

JOURNAL *of* PENSION BENEFITS

ISSUES IN ADMINISTRATION, DESIGN, FUNDING, AND COMPLIANCE
Volume 26 • Number 4 • Summer 2019

Cryptocurrency and Your Retirement Plan: What's in Your (Crypto) Wallet?

BY GARY BLACHMAN AND
JUSTIN STEFFEN

There are transaction, security, and regulatory risks, in addition to a volatile market price involved with cryptocurrency that should raise concerns for retirement plan fiduciaries. This article gives a brief explanation of virtual currency and highlights the risks that retirement plan fiduciaries should consider when deciding whether to invest in cryptocurrency.

Gary Blachman is a partner in the employee benefits and executive compensation group at Ice Miller LLP in Chicago, IL. His practice focuses on mergers and acquisitions, executive compensation, and the fiduciary and legal compliance requirements under ERISA.

Justin Steffen is a partner in the litigation and financial services groups at Ice Miller LLP in Chicago, IL. His practice focuses on the legal and regulatory issues with financial and emerging technologies.

For years, crypto industry insiders have speculated as to what great tech advances would unleash the institutional money that was seemingly content to sit on the sidelines. Advances in custody solutions and Exchange Traded Fund (ETF) applications receive significant press—like a crypto holy grail. However, it was Morgan Creek Digital's recent announcement that two pension funds for the Virginia Fairfax County police officers would become anchor investors in their

new \$40 million, crypto-focused venture fund that was both significant for the tech industry and even more surprising for the retirement plan industry. [[https://www.Bitcoin.Com/Two-US-Public-Pension-Funds-Back-New-\\$40-Million-Crypto-VC](https://www.Bitcoin.Com/Two-US-Public-Pension-Funds-Back-New-$40-Million-Crypto-VC), Feb. 12, 2019] The decision for these two pension funds to invest in blockchain startups and cryptocurrency reflects the bullish excitement of many investors who are eager to participate in this emerging opportunity.

Yale University, which has a reputation of seeking out unconventional investments, also recently plunged into the choppy waters of cryptocurrency investments. Yale University has the second largest endowment in higher education with \$29.4 billion in assets and, for strategic reasons, also decided to invest a portion of its endowment in two cryptocurrency funds. [<https://www.ccn.com/yale-university-has-invested-in-two-cryptocurrency-funds-report>, May 10, 2018]

While there are new entrants in the cryptocurrency space almost every day, there has been no manifest change explaining why pension fund managers are now suddenly comfortable investing in funds that target blockchain and crypto companies and may include sums of cryptocurrency. It appears for the moment that the crypto winter persists, but are these recent developments an aberration or the first sign of a thaw? No one knows for sure.

Although cryptocurrencies are permitted in most of the world's major economies, there are transaction, security, and regulatory risks, in addition to volatile market price movements that should raise concerns for retirement plan fiduciaries, 401(k) plan participants, and private investors. This article highlights those risks that retirement plan fiduciaries should consider when deciding if cryptocurrency is an appropriate investment option.

What Are Bitcoin, Blockchain, and Virtual Currencies?

Bitcoin is the seminal cryptocurrency—a digital or virtual currency. Often compared to a form of digital gold, bitcoin has become a valuable asset, trading between approximately \$3,000 and \$20,000 over the past 18 months. Bitcoin was first described in a 2008 whitepaper by a person or persons using the pseudonym Satoshi Nakamoto. [<https://bitcoin.org/en/bitcoin-paper>: “Bitcoin: A Peer-to-Peer Electronic Cash System” (2008)] Nakamoto's whitepaper described both bitcoin (the term “bitcoin” refers to the cryptocurrency, whereas the capitalized term, “Bitcoin,” refers to the protocol) and the blockchain technology underlying bitcoin.

Bitcoins are tracked on the Bitcoin blockchain, a large, decentralized ledger—similar to an excel spreadsheet that is copied and distributed across participating user machines and stored on every user's system. Anyone can edit the blockchain so long as the majority of other users (known as “nodes”) agree with the change. Because of the sheer size of the Bitcoin network and the means by which bitcoin transactions are validated, it is very difficult to “hack” the Bitcoin blockchain. To do so, an individual would need to overtake 51 percent of the nodes running the Bitcoin protocol. This would require incredible amounts of effort and money, which makes it extremely unlikely that a major attack of the Bitcoin blockchain would occur or even be successful. [See, e.g., <https://www.coindesk.com/blockchains-feared-51-attack-now-becoming-regular>; <https://media.consensys.net/the-current-cost-of-51-attack-on-proof-of-work-blockchains-91f87dbc1073>] This system works without a central repository (*i.e.*, a bank), as all transactions are conducted peer-to-peer. Bitcoin transactions are recorded by references to “public keys”—a coded “address” that everyone on the network can view. To redeem or control the bitcoin assigned to a “public key,” one also must possess the private key—another code known only to the owner that operates similar to a ticket that entitles the holder to access his or her bitcoin.

The blockchain on which bitcoin transactions are recorded was designed to prevent double spending. If an individual has one dollar bill, he can buy a lottery ticket or a Coke with that dollar, but not both. Likewise, by tracking all bitcoin transactions, the Bitcoin blockchain prevents individuals from paying with a particular bitcoin more than once.

While bitcoin was the first, it was far from the last cryptocurrency. By changing the publicly available bitcoin source code or protocol (*i.e.*, the code that creates the system's rules), other developers created “forks” of Bitcoin's code. After a change to the Bitcoin protocol, a fork can result in two different cryptocurrencies. Indeed, crypto entrepreneurs have created well over a thousand unique cryptocurrencies, some of which largely resemble bitcoin and some do not.

Bitcoins are controlled by the use of public and private keys (as discussed above). Some users store their private keys themselves, on their computers or on devices specifically designed to hold keys (*e.g.*, a Trezor hardware wallet). [“UseTheBitcoin.com//Trezor vs. Ledger vs. BC Vault Review: An Updated Analysis,” (April 2019)] These physical devices often resemble a Universal Serial Bus (USB) or external hard drive, and

often require a password to access. Others users allow third parties to store their keys for them. So called “wallet” services (e.g., blockchain.com) and custodial online crypto asset exchanges (e.g., Coinbase) store individuals’ private keys. Oftentimes, storage mechanisms are described as being either “hot” or “cold.” Hot storage refers to wallets storing private keys connected to the Internet. Cold storage refers to a device or other means of storage that is not connected to the Internet (e.g., flash drives or USBs).

Bitcoin transactions are said to be “pseudo anonymous.” Transactions are recorded on the Bitcoin blockchain, viewable to all via Websites such as blockchain.info. Transactions, however, are not linked to individuals; rather, they are only identifiable by public keys. Individuals, groups, or businesses (the “miners”) compete with one another to add tranches or “blocks” of new transactions to the blockchain, using high-powered computers to be the first to solve complex mathematical equations that result in the agreement of all participating miners that the block of transactions at issue shall be added to the blockchain. The first miner that solves the puzzle receives a “block reward” (i.e., a distribution of new bitcoin) from the software at pre-determined rates.

Despite its name, under the current United States accounting framework, cryptocurrency is not considered cash, currency, or a financial asset. Instead, cryptocurrency is viewed as an intangible asset because it lacks physical substance. This has significant implications for retirement plan record-keepers when valuing cryptocurrency that may be included in retirement plan portfolios. Difficulties in valuing cryptocurrency could create fiduciary challenges when, for example, retirees intend to withdraw these intangible assets from their retirement accounts and there is a disconnect as to the true value of the cryptocurrency.

Cryptocurrency Challenges for Employee Benefit Plan Fiduciaries

Virtual currencies are a fascinating combination of cryptography, consensus algorithms, and other features fully comprehensible to only a small group of academics, developers, and cypher punks. And while the protocols are complicated, many of the fiduciary issues presented by cryptocurrency are no different from the investment challenges for retirement plan sponsors as presented by other asset classes. These challenges include, for example, the following: security risks, recordkeeping and custody concerns, liquidity and diversification, transaction risk, government regulation, valuation, and risk-mitigation.

Security Risks

Crypto exchanges and other hot wallets, such as Parity [*Cryptocompare.com//How to Use the Parity Ethereum Wallet*, June 5, 2017], that are connected to the Internet are subject to attacks and hacks. If stolen, crypto assets can be extremely difficult, if not impossible, to recover. Lose your keys, lose your crypto.

Even cold storage solutions are not entirely fraud-proof. Notably, the Canadian exchange, QuadringaCX, has received considerable attention because its Chief Executive Officer (CEO) allegedly passed away and the exchange’s customer keys (\$190 million worth of assets) were purportedly lost. [*Ambcrypto.com//QuadringaCX CEO's death seems like a suspicious one, says Kraken's Jesse Powell*, March 8, 2019]

Aside from storage issues, moreover, computer viruses have been created to target crypto holdings and individual’s crypto assets have been stolen in Subscriber Identity Module (SIM)-swapping attacks. These security challenges create additional risk and exposure for retirement plan fiduciaries.

Recordkeeping and Custody Concerns

Crypto assets present recordkeeping and custodial risks. Retirement plan fiduciaries must be able to properly record-keep plan assets so that they can be timely valued and made available to pay retirement plan benefits and permissible plan expenses. Mutual funds, stocks, bonds, real estate, etc., can all be held in a custodial account and properly valued. However, because cryptocurrency exists as lines of computer code in a digital “wallet,” it cannot be held in the same way as mutual funds, stocks, bonds, or real estate, which makes it more difficult to establish ownership.

Although Coinbase [*Coincentral.com//Coinbase Review: Is Coinbase a Safe Exchange to Buy Cryptocurrency?*, January 10, 2019], Fidelity [*TheBlockCrypto.com//Fidelity's Bitcoin Custody Business is Live: A Conversation With Fidelity's Digital Assets head Tom Jessop*, March 8, 2019] and others are developing recordkeeping platforms, the current state of investor protection creates additional uncertainty for retirement plan fiduciaries trying to decide if cryptocurrency is a prudent investment option to include in a 401(k) plan or other types of retirement plans.

Liquidity and Diversification

Crypto assets have a host of liquidity issues. While anyone can engage in a peer-to-peer transaction of traditional assets (e.g., stocks, bonds, etc.), most individuals buy and sell crypto assets through exchanges such as Coinbase [*Coincentral.com//Coinbase Review: Is*

Coinbase a Safe Exchange to Buy Cryptocurrency?, January 10, 2019] and Kraken. [*Blockonomi.com//Beginner's Guide to Kraken: Complete Review*, January 23, 2019] Exchanges do not necessarily list every asset, the exchanges do not always publicize how transactions are processed, and exchanges often limit the amount of government-issued currency a customer can deposit or withdraw, thus impacting the amount of cryptocurrency customers can buy or sell.

Due to the relatively low-trading volume—at least compared to more traditional assets and markets, especially those that feature “market makers” who help provide liquidity—sellers cannot always obtain the market price that they anticipate and/or in the time period desired. Even the relatively low reported trading volumes may be a fiction. In connection with its exchange traded fund application, Bitwise explained that it believed 95 percent of reported exchange trading volume was faked or exaggerated. [*Bitcoin.com//Bitwise: Nearly 95% of Reported Bitcoin Trading Volume Are Artificially Created by Unregulated Exchanges*, March 22, 2019] Large crypto transactions, moreover, can have unexpected and unintended consequences. Large transactions, for example, may help precipitate flash crashes in more thinly-traded cryptocurrencies, where the price of certain cryptocurrencies temporarily plummets.

To satisfy the Employee Retirement Income Security Act of 1974 (ERISA) Section 404(c) requirements, which limits plan fiduciary liability in relation to participant-directed investments, retirement plan fiduciaries must be able to provide investment options of varying degrees of risk and reward, as well as information, for participants to make reasonable investment decisions about their plan accounts. The challenge with cryptocurrency is that it is not otherwise a tangible asset, such as gold or real estate. Cryptocurrency by its nature can be acquired and sold relatively quickly; however, it also is not as easy to map or convert to other types of plan assets, which may make investment decisions more difficult for the average 401(k) plan participants.

Transaction Risk

Crypto assets present transaction risks that increase their volatility. Today, most payment transactions are handled by financial institutions, such as banks, credit card companies, and other payment vendors. By contrast, cryptocurrency transactions do not necessarily involve an intermediary and are recorded on data records across a decentralized network. The benefits

of this approach include traceable and transparent historical records and international connectivity without geographic boundaries. However, the technology is still under development to improve efficiencies, reduce technical difficulties, and allow certain protocols to scale. This has led to increased regulatory concern and heightened scrutiny, which, in turn, creates additional volatility.

Bitcoin “tokens” kicked off 2017 at \$970 and climbed to nearly \$20,000 by December, 2017, a gain of 2,000 percent. But there were five selloffs of at least 30 percent during the year, driving prices down 45 percent before the value recovered to \$14,292 according to CoinDesk. Few investments grow by a factor of 19 in less than a year, and not many investments also lose over 60 percent of their value in two months' time. Despite these volatile results, many investment advisers have clients who are drawn to crypto assets like a moth to a burning flame. In the current environment, where participants are quick to bring a lawsuit for account balance losses, this should give retirement plan fiduciaries further cause for concern.

Government Regulation

Crypto assets face an uncertain regulatory future. The SEC's Rule 21(a) “DAO Report,” [Securities and Exchange Commission: Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO, July 25, 2017 (AUTHOR'S NOTE: A Decentralized Autonomous Organization is a virtual organization embodied in digital code and executed on a distributed ledger or blockchain)] subsequent enforcement actions, and guidance and enforcement actions from the Commodities Futures Trading Commission (CFTC), Financial Crimes Enforcement Network (FinCEN), [Financial Crimes Enforcement Network (a bureau of the US Department of Treasury). FinCEN.gov] and other state and federal regulators have helped provide some industry direction. These regulatory pronouncements, however, are far from comprehensive. Many issues still remain. Chief among them is that we still do not know whether the US Securities and Exchange Commission (SEC) (or, more critically, the courts) will find that certain crypto assets are “securities.” SEC Director of Corporate Finance William Hinman, for example, noted that, in his personal opinion, Ether, the token generated by the Ethereum protocol (and tracked on the Ethereum blockchain) was “sufficiently decentralized” and, thus, no longer qualified as a security. But how many nodes (users), how many miners (businesses), how many

holders of bitcoin does it take to meet the standard of being a “security”? What constitutes “sufficiently decentralized” has yet to be determined or tested. There is simply no ready answer, and the failure of cryptocurrency to qualify as a security has significant financial consequences and implications for retirement plan fiduciaries when, for example, a retirement plan is holding tokens that are later determined to be securities. But, classifying cryptocurrency as a security may have its own disadvantages. Registration requirements and restrictions on secondary sales embodied in SEC rules that apply to securities could make a token that is held to be a “security” relatively worthless.

Retirement plan fiduciaries must consider that rules and regulations to govern the cryptocurrency markets have yet to be established. The challenge with cryptocurrency is that it is not controlled by banks, and the Internal Revenue Service (IRS) and SEC have not yet provided substantial guidance in this area. Fiduciaries also must be wary that government entities may decide to restrict or even prevent the investment in cryptocurrency within retirement plans at any time.

On the other hand, the fact that cryptocurrency is not under direct control by any government is one of the characteristics that fuel its growth as an alternative currency. Cryptocurrency largely is immune to the impact on Wall Street of government policies. Additionally, central banks often can change the value of traditional currency, such as the US dollar, when shifting directions on monetary policy. For this reason, cryptocurrency often is considered a contrarian investment like gold in that it moves in the opposite direction of the prevailing market winds. While this may be appealing to certain investors, it raises fiduciary concerns for those who are proponents of its everyday use in retirement plans.

Valuation

The confluence of the aforementioned issues and other factors make valuing crypto assets incredibly difficult. How much of a token can you sell and in what time period? Is a particular token a security? What is the size of a protocol’s network or ecosystem? How long are assets held? What is the nature of the token (utility, protocol, both, a store of value)? All of these factors are either unclear or, at a minimum, difficult to ascertain. Further, economic models for valuing different crypto assets are either nonexistent or in their early stages.

Retirement plan fiduciaries must know how assets are valued so that they can measure rates of return and other investment factors over the life of the asset.

However, finding a method to “value” a crypto asset is complicated, at best. Given this challenge, retirement plan fiduciaries must carefully evaluate the nature and types of crypto they might offer to plan participants.

Risk-Mitigation

The still maturing state of crypto means that a number of traditional risk-mitigation options are unavailable or untested. Insurance, for example, is not widely available. While some companies, such as Aon, have reportedly created very narrow products, such as insurance for lost “keys” on certain exchanges, special crypto-specific policies are not widely available. Moreover, it is unclear whether certain risks posed by cryptocurrencies are covered by more traditional insurance offerings (cyber insurance, comprehensive general liability insurance, etc.)

Given the interest in cryptocurrency and the many risk factors described above, Marsh reports that many US clients are buying cyber insurance with higher limits and that average coverage limits purchased in 2018 rose by 11 percent to \$20.9 million. For companies with greater than \$1 billion in revenue, the average coverage limit rose by more than 25 percent to \$62.4 million. [<https://www.cfo.com/cyber-security-technology/2019/04/cyber-coverage>, April 11, 2019] Whether those cyber policies will cover crypto losses, moreover, is untested, at best.

What Is a Pension Fund Manager to Do?

Currently, there is nothing to prevent the use of bitcoin to fund a retirement plan or to convert the funds in a retirement plan to bitcoin. The IRS has determined that bitcoin is a virtual currency that has “an equivalent value in real currency.” In fact, the IRS explicitly refers to bitcoin in its IRS Virtual Currency Guidance: Notice 2014-21. [Internal Revenue Service Notice 2014-21] The IRS noted that bitcoin can be digitally traded between users and can be purchased for, or exchanged into, US Dollars, Euros, and other real or virtual currencies. In essence, the IRS is stating that the direct convertibility of bitcoin for real currencies, such as US Dollars and Euros, qualifies it as a legal tender.

That said, several wire firms are telling advisors and investors that products related to cryptocurrency are not being sold on their platforms. For instance, Merrill Lynch moved to end client purchases of the Grayscale Bitcoin Investment Trust on December 8, 2018. [<https://www.thinkadvisor.com/tag/merrill-lynch>] This move was coupled with an announcement not to allow advisors and clients to trade bitcoin futures, which

began trading on December 10, 2018. With this decision, Merrill Lynch expressed serious concerns about the suitability and eligibility standards of bitcoin and cryptocurrency.

Similarly, Morgan Stanley does not offer its Wealth Management clients access to securities or derivatives linked to the price of bitcoin or other digital currencies. [<https://www.thinkadvisor.com/tag/morganstanley>]

Further, UBS-Americas does not provide access to bitcoin or similar products, including bitcoin futures, as it does not consider cryptocurrency to be an asset class. The Chief Investment Officer (CIO) believes crypto valuations are a “speculative bubble.” [<https://www.thinkadvisor.com/tag/UBS>]

Plan Fiduciaries and the Duty of Prudence

ERISA imposes a standard of care on plan fiduciaries. Fiduciaries are subject to the prudent expert standard of care and owe a duty of loyalty to the plan participants. A prudent expert acts with the care, skill, and diligence that the circumstances call for a person of like character and like aims to use. Fiduciaries must act prudently and in the best interests of plan participants and beneficiaries. [ERISA Section 404(a)]

Typically, plan fiduciaries offer investments in a retirement plan that are regulated by government agencies (*e.g.*, IRS, DOL, SEC). For example, traditional investments in brokerage accounts or mutual funds are protected by the Securities Investor Protection Corporation (SIPC), while bank accounts are protected by the Federal Deposit Insurance Corporation (FDIC) up to certain monetary limits.

Cryptocurrency currently is not protected by any government agency and investors have little or no recourse if their accounts are hacked or subject to fraud. Fiduciaries must take prudent steps to protect participant accounts and plan assets from theft by means of a cyberbreach.

Bitcoin wallets may have only one password and, if it is lost or forgotten, there is no ability to reset the password, which means that bitcoin can be lost forever. There currently is no clear direction as to who should maintain the password for the entire 401(k) plan and who is liable if that password or cryptocurrency is hacked or the bitcoin investments are stolen. If retirement plan participants are permitted to retain the password or bitcoin wallet, what type of liability exists for plan fiduciaries, trustees, or record-keepers in situations where plan administration or recordkeeping goes sideways?

Return on Investment

Prudent fiduciaries must know how to evaluate the long-term potential for bitcoin to generate a return on investment for retirement plan participants. Typically, rates of return are measured by an increase in the asset price, the interest paid, or the dividend stream on a specific investment medium. Most retirement plan portfolios have a mix of stocks, bonds, and mutual funds to provide varying rates of risk and return. However, bitcoin does not pay interest as do bond investments, and only certain cryptocurrencies pay implied dividends. The only source of earnings is for bitcoin to increase its price. Although the returns since bitcoin’s introduction have been extremely strong, they also have been volatile, and it is unclear whether the rate of bitcoin demand will increase over time.

To Invest or Not to Invest?

Generally, a retirement plan returns from 5 percent to 8 percent annually, based on a portfolio of 60 percent stocks and 40 percent bonds and other conservative investments. Even if a retirement plan is meeting these expectations, plan participants may be tempted by the significantly higher returns of crypto currencies such as bitcoin. Currently, there are over 1,600 types of cryptocurrencies, with bitcoin being the most well-known, which confirms that the demand for this investment medium remains strong.

There are many reasons that cryptocurrencies are in high demand:

- Corporate, banking, and political regulations and oversight are minimal.
- No single entity has control over digital currency, because the digital ledger is not stored or managed by one entity within its walls, but rather is stored around the world.
- Digital currency is easily transferable (assuming there is a market for it).
- Fees/costs often are less than those in traditional retirement plans, as fewer middlemen are involved in transactions.

However, there are just as many concerns for retirement plan fiduciaries:

- Cryptocurrency is very specialized, and most participants do not have sufficient knowledge or expertise to make informed decisions or prudent allocations within their account balances.

- Cryptocurrency as an investment option would greatly increase fiduciary risk and liability.
- Traditional valuation methods for determining what a stock is worth do not necessarily work when evaluating bitcoin, blockchain, or other cryptocurrencies.
- Crypto volatility requires retirement plan participants to be patient over the long term and during significant up and down swings, which could result in poor investment outcomes if participants exit the sector too quickly.
- Whether justified or not, many still associate cryptocurrency with the sale of illegal goods, and this causes potential entrants to question its legitimacy.
- An improved infrastructure is needed to accommodate investments and encourage more widespread acceptance of cryptocurrency.
- Potential regulatory and legal hurdles create market hesitation to use cryptocurrency.

At the present time, it makes more sense for cryptocurrency to be available for savvy investors outside of a company's retirement plan, for instance, in a self-directed Individual Retirement Account or a personal portfolio.

For most retirement plan participants, investing in cryptocurrencies is like a trip to the casino. Plan participants should be careful not to allow the excitement and promise of "big wins" to cloud their judgment and invest more than they can afford to lose from their retirement accounts.

For retirement plan fiduciaries, it is important not to confuse investing with speculating or gambling with other people's money. Despite the alluring investment returns of cryptocurrency, those entrusted with the safety of retirement plan assets must consider their fiduciary obligations and the best interests of the participants and beneficiaries when selecting the investment options that are available within a retirement plan. ■

Copyright © 2019 CCH Incorporated. All Rights Reserved.
Reprinted from *Journal of Pension Benefits*, Summer 2019, Volume 26, Number 4,
pages 31–36, with permission from Wolters Kluwer, New York, NY,
1-800-638-8437, www.WoltersKluwerLR.com

