JOURNAL of PENSION BENEFITS

Issues in Administration, Design, Funding, and Compliance
Volume 28 • Number 3 • Spring 2021

Multiple Employer Plans

Bitcoin for Fiduciaries—Part 1

To many people, Bitcoin and other cryptocurrencies are a science fiction delusion or a digital Tulipomania. But this is changing, and fiduciaries need to know what to do about it. This column has two parts. In Part 1, the focus is on the nature of cryptocurrencies and their place in the regulatory scheme. Part 2 will examine crypto through the lens of fiduciary law and practice.

By Pete Swisher

Pete Swisher is Founder and President of Waypoint Fiduciary LLC, and is known nationally for his work on retirement plan governance. He is a prolific writer and speaker for the financial community and was the founding Chair of NAPA's government affairs committee. In 1988 he graduated with a degree in Linguistics from the University of Virginia, where he was selected for the prestigious Echols Scholar Program. He served in the first Gulf War as Executive Officer of a US Marine infantry company. He lives with his family in the horse country of Central Kentucky, and can be reached at *pete.swisher@waypointfiduciary.com*.

Disclosure: Yes, I own Bitcoin. And yes, I would enjoy it if you bought some and drove up the price so I can be rich.

Most people in the United States today have heard of Bitcoin but few know what it actually is or why a rational investor would ever consider owning any. The term "cryptocurrency" seems to generate one of two responses: (1) a skeptical dismissal of this magic Internet money or (2) an insatiable urge to become a day trader.

Cryptocurrency (crypto for short) is risky, volatile, and full of potential pitfalls for financial professionals and their clients. But Bitcoin brought us the blockchain, blockchain-based technologies are in the early stages of disrupting almost every major industry, and crypto is going to become so pervasive that no fiduciary or investment professional can afford not to understand it.

In fact, I will make two predictions about the future of Bitcoin and other cryptocurrencies.

Prediction No. 1—Within the Next Decade, Fiduciaries Will Accept Crypto as Prudent

The prediction does not say crypto is a prudent part of an investment portfolio, but that *it will be accepted as such*. The prediction is not about making an argument for the prudence of Bitcoin or other cryptocurrencies—I intend no such argument—the point is *crypto will be accepted*.

In point of fact, fiduciaries are not safe today recommending crypto investments due to liability, but that will change in time, because "crypto" is not some online Ponzi scheme (except when it is). It is a cost-effective, global, nearly instantaneous set of technologies for owning, buying, selling, trading, or agreeing to *anything*. Crypto will be accepted as prudent someday in the same way that mutual funds, C Corporations, and the Internet are considered prudent—as part of the infrastructure.

Prediction No. 2—There Is Substantial Fraud, Money Laundering, and Market Manipulation in Crypto

This is more observation than prediction. The point of the observation is that, in order for Prediction No. 1 to come true, regulators must bring bank-style regulation and enforcement to the crypto space. A corollary to this prediction is that some of the misbehavior will never be discovered, but some of it will. Major crypto market crashes driven by discovery of a fraud or two are bound to happen. For examples of what happens regularly, see Charlie Osborne's "2020's worst cryptocurrency breaches, thefts, and exit scams" [Charlie Osborne, *https://www.zdnet.com/article/2020s-worst-cryptocurrency-breaches-thefts-and-exit-scams/*, last visited 12/7/2020] and Jordan Atkins "Crypto Crime Cartel: The end is nigh for Tether" [Jordan Atkins, *https://coingeek.com/crypto-crime-cartel-the-end-is-nigh-for-tether/*, last visited 1/15/2021].

Bitcoin—or any other individual crypto asset—might become "digital gold" as some expect, and it might not. Bitcoin or its siblings might crash and burn in spectacular fashion due to massive global fraud and market manipulation any day now and pull the entire crypto market down with them. Or not. Yet I stand by my predictions. "Crypto" is a movement. Financial professionals need to understand the movement.

A Note on Terminology

"Bitcoin" with a capital "B" describes the entire system. An individual coin is a "bitcoin," and multiple coins are "bitcoins." The abbreviation BTC is commonly used to refer to Bitcoin or bitcoins.

"Crypto" is used in this column to refer broadly to cryptocurrencies. A cryptocurrency, generally speaking, is a store of value or medium of exchange that is not issued by a government and exists only digitally. "Coin" also is used to refer to any specific crypto asset, as is "token." When an asset or service is wrapped into a crypto wrapper it is said to be "tokenized."

Some people do not believe Bitcoin or other cryptos are properly called "currencies" and are keen to advance reasons why this is so. But the world generally uses the words "currency" and "cryptocurrency" in talking about Bitcoin and other cryptos, and this column does not attempt to buck the trend. Regulators use the term "CVC" or "convertible virtual currency" to describe Bitcoin and many other crypto assets. [For example, *see* IRS Notice 2014-21]

"Fiat currencies" are those issued by governments "by fiat" (from the Latin, "make it so"), including the big six: the US, Australian, and Canadian dollars; the Chinese yuan; the British pound; and the Swiss franc. Those wishing for a waning of the US dollar's position as the global reserve currency of choice sometimes suggest a basket of these six currencies as an alternative. Such a basket would be relatively easy to tokenize.

The Birth of Bitcoin

Software developers love the word "manifesto." The best-known example is probably the "Agile Manifesto," written by a group of programmers to describe a new paradigm for writing code. [*agilemanifesto.org/history.html*]

Early cryptocurrency programmers called themselves "cypherpunks" and "crypto-anarchists" and had their own manifestos. Former Intel scientist Tim May published the *Cyphernomicon*, which included his "Crypto-Anarchist Manifesto," in the 1990s. A representative quote:

> Some of us believe various forms of strong cryptography will cause the power of the state to decline, perhaps even collapse fairly abruptly. We believe the expansion into cyberspace, with secure communications, digital money, anonymity and pseudonymity, and other crypto-mediated interactions, will profoundly change the nature of economies and social interactions. Governments will have a hard time collecting taxes, regulating the behavior of

> individuals and corporations (small ones at least), and generally coercing folks when it can't even tell what continent folks are on!

Eric Hughes published "A Cypherpunk's Manifesto" in 2003, one of the main points of which is, "We must defend our own privacy if we expect to have any":

> 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 in an open society requires anonymous transaction systems. Until now, cash has been the primary such system. An anonymous transaction system is not a secret transaction system. An anonymous system empowers individuals to reveal their identity when desired and only when desired; this is the essence of privacy.
>
> Privacy in an open society…requires cryptography.
>
> We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy out of their beneficence.
>
> We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money.

[*https://www.activism.net/cypherpunk/manifesto.html*]

Cypherpunks and crypto-anarchists often are known only by online pseudonyms (nyms), the most famous of which is Satoshi Nakamoto—the name used by the still-unknown creator(s) of Bitcoin in the paper that launched the world's best-known cryptocurrency in 2008, *Bitcoin: A Peer-to-Peer Electronic Cash System*.

The Blockchain

Think about what banks have done for millennia: stored people's money to keep it safe. A person deposits coins, bills, stock certificates, gold, and other valuables, and the bank (mostly) keeps it safe. The majority of today's monetary deposits are non-physical—the dollars exist only on the bank's computers, not as physical dollars in a vault—but the custody paradigm centers on the bank as safe storage.

This leads to banks being critical in the global transaction infrastructure. Transactions usually involve multiple banks. If Bob wants to give Sue $10, safely and with a clear transaction record, then Bob's bank sends money to Sue's bank, usually via global bank clearing networks such as the Federal Reserve's Fedwire or the SWIFT network (Society for Worldwide Interbank Financial Telecommunication). The money and all information about the transfer stay within the banks.

Bitcoin is a "peer-to-peer" cash system, allowing Bob to send Sue the $10 with no intermediary. To do this electronically, Bitcoin uses encryption to "publicly" post information to a transaction ledger that is stored in identical form on a widely distributed/dispersed network of computers owned by unrelated individuals or "pools" of such individuals. These computers continuously examine the public ledger to see the latest transactions and incorporate them into a "block" of transaction information.

As long as everyone can see what's in each block, publicly, the idea is that no one can corrupt the system because it is so widely distributed. From the *Bitcoin* white paper: "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." In other words, there is a chain of blocks of information (the blockchain) that can be trusted because there are so many separate computers around the world able to verify the information.

The transaction is public in that anyone in the world can see, via the "distributed" public ledger, $10 worth of Bitcoin moving from address 3J98… (each address is 256 bits of "hash" long) to address bc1q…But no one knows that Bob and Sue own those addresses. Part of the public concern over crypto in general is that privacy lends itself to criminal pursuits. After all, Bob could be a narco-terrorist and he could be sending Sue, his money launderer, money via multiple transactions at multiple addresses. Unless Bob and Sue reveal their identities, the idea is that there is no way to connect the $10 transaction to them.

Here are a few key points about Bitcoin:

- Launched in 2009 and can be considered the first major cryptocurrency.
- Can be used to buy and sell goods where accepted—including on Square and Paypal.
- Private in the sense that no one knows who transacts or owns a given BTC unless owners reveal their identities.
- Public in that the ledger of transactions (but not identities) is accessible by anyone.

- "Safe" from corruption of the data record as long as hacker(s) do not control more than 50 percent of the distributed network of computers (which means that, to be successful, an attack must be a "51% attack").
- Built into the code is that there will never be more than 21 million BTC. Contrast this with roughly 1 percent to 2 percent growth in the gold supply annually, and the growing supply of fiat currencies. This is a much-touted aspect of Bitcoin as an asset.
- A favorite statistic of Bitcoin fans is that if every millionaire on Earth wanted to own half a bitcoin, there would not be enough.
- Like gold, Bitcoin pays no interest or dividends, so its value is determined in the market solely by its price.
- The Bitcoin network currently is too slow to handle global transactions at the scale necessary for it to become a major reserve currency for transaction purposes, though various technologies could theoretically change this in the future.
- Many commentators seem to focus on Bitcoin's value as "digital gold"—a store of value that can act as a hedge against inflation and devaluation of global fiat currencies—more so than its value as a medium of exchange.

Metcalfe's Law

Metcalfe's Law is like a version of Moore's Law (which states that computer chip processing power doubles every 18 months) for networks. It can be summarized as, "The value of a system is proportional to the square of the number of users." One cell phone is useless. Two phones let two people communicate. But as the whole world gradually becomes connected by cell phones, the value of the network expands as the square of the number of users. That is the theory, anyway.

The concept is intuitively sensible and some commentators claim that the growth in Bitcoin's price tracks the growth that would be expected under Metcalfe's Law. Growth in the number of users is therefore the holy grail for cryptocurrencies just as it is for software-as-a-service companies and social networks. The actual number of users and the growth or shrinkage of that number is therefore an important investment consideration.

There are over 7 billion people on Earth, but probably only about 20-100 million of them own any Bitcoin—call it 1 percent of global population. If Metcalfe's Law is conceptually correct, then if 5 percent of humans became Bitcoin owner/users, the value of the network would increase roughly 25-fold. Note that this is not the same as saying the *price* would grow that much, or at all—it means the *value* of the network grows exponentially. It seems logical that this would increase the price over time even if the price today were in a bubble relative to the current size of the user network.

Bottom line: It's all about the users.

Regulatory Risks and Rewards

Regulation is coming to a cryptocurrency exchange near you. If you are a cypherpunk, this causes you to rant and wheeze. But institutional investors have a different view—regulation is a precondition for mass adoption.

Government Takeover?

One fear of crypto advocates is that governments will make Bitcoin and other cryptos illegal. Several major governments have done so to some extent: China, Russia, and India, for example, all have laws limiting or prohibiting the use of cryptocurrencies as a means of payment. In general, on the other hand, the United States and Europe have taken an approach of regulating crypto as it would any other asset. It is important to note that countries "banning" crypto as a payment mechanism generally are not prohibiting ownership of or trading in crypto assets.

If Bitcoin were to become so successful—in terms of number of users and transactions—that it could approach the scale necessary to become an actual global reserve currency, as some have suggested it could, it is not hard to imagine scenarios in which governments would work to protect their fiat currencies by restricting the use of crypto. This does not mean crypto would necessarily become "illegal" any more than a work of art or a lump of gold is illegal today, but talk of regulation makes Bitcoin investors skittish, and regulatory news will surely cause price volatility even if, ironically, the regulations are good for long term Bitcoin prices.

It is the essence of cryptocurrencies that they cannot, ultimately, be controlled by governments if people want to work hard enough to use them. But it seems likely that the crypto world is on the verge of being pulled under mainstream financial regulation, and this is probably bullish for Bitcoin, but there is no way to know this. After all, it has been profitable to be a long-term holder of gold across the

decades, but the US government introduced massive volatility in gold prices by confiscating gold in the 1930s as part of devaluing the dollar, then going off the gold standard completely in 1971. The bottom line is that the regulatory risk for Bitcoin and other cryptos is substantial even though the movement toward the mainstream may be a path to high rates of return.

Tax Treatment

The Internal Revenue Service (IRS) considers Bitcoin to be property, and gains are therefore taxable—even if the gain is realized when paying for a pizza with appreciated Bitcoin via Paypal. One of the challenges with widespread adoption of crypto is the tracking and reporting of gains and losses for tax purposes. [IRS Notice 2014-21]

The Collision of Cypher-Anarchist Privacy with KYC

The cryptographic point of crypto is that it lets people transact without Big Brother watching. But Big Brother wants to watch. Big Brother, one could argue, needs to watch. Financial regulation in the developed world has moved inexorably toward a paradigm in which financial institutions and "money service businesses" of all kinds are expected to:

- "Know your customer" (KYC) by gathering identity documentation and checking it against various databases;
- Report suspicious transactions (via currency transaction reports or CTRs, for example, when a transaction is $10,000 or more);
- Support tax reporting and collection efforts; and
- Deny service to known criminals, terrorists, and regimes under international sanction.

Bitcoin and other cryptos do none of that, on their own. Neither does cash—the anonymous criminal's historical currency of choice. But the government can create rules requiring cryptocurrency exchanges and other financial institutions to implement KYC, anti-money laundering (AML), and other rules. This appears to be exactly what is happening. For example:

- Financial Crimes Enforcement Network (FinCEN) published interpretive guidance [FIN-2019-G001], Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies, in 2019, reaffirming prior guidance that many cryptos are in the money transmission business and subject to the Bank Secrecy Act's KYC and AML rules.
- FinCEN also published proposed regulations in December 2020 requiring crypto wallets and exchanges to follow the Bank Secrecy Act. [Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets, FR Doc. 2020-28437]
- In October 2020, the Department of Justice (DOJ) published its Report of the Attorney General's Cyber Digital Task Force on the cryptocurrency enforcement framework. The DOJ's emphasis is on criminals and terrorists.

Is a Crypto Asset a Security?

On December 22, 2020, the Securities and Exchange Commission (SEC) initiated an enforcement action against Ripple Labs Inc. alleging that the company's cryptocurrency token, XRP, is a security and that Ripple was therefore offering an unregistered security. [SEC Press Release 2020-338] At issue is whether XRP is a security or a currency—the determination of which will be critical to all cryptocurrencies in the future.

The primary test of status as a security is the *Howey* test, named after the US Supreme Court case, *SEC v. W.J. Howey Co*. [328 U.S. 293 (1946)]. A full discussion is beyond the scope of this column, but the key is that any cryptocurrency may or may not be a "currency" but rather a security that is subject to registration under the Securities Act of 1933 depending on the facts and circumstances.

Anyone with a computer and the knowhow can launch a cryptocurrency, but classifying that crypto as a security means that its launch is supposed to be more like an initial public offering (IPO) of a registered security versus an informal "initial coin offering" (ICO). There have been thousands of ICOs in recent years, and it is possible—perhaps probable—that the SEC would consider many of them to be securities.

It is worth noting that SEC officials have previously implied that the two largest cryptocurrencies, Bitcoin and Ethereum, are not securities. [For example, *see* "Digital Asset Transactions: When Howey Met Gary (Plastic)," remarks of SEC Director William Hinman at the Yahoo Finance All Markets Summit, June 14, 2018]

Custody—The Big Challenge for Crypto

Bitcoin is essentially a modern bearer bond. A "bearer" bond is one that, like a dollar bill, gives its value to whoever bears it. If you find a dollar on the street, it is yours. If you steal a suitcase of bearer bonds, it is as if you stole a suitcase of cash. Bitcoin works the same way, because whoever holds the private key to an online wallet effectively "owns" the bitcoins. Furthermore, just like with a dollar bill you drop in the street, if you lose your private key, you lose your bitcoins. The private key is like a password. If you forget your password and have no way to restore it, you lose. If someone else gets your password, they can rob you.

Stealing crypto assets is a cybercriminal's dream come true. If they manage to get your private keys, they can cover their tracks (generally speaking) and steal your coins. And the coins are held anonymously, so the money laundering has already been done for them by the nature of the system. It's a win-win, hacking-wise.

Do an Internet search for "lost bitcoin" or "cryptocurrency exchange hacked" and you will think twice about putting even a small fraction of your life's savings into crypto. But if you could buy, sell, and hold it as easily as any other asset, via a regulated financial institution, you would likely feel safer.

As a result, a tremendous amount of institutional investment has gone into the crypto custody challenge, and the evidence is that the problem is mostly solved. Multiple large financial institutions have recently announced the launch of crypto subsidiaries that rely on various solutions to the custody problem. Solutions include things like patented blockchain innovations and dividing private keys into multiple pieces and storing them in separate, geographically dispersed "cold" wallets (offline storage that is like a bank vault for crypto). Insurers are devising new policies for the unique risks, so that the institutional custodians can protect both themselves and their clients.

Institutional custody will mean crypto has a launch pad for going mainstream. Increasingly, investors will be able to buy and sell crypto assets as easily as they trade other assets in brokerage accounts. This makes it easier for the number of users to grow, potentially feeding the value of the network via Metcalfe's Law.

Altcoins and Market Manipulation

Bitcoin is, by far, the largest crypto asset. Its market capitalization (cap) as of this writing was over $500 billion. By comparison, gold held for investment purposes might have a market cap of roughly $10 trillion. The next largest crypto, Ethereum, was over $100 billion. Bitcoin and Ethereum together accounted for 66 percent and 8 percent, respectively, of total crypto market cap in 2020. [Statista.com, "Distribution of the biggest cryptocurrencies from 2015 to 2020, based on market capitalization"]

The other 26 percent of the crypto universe consists of thousands of small cryptocurrencies commonly referred to as "altcoins." Altcoins remind me of dot-com startups during the 1990s Internet stock bubble, only brainier. Some of these coins are the real deal, the next great technology. Others are probably more like pets.com.

Thousands of tiny assets that are readily tradeable online without any regulatory oversight is an environment poised for drama. Market manipulation is generally legal—big traders can buy aggressively to push the price up, sell enough to spook the market, then buy when the panic selling ends. This sort of manipulation used to be legal in US securities markets before modern securities law was born. Even Bitcoin and Ethereum are subject to manipulation, but altcoins have such small market caps that manipulation is far easier. These are serious risks for fiduciaries to consider.

The China Risk

As anyone who watches enough Netflix knows, the concept of an international conspiracy to bring the world's premier cryptocurrency to its knees is perfectly plausible. Joking aside—think about it. To hijack a crypto, you need to control more than 50 percent of its distributed computing power—therefore a "51% attack" can rewrite the blockchain going forward (the historical blockchain is immutable, or so they say). And the computing pools (mining pools) in which miners band together to compete for new bitcoins are headquartered, largely, in China—within the jurisdiction of the Chinese government. Could we suppose, for the sake of argument, that the Chinese government is aware of these large mining pools, their headquarters, who their leaders are, and where they live? Might it be possible they have had discussions with some of these people?

Quite a few institutional investors, who presumably have done their homework, have been public in expressing their comfort level with Bitcoin, so perhaps this is nothing to worry about. But it is worth noting for fiduciaries that a successful 51

percent attack on Bitcoin would likely lead to a catastrophic and probably permanent drop in price. Advocates say this cannot happen, and that there is a strong movement to diversify the network, but no one appears to dispute the fact that over half of Bitcoin miners are in mining pools out of China.

Decentralized Finance

Crypto assets allow peer-to-peer, electronic, global everything. Using a crypto platform, individuals and businesses can buy things, sell things, lend money, enter into contracts, raise capital, securitize other assets, and do pretty much anything the traditional financial system can do. This is sometimes referred to as shadow banking—a financial system that cuts out traditional intermediaries and is (for now) outside the reach of governments and their regulators. The crypto community calls it "DEFI" for "decentralized finance."

Do you want to turn your comic book masterpiece into a package that can be easily sold online? I wrote that example as a joke, then thought to myself, "Hmmm. I wonder if someone has actually done that?" Yep: visit cryptocomics.com. Bring Ethereum. Are you a rich Chinese Bitcoin miner who is tired of being sold fake bottles of Bordeaux wine, which is apparently a big thing in China? Use the new Vinsent app, powered by Ravencoin, to make sure you're getting the real thing.

Crypto lending is available—similar to securities lending in the United States. You can make 8 percent or more on certain coins. You can buy gold via Pax Gold (PAXG), which resembles a securitized version of an ounce of physical gold, like a mutual fund but in the form of a digital coin that trades around the clock. There are coins that make it possible to hold video conference calls using minimal bandwidth or exchange messages privately. Other coins are creating interconnectivity among different crypto networks, allowing banks or other businesses to build applications without having to build their own distributed networks. Some of these capabilities may be in for some regulatory trouble ahead, but the salient fact is that the blockchain technology popularized by Bitcoin is making it possible to imagine faster, simpler, safer, cheaper, around-the-clock ways of doing things.

Back to the Future: The Prediction

Bitcoin has moved from being a curiosity and a fad to something that people are trading in droves, making real money (as long as the price holds). Ethereum is viewed by some as being likely to outperform Bitcoin in 2021 due to its nature and growing popularity. And various altcoins "go vertical" in price with some regularity. Clearly, there is money to be made—and lost—in crypto. It has therefore fired the imagination of the world. But is it prudent?

Early in the column I predicted that Bitcoin and other cryptos would be accepted as prudent by fiduciaries within a decade. My faith in this prediction is based on the fact that cryptos are a new type of software platform, one that has the potential to reshape financial services and other industries, and one that is increasingly falling under the umbrella of regulation and institutional custody, which is likely to drive acceptance. Fiduciaries therefore have a powerful need to understand crypto assets.

In Part 2 of this column, we discuss ERISA, the common law of trusts, and how modern concepts of prudence apply to crypto—and how fiduciary thinking may need to evolve. ■