	-8.5%	3.6%	-1.8%	4.7%	2.9%	-1.4%	8.3%	10.1%	42.3%	3.6%
EEM	EM Stocks	-18.8%	19.1%	-3.7%	-3.9%	-16.2%	10.9%	37.3%	-15.3%	18.2%	13.7%	30.0%	2.7%
GLD	Gold	9.6%	6.6%	-28.3%	-2.2%	-10.7%	8.0%	12.8%	-1.9%	17.9%	20.7%	24.3%	2.2%
BIL	US Cash	0.0%	0.0%	-0.1%	-0.1%	-0.1%	0.1%	0.7%	1.7%	2.2%	0.4%	4.8%	0.5%
DBC	Commodities	-2.6%	3.5%	-7.6%	-28.1%	-27.6%	18.6%	4.9%	-11.6%	11.8%	-10.7%	-46.8%	-6.1%
Highest Return		BTC	BTC	BTC	VNQ	BTC	BTC	BTC	BIL	BTC	BTC	BTC	BTC
Lowest Return		EEM	BIL	GLD	BTC	DBC	BIL	BIL	BTC	BIL	DBC	DBC	DBC
% of Asset Classes Positive		65%	94%	41%	65%	41%	100%	100%	6%	100%	88%	94%	94%

The challenge in evaluating Bitcoin is that it is a genuine innovation; not only as a technology, but also as an asset class. Bitcoin is one part digital gold, one part commodity, and one part currency –something unique. When was the last time a new asset class appeared? As a result, tried-and-true frameworks for evaluating asset classes for investment need to be reconfigured, if not altogether thrown out.

In our view, the case for Bitcoin is straightforward: do your clients wish to preserve their purchasing power? Whether they need income today or twenty years from now, we believe the policy of unchecked monetary and fiscal stimulus pursued by global central banks will both:

a) increase the probability of inflation and

b) accelerate currency devaluation as policymakers seek to monetize the debt they've incurred, rather than raise taxes.

The mere prospect of either (or both) of those outcomes justifies a serious inquiry into the merits & potential risks that Bitcoin presents. Furthermore, decades of Quantitative Finance have provided ample evidence of how we might harness the mighty volatility of this new asset class to achieve something appealing for the modern fiduciary and their clients.

Central banks often hold gold and a reserve currency (usually the US Dollar) because in combination they offer complementary trade-offs. Gold has been a store of value for thousands of years. There's only so much gold that can be mined, making it scarce. Critically, gold is easy to recognize, it's easy to weigh, and can be verified by melting it. However, it's hard to transact – gold is heavy! Paper currencies like the US Dollar exist to simplify the daily use of gold. Once the dollar was depegged from the gold standard and allowed to free float, investors then had to trust the government to responsibly manage monetary policy. Fiat currencies can provide economic efficiency, but not without risk. In an extreme case like the Weimar Republic, or more recently, Venezuela, currencies can rapidly become worthless when trust in the government erodes and hyperinflation sets in. You can't print more gold, and you can't regain lost trust.

We find it helpful to think of gold as the decentralized asset whose value can't be devalued by the government's action. The value of the US Dollar (or any fiat currency), by contrast, ***depends*** on the government's actions (and prudence). In our view, Bitcoin combines the features and benefits of both gold and the US Dollar. Namely, that it is decentralized like gold but also easy to transport and transact like paper currencies.

Bitcoin vs. gold vs. US dollar

Traits of money	Gold	Fiat (US Dollar)	Crypto (Bitcoin)
Fungible (Interchangeable)	High	High	High
Non-Consumable	High	High	High
Portability	Moderate	High	High
Durable	High	Moderate	High
Highly Divisible	Moderate	Moderate	High
Secure (Cannot be counterfeited)	Moderate	Moderate	High
Easily Transactable	Low	High	High
Scarce (Predictable Supply)	Moderate	Low	High
Sovereign (Government issued)	Low	High	Low
Decentralized	Low	Low	High
Smart (Programmable)	Low	Low	High

We believe we're in the nascent stages of Bitcoin's adoption. We've yet to cross into the early majority of the technology adoption cycle, where (typically) 34% of an innovation's potential consumers exist. We're still among the *Innovators* (2.5%) and *Early Adopters* (13.5%). If and when Bitcoin makes the jump from the *Early Adopters* to the *Early Majority,* the capital flows alone would be a powerful force for positive price action, not unlike the migration from active to passive funds.

Bitcoin as Digital Gold

This case is perhaps the most familiar because it's the case most commonly debated and discussed. A valid monetary asset must be scarce, portable, fungible, divisible, durable, and universally accepted. In this way, Bitcoin reflects similar characteristics as physical gold, but it also improves upon many of physical gold's trade-offs. By it's design, Bitcoin is scarce, durable and divisible (up to eight decimal points), verifiable, portable (using a wallet), and transferable.

According to CoinMarketCap, Bitcoin's current market capitalization – or network value – is approximately $900 billion. ARK Investment Management estimates that if Bitcoin was able to take just 10% share of the physical gold market, its network value could increase five fold to $4.5 trillion.

Bitcoin to Hedge Currency Debasement

Central banks worldwide are printing money to provide monetary and fiscal stimulus, an unquestionably inflationary tactic. Historically, a spike in inflation tends to reduce confidence in monetary authorities, further devaluing the currency. Inflationary periods tend to be good for decentralized assets like gold, and now, Bitcoin.

This scenario could be particularly salient in emerging markets outside of the sphere of influence of the four largest fiat currencies – US Dollar, Japanese Yen, Chinese Yuan, and the Euro. If we push this scenario to the extreme of hyperinflation, fiat-based economies could buckle beneath the weight of their obligations.

ARK Investment Management estimates that if Bitcoin were to capture 5% of the global monetary base outside of the four largest fiat currencies, it's market cap could increase six-fold from $900 billion today to $5.4 trillion.

Bitcoin as Protection Against Asset Seizure

In the same vein as above, Bitcoin's decentralized and entirely digital infrastructure has already helped those seeking to protect their assets from seizure and demonetization. India's 2016 Indian banknote demonetization is perhaps the most notable example. On November 8, 2016, India's Prime Minister, Narendra Modi, announced that the 500-rupee and 1,000-rupee notes would no longer be legal tender. Citizens were given fifty days to deposit the now-invalid notes or convert them to the smaller bills. While the IMF praised the move to combat illegal activity, many others criticized the Modi Administration for being tone-deaf to the realities on the ground. By some estimates, 90% of India's financial transactions were conducted in cash. 85% of India's workers' wages were paid in cash. 50% of the nation of 1.3 billion were non-banked citizens. The move sent shock-waves throughout the country. If more Indians had access to Bitcoin, the move's impact could have been softened substantially.

ARK Investment Management suggests that if there's a 5% probability of asset confiscation by a corrupt regime in an individual's lifetime, Bitcoin's value could 10x from $900 billion to $9 trillion.

Bitcoin as a Global Settlement Network

Satoshi's vision of Bitcoin as a global settlement network could be its most compelling opportunity; It has the capacity. According to ARK Investment Management's analysis, Bitcoin's infrastructure can handle 2,000 global settling transactions every ten minutes or so, from anywhere at any time. They estimate that deposits totaling $14.7 trillion generate $1.3 quadrillion in interbank volume each year. If Bitcoin captured 10% of this volume, the cryptocurrency's market cap could increase seven-fold, up to $6.3 trillion.

We may be seeing the shift already taking place. Currently, Bitcoin facilitates mostly large volumes of low value transactions. As institutional investors begin to participate, Bitcoin could evolve to facilitate both low value and large transactions between institutions and across geographies.

IV: What About the Risks?

Each of these scenarios imagines a world in which Bitcoin's market cap will increase significantly with a modest growth rate applied to the adoption model. In many cases, even with a fractured realization of the expectations previously stated, an increased adoption rate would generate positive price appreciation in Bitcoin's; as seen in all free markets, reflexivity can be a powerful force.

Let's now discuss the risks.

Regulation

By design, Bitcoin sits outside of the traditional sandbox of financial intermediaries and their regulatory agencies. It's a challenge for a regulatory agency tasked with oversight to regulate something designed to bypass these very controls. We believe that governments will respond to cryptocurrencies in such a way that hopes to maintain the status quo of the global financial system, but the question remains as to how they intend to interject their authority into this rapidly developing ecosystem. If global governments pursue nuanced regulation and oversight, innovation will continue to foster the realization of a truly global economy. Alternatively, governments could choose to pursue onerous regulations that intentionally hinders the adoption of Bitcoin and digital assets by the majority. At the time of this writing, the US government taxes Bitcoin as a capital asset (real property), and it is therefore subject to capital gains tax. Given Bitcoin's significant price appreciation over the past decade, the tax implications for many participants and investors could alone slow the liquidation of Bitcoin holdings during bouts of volatility. Optimistically, the SEC has permitted companies to use Bitcoin and other digital assets for their treasury reserves, so there exists the possibility that adoption can continue, and encouragingly so.

Technical Risk

Bitcoin's code base and network infrastructure is strong and growing stronger. It has held up to challenges and tests over its first twelve years of life, including four distinct bubbles thus far. The continued growth in new mining activity, and the increased global decentralization of computational nodes, provide further justification for the survivability of the asset class. There still remains, however, an open question about how the infrastructure could behave in the long run, particularly as we approach the 21 million Bitcoin issuance cap. How might the behavior and participation of miners change when they are compensated as market makers and liquidity providers via transaction fees rather than the harvesters of newly minted Bitcoins?

Hindered Adoption

Bitcoin has earned its credibility among the early adopters (and, notably for fiduciaries, among Millennial's in particular), but it still remains a niche asset class consumed by technology enthusiasts and risk seekers alike. All things considered, there's a non-zero chance that Bitcoin finds a new high among early adopters and then never crosses to the early majority. Of course, that's why we remain optimistic: if Bitcoin was already widely adopted, there wouldn't be much upside left for new participants.

Competitive Risk

Bitcoin's code is open source. Anyone can contribute to the development of the network, but that also lends itself to the potential competitor networks of Bitcoin. As we saw in the first section, Bitcoin itself owes it's existence to the innovations derived from a free exchange of ideas, organized by the principles of privacy and verification. Bitcoin has a strong first-mover advantage. Measured by the market share, there is a significant gap between Bitcoin and its next competitor Ethereum. In our view, Bitcoin's greatest competitive risk isn't from other cryptocurrencies, it's from central banks. As we've detailed in a separate paper, China's economy already uses 90% digital payments. They intend to roll out their own centralized digital currency at the 2022 Olympics. Additionally, the largest global pandemic experienced in modern times, the coronavirus, has greatly exacerbated challenges with the global Fiat currency regime, and has accelerated the global adoption digital payments, by individuals and sovereignties alike. A stable, centralized digital currency could potentially hinder the broader global adoption of Bitcoin, but only time will tell if such an event yields a positive or negative circumstance for the blossoming digital currency.

Volatility

In our view, volatility is Bitcoin's principal risk, as price volatility may limit the adoption by fiduciaries and their clients. For starters, Bitcoin's out-sized volatility characteristics certainly do not help the argument for a reliable store of value; certainly not when compared to other liquid assets such as cash (USD) and US treasuries. Unless something fundamentally changes within Bitcoin's infrastructure, it's price will continue to reflect swings in investor confidence, as does any free market that is subject to the forces of supply and demand. It would also be a reasonable expectation that Bitcoin's sensitivity to changes in demand may be lessened as it achieves adoption from a wider, deeper, and more sophisticated global constituency. The adoption by a more sophisticated audience should bring about more order to the market, with greater liquidity, tighter confidence bands around price discovery, and thus a reduction in volatility; of course volatility is characterized in relative terms and the standard caveats should apply. Last on the topic, for the participants and spectators hoping for the normalization of volatility in Bitcoin relative to other traditional asset classes, think again. The artificial suppression of volatility, which traditional market participants have grown accustom to post Global Financial Crisis, is the game of central bankers and policy makers, who have the power to borrow from the future and extend the day. In a decentralized free market economy, where asylum from fear comes with a steep price tag, this liquidity mechanism (support) is left to the evangelists and the value investors, solely.

Unknown Unknowns

Bitcoin is a brand-new asset in a brand-new asset class. We're in uncharted territory, so we must acknowledge that there are potential risks that are difficult to anticipate; the Black Swan's.

IV: Discussion: Bitcoin Pros and Cons, from the Perspective of a Fiduciary

Any discussion of Bitcoin can seem a bit like chasing rabbits. It combines philosophy, monetary policy, computer science, and puzzles into one confounding box. Filmmaker Christopher Nolan couldn't have dreamed up a more multifaceted narrative. Let's divert from the parentheticals and digressions to focus on the business case.

A tale of four advisors:

Advisor A: Let's say Advisor A chooses not to allocate to Bitcoin. In the next few years, less volatile products flood the market (known as stablecoins). In the interest of consumer protection, policymakers and regulators produce legislation that favors stablecoins and punishes Bitcoin investors. In response, investors flock toward the less-volatile and regulator-blessed option, and Bitcoin's price never reaches its previous highs again. In this scenario, you're the hero. You correctly prophesied Bitcoin as another fad and avoided the risks. You even win some new clients from less-fortunate advisor adopters.

Advisor B: Again, let's say Advisor B chooses not to allocate to Bitcoin. Except for this time, Bitcoin takes off, and all the prophecies are true. It's digital gold, a global settlement network, protection against demonetization and asset seizure, and a hedge against inflation. Using ARK's analysis as a baseline, this could mean a five- to ten-fold increase in Bitcoin's market cap, and that's assuming a 5-10% market share. You now have to explain to your clients WHY you avoided THE investment of the 21st century.

Let's flip to the other side of the coin:

Advisor C: Assume Advisor C determines that the risks of a long-only exposure to Bitcoin is prudent and aligns with the suitability standards of his or her clients. Bitcoin's price subsequently "goes to the moon" for all of the aforementioned reasons in the Advisor B example. The result? Happy clients, new client referrals, and increased revenues from customer acquisition and investment performance.

Advisor D: Let's say Advisor D makes a similar election to Advisor C (gain long-only Bitcoin exposure for clients), however, he or she is not as fortunate. This scenario would look more similar to Advisor A, with the asset class going down significantly. Now advisor D is hemorrhaging clients and assets, and potentially facing law suits from litigious investors. All the while, Advisor D is wondering how they got sucked up in the euphoria of the asset class, when history has provided so many anecdotes to counter such a fate; after all, Bitcoin and digital assets did endure an 80% draw down from 2018-2020, and hindsight would say the writing was on the wall.

IV: Discussion: Bitcoin Pros and Cons, from the Perspective of a Fiduciary (cont.)

In all four of the above scenarios, Bitcoin's volatility will remains a constant. It is the principal risk any fiduciary must resolve before deciding whether to allocate to the asset class, or not. You can invest in the long-only ETPs or via a Bitcoin wallet on an exchange like Coinbase, but that doesn't solve for the volatility related constraints and issues. Hedge funds may offer a risk-managed approach to gaining exposure to digital assets, but also carry additional trade-offs, not least of which is restricted participation to 'accredited investors'. Most reputable hedge funds also carry high account minimums and high expense ratios; they're also illiquid. In other words, allocating to the wrong fund manager with the wrong strategy, can yield its own challenges if something were to go awry.

We believe a risk-managed approach is requisite for any fiduciary to confidently allocate client capital, especially when it's a newly developing asset class like Bitcoin and Digital Currencies. The IDX team has decades of experience unpacking the underlying return factors and risk premia associated with hedge funds, active management, and alpha generation. The investment insights utilized by the IDX team are deeply rooted in academic research and proven empirically out-of-sample. We believe that a robust, repeatable, and transparent approach to risk management, rewards investors and market participants over-time. Through this lens we seek to provide a disciplined, risk-mitigated approach for fiduciaries and their clients who wish to gain exposure to Bitcoin and Digital Assets.

IV: How to Answer Common Client Questions

Q1: Explain Bitcoin to Me Like I'm Five

Let's say we're sitting on a park bench. I have one apple with me. I give the apple to you. You now have one apple and I have zero. Simple, right? I physically put the apple in your hand. You know the apple is in your hand because we both watched it go from my hand to yours. We didn't need a third person to tell us that it happened.

Now, let's say I have a virtual apple I want to give you. It has all the characteristics of a physical apple, we just can't physically touch it. If I tell you I gave you the virtual apple, how would you know that the apple is now yours?

Suppose it's really important to you that you get this specific virtual apple as-is. How can you be sure that I didn't make a copy of the virtual apple before I gave it to you? Or that I sent to my uncle before I sent it to you?

If we're just trading physical apples in each other's presence, then a third-party to verify the transaction is unnecessary. But if we're trading virtual apples, that's where a third-party to verify the transaction becomes important. Problem is, the third-party will take a bite of the apple – virtual or physical – before the transaction is complete.

Now, let's say we're trading virtual apples all the time. It makes sense to keep track of who has which virtual apple at what point. That's called a ledger or an accounting book. It doesn't make sense to have a physical ledger to track virtual apples. So where should it go? The virtual ledger needs a place in the virtual world.

You could ask a third-party to keep the virtual ledger. But they will take a bite out of every apple they need to keep track of. Not very hygienic. Also, we're assuming our third party is honest. What if they simply decide to create more virtual apples?

At this point, isn't there a way for us to get back to the park bench? Imitate the mechanics of me giving you a physical apple, just virtually? That pesky third-party seems to keep showing up.

What if we took the ledger – the accounting of who sent a virtual apple and who received a virtual apple – and gave it to everybody? Instead of our pesky third-party, the record of who traded which apple will live on a bunch of computers around the world. Like a mosaic! Zoom out, and you see the whole ledger. Zoom in, and you just see a dot. To make the whole picture complete, every dot needs to be in the right spot. Any dots that are out of place or blank will ruin the picture.

In this way, you can't break the mosaic. If I wanted to send you virtual apples but didn't have any, my spot in the mosaic wouldn't line up with the rest of the bigger picture. As the picture gets bigger, it fills with more dots. More dots make the mosaic clearer because the picture cannot be completed unless every dot is exactly where it should be.

No one controls what the mosaic looks like. Instead, the mosaic reconstitutes into something else as the dots grow. Whether that's as a ledger, an apple, or a park bench.

IV: How to Answer Common Client Questions (cont.)

Q2: What is a Blockchain?

To understand Bitcoin's potential long-term value, it is crucial to understand the blockchain.

Where Bitcoin goes, the blockchain follows. For good reason: blockchain is the chassis that Bitcoin and all other cryptocurrencies operate on. You cannot have Bitcoin without blockchain. To understand this, let's approach the word by looking at its distinct pieces –*block* and *chain*.

In cryptography, block refers to a database, a term that should be familiar. If you've ever searched through a phone book you've used a database. In cryptography, a spreadsheet differs from a database. Spreadsheets are designed for a limited number of people to store and access a limited amount of information. A database is designed to house large amounts of information that can be accessed, filtered, and manipulated quickly by any number of users - simultaneously.

There was a time when the phone book was an essential part of every home, but thousands of people lacked the ability to interact simultaneously with that data.

To publish a phone book that someone can use, the person or business name must correspond to the phone number and address. In any other format, it's not useful. Once one page is full, one must start a new page of information. Think of "blocks" as one page in the phone book. You complete each page sequentially, starting with "Aaron A. Aaronson," and move on alphabetically from there. When finished, there is a chain of data, organized alphabetically. "Barry B. Barishnikov" cannot come before "Aaron A. Aaronson."

In the case of Bitcoin, the blockchain represents an irreversible timeline of transactions, listed oldest to newest. Meaning, a Bitcoin transaction that occurred yesterday will never come before one that occurs today. Just as there are numbered pages of any phone book, each transaction is given an exact timestamp - when it is added to the blockchain.

So, the blockchain is like a phone book. It stores chunks of data (blocks) in sequential order (chain). It enables verification that a transaction occurred when it did. It is a sequential, irreversible timeline.

Q3: What is Mining?

To complete each page of a phone book and make it useful, two components must match: the person's name and the phone number. In Bitcoin's case, these components are two parties trying to complete a transaction. One person is sending money, the other person receiving it. Computing power, distributed through machine learning and AI, enables millions of potential transactions. Once a machine figures out a transaction, it adds the block to the chain

So one page in a phone book is analogous to one 'block of transactions' on the blockchain.

Now comes the leap of faith. If thousands if not millions of computers are working on a digital phone book of transactions 24/7, where is the remuneration?

IV: How to Answer Common Client Questions (cont.)

This is what is referred to as 'mining' Bitcoin. Computers allot a price for computation at a rate per block.

As of this writing (February 2021), one Bitcoin is worth around $55,000. Picture the inches thick phone books of the past, and the profit motive starts to become clear. Now, add scarcity to the picture. Per Bitcoin's original rules, only 21 million Bitcoin will be issued. As of December 2020, it's estimated that we've mined 18.5 million Bitcoin. On the surface, it looks like we're practically a rounding error away from finding out what happens when we exhaust our Bitcoin supply. However, Bitcoin contains code to slow down the mining speed, something called halving. Without a clear regulatory authority or mining 'roadmap', halving events and their implications can be non-trivial to the network.

What's important to know for now is that the matching, verifying, and pricing of these transactions is exact and irreversible. They are connected by design.

Q4: Who Controls Bitcoin's Network?

Nobody controls the Bitcoin network. It's like asking who controls the internet. Anyone who uses Bitcoin contributes to Bitcoin's network. There are developers constantly proposing improvements to the software, but they are unable to force a change unless there is total consensus among all users. By one estimate, there are 300,000 to 500,000 unique users either sending or receiving Bitcoin per day. Others estimate over 1 million unique users.

Q5: Is Bitcoin Secure? Has it Ever Been Hacked?

Bitcoin has a strong security track record. Bitcoin's original rules are still operating twelve years in, which suggests a robust, and well-designed concept. It's important to draw a distinction between Bitcoin getting hacked and ***exchanges*** getting hacked. The most notable is the Mt. Gox hack. Bitcoin itself wasn't compromised. Instead, the addresses to digital wallets were stolen. Moving to segregated, "hard wallets" (that are not stored online) has emerged as a security protocol that, many believe, make ownership of Bitcoin safer than a bank. Since the Mt. Gox days, custodial options like Coinbase and Fidelity Digital Assets Group have emerged as true, regulated custodians of bitcoin.

IV: How to Answer Common Client Questions (cont.)

Q6: Is Bitcoin a Ponzi Scheme?

A Ponzi scheme pays investors from their own money, or the money paid by subsequent investors, rather than the profits earned from running the enterprise. Ponzi schemes collapse when there aren't enough new participants. Critically, they often require a central authority to operate the scheme.

Bitcoin is computational network independently distributed around the world. No one speaks for Bitcoin. Satoshi Nakamoto invented Bitcoin, but he isn't the leader, or central authority, because such a position does not exist. We don't even know his (or her) real identity.

Returns were never part of Satoshi's thinking when he designed the protocols. Bitcoin spent the first years of its existence as little more than a highly volatile speculative asset. Presciently, he wrote, "Bitcoins have no dividend or potential future dividend, therefore they are not like a stock. More like a collectible or a commodity."

Q7: Will I Buy Groceries With Bitcoin?

The subtext of this question is meant to wave away the potential for Bitcoin's wider adoption. This attitude is more common in the United States, where our digital payment adoption lags countries like China, Singapore, and South Korea. Sweden could be cashless as early as 2023. China intends to release it's Digital Currency Electronic Payment (DCEP) in 2022, a centralized version of a cryptocurrency. As long ago as 2013, the Wall Street Journal profiled a couple able to to travel to three different continents using just Bitcoin. That was in 2013! If you live in a nation with a robust e-commerce market supported by reliable, high-speed internet access, chances are you *can* buy your groceries with Bitcoin. There just hasn't been a need in the US. We're currently blessed with a (relatively) stable government and the world's reserve currency; with little-to-no fear of asset forfeiture, hyperinflation, or demonetization.

Q8: How Are Bitcoin Transactions Taxed?

The IRS covered cryptocurrencies in the recent IRS Revenue Ruling 2019-24. in the Frequently Asked Questions section. In short, tax treatment depends on how the cryptocurrency in question is held and used. If Bitcoin is held as a capital asset, like a stock or bond, then you must treat it like property. Any gain or loss from the sale or exchange will be taxed as a capital gain or loss.

VII: Conclusion

While this eBook is meant to act as a high-level resource for you, the advisor, to gain confidence in the asset class, we acknowledge that it falls short in thoroughly evaluating:

- every risk that investors might face when investing in digital assets
- all of the options that are available for investing in digital assets
- the discussion of the research underpinning IDX's risk mitigation strategies

We at IDX believe that the blockchain revolution will bring about opportunities for wealth creation and innovation not seen since the formation of the internet. Ultimately, we believe that this technology will bring about the transparency and confidence required to rapidly settle transactions on a global basis, and will continue to unite humans from all corners of the world, and all walks of life.

As with any new innovation, participation in the evolutionary process does not come without significant risks; and sometimes rewards. It is our goal as a fiduciary, and a risk-manager in digital assets, that we embrace, understand, and communicate the good and bad realities of this emerging asset class. We seek to enable the responsible participation in the blockchain network and digital assets ecosystem for fiduciaries and their clients throughout the asset classes development over time.

Resources

[1]Last Week Tonight. “Cryptocurrencies.”https://www.youtube.com/watch?v=g6iDZspbRMg

[2]Nakamoto, Satoshi. “Bitcoin: A Peer-to-Peer Electronic Cash System.”https://bitcoin.org/bitcoin.pdf

[3]Narayanan, Arvind; Clark, Jeremy.Communications of the ACM. “Bitcoin’s Academic Pedigree.”https://cacm.acm.org/magazines/2017/12/223058-bitcoins-academic-pedigree/fulltext

[4]Kahn, David. “The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet.”https://books.google.com/books?id=3S8rhOEmDIIC&q=Arabs+cryptology+born#v=snippet&q=Arabs%20cryptology%20born&f=false

[5]Broemeling, Lyle D. “An Account of Early Statistical Inference in Arab Cryptology.”https://www.tandfonline.com/doi/abs/10.1198/tas.2011.10191

[6]Schneier, Bruce. “Applied Cryptography, Protocols, Algorithms, and Source Code in C.”https://en.wikipedia.org/wiki/Data_Encryption_Standard

[7]Qureshi, Haseeb. “Merkle Trees.”https://nakamoto.com/merkle-trees/

[8]Frankenfield, Jake. “Merkle Tree.”https://www.investopedia.com/terms/m/merkle-tree.asp

[9]Chaum, David. Publications.https://www.chaum.com/publications/

[10]Chaum, David. “Blind Signatures for Untraceable Payments.”http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF

[11]Hughes, Eric. “A Cypherpunk’s Manifesto.”https://www.activism.net/cypherpunk/manifesto.html

[12]Lopp, Jameson. “Bitcoin and the Rise of the Cypherpunks.”https://blog.lopp.net/bitcoin-and-the-rise-of-the-cypherpunks/

[13]Levy, Stephen. “Battle of the Clipper Chip.”https://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html

[14]Paloalto Networks. “What is a denial of service attack (DoS)?”https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos#:~:text=A%20Denial%2Dof%2DService%20(,information%20that%20triggers%20a%20crash,

[15]Dai, Wei. “bmoney.”http://www.weidai.com/bmoney.txt

[16]Peck, Morgan E. “Bitcoin: The Cryptoanarchists’ Answer to Cash.”https://spectrum.ieee.org/computing/software/bitcoin-the-cryptoanarchists-answer-to-cash

[17]Ibid.

[18]Nakamoto, Satoshi. “Bitcoin: A Peer-to-Peer Electronic Cash System.”https://bitcoin.org/bitcoin.pdf

[19]Ibid.

[20]“Honoré Gabriel Riqueti, comte de Mirabeau.”https://en.wikipedia.org/wiki/Honor%C3%A9_Gabriel_Riqueti,_comte_de_Mirabeau

[21]Hart, Keith. “The Persuasive Power of Money.”Pg. 138.

[22]Elmandjra, Yassine. “Bitcoin as an Investment, Part 2.”https://www.lopp.net/pdf/theses/ARKInvest_Bitcoin_Part_2.pdf

[23]Ibid.

[24]Marthinsen, John E. “India’s Demonetization: What Were They Thinking?”https://www.babson.edu/academics/executive-education/babson-insight/finance-and-accounting/indias-demonetization-what-were-they-thinking/

[25]Elmandjra, Yassine. “Bitcoin as an Investment, Part 2.”https://www.lopp.net/pdf/theses/ARKInvest_Bitcoin_Part_2.pdf

Resources

[26]Ibid.

[27]TurboTax.“Tax Tips for Bitcoin and Virtual Currency.”

[28]Bitcoin’s source code.https://github.com/bitcoin/bitcoin

[29]Hayes, Adam. “Stablecoin.”https://www.investopedia.com/terms/s/stablecoin.asp

[30]Buy Bitcoin Worldwide.“How Many Daily Users of Bitcoin?”

[31]Alden, Lyn. “Why Bitcoin is Not a Ponzi Scheme: Point by Point.”https://www.swanbitcoin.com/why-bitcoin-is-not-a-ponzi-scheme-point-by-point/

[32]Neufeld, Dorothy. “Visualizing the Rise of Digital Payment Adoption.”https://www.visualcapitalist.com/digital-payment-adoption/

[33]Vigna, Paul. “Bitcoin Couple Travels the World Using Virtual Cash.”https://www.wsj.com/articles/SB10001424052702303789604579196171277465460

[34]IRS. “Rev. Rul. 2019-24.”https://www.irs.gov/pub/irs-drop/rr-19-24.pdf

Disclosures: This document has been provided to you solely for information purposes and does not constitute an offer or solicitation of an offer or any advice or recommendation to purchase any securities or other financial instruments and may not be construed as such. The factual information set forth herein has been obtained or derived from sources believed by the author and IDX Insights, LLC ("IDX") to be reliable but it is not necessarily all–inclusive and is not guaranteed as to its accuracy and is not to be regarded as a representation or warranty, express or implied, as to the information's accuracy or completeness, nor should the attached information serve as the basis of any investment decision. This document is intended exclusively for the use of the person to whom it has been delivered by IDX, and it is not to be reproduced or redistributed to any other person. The information set forth herein has been provided to you as secondary information and should not be the primary source for any investment or allocation decision. Information contained herein has been obtained from sources believed to be reliable, but not guaranteed. Forward-looking statements are not guarantees of future results. They involve risks, uncertainties and assumptions, there can be no assurance that actual results will not differ materially from expectations. Past performance is no guarantee of future results. No part of this material may be reproduced in any form, or referred to in any other publication, without express written permission from IDX. The information contained herein is only as current as of the date indicated, and may be superseded by subsequent market events or for other reasons. Charts and graphs provided herein are for illustrative purposes only. The information in this document has been developed internally and/or obtained from sources believed to be reliable; however, neither IDX nor the author guarantees the accuracy, adequacy or completeness of such information. Nothing contained herein constitutes investment, legal, tax or other advice nor is it to be relied on in making an investment or other decision. There can be no assurance that an investment strategy will be successful. Historic market trends are not reliable indicators of actual future market behavior or future performance of any particular investment which may differ materially, and should not be relied upon as such. This document should not be viewed as a current or past recommendation or a solicitation of an offer to buy or sell any securities or to adopt any investment strategy. The investment strategy and themes discussed herein may be unsuitable for investors depending on their specific investment objectives and financial situation. IDX provide links to third-party websites contained herein only as a convenience and the inclusion of such links does not imply any endorsement, approval, investigation, verification or monitoring by us of any content or information contained within or accessible from the linked sites. If you choose to visit the linked sites you do so at your own risk, and you will be subject to such sites' terms of use and privacy policies, over which IDX.com has no control. In no event will IDX be responsible for any information or content within the linked sites or your use of the linked sites. Information contained on third-party websites that IDX may link to is not reviewed in its entirety for accuracy and IDX assumes no liability for the information contained on these websites. It is not possible to invest directly in an index. Exposure to an asset class represented by an index may be available through investable instruments derived from that index. IDX makes no representations regarding the advisability of investing in investment products based on the Index, which is not sponsored, endorsed, sold or promoted by IDX. Index returns do not reflect payment of certain sales charges or fees an investor may pay to purchase the securities underlying the Index or investment vehicles intended to track the performance of the Index. The imposition of these fees and charges would cause actual performance of the securities/vehicles to be lower than the Index performance shown. IDX gives no representations or warranties as to the accuracy of such information, and accepts no responsibility or liability (including for indirect, consequential or incidental damages) for any error, omission or inaccuracy in such information and for results obtained from its use. Information is as of the date indicated, and is subject to change without notice. This material is intended for informational purposes only and should not be construed as legal, accounting, tax, investment, or other professional advice.