Official Publication of the California Lawyers Association
Trusts and Estates Section

California Trusts and Estates Quarterly

Volume 24, Issue 3 • 2018

Inside this Issue:

CRYPTOCURRENCIES AND TRUSTEES' DUTY TO INVEST PRUDENTLY: NAVIGATING FIDUCIARY DUTIES IN THE AGE OF DECENTRALIZATION[1]

By Adam F. Streisand and J.D. Rees **

I. INTRODUCTION

A now-infamous Australian man mistakenly threw away a hard drive containing 1400 bitcoin.[2] He bought those 1400 bitcoin for $25—total. But with the price-per-bitcoin hovering around $8,200 as of May 31, 2018, those 1400 bitcoin are worth more than $11 million. This incident demonstrates how important it is for every trustee to have some understanding of cryptocurrency. It is simply no longer acceptable to ignore it as a fad, a scam, or a play toy for geeks and day traders.

Some terms may have become familiar. Bitcoin. Cryptocurrency. Blockchain. What are they? To begin with, Bitcoin, cryptocurrency (a.k.a. "crypto"), and blockchain are not synonymous. Bitcoin is a crypto, but not all cryptos are Bitcoin. Cryptos are built upon blockchain technology, but not all blockchains are cryptos. Why does it matter? The story above illustrates the obvious: be careful what is discarded in the trash. But there is more. Much more. As crypto and blockchain technologies go mainstream—and by all accounts, they are well on their way[3]—fiduciaries will increasingly find it necessary to apply knowledge of new technologies and ways of investing to familiar rules governing their fiduciary duties.

Fiduciaries will have to understand cryptos because they will inherit responsibility for securing, managing and making investment judgments about cryptos. Fiduciaries will need to understand how to obtain control over and protect crypto assets, a more complex undertaking than obtaining control over and managing stocks and bonds. If, as predicted, the growth of cryptos continues, investment managers will be recommending cryptos as a staple of a properly diversified investment portfolio. Without understanding cryptos and having some comfort level with making investment decisions about cryptos, fiduciaries will be tempted to liquidate holdings or avoid opportunities to invest. The staggering returns we have witnessed make the path of least resistance a potentially dangerous one, while the specific risk characteristics of cryptos require greater understanding to make decisions, yay or nay. Sooner rather than later, ignorance of cryptos will no longer be a choice for any fiduciary.

This article will shed light on three overarching topics. Part II provides a general overview of what blockchain technology and cryptos like Bitcoin are, and what advantages and risks they offer. The authors do not wade into intricacies of the blockchain or how cryptographic algorithms drastically reduce certain risks of fraud, but they do endeavor to provide a basic understanding of the critical concepts. Part III examines how people have begun to invest in blockchain technologies, with an emphasis on the nuts and bolts of buying and selling cryptocurrency. Part IV surveys the current web of investment-related fiduciary duties of California trustees, including the duties to invest prudently, to diversify, and to protect trust assets. Part IV also looks at how those fiduciary duties might apply to investments in crypto and other blockchain technologies, providing guidance to trustees who want to insulate themselves from liability when investing, and it illuminates how settlors can ensure that fiduciaries have access to crypto assets.

Although this article cannot answer every question a trustee or other fiduciary might have when it comes to investing in the blockchain space, it will provide trustees with the lexicon and other tools necessary to educate themselves and proceed as a prudent investor might.

II. WHAT ARE CRYPTOCURRENCIES AND THE BLOCKCHAIN?

Although people sometimes conflate the terms, cryptocurrency, Bitcoin and the blockchain are neither synonymous nor coextensive. Cryptocurrency or "crypto" is a digital asset designed to function as a medium of exchange, or a currency, which uses cryptography to secure the transactions and control the creation of additional units of the currency.[4] Bitcoin is one type of crypto, just as the U.S. dollar is one type of fiat currency (i.e., legal government tender). "Blockchain" (or "the blockchain") is the technology that makes cryptocurrencies possible; neither Bitcoin nor any other cryptocurrency would exist without blockchain technology. But, again, cryptocurrencies are just one form of blockchain technology.

With well over 1,500 cryptocurrencies in existence as of April 2018, and many of them having unique combinations of attributes, and even more uses of blockchain technology that have nothing at all to do with cryptocurrency, there are simply too many variations to provide a tidy, accurate, all-encompassing definition. As one author observed, "imprecise vocabulary usage can suggest that each variation of [blockchain] technology has the same fundamental characteristics, when the characteristics

of a given variant may be vastly different from characteristics of other forms of the technology that are also labeled 'blockchain.'"[5] Taking care to avoid contributing to what that author called a "fog of confusing terminology" surrounding blockchain technology, the following section endeavors to provide an overview of blockchain technology and the potential benefits and risks of the most prevalent use of it: cryptocurrency.

A. A Blockchain is a Decentralized, "Immutable" Ledger

At its core, a blockchain is simply a digital ledger of transactions, and these do not necessarily have to be financial transactions or transactions related to cryptos. A blockchain is a chain of "blocks," or groups of transactions that cannot easily be broken or changed. Similar to the way that a county recorder's office (theoretically[6]) keeps track of all transactions affecting certain parcels of real property, a blockchain is a digital technology that keeps track of all transactions in that ledger's history. In addition to keeping track of transactions, a blockchain's use of decentralization maintains the integrity of the ledger.

Decentralization is one of the key features and attractions of blockchain technology.[7] Instead of relying on a single, centralized database to keep track of transactions, a blockchain's master ledger of transactions is "decentralized," i.e., maintained by many individuals across a peer-to-peer network. No single computer is responsible for maintaining a blockchain's ledger; rather, a network of computers support and preserve the ledger communally. Before a transaction on a particular blockchain is finalized and etched into a "block," it must be "verified," i.e., confirmed as a legitimate transaction.

Blockchain uses a combination of computer science, cryptography, and game theory (collectively referred to as "cryptoeconomics") while leveraging the consensus of many computers—sometimes, thousands—to verify that new proposed transactions are legitimate. In this way, blockchain offers the promise of an "immutable" ledger of transactions free from human error, a ledger highly resistant to would-be hackers or fraud or impropriety.[8] This, in turn, enables parties to transact confidently and efficiently without a third-party intermediary, in so-called "trustless" transactions, because although transactors may not know the identity of the other party, they can be confident (based on cryptoeconomics) that the other party has the right to transact with the item (e.g., cryptocurrency) that is the subject of the proposed transaction, and that cryptocurrency received is legitimate.[9] The parties to a trustless transaction do not need to trust each other to complete the transaction, meaning they can transact without even a modicum of trust.[10]

B. An Example of a Blockchain Transaction Using Bitcoin

To understand, let us look at a hypothetical Bitcoin transaction. Suppose Alice wants to send Bob 100 bitcoin.[11] Before Bob actually receives Alice's bitcoin, the transaction must be "verified," or confirmed as a legitimate transaction; the Bitcoin network must ensure that Alice actually has 100 bitcoin in her "account" and, for example, has not already "signed a check" (figuratively speaking) to another for the 100 bitcoin she now proposes to send to Bob.[12]

The process for verification is technologically complex and nuanced, but can be summarized as follows:[13]

Alice initiates a transaction by agreeing to send Bob 100 bitcoin. Alice and Bob's proposed transaction is then broadcast in a gossip-like way to all the computers (i.e., "nodes") in the Bitcoin network. Nodes each independently verify Alice and Bob's proposed transaction by confirming that Alice, in fact, owns the 100 bitcoin and that she intends to send them to Bob.

The confirmation process feels a bit like a sophisticated video game being played out in cyberspace with the constructive, real-world purpose of challenging the proposed invaders in the chain to ensure they are worthy and keeping the chain secure. Once a critical mass of nodes verify Alice's proposed transaction with Bob, their transaction goes into what is called the "memory pool," where it awaits final confirmation. Every so often, validator nodes group transactions waiting in the memory pool into a new "block" of transactions. The new block is then broadcast across the network in the same way that Alice's transaction with Bob was initially. This new block not only contains new proposed transactions (like that between Alice and Bob), but also cryptographic, timestamp summaries of all previous blocks; "timestamp" means the summary includes the times and details of all previous transactions, and "cryptographic" means that data is encrypted or scrambled, making it difficult for someone to deceive the validator nodes.

Validator nodes each independently verify the new block by running mathematical computations that, in essence, confirm two things: (1) that the transactions in the new block contain bitcoin that can be verified and unencumbered (i.e., that no one is trying to spend what they do not have), and (2) that the new block contains an accurate summary of each previous block in the chain (each transaction that led Alice and Bob to the point of Alice's proposal to transfer 100 bitcoin to Bob). If a proposed new block fails either of those tests, that version of the block will be rejected in favor of the first version approved by a consensus of nodes. In the end, only a block accepted by a consensus of nodes

prevails.[14] Once a new block is adopted across the network as the official block of new transactions, future blocks are built on top of it, because they too must contain an accurate, encrypted summary of this new block, meaning that the chain is verifiable and secure for both past and future blocks.

In sum, "cryptography ensures that all computers in the network have a constantly updated and *verified* record of all transactions within the Bitcoin network, which prevents double-spending and fraud."[15]

C. E-Currency, Smart Contracts, and Much More

Bitcoin emerged as the first cryptocurrency in 2008, but many cryptocurrencies have been "minted" in Bitcoin's image since then. As noted above, there were more than 1,500 cryptocurrencies in existence as of April 2018,[16] with many more planned for release soon.[17] Although some cryptocurrencies, including Bitcoin, leverage blockchain technology simply as a digital-payment system, others have put forward brilliant, innovative uses for the blockchain.

For instance, in 2013, a then-19-year-old programmer named Vitalik Buterin released a white paper proposing the Ethereum protocol.[18] Ethereum, like Bitcoin, is an open-source, distributed ledger.[19] But in addition to allowing users to exchange cryptocurrency tokens (called "ether"), Ethereum also permits the creation and implementation of so-called "smart contracts." First discussed in 1996,[20] smart contracts enable parties to create transactions that self-execute once certain predetermined conditions are met. Smart contracts have been proposed as a way to, among other things, (1) transfer title to real or personal property once a party transmits an agreed-upon sum of money,[21] (2) impose a lien when a car owner or mortgagee fails to make a monthly loan payment,[22] and even (3) distribute an estate's assets upon the death of the testator.[23] Smart contracts thus have the potential to eliminate the need for escrow companies and even to replace altogether other third-party fiduciaries, such as executors and trustees. Imagine that. After all, why pay someone to do what a computer can be programmed to do automatically once certain specified conditions are met (for a fraction of the price)?

Applications of the blockchain are also predicted to go far beyond mere contracts. Some believe the blockchain can make "unhackable" electronic voting in political elections possible;[24] which would enable voters to trust the voting process, and subsequently audit votes for fraud.[25] Others have suggested using a blockchain to maintain databases of records, such as those maintained by a DMV,[26] a county recorder's office,[27] and even hospitals.[28] The list of ideas for blockchain uses goes on[29] and on.[30]

If these proposed uses for blockchain do not excite the imagination, consider that it likely took some time to imagine the highest and best uses for the Internet, too. Cryptocurrency itself is a prime example of a new use for the Internet that was probably not readily apparent when the Internet was created, or even when Jeff Bezos had the radical and implausible notion of selling books online. Ultimately, many believe the potential for the blockchain is enormous, and that the most profound uses may not yet have been conceived.

In sum, the blockchain is being heralded as a revelation and the hype about it is growing, both among investors and businesses seeking to leverage the blockchain.

D. Crypto Values and Blockchain Usage Soar in 2017

As more users have come to understand the potential of blockchain technologies, the values of uses that leverage the blockchain have risen. The value of crypto in particular has swelled rapidly over the last year. The market capitalization of all cryptocurrencies (i.e., the total value of all cryptocurrency tokens multiplied by the number of those tokens in circulation) has exploded from just over $8 billion on April 1, 2016,[31] to more than $250 billion as of April 1, 2018.[32]

The number of people and businesses using cryptocurrency also has grown substantially over that timespan. In May 2017, a study by the University of Cambridge estimated that there were between 2.9 million and 5.8 million people actively trading crypto, and that there were between 5.8 million and 11.5 million "wallets," i.e., accounts that hold crypto.[33] The disparity between users and wallets is due to the fact that a single user can create and use multiple wallets. As of April 1, 2018, there were just shy of 24 million blockchain wallet users.[34]

Household investors are not the only ones captivated by the blockchain. One recent study found that 57% of large companies (i.e., those with more than 20,000 employees) are considering the deployment of their own blockchain solutions. That same study found that two-thirds of companies said they expected to integrate blockchain technology into their systems by the end of 2018.[35] An August 2017 news article noted that there are already more than 50 hedge funds dedicated to investing in cryptocurrency.[36] We have transcended the realm where Bitcoin is considered merely a cypherpunk[37] fad or a Ponzi scheme.

E. Benefits of Cryptocurrencies

As the primary focus of this article is on cryptocurrency, the discussion of benefits and risks will center on it, as opposed to blockchain technologies generally.

The benefits of a distributed-ledger system, like that employed by Bitcoin, are manifold. Decentralization eliminates the need for third-party trust companies and allows users to transact directly. Both parties save time and money. A wire transaction from one domestic bank account to another might take days to clear, while incurring significant fees. Someone can typically send crypto across the world in a fraction of that time—sometimes almost instantaneously—for a modest fee. Crypto can also be sent outside traditional banking hours, like at four in the morning, on a Sunday, or on a holiday.

Furthermore, decentralized ledgers also offer transparency and neutrality. As one source remarked of Bitcoin, which is true of public, decentralized ledgers generally:

> All information concerning the Bitcoin money supply is readily available on the block chain for anybody to verify and use in real-time. No individual or organization can control or manipulate the Bitcoin protocol because it is cryptographically secure. This allows the core of Bitcoin to be trusted for being completely neutral, transparent and predictable.[38]

Decentralized ledgers are also relatively resistant to traditional forms of hacking because they employ the consensus of thousands of nodes to thwart attacks. As Bitcoin's mysterious founder, Satoshi Nakamoto, explained, a cyberattack against Bitcoin will fail "[a]s long as a majority of CPU power [supporting Bitcoin] is controlled by nodes that are not cooperating to attack the network."[39] Decentralization is generally viewed as a major step forward in cybersecurity because it increases the number of systems that must fail before a cyberattack can succeed.[40] Hackers have recently perpetrated massive data breaches at companies like Target[41] and Equifax,[42] demonstrating inherent vulnerabilities in centralized systems that may be mitigated by a move to a decentralized system.

For all these reasons and more, decentralized ledgers have been called "transformative."[43] While the realization of trustworthy digital currencies is significant in its own right, many commentators have equated the blockchain's arrival with the advent of the steam engine, electricity, and the Internet.[44] The "age of decentralization" may very well be upon us.

F. Risks of Cryptocurrencies

First and foremost, Bitcoin and other cryptocurrencies have generally experienced tremendous volatility compared to other investments. Many commentators have analyzed cryptocurrencies by comparing their volatility and average returns with those of more traditional equities. One author found, for instance, that "Bitcoin's volatility has generally been about five to ten times that of [the S&P 500 index, SPY] but has been declining over time."[45] He also found that Bitcoin's "relative volatility, while experiencing some variation, has overall remained quite steady at about 5 times that of [gold]." As another article notes, "[e]xplanations for cryptocurrency volatility abound—perhaps its market thinness, bubble dynamics, difficulty of pricing, uncertainty, hoarding, frenzies around initial coin offerings or something else."[46] Regardless of the reasons behind the volatility, it is critical for potential investors to understand that meteoric rises in cryptocurrency values are often followed by significant retracements. Indeed, the explosion in values of various cryptos in 2017 (which, for instance, saw the price of Bitcoin rise from around $1000 on January 1, 2017, to nearly $20,000 by mid-December), was followed by a brutal retracement in 2018, during which many cryptos fell to less than a third of their December 2017 values. In short, crypto has proven to be incredibly volatile.

Second, many cryptos are, in all likelihood, scams. Cryptos are currently operating in a largely unregulated market, similar to the way that American securities operated before Congress enacted blue-sky and federal-securities laws. Thankfully, this lack of oversight is beginning to change. The SEC has already brought actions against several companies that raised money through initial coin offerings, or "ICOs," which are essentially initial public offerings for new cryptos.[47] In tandem with SEC proceedings, individuals have also begun filing class-action and other lawsuits against purported crypto fraudsters.[48] Countries and international organizations alike have signaled their intent to regulate cryptos.[49] Unfortunately, there is no simple test one can conduct to determine whether a particular cryptocurrency is legitimate. However, one must still conduct due diligence on that front before investing. Section IV of this article identifies strategies for that process.

Third, despite their resilience against some forms of hacking, cryptocurrencies and companies that support them have experienced devastating cyberattacks.[50] Some of these attacks targeted exchanges and cryptocurrency-wallet companies, resulting in hundreds of millions of dollars in cryptocurrency being stolen. For instance, Mt. Gox, a Japan-based exchange that at one point accounted for as much as 70% of bitcoin trading volume, was the victim of a major cyberattack in 2014 that looted almost 850,000 bitcoin from its users.[51] Another infamous hack was perpetrated in 2016 against the "DAO," a decentralized autonomous organization that served as an investment vehicle for ether holders.[52] There also have been run-of-the-mill cyberattacks and scams perpetrated against individual crypto holders, such as so-called "phishing" scams.[53] One recent crypto-related scam involved people creating social-media accounts and impersonating thought leaders, like Vitalik

Buterin, and encouraging others to send them crypto.[54] Further, although it would take a tremendous amount of coordination and financing to overwhelm something like Bitcoin's consensus-based defenses against hackers, several authors have pointed out that state-sponsored cyberattacks (like the one North Korea is suspected to have perpetrated against Sony[55]) against one or more cryptos are well within the realm of possibility. Some commentators are already reporting links between states and crypto cyberattacks.[56]

Lastly, cryptocurrencies and the blockchain are still-developing technologies, meaning it is not possible to know all the risks involved.[57] As Donald Rumsfeld put it, "there are things we do not know we don't know." Especially considering many blockchain technologies are open-source, it is conceivable that a user might find a way to exploit vulnerabiilites in that source code in the future. Unless and until regulation can provide comprehensive law and order, bad actors will have opportunities to exploit weak points. Even though those weaknesses may not be fatal, successful attacks (and responses thereto) can dramatically impact a cryptocurrency's value.

In sum, cryptos—and blockchain technologies generally—are not without legitimate risks.

III. HOW PEOPLE INVEST IN CRYPTOCURRENCY AND OTHER BLOCKCHAIN TECHNOLOGIES

Nobody can be certain where the values of Bitcoin and other blockchain technologies are headed. A September 7, 2017 news article noted that Bitcoin had risen sevenfold in value since Warren Buffett called it a "mirage" in 2014.[58] Jamie Dimon, JPMorgan's chairman, president, and chief executive, called Bitcoin a "fraud" on September 19, 2017. Bitcoin then reached a new all-time high of more than $5,800 per bitcoin during the second week of October 2017 before rocketing up to nearly $20,000 in December 2017. As of April 2018, Bitcoin had been declared dead in one form or another over 275 times since 2010.[59] "And yet it moves," Galileo might say.

A. Buying and Selling Crypto is Not the Only Option

While trading cryptocurrencies is perhaps the most common way to invest in blockchain technology, it is important to recognize that one need not buy and sell crypto to gain exposure to blockchain technology.

The focus of this article is on how to buy and sell cryptocurrency, but investors generally and fiduciaries in particular should consider that other, potentially less risky ways of riding the blockchain wave are available to them. For example, one can invest in companies that serve blockchain technologies, such as companies that manufacture computer processors. Bitcoin and many other blockchains require significant computing power, hardware, and electricity to verify transactions and support the networks.[60] Profits from crypto mining have thus been linked with modest increases in sales and profits for some computer-hardware manufacturers.[61] [62] Alternatively, one can buy securities of publicly traded companies (like the Bitcoin Investment Trust (NYSE: GBTC)) that offer indirect ownership of bitcoin and other cryptos.[63] One might also decide to invest in companies that are developing ways to leverage the blockchain, like Microsoft, which was recently reported to be a leader in blockchain research and development.[64] Some commentators even believe governments are on the verge of sanctioning exchange-traded funds for crypto, although that remains to be seen.[65]

B. How to Buy and Sell Crypto

It is generally quicker and easier to create and fund a crypto-trading account than a brokerage account for trading stocks and other equities. Assuming one has done his or her due diligence (more on that in Section IV) and has decided which cryptocurrencies to buy or sell, the following is a general description of how one actually trades crypto, like bitcoin and ether.

1. Open an Account on a Cryptocurrency-Trading Platform ("Exchange")

There are many online crypto "exchanges" where one can buy and sell crypto.[66] Some exchanges, like Coinbase.com, require somewhat-detailed personal information to open a crypto-trading account. Others are more lax in the amount of personal information they demand from a user. Because some users consider privacy to be a pillar of cryptocurrency, some exchanges pay homage to that principle by helping users remain pseudonymous. On the other hand, exchanges that require personal information generally do so to remain compliant with laws governing entities like banks and other financial institutions, which typically require details about account holders' identities. To each their own, and until a law or judicial decision outlaws certain exchanges, one can generally use whichever type of exchange one prefers.

Exchanges differ in the types of crypto they allow users to trade. For instance, Coinbase.com currently allows users to trade only four types of crypto: bitcoin, bitcoin cash, ether, and litecoin. Other exchanges, such as Bittrex.com and Poloniex.com, allow users to trade dozens of so-called "alt-coins"[67] in addition to bitcoin. Many traders opt to open accounts on several exchanges and move funds between exchanges depending on which types of crypto they want to buy or sell.

Deciding which cryptocurrencies one wants to buy or sell will largely drive which exchange to use. If someone wants to buy or sell one of the 1,500-plus alt-coins in existence, the buyer or seller will need to set up an account on an exchange that permits trading of the desired alt-coin. If the buyer or seller just wants to trade bitcoin, the buyer or seller can make an account on Coinbase.com, which many consider to be the most-widely-used and user-friendly exchange in the United States (although it is limited in the types of trades and cryptocurrencies it supports).[68] An easy way to figure out which exchanges support the desired crypto is to refer to Livecoinwatch.com, which provides information about most major cryptocurrencies in existence, including on which exchanges one can buy and sell them.

Once an investor has identified the exchanges that carry the desired cryptocurrency, the investor can examine those exchanges for ease of use and security.[69] It is important to pay particular attention to whether the exchange has had any major security breaches or other safety concerns. Some exchanges have notoriously unresponsive customer-support teams. As discussed above, some exchanges have been hacked and their users' accounts pillaged. Some exchanges (including Coinbase.com) insure their users' deposits against various risks of loss, adding an additional layer of safety to consider.[70] Trustees would do well to select an exchange with security as a paramount consideration.

2. Deposit/Transfer Funds into an Exchange "Wallet"

Not all exchanges allow funding an account in the same way. Some exchanges permit funding an account by wiring fiat money (e.g., dollars) from bank accounts. Some allow crypto to be purchased directly with credit cards. Some do both. Some do not support fiat currencies at all; instead, they only allow trading of crypto, which means one must first convert fiat to crypto on another exchange, and then transfer that crypto to the exchange that supports the desired type of crypto.[71]

Exchange accounts generally have different "wallets" for each type of crypto. An account on Coinbase.com, for instance, has five wallets: one for each of four cryptos (bitcoin, bitcoin cash, ether, litecoin), and one for dollars. Some exchanges have multiple wallets for each type of crypto; Bittrex.com, for example, offers a funding wallet, an exchange wallet, and a margin wallet for each kind of crypto it carries. Many investors might not need multiple wallets for each kind of crypto, but there are scenarios where it can be helpful.

When sending crypto (e.g., from one exchange to another), it is imperative to do two things. First, ensure the recipient's wallet address has been typed or copied verbatim; an error in the recipient address will likely cause coins to be sent to another person's account, where they cannot be retrieved without that person's consent. Second, send to a recipient wallet only the kind of crypto that wallet is set up to receive, because a wallet for a particular cryptocurrency can only send and receive that kind of cryptocurrency. In other words, a bitcoin wallet can only send and receive bitcoin, and a litecoin wallet can only send and receive litecoin. Sending one kind of crypto to a wallet for another kind of crypto may cause those funds to disappear with limited possibilities for recovery.

Great care should be taken to avoid these two missteps, particularly when transferring large amounts of funds. The possibility can be minimized by first completing a test transfer of a small amount of crypto. Once the first transfer is confirmed, the remaining balance can be sent with confidence.

3. Trade Cryptocurrency Like Stocks

Once an exchange wallet is funded, its owner is ready to enter buy and sell orders, just as with an ordinary brokerage account for equities. Most exchanges allow entry of market orders, which buy or sell a currency at the current market price. Some exchanges also allow entry of limit orders, which only fill at a specified price and assuming there is a buyer/seller willing to trade at that price. Depending on the particular trade desired, the going price of a crypto might be shown in fiat or crypto. Some exchanges even permit buying and selling crypto options, although only highly experienced traders should consider such a risky investment. Keep in mind that all orders, once they go through, are final.

Depending on what kind of crypto is being bought or sold, and in what amount, transactions may take some time to be confirmed. Crypto trades are fast, but not always instantaneous. For instance, Bitcoin confirms a new block of transactions about every ten minutes.[72] But a proposed Bitcoin transaction is not always immediately included in the next block. Parties to a crypto transaction can sometimes incentivize miners or validators to validate their transaction more quickly by offering to pay transaction fees in addition to bounties miners already receive. If time is not of the essence, parties may wait a while until their transaction is confirmed.

4. Move Crypto to a Safe Location (e.g., a Hardware or "Cold Storage" Wallet)

As hackers have been known to raid exchange accounts, experts recommend removing crypto holdings from exchange wallets and transferring them into a safer form of storage. So-called "cold wallets" or "cold storage," i.e., wallets that do not have a "hot" Internet connection and are therefore inaccessible to would-be hackers, are a best practice. Similarly, "hardware wallets" require two-step authentication with an external device, without which one cannot access their crypto. Protecting crypto via a hardware or cold-storage wallet is a no brainer, and a trustee's failure to use them or a similar mechanism to protect crypto assets may be viewed as careless—as would storing a trust's gold bars in an unsecured office drawer. Trustees holding crypto must take reasonable steps to protect them (more on that in Section IV), and should therefore investigate their options.

In addition to employing a hardware or cold-storage wallet, one should keep that storage device somewhere safe. Hiding a cold-storage wallet under a pile of papers at work might keep it safe from online hackers, but it will not protect crypto from old-fashioned thieves. Storing a cold-storage wallet under a mattress might seem safer, but a prudent investor would probably store a cold wallet somewhere more secure, such as a fire safe or safe-deposit box at a bank. Reading a few horror stories of lost or stolen crypto will show added caution is well worth the extra time and effort—particularly where someone (like a trustee) owes fiduciary duties to safeguard those assets.

5. Move Crypto Back to Exchange Wallet to Sell—Or Save and Use

Although internet communities, such as the one on Reddit. com/r/bitcoin, joke about "hodling"[73] [sic] crypto indefinitely, there will likely come a time for a crypto holder to sell some or all of his holdings. To do so, the holder simply transfers the crypto from storage back to an exchange wallet and then enters a sell order (either for fiat currency or another kind of crypto which can then be converted into fiat). If the exchange permits fiat withdrawals, the fiat can be cashed out by transferring it to a bank account. If the exchange does not support fiat withdrawals, the holdings will have to be transferred to an exchange that does. Coinbase.com, for example, lets users sell their crypto for dollars and then withdraw those dollars to a bank account.

Keep in mind that some exchanges only allow cashing out limited amounts of fiat at a time. If a large number of users suddenly wanted to sell their crypto for fiat and withdraw that money, for example in the case of a crypto-market crash, the exchange might not be able to fill all withdrawal requests. In the same way a run on banks during the Great Depression led many banks to run out of cash. A wise crypto owner should plan accordingly to be sure he or she is not left holding the proverbial bag.

Alternatively, if a crypto holder believes (as many do) that more businesses, institutions, and individuals will continue to adopt crypto as a payment system, she can save her crypto to purchase her next Lamborghini,[74] or perhaps even a parcel of real estate from a forward-thinking seller.[75] Bear in mind that, pursuant to IRS Notice 2014-21, using crypto to buy anything from a cup of coffee to a mansion can generate taxable gains or losses.[76]

IV. HOW CAN A TRUSTEE INVEST "PRUDENTLY" IN CRYPTOCURRENCY?

With this background, why would a prudent fiduciary even consider investing in cryptocurrency? The "unhackable" technology has been the victim of terrible hacks. It is complicated to understand and, therefore, difficult to explain—especially if a fiduciary is trying to justify a crypto investment after a problem related to that investment has arisen, such as an attack by hackers or a change in value during a downturn in the volatile market.

The authors believe that cryptos and blockchain eventually will be akin to other forms of new technologies and investments that became a part of our daily lives, and could no longer be brushed aside as only for geeks, or at least only something our kids could grasp. In time, trustees will inherit cryptos in their trust portfolios and will have to make prudent investment decisions, not ones based solely on the fear of holding an asset we do not understand. Soon, people will be investing indirectly in cryptos and blockchains as more hedge funds and companies take the plunge. In relatively short order, we believe investment managers will recommend cryptos due to the untapped growth potential in the same way that it became difficult to avoid tech stocks during their boom as part of a diversified portfolio. It will become important for trustees to have some understanding of this brave new world, whether the trustee then decides to invest in or to avoid cryptocurrency. Below, we offer some guidance in the framework of the familiar prudent investor rules to those trustees who confront the question to invest or not to invest.

A. Laws Governing California Trustees

There is, of course, nothing that prohibits a trustee from investing in crypto *per se*. Trustees generally enjoy broad discretion to invest in any type of property. California's version of the Uniform Prudent Investor Act (the "CUPIA"), codified at Sections 16045[77] *et seq.*, provides that "a trustee may invest in any kind of property or type of investment or engage in any course of action or investment strategy consistent with"

the CUPIA.[78] Generally speaking, a trustee must invest as a reasonable, prudent person would.[79] The CUPIA obligates trustees to invest "trust assets as a prudent investor would, by considering the purposes, terms, distribution requirements, and other circumstances of the trust."[80] "In satisfying this standard, the trustee shall exercise reasonable care, skill, and caution."[81] Additionally, the CUPIA identifies eight other specific factors as being "among the circumstances that are appropriate to consider in investing and managing trust assets:"

(1) General economic conditions;

(2) The possible effect of inflation or deflation;

(3) The expected tax consequences of investment decisions or strategies;

(4) The role that each investment or course of action plays within the overall trust portfolio;

(5) The expected total return from income and the appreciation of capital;

(6) Other resources of the beneficiaries known to the trustee as determined from information provided by the beneficiaries;

(7) Needs for liquidity, regularity of income, and preservation or appreciation of capital; and

(8) An asset's special relationship or special value, if any, to the purposes of the trust or to one or more of the beneficiaries.[82]

Trustees must make reasonable efforts to "ascertain facts relevant to the investment and management of trust assets," which include the considerations listed above, as well as any others that might bear on the particular trust, investment or management decisions at hand.[83]

Lastly, compliance with the CUPIA is judged "not by hindsight" but rather "in light of the facts and circumstances existing at the time of a trustee's decision or action."[84] Thus, trustee liability for an investment decision does not turn on how well or poorly the investment performs; rather, it turns on what a reasonably prudent person in the trustee's position would have known and done in similar circumstances. Furthermore, the CUPIA adopts the approach espoused by modern portfolio theory, which evaluates prudence of investment decisions on a portfolio-wide basis, as opposed to evaluating individual investments in isolation.[85]

Applying these rules in the context of cryptocurrencies raises many important issues for California fiduciaries.

B. Step One: A Prudent Process of Gathering Information is Paramount

What does the CUPIA require of trustees who want to invest in crypto and other investments leveraging the blockchain? And perhaps more importantly, how will investments in crypto be evaluated if challenged in court? The court's role is not to evaluate whether the decision turned out to be a good one, but whether the process in making the decision was sound. At a minimum, a trustee must demonstrate, and preferably document, a cogent, prudent thought process that led to the ultimate investment decision. The trustee should be able to explain how the decision to invest in blockchain technology generally was a wise choice, and why the particular crypto or other assets invested in were sensible options. The following discusses what that decisional process should entail.

1. Consider the Purposes, Terms, Distribution Requirements and Other Circumstances of the Trust

First and foremost, a trustee's decision-making process must demonstrate that due consideration was given to the factors identified in Section 16047(a)—i.e., "the purposes, terms, distribution requirements and other circumstances of the trust."[86] Of course, a trustee should review the terms and apparent purposes of the trust to see whether investing in crypto is appropriate. While it is unlikely that an instrument would mention crypto specifically, it might indicate the appropriate level of risk that it is prudent for the trustee to accept. Indeed, it might even waive the CUPIA in favor of broad discretion when the trustee makes investment decisions, and absolve the trustee of liability to the full extent of California law (i.e., except for gross negligence, bad faith and reckless indifference). The trust instrument may specifically authorize the trustee to hold certain assets that exist in the portfolio with the same absolution. Even so, the authors believe that slavish adherence to a waiver of diversification may well be gross negligence or reckless indifference. In the authors' view, trustees still must evaluate periodically whether it is reasonable to continue to hold or invest in cryptos notwithstanding these types of trust provisions. With respect to distribution requirements, an investment in crypto is less likely to be deemed prudent where there will be a need for regular distributions: crypto's volatility makes it difficult to forecast reliably when liquidation will be prudent, and crypto generally[87] pays no dividends. If there will be no need for distributions for years (or longer), speculating greater amounts in crypto might be deemed less problematic.

2. Evaluate the Eight Additional Factors Identified in Section 16047(c)

Trustees also must evaluate the eight factors listed in Section 16047(c)(1)–(8). Without exhaustively drilling down on each topic, a brief review of how these factors might play a role when investing in crypto is appropriate.

a. General Economic Conditions and the Possible Effect of Inflation or Deflation

General economic conditions, including inflation or deflation, might cut against the prudence of investing in crypto when the market is booming. If an investment in a standard S&P 500 index fund can generate returns of 15% annually, a prudent trustee might opt for such an investment over a much riskier investment in crypto. On the other hand, crypto has seen a boom in places like Venezuela because hyperinflation and poor market returns have made holding fiat currency a losing proposition.[88] Some commentators even have made compelling arguments that crypto might be a useful hedge against a downturn in the market, particularly as investors become increasingly concerned that equities are overpriced and the market is overheated. The reasons for this are that (1) crypto is "non-correlating," meaning that it exists as an investment whose performance is not correlated with other types of investments, like stocks and bonds, and (2) crypto may even become a substitute for gold, which is traditionally counter-cyclical during a recession, when investors traditionally move investments from equities to commodities like gold that are perceived to be difficult to manipulate by central authorities.[89]

b. Expected Tax Consequences

Tax consequences also should factor into the decisional calculus. The IRS is taking a hard look at crypto. The IRS has expressed concern that crypto transactions are occurring in ways that are difficult for taxing authorities to detect, so the IRS is taking aggressive measures to gain access to information about trading activity to tax that activity.[90] In March 2014, the IRS released Notice 2014-21, which announced that "virtual currencies" would be treated for tax purposes not as actual currency, but instead as property.[91] As a Forbes article observed,

> [IRS Notice 2014-21] further stated, "General tax principles that apply to property transactions apply to transactions using virtual currency." In other words, the IRS is treating virtual currency, such as Bitcoin, as a capital asset, with the income or gains from the sale subject to either short-term (ordinary income tax rates) or long-term capital gains tax rates, if the asset is held greater than twelve months (15% or 20% tax rates based on income).[92]

The full extent of tax laws and considerations that might apply to crypto investments is beyond the scope of this article, so a trustee should consult with an attorney well versed in these issues before proceeding.[93] The tax treatment of cryptos appears to be similar to other securities and should be evaluated in the same vein in making decisions about investing in it.

As one example of the potential tax risks with crypto, consider that many investors who bought and sold crypto as prices skyrocketed in 2017 were left owing a hefty tax bill. When crypto prices plummeted at the start of 2018, many investors had tax bills that far outstripped the current value of their crypto. Some were even forced to liquidate their holdings at significant losses just to cover the taxes on gains they theoretically realized in 2017, even though the amount of fiat they ever held remained unchanged. If a trustee were to make the same mistake, the liability could be tremendous.

c. The Role That Each Investment or Course of Action Plays within the Overall Trust Portfolio

The CUPIA evaluates prudence of individual investment decisions by looking at the trust portfolio as a whole.[94] Thus, trustees must ensure that their investment strategies "hav[e] risk and return objectives reasonably suited to the trust."[95] Suitability of an investment to the trust will require examining not only the investment's risk/reward, but also the beneficiaries' needs for liquidity, regularity of income, and preservation or appreciation of capital. For instance, if a trust is held for the benefit of a retired couple, investing large portions of the estate in volatile cryptocurrency is less likely to be seen as prudent, because retirees typically prioritize regular income and principal protection in their investments. On the other hand, if the trust will not need to make distributions to beneficiaries for decades, and the beneficiaries are independently wealthy, larger investments in assets with greater risk and reward, like crypto, might be justified. Cryptos are more suitable for trusts with a significant tolerance for risk.

d. An Asset's Special Relationship or Special Value, if any, to the Purposes of the Trust or to the Beneficiaries.

Typically, an asset with a "special relationship or special value" would include things like land used in a family farming operation, assets or shares of a family business, or shares of stock that represent or influence control of a closely or publicly held corporation.[96] Absent a specific direction in the trust to hold crypto, or the trustor's own involvement or relationship with the crypto in question, it is not the type of asset that would generally be considered as an asset with a special relationship or value. Still, a trustee should be prepared to explain why the crypto at issue has a special value, including by pointing to steps the trustee took to evaluate (1) whether the assets have special value, and (2) what benefits or risks were posed by retaining those assets.

3. Do a Deep-Dive on the Particular Blockchain Investments Being Considered

In addition to demonstrating a reasonable evaluation of the statutorily prescribed factors in the CUPIA, a trustee also should be prepared to show the research supporting the trustee's investment in particular cryptocurrencies. Many observers liken the hype surrounding crypto to the dot-com craze of the 1990s, where "[i]nvestors poured money into Internet startups . . . in the hope that those companies would one day become profitable."[97] Just like many of those internet startups were scams that left many investors holding worthless assets, evidence is mounting that many cryptocurrencies are doing the same.[98] Even if they are not outright scams, many cryptocurrencies provide little to no improvements over their competitors, making claims that they will provide solid returns dubious, at best.

To that end, trustees need to take steps to learn some basic information about the cryptocurrencies in which they are considering investing. The following is a useful checklist of topics and problems that trustees should consider when evaluating an investment in cryptocurrencies:

1. **The Problem.** Cryptocurrencies—like all businesses—need to solve a problem to have value. What problem is this cryptocurrency/blockchain technology addressing? Why is it important to solve this problem?
2. **The Solution.** What is the proposed solution to the problem? Are there other solutions to the problem? Why is this particular solution better than others at addressing the problem? Can the solution be described in plain language? Is this solution already live and usable?
3. **The Team.** Who is on the management team? Can the management team implement this solution? Why are they qualified to implement this particular solution and deliver it to market? What is missing from their team? How "hungry" is the management team?
4. **The Market.** Who will be the user-customers? How large is that market? Is it large enough to support substantial growth? How will they target customers to use their product? What do people use now? Why will people start using this product?
5. **The Competition.** Are there existing competitors in this market? How is this product differentiated from those offered by competitors? Why is their value proposition unique? Are there barriers to entry that will make it difficult for new competitors to enter the market? How will this team respond to new entrants?
6. **The Business.** What is the business plan? Why hasn't this product been offered before? How much money do they plan to raise? When do they need this money? Why do they need this money, and how exactly will this money be spent? How quickly can this be implemented?
7. **The Return.** How will investors see a return on their investments? What type of growth is expected, and on what factors is that estimate based?
8. **Transparency.** How transparent is the management team? Has anyone ever seen their product? Is it clear how their product will work or is it vaporware (i.e., advertised but not yet available)? Do they have a github page where people can go and check their code, smart contracts, etc.? Does the team have a Slack channel where it is possible to go and talk to members of the team? How responsive is the management team?
9. **Likelihood of Critical Mass.** Does this product have the potential to achieve critical mass? Can it achieve enough of a user base to create a moat against competitors?[99]

While compiling answers to these questions may seem arduous, it will be time well spent. Not only will the increased knowledge likely give the trustee an advantage as an investor, it will also protect the trustee if the decisions are challenged. The more time the trustee spends investigating—and documenting the investigations of—these factors, the stronger the case against imprudence will be.

Lastly, in addition to exploring these questions, one would be wise to heed the suggestions of Angela Walch, J.D., whose article providing guidance to policymakers about how to approach regulating cryptocurrencies can similarly guide trustees. Ms. Walch makes two overarching recommendations.[100]

First, she recommends learning everything one can about blockchain technology. One can cultivate expertise through self-study and by consulting experts, such as consulting firms, academics, companies, and attorneys operating in the blockchain industry. There is a rapidly growing body of literature, both academic and practical, relating to blockchain technologies. There are also reputable news sites, like Coindesk.com, that report on current events in the blockchain space. Take advantage of these resources and document the research.

Second, Walch underscores the importance of adopting a critical mindset in this education process. It is important to separate misleading hype, whether intentionally or unintentionally misleading, from reality. Consider the source of the information, including whether the writers are qualified and reliable, or self-interested. Do not take any claims—particularly those from people poised to benefit from an investment—at face value, and instead investigate them critically. Seek diverse perspectives by consulting a variety of sources about a particular investment. Approach this education with a skeptical mindset about the alleged limitless potentials and minor risks involved with the potential blockchain investment.

Walch notes in the context of policymakers that "[t]aking a slow, inquisitive, and deliberative approach is in tension with the need to quickly get up to speed on the technology to ensure that imminent risks are identified and addressed efficiently."[101] This is surely true for both policymakers and trustees—neither of whom should rush their education on this subject. While a policymaker's failure to grasp fully the risks associated with blockchain technology might lead to sloppy laws or regulations, it will not lead to personal liability for that policymaker. Trustees are not so lucky, and should therefore take a particularly deliberative and cautious approach to ensuring they fully understand the crypto and other blockchain assets in which they are investing for the benefit of their beneficiaries.

C. Step Two: Manage Risk

1. Diversify, Diversify, Diversify

Diversifying a trust portfolio is imperative to managing risk and minimizing potential liability, even though the investment market in 2008 demonstrated that even the most diversified portfolios are not immune from suffering substantial losses. The CUPIA provides that "a trustee has a duty to diversify the investments of the trust unless, under the circumstances, it is prudent not to do so."[102] There are certainly conceivable scenarios where not diversifying would be prudent, but a trustee will struggle to defend missteps without it; diversification is simply too well established as a means of diminishing risk in investing.[103]

When evaluating whether crypto fits within a diversified portfolio, one might ask how much diversification is enough to justify holding assets that are potentially more volatile on the risk and reward spectrum. Neither the CUPIA nor case law defines what an unreasonably concentrated investment is, or what proper diversification is. "There is no automatic rule for identifying how much diversification is enough."[104] As the Restatement (Third) of Trusts explains, "[s]ignificant diversification advantages can be achieved with a modest number of well-selected securities representing different industries and having other differences in their qualities. . . . The ultimate goal of diversification would be to achieve a portfolio with only the rewarded or 'market' element of the risk."[105] Understanding what proper diversification means requires a brief foray into investment and economic theory. As one author succinctly explained,

> A fundamental tenet of [Modern Portfolio Theory ("MPT")] is the premise that all investments, including U.S. Treasuries, may . . . not perform in the manner anticipated, a concept referred to as 'risk.' Every investment faces internal and external factors that give rise to risk. . . .To reduce the risk that a single market event will substantially impact the investor's net worth, an investor should diversify by purchasing investments that move in different directions as market conditions change. . . . To reduce risk, an investor should invest in a wide range of stocks and even in different asset classes that move in different directions as various external market changes occur. In MPT parlance, investors should acquire investments that have negative or low correlations to each other. By purchasing assets with negative or low correlations to each other, an investor can substantially reduce the risk associated with a specific investment.[106]

Essentially, a trustee who does not diversify is taking on "uncompensated" risk, i.e., additional risk for which there is no additional compensation. If hypothetical asset A is riskier than hypothetical asset B, MPT posits that a prudent investor should demand greater compensation for investing in asset A. Concentrated investments in a single asset entail greater risk without concomitant greater returns, which a prudent investor would not tolerate. Thus, MPT requires a prudent trustee to minimize uncompensated risk, also known as "diversifiable risk," because it can be diminished simply by diversifying

holdings. In the context of cryptocurrency, diversification can and should mean several things.

First, a trustee seeking to bolster the argument that the investments in crypto were prudent must offset those crypto holdings with less-risky, non-crypto holdings. Whether one opts for treasury bills, mutual funds, or index funds, there are a variety of investments available that carry substantially less risk and volatility than cryptocurrency, and which are likely to have low or negative correlations with crypto. Unless the trustee balances crypto holdings with non-correlated holdings of other assets, the trustee is taking on significant amounts of uncompensated risk. MPT says that is imprudent, meaning a court may conclude crypto investments to be imprudent, if the trustee does not balance the portfolio sufficiently with non-crypto investments.

As discussed above, commentators have been publishing analyses of the correlations among cryptocurrencies and between crypto and non-crypto investments.[107] Unsurprisingly, many major cryptocurrencies appear to be moderately correlated with one another, in a range "typical of publicly traded common stock."[108] However, data have shown very weak correlations between Bitcoin and other traditional investments, including gold, SPY (an S&P500 Exchange Traded Fund), and equities issued by Apple, Amazon, Google, and Facebook. While some cryptocurrencies were less correlated than others, the data suggest that proper diversification cannot be achieved by simply investing in a handful of cryptocurrencies—the correlation among cryptos is just too high.[109] Thus, a properly diversified portfolio must include a significant amount of non-correlated, non-crypto assets.

Second, along these same lines, a trustee should not invest in just one particular type of crypto. There are risks that pertain to each individual cryptocurrency, meaning that unless the trustee diversifies the crypto holdings, the trustee is taking on additional, uncompensated risk. For instance, when the DAO was hacked, the value of ether dropped by about half, but the prices of other cryptocurrencies were not impacted nearly as much.[110] As a result, a prudent investor would likely divide crypto-investment funds across multiple types of cryptocurrency. Instead of investing $10,000 of trust funds in bitcoin alone, a prudent investor would invest $2,500 in four different cryptocurrencies, or better yet, $1,000 in ten different cryptocurrencies. At the same time, dividing crypto funds among the 1,500-plus cryptos likely would not be prudent; instead, established flagship cryptos such as Bitcoin and Ethereum might reasonably make up a larger segment of one's portfolio than newer, less-established alt-coins.

Third and finally, trustees should consider subdividing funds they want to invest in blockchain technologies among both crypto and non-crypto assets. As discussed above, one can ride the blockchain wave by investing in companies that sell computer hardware to transaction validators, or companies that are finding ways to harness the power of blockchain. Although the correlations between most equities and crypto has not yet been examined comprehensively to these authors' knowledge, it seems likely that investments like these are likely to have a much lower correlation with bitcoin than, say, ether or litecoin.[111]

The more layers of diversification a trustee can create in a trust portfolio, the more likely that trustee is to survive scrutiny when a particular crypto investment goes poorly. Again, it is critical to highlight that blockchain investments including crypto should make up only as large a portion of the portfolio as is reasonable considering the makeup of the rest of the portfolio.

2. Do Not Forget about Inception Assets

Trustees need to be aware that their investment-related fiduciary duties apply to *all* assets under their control, including so-called "inception" assets (i.e., assets held by the trust before that trustee's involvement). Thus, if a successor trustee is appointed and learns that the trust has significant crypto assets, the trustee must promptly evaluate the prudence of those holdings and the needs for diversification. Section 16049 states that trustees must:

> within a reasonable time after accepting a trusteeship or receiving trust assets, review assets and make and implement decisions concerning the retention and disposition of assets, in order to bring the trust portfolio into compliance with the purposes, terms, distribution requirements, and other circumstances of the trust, and with the requirements of [the CUPIA].[112]

Although no California case has yet construed this statute, a leading article on the trustee's duty to diversify noted that, as of 2012, "[43] states and the District of Columbia [had] impose[d] upon . . . trustee[s] the duty to diversify all assets in the trust *regardless of who contributed or purchased the asset and regardless of when the trust was created*."[113] Thus, if a successor trustee takes office and learns that the sole asset of a trust is a million dollars' worth of bitcoin, the trustee should immediately evaluate how much bitcoin to liquidate and re-invest in other assets—just as the trustee should do for any other type of asset that was overrepresented in the trust portfolio. Trustees unable or unsure of how to get up to speed on this issue "within a reasonable time" should consult third-party professionals well

versed on the topic, to avoid potential liability for losses that occur shortly after they take office.

3. Take Reasonable Steps to Protect Crypto

Trustees also are charged with safekeeping trust assets and investments. To that end, trustees must "take reasonable steps under the circumstances to take and keep control of and to preserve trust property."[114] As discussed above in Section III(B)(4), the current best practice is to employ some form of cold or hardware storage and to protect that storage device like a gold bar.

D. Ensuring Access to Cryptocurrency

1. Problems with Access

The decentralized nature of crypto poses some unique issues with respect to custody of crypto assets.[115] Remember the story about the Australian man who threw away an old hard drive that contained the digital keys to nearly $10 million in bitcoin?[116] Fortunately, as if on cue, the California legislature recently laid the groundwork for providing trustees and other fiduciaries access to digital assets such as cryptocurrency.

2. The Solution: Revised Uniform Fiduciary Access to Digital Assets Act

In 2016, the California Legislature enacted the Revised Uniform Fiduciary Access to Digital Assets Act ("RUFADAA"). RUFADAA which "authorize[s] a decedent's personal representative or trustee to access and manage digital assets and electronic communications," and also enables people to "give directions to the custodian of his or her digital assets regarding the disclosure of those assets."[117] While "digital assets" covered by RUFADAA include any type of "electronic record in which an individual has a right or interest," such as Facebook photos and emails, they also include underlying assets or liabilities where "the asset or liability is itself an electronic record."[118] No court has yet ruled on this, but it seems likely that crypto would qualify as a "digital asset" under RUFADAA.

RUFADAA enables an individual (referred to as a "user") to grant fiduciaries access to their digital assets upon the user's death. RUFADAA does so by authorizing "custodians" of digital assets (e.g., third-party companies like Facebook or Gmail that host the content) to disclose to certain designated recipients "some or all of the user's digital assets."[119] Users may designate recipients using an "online tool," such as a preference setting on the custodian's website, or by stating their disclosure preferences in an estate planning instrument.[120]

A custodian is required to disclose and provide access to digital assets only where a fiduciary provides the custodian with three things: (1) a written request for disclosure, (2) a certified copy of the user's death certificate, and (3) a certified copy of the letter of appointment or a court order.[121] Moreover, a custodian can request that the fiduciary also provide any of the following items before granting the fiduciary access to a user's digital assets:

1. A number, username, address, or other unique subscriber or account identifier assigned by the custodian to identify the user's account;
2. Evidence linking the account to the user;
3. An affidavit stating that disclosure of the user's digital assets is reasonably necessary for estate administration; and
4. A court order finding either (a) that the user had a specific account with the custodian, identifiable by the username, number, or other account identifier, and (b) that disclosure of the user's digital assets is reasonably necessary for estate administration.[122]

What does RUFADAA require of those users seeking to give fiduciaries access to their crypto? At a minimum, it requires them to provide their username and password for exchanges or other wallets where they store crypto. If the user was smart enough to use cold storage, the user should provide instructions on where to locate the cold storage wallet and the passcode to access it. Keep in mind that providing someone with access to a crypto account will enable them to loot the funds, and they might not be recoverable. For that reason, a settlor should consider splitting up each account's password or "private key" among multiple people or locations, or only provide it to someone the settlor trusts.

V. CONCLUSION

The future is here. Trustees need to have an understanding of crypto and blockchain as these assets may be among inception assets that require their attention, or because they need to obtain access to and secure and control such assets. If the trend continues, and it seems it will, it also will be impossible to ignore crypto and the blockchain in making prudent investments whether to take advantage of the rewards they promise, or to hedge against non-correlated assets or market downturns. The authors hope this article will help trustees begin the education leading to the process of sound analysis, not only for managing risk in their portfolios, but responding to beneficiaries who challenge decisions of trustees buying and selling crypto.

* *Sheppard Mullin Richter & Hampton LLP, Los Angeles, California*

1 Information in this article is intended for educational purposes only. It should not be considered legal or financial advice. You should consult an attorney or other investment professional to determine what is best for your individual needs. The authors do not make any guarantee or other promise as to any results that may be obtained from using our content, or from websites or sources cited herein. No one should make any investment decision without first consulting his or her own financial advisor and conducting his or her own research and due diligence. To the maximum extent permitted by law, the authors disclaim all liability in the event that any information, commentary, analysis, opinions, advice and/or recommendations contained herein prove to be inaccurate, incomplete, or unreliable, or result in any investment or other losses.

2 See <https://www.gizmodo.com.au/2017/05/i-threw-away-4-8-million-in-bitcoin/> (as of May 31, 2018) (describing the story of the man who lost 1400 bitcoin that he purchased at approximately 1.5 cents each).

3 See <https://www.cnbc.com/2017/07/31/blockchain-technology-considered-by-57-percent-of-big-corporations-study.html> (as of May 31, 2018) (discussing businesses' plans for adoption of the blockchain).

4 Chohan, Usman W., Cryptocurrencies: A Brief Thematic Review (Aug. 4, 2017) p. 1 <https://ssrn.com/abstract=3024330> (as of May 31, 2018).

5 Walch, Angela, The Path of the Blockchain Lexicon (and the Law), *Review of Banking and Financial Law* (2016–2017) pp. 753–54 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2940335> (as of May 31, 2018).

6 The American Land Title Association estimates that "[a]pproximately 25% of all residential real estate transactions have issues with title" that must be resolved before closing. See Title Insurance: A Comprehensive Overview, p. 4 <https://www.alta.org/press/TitleInsuranceOverview.pdf> (as of May 31, 2018).

7 Celebrated programmer and innovator, Vitalik Buterin, wrote that "decentralization is often even viewed as a blockchain's entire raison d'être, but it is also one of the words that is perhaps defined the most poorly." As he clarifies, there are many ways that decentralization can take shape in a given blockchain. The discussion in this article is, by necessity, limited to an introduction to the core concept of decentralization. For a closer look at various types of decentralization, see Buterin, Vitalik, *The Meaning of Decentralization* (Feb. 6, 2017) Medium <https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274> (as of April 23, 2018).

8 Much ink has been spent to clarify that "immutable" is actually a misnomer. In fact, most blockchains provide for a ledger to be edited under certain circumstances (e.g., by consensus of the community of users). As one author remarked, "[i]n blockchains, there is no such thing as perfect immutability. The real question is: What are the conditions under which a particular blockchain can and cannot be changed? And do those conditions match the problem [that blockchain is] trying to solve?" See <https://www.coindesk.com/blockchain-immutability-myth/>; see also Walch, Angela, note 6, *ante* (discussing how imprecise language in discussions of blockchain technologies poses challenges to regulators and the public, and exploring use of the term "immutable" as an example of this).

9 See <https://blockchainatberkeley.blog/blockchains-cryptocurrencies-the-new-decentralized-economy-part-1-a-gentle-introduction-edcb4824b174> (as of May 31, 2018) (discussing cryptoeconomics).

10 For a fascinating introduction to the concept and implications of trustless transactions, blockchain thought leader and adjunct professor at Syracuse University Richie Etwaru gives an inspired TEDx talk that can be accessed at: <https://www.youtube.com/watch?v=k53LUZxUF50> (as of May 31, 2018).

11 While "Bitcoin" refers to the crypto known as "Bitcoin," the term "bitcoin" is used to signify the individual units of Bitcoin (such as, "he has 20 dollars in his wallet," as opposed to, "he is investing in the U.S. Dollar").

12 The double-spending problem is the risk of someone spending the same digital currency in more than one transaction. Fiat currencies are generally difficult to counterfeit, but for years, it was relatively easy to double-spend digital currency by simply copying the underlying data file for the digital currency and sending them to multiple recipients. See <http://www.investopedia.com/terms/d/doublespending.asp> (as of May 31, 2018) (defining the double-spending problem and generally reviewing Bitcoin's approach to solving it).

13 Khan Academy, a free, online learning resource, has a helpful set of short videos explaining all the steps in a Bitcoin transaction in greater detail. <https://www.khanacademy.org/economics-finance-domain/core-finance/money-and-banking/bitcoin/v/bitcoin-what-is-it> (as of May 31, 2018).

14 This leaves the network open to the possibility of a so-called "51% attack," in which a bad actor gains control of 51% of the network validators' computing power. The bad actor could then double-spend, refuse to confirm new transactions unless ransoms are paid, etc. See <https://www.coindesk.com/51-attacks-real-threat-bitcoin/> (as of May 31, 2018) (discussing generally the risk of a 51% attack to Bitcoin); see also <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/≥ (as of May 31, 2018) (discussing generally the pros and cons of "public" [a.k.a. "permissionless"] blockchains—in which anyone can validate transactions—and "private" [a.k.a. "permissioned"] blockchains—in which only pre-approved individuals may validate transactions, including the fact that only public blockchains are vulnerable to 51% attacks).

15 Brito, Jerry, and Castillo, Andrea "Bitcoin: A Primer for Policymakers" Mercatus Center, George Mason University (2013) p. 5 <https://www.mercatus.org/system/files/Brito_BitcoinPrimer.pdf> (as of May 31, 2018).

16 See <https://coinmarketcap.com/all/views/all/> (as of May 31, 2018) (listing most cryptocurrencies in existence).

17 See http://coinschedule.com/ (as of May 31, 2018) (listing current and future initial coin offerings, or "ICOs").

18 <https://github.com/ethereum/wiki/wiki/White-Paper#conclusion> (as of May 31, 2018) (Ethereum white paper).

19 Many authors and thought leaders in the blockchain space are imprecise with their use of terminology. "Blockchain technology" is also sometimes referred to as, among other things: "the blockchain" or just "blockchain"; "distributed ledger technology" (DLT); "shared ledger technology" (SLT); "consensus ledger" technology; "mutually distributed ledger" technology; or even a decentralized or "distributed database." Walch, Angela, note 6, *ante*, p. 719–720 (identifying the various nicknames blockchain technology has received). This article attempts to avoid casual conflation of these terms, but occasionally uses the term "decentralized" and "distributed ledger" as synonyms.

20 See Szabo, Nick, *Smart Contracts: Building Blocks for Digital Markets* (1996) <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html> (as of May 31, 2018) (discussing concept of smart contracts).

21 See <https://medium.com/@RagnarLifthrasir/permissionless-real-estate-title-transfers-on-the-bitcoin-blockchain-in-the-usa-5d9c39139292> (as of May 31, 2018) (discussing transfers of real estate titles on the blockchain).

22 See <https://zootsolutions.com/blockchain-whats-next/> (as of May 31, 2018) (discussing liens on real estate and vehicles in the context of blockchain technology).

23 See <https://cointelegraph.com/news/bitcoin-investment-heritage> (as of May 31, 2018) (describing what happens to crypto upon one's death and proposing various solutions, including the use of so-called "multisignature" accounts, which require multiple passwords before a crypto transaction may be signed).

24 See Barnes, Andrew *et al*., *Digital Voting with the Use of Blockchain Technology* <https://www.economist.com/sites/default/files/plymouth.pdf> (as of May 31, 2018) (proposing mechanism for voting with blockchain technology).

25 <http://www.huffingtonpost.com/entry/want-tamper-proof-elections-start-with-blockchain_us_5866c485e4b04d7df167d483> (as of May 31, 2018) (proposing the use of blockchain to provide "secure, verifiable, tamper-proof voter registration records" and ballots).

26 See <https://cointelegraph.com/news/hashcoin-uses-emercoin-blockchain-for-vehicle-registration-and-tracking/> (as of May 31, 2018) (discussing creation of vehicle registry using blockchain technology).

27 See <http://www.chicagotribune.com/classified/realestate/ct-re-0715-blockchain-homebuying-20180628-story.html> (as of August 28, 2018) (discussing pilot program in Cook County, Illinois, where recorder of deeds investigated possibility of using blockchain technology to record real-estate transactions).

28 See <https://www.technologyreview.com/s/608821/who-will-build-the-health-care-blockchain/> (as of May 31, 2018) (opining on uses of blockchain in the healthcare industry).

29 See, e.g., <http://www.the-blockchain.com/potential-uses-of-blockchain/> (as of May 31, 2018) (listing blockchain use cases).

30 See, e.g., <https://www.weusecoins.com/blockchain-uses/> (as of May 31, 2018) (listing blockchain use cases); <https://www.pcmag.com/article/350088/blockchain-in-2017-the-year-of-smart-contracts> (as of May 31, 2018) (describing use cases for smart contracts).

31 See <https://coinmarketcap.com/charts/> (as of May 31, 2018) (showing growth over time of crypto market cap)

32 *Ibid*.

33 See <http://www.newsbtc.com/2017/05/07/three-million-cryptocurrency-users/> (as of May 31, 2018) (detailing findings of Cambridge Center for Alternative Finance's study on the number of crypto users worldwide).

34 See <https://blockchain.info/charts/my-wallet-n-users> (as of May 31, 2018) (charting growth in number of blockchain wallet users over time).

35 See <https://www.cnbc.com/2017/07/31/blockchain-technology-considered-by-57-percent-of-big-corporations-study.html> (as of May 31, 2018) (summarizing research on blockchain adoption by companies around the world).

36 See <http://www.businessinsider.com/bitcoin-price-surge-leads-to-growth-in-hedge-funds-2017-8> (as of April 23, 2018) (examining growth of hedge-fund investments in cryptocurrencies).

37 See https://www.coindesk.com/the-rise-of-the-cypherpunks/ (discussing how the seeds of cryptocurrency were sowed by a social movement emerging in the 1980s called "cypherpunks," many of whom later went on to prominence in technology, blockchain, and cybersecurity spheres).

38 <https://bitcoin.org/en/faq> (as of May 31, 2018) (answering frequently asked questions about Bitcoin).

39 Nakamoto, Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System" (2008) p. 1 <https://bitcoin.org/bitcoin.pdf> (as of May 31, 2018) (proposing Bitcoin protocol).

40 As one author put it, "[i]n general, more points of failure means that the system is more resilient because an attacker would have to compromise a larger number of parts of a system in order to cause it to fail. Decentralization, such as is found in the systems underlying cryptocurrencies like Bitcoin, can greatly increase the number of points of failure… therefore mak[ing] systems more robust." Dennis, Stewart, "How Can Decentralization Improve Cybersecurity?" <https://medium.com/@stewart_dennis/how-can-decentralization-improve-cybersecurity-d9b835c69834> (as of May 31, 2018) (noting that increasing the number of points of failure via decentralization can improve cybersecurity).

41 See <https://www.nbcnews.com/business/business-news/target-settles-2013-hacked-customer-data-breach-18-5-million-n764031> (discussing Target's $18.5 million settlement in the wake of its 2013 customer data hack).

42 See <http://www.businessinsider.com/equifax-hack-data-breach-march-2017-9> (as of May 31, 2018) (recounting Equifax's data breach that affected more than 143 million Americans).

43 See <https://futurism.com/blockchain-is-transforming-our-society-and-our-world/> (as of May 31, 2018) (opining on the blockchain's potential transformative uses).

44 *Ibid*.

45 See <https://seekingalpha.com/article/4105078-cryptocurrency-volatility-lessons> (as of May 31, 2018) (evaluating correlations, average returns, and other data among crypto and other non-crypto investments).

46 <https://bankunderground.co.uk/2017/08/24/bitesize-the-very-volatile-value-of-cryptocurrencies/> (as of May 31, 2018) (analyzing the "extreme volatility" of cryptocurrencies).

47 See <https://www.sec.gov/news/press-release/2017-185-0> (as of May 31, 2018) (discussing SEC action against businessman and two companies who allegedly "defraud[ed] investors in a pair of so-called initial coin offerings (ICOs) purportedly backed by investments in real estate and diamonds").

48 For instance, the founders of Centra Tech, an ICO startup company that was hyped by celebrities Floyd Mayweather Jr. and DJ Khaled, were hit with an SEC lawsuit in April 2018, not long after a class action lawsuit was filed against them in December 2017. See <https://www.coindesk.com/justice-department-sues-founders-mayweather-backed-

ico/> (as of May 31, 2018) (discussing SEC action against Centra and its founders); http://fortune.com/2017/12/17/cryptocurrency-floyd-mayweather-centra-lawsuit/ (as of May 31, 2018).

49 See <https://bitcoinmagazine.com/articles/cryptocurrency-regulation-2018-where-world-stands-right-now/> (as of May 31, 2018) (discussing various countries' approaches to regulating bitcoin and other cryptocurrencies).

50 See <https://storeofvalue.github.io/posts/cryptocurrency-hacks-so-far-august-24th/> (as of May 31, 2018) (cataloguing some of the highest profile hacks against cryptocurrencies as of August 24, 2017).

51 See <https://www.coindesk.com/mt-gox-the-history-of-a-failed-bitcoin-exchange/> (as of May 31, 2018) (detailing the timeline of the Mt. Gox hack and subsequent fallout); <https://www.wired.com/2013/11/mtgox/> (as of May 31, 2018) (discussing Mt. Gox hack and its significance).

52 See <https://www.nytimes.com/2016/06/18/business/dealbook/hacker-may-have-removed-more-than-50-million-from-experimental-cybercurrency-project.html> (as of May 31, 2018) (discussing hack where $50 million was siphoned from the DAO).

53 See <https://www.coindesk.com/cisco-50-million-bitcoin-phishing-scam-mimicked-blockchain-web-wallet/> (as of May 31, 2018) (detailing phishing scam that has netted nearly $50 million in crypto over a three-year period).

54 At the time of publication, Mr. Buterin's twitter profile lists his name as "Vitalik 'Not giving away ETH' Buterin" in an attempt to dissuade his followers from continuing to fall victim to these kinds of scams. See <https://twitter.com/VitalikButerin> (as of May 31, 2018).

55 See <http://www.businessinsider.com/north-korea-sony-hack-2016-6> (as of May 31, 2018) (discussing whether North Korea was behind Sony's 2014 hack).

56 See <http://www.businessinsider.com/north-korea-hackers-more-bitcoin-attacks-2017-9> (as of May 31, 2018) (commenting on research linking North Korean hackers to numerous cryptocurrency attacks).

57 As one example, many have wondered whether the burgeoning science of quantum computing might make certain cryptos fatally susceptible to 51% attacks and the like. See, e.g., <https://www.forbes.com/sites/amycastor/2017/08/25/why-quantum-computings-threat-to-bitcoin-and-blockchain-is-a-long-way-off/2/#69dc00f529a9> (as of April 19, 2018).

58 See <https://www.cnbc.com/2017/09/07/bitcoin-up-sevenfold-since-warren-buffett-warned-digital-currency-was-a-mirage.html> (as of May 31, 2018).

59 See <https://99bitcoins.com/obituary-stats/> (as of May 31, 2018) (collecting articles predicting bitcoin's alleged imminent demise).

60 See <https://www.thestreet.com/story/14248092/1/the-cryptocurrency-mining-craze-that-has-boosted-amd-and-nvidia-may-be-ending.html> (as of May 31, 2018).

61 See <https://www.cnbc.com/2017/07/26/wall-street-stunned-over-amds-cryptocurrency-mining-demand.html> (noting Advanced Micro Devices, Inc.'s strong financial performance resulting partially from strong demand in the cryptocurrency-validating, or "mining," space, but cautioning that "the [crypto-mining] craze is waning").

62 Transaction validators, or "miners," receive so-called "bounties" as well as transaction fees for being the first to validate a new block or transaction, which has led some investors to start crypto-mining businesses. These businesses employ massive amounts of computing power to validate transactions, which enables them to validate transactions more quickly than individual miners. The crypto-mining arms race that has erupted has effectively foreclosed the window for individuals with ordinary computers to profitably mine bitcoin and some other kinds of crypto. For a brief introduction to crypto mining, see <https://www.coindesk.com/information/how-bitcoin-mining-works/> (as of May 31, 2018).

63 See <https://grayscale.co/bitcoin-investment-trust/> (as of May 31, 2018) (offering indirect ownership of bitcoin); https://grayscale.co/ethereum-classic-investment-trust/ (as of May 31, 2018) (offering indirect ownership of Ethereum classic).

64 See <https://www.cnbc.com/2017/09/18/ibm-far-outranks-microsoft-as-blockchain-industry-leader-report.html> (as of May 31, 2018) (discussing IBM and Microsoft's "race towards building distributed ledger solutions").

65 The federal government rejected early proposals for such ETFs, but as one article predicts, "some analysts argue that it's only a matter of time before the first bitcoin ETF is launched." <https://hacked.com/sec-initiates-formal-proceedings-on-coveted-bitcoin-etf/> (as of April 19, 2018).

66 Interestingly, there is also a growing number of crypto ATMs, where one can buy and sell crypto for cash. One September 20, 2017, CBS article counted approximately 1600 Bitcoin ATMs worldwide, including over 900 in the U.S. The use of crypto ATMs is beyond the scope of this article, but they are nevertheless worth investigating. See <https://www.cbsnews.com/news/wait-i-can-get-bitcoin-at-that-atm/> (as of May 31, 2018).

67 All cryptocurrencies other than Bitcoin are colloquially known as "alt-coins," which is short for alternative coins.

68 See <https://www.nasdaq.com/article/the-3-best-cryptocurrency-exchanges-cm902049> (as of May 31, 2018) (comparing various exchanges and noting that Coinbase.com is "the largest crypto exchange, boasting over $20 billion in trading volume and over 10 million registered users" as of January 8, 2018).

69 There are websites, like <https://www.bestbitcoinexchange.io/>, that aggregate reviews of exchanges. However, multiple sources should be considered before making a final decision on which exchange(s) to use.

70 See <https://support.coinbase.com/customer/portal/articles/1662379-how-is-coinbase-insured> (as of May 31, 2018) (describing insurance covering Coinbase accounts' digital currency and cash balances).

71 For instance, to purchase an alt-coin on Bittrex.com if you only have U.S. dollars, you must first purchase crypto on another exchange (e.g., Coinbase.com), then transfer that crypto to your account on Bittrex.com, where you can then exchange that crypto for the actual crypto you wanted in the first place.

72 See <https://bitcoin.org/en/faq#why-do-i-have-to-wait-10-minutes> (as of May 31, 2018) (explaining that Bitcoin transactions are confirmed "between a few seconds and 90 minutes, with 10 minutes being the average").

73 See <https://medium.com/dash-for-newbies/whats-the-backstory-on-the-word-hodl-27756392b698> (as of May 31, 2018) (recounting the etymology of "hodl").

74 See <https://www.coindesk.com/lamborghini-mclaren-bitcoin/> (as of May 31, 2018) (observing that certain Lamborghini and McLaren dealerships have reportedly begun accepting bitcoin as payment).

75 See <https://www.enterprisetech.com/2017/09/26/blockchain-advances-first-real-estate-deal/> (reporting that an international real estate broker in California had completed "the first real asset transfer via blockchain" in September 2017 using ether to purchase an apartment in Kiev, Ukraine).

76 <https://www.irs.gov/pub/irs-drop/n-14-21.pdf> (as of May 31, 2018) (discussing IRS guidance about federal taxation of "virtual currencies," i.e., crypto).

77 All references to "Section" are to the California Probate Code unless otherwise noted.

78 Prob. Code, section 16047, subd. (e).

79 Prob. Code, section 16046, subd. (a).

80 Prob. Code, section 16047, subd. (a).

81 *Ibid*.

82 Prob. Code, section 16047, subdivisions (c)(1)–(8).

83 Prob. Code, section 16047, subd. (d).

84 Prob. Code, section 16051.

85 See Prob. Code, section 16047, subd. (b).

86 Prob. Code, section 16047, subd. (a).

87 A small group of cryptos, however, do offer what essentially amounts to dividends. For instance, holding cryptos like NEO and COSS gives one the right to obtain small amounts of other crypto. See, e.g., <https://coinsutra.com/cryptocurrency-dividends/> (as of May 31, 2018).

88 See <https://cointelegraph.com/news/bitcoin-mining-thrives-in-venezuela-thanks-to-hyperinflation-and-free-electricity> (as of May 31, 2018) (explaining that Venezuela's "annual inflation rate has surged to 1,600 percent," which has driven many Venezuelans to store value in crypto).

89 See <https://cryptofundamental.com/golden-hedge-bitcoin-will-likely-rise-in-the-next-recession-6806ffefcb05> (as of May 31, 2018) (analyzing lack of correlation between Bitcoin and non-cryptoassets, and suggesting that "Bitcoin will likely be counter-cyclical in the next recession, rising in value as equities and correlated assets drop").

90 See <https://www.forbes.com/sites/greatspeculations/2017/07/10/what-you-need-to-know-about-cryptocurrencies-and-taxes/#5e287a6c1a95> (as of April 19, 2018) (summarizing IRS treatment of crypto); *see also* <https://www.marketwatch.com/story/bitcoin-exchange-coinbase-is-handing-over-user-information-to-the-irs-2018-02-27> (as of May 31, 2018) (reporting that Coinbase would be providing more than 13,000 users' data to the IRS to determine whether users were attempting to evade taxes).

91 See IRS Notice 2014-21 <https://www.irs.gov/pub/irs-drop/n-14-21.pdf> (as of May 31, 2018).

92 See note 91, *ante*.

93 For an introduction to IRS Notice 2014-21 and the federal taxation of crypto, *see* Rees, J.D. *Bitcoin Taxation: IRS Notice 2014-21 Is Just The Beginning*, Los Angeles Lawyer (April 2018), p. 12 <https://www.lacba.org/docs/default-source/lal-back-issues/2018-issues/april-2018.pdf> (as of May 31, 2018).

94 Prob. Code, section 16047, subd. (b).

95 *Ibid*.

96 See comment (a) to Restatement of Trusts (Third), section 92.

97 <http://www.investopedia.com/terms/d/dotcom-bubble.asp> (as of May 31, 2018).

98 <https://www.forbes.com/sites/johnwasik/2017/09/27/why-u-s-is-probing-bitcoin-scams/#3606f9257290> (as of April 19, 2018) (discussing SEC enforcement actions against various ostensible crypto scams).

99 This list of considerations is largely based on one proposed in an online community that discusses cryptocurrencies. <https://www.reddit.com/r/CryptoCurrency/comments/6l130v/a_boring_investors_guide_to_cryptocurrency> (listing questions to investigate before investing in a cryptocurrency).

100 *See* Walch, Angela, note 6, *ante*.

101 *See* Walch, Angela, note 6, *ante*, p. 763.

102 Prob. Code, section 16048.

103 As aptly stated by comment e(1) to Restatement of Trusts (Third), section 90, "one pervasive generalization prevails concerning the prudent investor's duty of caution: reasonably sound diversification is fundamental to the management of risk, regardless of the level of conservatism or risk appropriate to the trust in question. Therefore, trustees ordinarily have a duty to diversify investments."

104 Kiziah, Trent S., *The Trustee's Duty to Diversify: An Examination of the Developing Case Law* (2012) American Law Institute, section 2.6, p. 7.

105 *See* comment (g) to the Restatement of Trusts (Third), section 90.

106 Kiziah, Trent S., *The Trustee's Duty to Diversify: An Examination of the Developing Case Law* (2012) American Law Institute (formerly known as ALI-ABA), section 2.3, p. 6.

107 See note 46 *ante*; *see also* <https://www.sifrdata.com/cryptocurrency-correlation-matrix/> (providing analytics and data about cryptocurrencies, including their correlations with various other cryptocurrencies).

108 <https://seekingalpha.com/article/4105078-cryptocurrency-volatility-lessons> (as of May 31, 2018).

109 See <https://www.sifrdata.com/cryptocurrency-correlation-matrix/> (as of May 31, 2018) (collecting data about correlation among cryptos and other equities, e.g., the S&P 500 Index (SPX) and the SPDR Gold Shares (GLD)).

110 See <https://www.coindesk.com/understanding-dao-hack-journalists/> (discussing decline in ether's value after attack on the DAO).

111 Indeed, a comprehensive analysis of cryptos' correlations with various types of assets—particularly equities of blockchain-industry companies—would be of great utility to both trustees and the legal community more broadly.

112 Prob. Code, section 16049.

113 Kiziah, Trent S., *The Trustee's Duty to Diversify: An Examination of the Developing Case Law* (2012) American Law Institute, Section 2.4(a), p. 7 (emphasis added).

114 Prob. Code, section 16006.

115 Generally, if someone loses the private key to their crypto (e.g., the password to their wallet), chances are that it is gone forever.

116 <https://www.gizmodo.com.au/2017/05/i-threw-away-4-8-million-in-bitcoin/>.

117 Legislative Counsel's Digest to Assembly Bill No. 691, Ch. 551.

118 Prob. Code, section 871, subd. (h).

119 Prob. Code, section 873, subd. (a).

120 Prob. Code, section 873, subd. (b).

121 Prob. Code, section 877, subdivisions (a)–(c).

122 Prob. Code, section 877, subd. (d).


CLA
CALIFORNIA LAWYERS ASSOCIATION