Estate Planning Studies®

January 2020

Cryptocurrency—January 2020
What estate planners need to know

by Gerry W. Beyer*

Cryptocurrency is no longer an asset held only by tech-savvy nerd investors. Instead, it is becoming increasing common. In fact, you can find kiosks in grocery stores that make cryptocurrency investing available to the masses. This Study will provide you with what you need to know about cryptocurrency, including:

- How Cryptocurrency operates
- Potential benefits
- Potential problems
- Taxation
- Recommendations

INTRODUCTION

Less than a decade ago, if an estate planner asked clients whether they owned any cryptocurrency, the most likely response would be, "You mean, money to buy a crypt?" Now, due to the widespread media coverage of Bitcoin, the most famous of all crypto-currencies, most clients will have some basic idea about what the estate planner is inquiring.

The use of cryptocurrency is increasing at a rapid pace. As of August 29, 2019, there were approximately 17.9 million Bitcoins in circulation worth over $67 billion. Although only a few cryptocurrencies in addition to Bitcoin are well-known outside the cryptocurrency community (e.g., XRP, Ethereum, EOS, and Stellar), over 2,300 different virtual currencies are traded actively. These other cryptocurrencies are sometimes referred to as *altcoins*, meaning that they are an alternative to Bitcoin.

According to a 2018 Edelman Financial survey, 25% of individuals between the ages of 24 and38 who had either $50,000 of investable assets or earned $100,000 or more per year own cryptocurrency. A growing number of mainstream businesses already accept Bitcoin, such as Microsoft, Subway, KFC Canada, many Etsy vendors, Overstock.com, Whole Foods, Dish Network, AT&T, and Expedia. In addition, some law firms are accepting Bitcoin in payment of legal services.

This article starts by building a basic foundation about virtual currencies and how they operate. The article then reviews the estate planning and administration issues that arise with owning cryptocurrency and concludes with recommendations for how to address virtual currency in your practice.

THE BASICS OF CRYPTOCURRENCY

Before looking at cryptocurrency in detail, itis helpful to place this specialized asset into proper context. The overarching category under discussion is called digital currency. Digital currency refers to all monetary assets in digital form, whether the money it represents is actually a nation's currency (e.g., dollars, euros, or yen) or whether it is privately issued. Virtual currency

Montecito Bank & Trust®
Wealth Management

1106-E Coast Village Road
Montecito, CA 93108

is not connected to a nation's actual currency, and it is instead "an electronic representation of monetary value that may be issued, managed and controlled by private issuers, developers, or the founding organization."[1] *Virtual currency* is nothing more than ones and zeros stored on computer media. *Cryptocurrency* is virtual currency that uses sophisticated cryptography to make certain that transactions are secure and authentic.

The discussion below is admittedly simple and omits sophisticated high-level computer discussion. Nonetheless, the discussion should provide the estate planner with a basic understanding of the workings of cryptocurrency.

A cryptocurrency is "born" through a computer process called *mining*. The "parent" of the virtual currency creates complex mathematical equations that the parent expects other people (the *miners*) to solve using high-powered computers. As a reward for solving these equations, the miners receive a virtual coin that they may then use to purchase real-world assets, assuming they can find someone willing to accept it. As more coins are mined, it becomes harder (that is, more processing power is needed over a longer period of time) to mine each subsequent coin until a cap is reached, either because one was provided by the parent or mining is no longer a cost-effective way of obtaining a coin.

These virtual coins rely on *blockchain* technology for security and validity. A blockchain is a distributed database often referred to as the *ledger*; that is, a list of transactions and their details, such as the number of coins added or subtracted along with the date and time of the transaction, that is held by individuals who agree to share the database with all other users of the same database of virtual currency. The data-base then is continuously updated and synchronized. This results in all users having the complete record of the virtual currency instead of having only one central computer or entity that processes all transactions. Each transaction or *block* is added to the chain, along with a timestamp and link to the previous block. These transactions immediately revise all of the other copies of the database.

The owner of cryptocurrency has a very long and complex "password" called a *private key* to access the portion of the blockchain containing the owner's coins. This private key is mandatory to access the owner's virtual currency. To transfer virtual currency from one person to another person as payment for goods or services, or perhaps as a gift, the owner uses the owner's private key to authorize the transaction and then sends a message to the recipient containing a *public key*, which is mathematically related to the location of the owner's virtual currency so that the recipient can receive the transfer. Complex software running on many different computers then verifies the transaction. If the transaction is determined to be valid by enough computers, it becomes the next block in the chain. "To prevent people from generating counterfeit currency, the math required to verify a transaction takes so much computing power that no one user or group could do it."[2] In fact, one writer claims it would take the world's most powerful supercomputer over a trillion years to determine the owner's private key from the public key.[3]

There are two primary ways that various crypto-currency networks go about verifying the transactions that occur on their blockchains. The first way, which is deemed more secure but less efficient, is done in a process referred to as "proof of work." This is the scenario in which a miner receives a reward for verifying transactions on the ledger. More than one miner will verify the same transaction, and often a transaction will be verified several times. This system ensures the open-access security of the blockchain, but can be costly in terms of computing power. The other type of verification process is known as "proof of stake." This system attempts to conserve resources by using a preference-based model to choose who will verify the next transaction based on the amount of that user's ownership, or "stake," in the cryptocurrency.[4]

Most cryptocurrency owners do not need to concern themselves with these details. Businesses called *cryptocurrency exchanges* have sprung up that handle the complex details making it easy for a person to buy, sell, and transfer virtual coins such as Coinbase and Uphold. For example, these exchanges hold the private keys and public keys and generate the messages necessary to effectuate transfers.

Cryptocurrency resides in "wallets" that can be stored in many different ways, such as on an exchange accessed over the Internet, software on a computer, tablet, or cell phone, or on a dedicated flash drive. To be able to retrieve cryptocurrency and transfer it, you must have the private key or the *seed* phrase; that is, a list of random words that allows the person to recover the wallet containing the virtual currency. A seed phrase would look something like the following: "warlock implode lawyer drink love close cactus river street double water most." These words are tied to the private key through a complex computation process. The seed phrase needs to be kept secure at all times. Otherwise, anyone with knowledge of the phrase could access the currency. If the wallet resides on a commercial exchange, the cryptocurrency may be accessible by a person who knows the user name, password, and answers to security questions and has the ability to

satisfy other verification steps.

BENEFITS OF CRYPTOCURRENCY

Security

Because of the high-level of encryption, crypto-currency is extremely safe from being used by an unauthorized person, unless the owner is careless in protecting the owner's private key or seed phrase. In addition, because the ledger is stored on many computers all over the world, it is very safe against hacking and other cyber-attacks.

If a currency exchange is used, this security is necessarily reliant upon the integrity of the exchange upon which the cryptocurrency is being held. If the exchange is compromised, then the security of the private key also is compromised. This particular type of security breach is what leads to many of the hackings that critics of cryptocurrency point to when discussing its relative insecurity in terms of actually ensuring ownership of one's cryptocurrency. It is important for those handling estates with cryptocurrency assets to understand the distinction between the security that is gained from the blockchain verification technology itself, as compared to the security of the exchange.

Even further, it is important to remain cognizant that real humans and not computers are the ones who will make the decisions in terms of how various blockchains will be regulated and how big questions regarding network security will be approached. For instance, after an exploitation of code during a round of capital-raising for Ethereum, a large amount of ether (the primary trading unit) was "siphoned" from the capital fund.[5] Instead of treating the ether as stolen and simply moving forward, the creator of the platform, via a software update, basically reset the entire system to the point on the chain prior to the exploitation. Although the move created what is known as a "fork" in the cryptocurrency and dis-satisfied some holders, it also led to a philosophical discussion about the intervention. Most importantly for the purposes of the estate planner, this example highlights the limits of the security provided by these assets.

Privacy

Cryptocurrency is virtually untraceable and some-times gets a "bad rap" as being used by people involved in illegal activities such as drugs, gun-running, murder for hire, and prostitution. Of course, the same could be said of traditional hold-in-your-hand cash, which is also normally untraceable absent the recording of serial numbers, being marked with invisible ink, or containing traceable electronic devices.

Many individuals do not wish for their financial transactions to be public for reasons that do not involve covering up unseemly activities. Instead, they believe that it is no one's business how much they own, what they buy, and what they sell. Perhaps they merely want to avoid the endless advertisements that appear after making a purchase on a traditional website that collects a considerable amount of private data.

However, although the blockchain itself is close to anonymous, exchanges themselves can be forced to divulge information about their users. Less than two years ago, the Internal Revenue Service won a court case against a popular cryptocurrency exchange, mandating that the exchange divulge information on almost 15,000 users who, over the period of 2013 to2015, engaged in individual transactions valued at over $20,000 at the time of the exchange.[6] Although the court eventually limited the initial scope of the government's information request, the larger take-away for estate planners is that transactions over cryptocurrency exchanges are not as anonymous as popularly perceived. Further, during the litigation, the IRS revealed that fewer than 1,000 taxpayers reported cryptocurrency gain or loss in 2014 and 2015, so stepped-up enforcement is expected tocontinue.[7]

Shorter Transfer Delay, Lower Cost, and Finality of Transfer

Transferring hard currencies takes time (often many days or up to a week or more), involves many intermediary steps (e.g., customer, customer's bank, intermediary banks, business' bank, and business), and incurs transfer fees. On the other hand, transfers of cryptocurrencies may occur immediately or within a few minutes and, unless an exchange is used, without a transfer cost. Even if an exchange is involved, the cost is often considerably less than traditional banking fees.

An additional advantage is the finality of the transfer that cryptocurrency's peer to peer block-chain technology provides. With other electronic transactions that are denominated in government currency, there are significant periods of time spent waiting for the transaction to close, and any number of actors that could stop, reverse, or undo the transaction. On the blockchain, once a transaction has been verified and added to the blockchain, there is no practical way to reverse the transaction.

RISKS OF CRYPTOCURRENCY

No Recovery Without Private Key or Seed Phrase

If the owner of cryptocurrency forgets, misplaces, or loses the private key and seed phrase, there is no way that the owner can recover it. There is no "forgot

password" link that the owner can use to recover the private key or seed phrase. If the cryptocurrency is stored on an exchange, there will be a greater chance of being able to regain a lost password because the owner is gaining access to the exchange rather than the cryptocurrency directly.

James Howells of Newport, Wales, learned this lesson the hard way. He chose to store his 7,500 Bit-coins on a hard drive in 2009, when they were nearly worthless. Several years later, he discarded the hard drive in the trash, which ended up in a landfill the size of a football field. He searched the landfill to no avail even after funding a more extensive search with an Indiegogo account.[8] If he had those Bitcoinson November 25, 2019, they would have been worth approximately $53 million.

Another example touches upon the important distinction between the security of the cryptocurrency's blockchain itself and the security of an exchange. Early in 2019, a thirty-year-old owner of a crypto-currency exchange died unexpectedly while on an aid mission to India, and "a sworn affidavit [by his wife] as she filed for credit protection … [stated he] held 'sole responsibility for handling the funds and coins.'"[9] The owner's digital key was necessary to access the cryptocurrency assets held in what the company called "cold wallets," but that digital key was held on the decedent's laptop. In filing for creditor protection, the company publicly acknowledged that their efforts to locate the key and free the assets had been unsuccessful. This unfortunate scenario could have been avoided with proper estate planning, but it serves to highlight the drawbacks of the peer-to-peer privacy model.

Value Fluctuation

Cryptocurrency is not backed by any government, and thus its value is likely subject to greater, and perhaps extreme, fluctuation. Even the most popular virtual currency, Bitcoin, has seen huge value shifts. For example, in 2010, one Bitcoin was worth $.01 but had increased to $1,000 by January 1, 2017. At the end of 2017, one Bitcoin was worth almost $20,000.On November 25, 2019, the value of one Bitcoin was approximately $7,198, with value changing by several dollars every second. Some players in the cryptocurrency industry have recognized the need for greater stability to meet investors' desires and have created "stable coins" to enjoy the privacy and security benefits of cryptocurrency while minimizing the negative effects of holding or trading in what has historically been a volatile, unstable market.[10] To alleviate the rapid swings, some of these crypto-currencies are physically pegged to a particular currency, like the U.S. dollar, or to a certain commodity, such as gold.

No Regulation

Cryptocurrencies are not subject to any central authority, such as a government or governmental entity, which can provide a type of security or insurance from value fluctuations, cheaters, scammers, and other evil conduct. If something "happens" to cryptocurrency, the owner is without any recourse.

For example, "[in] February 2014, the then-largest bitcoin exchange, Mt. Gox, went bankrupt after hackers stole some 850,000 bitcoins that at the time were worth roughly $450 million."[11] However, defenders of cryptocurrency correctly point out that the compromise of an exchange (or wallet) is not a threat to the actual security of the blockchain's encryption, and they liken the situation to a bank robbery—poor security at a bank does not inherently threaten the security of the monetary systemitself.[12] It also appears that although cryptocurrencies are not under the direct control of any government authority, not all coins are operationally the same in terms of a purely decentralized approach to their blockchain source code—thus manipulations of the asset can take place, albeit in limited form. However, as demonstrated by the unfortunate passing of the Canadian exchange owner, there is no entity like the Federal Deposit Insurance Corporation or similar government body to "maintain stability and public confidence" through insuring the unlucky cryptocurrency investor, nor a Federal Reserve Bank tasked with a mandate and power to "moderate … the U.S. economy" through currency stabilization efforts.[13] Although some individuals with cryptocurrency assets may believe the lack of regulation surrounding their investment to be a net positive, it is important for estate planners to acknowledge the inherent risks that come with a currency largely free of government regulation by design.

Prudent Investment and Fiduciary Concerns

Cryptocurrency is risky. As one commentator stated, it is more risky than gambling. "In roulette, if you put $1 on every number, you'll spend $38 and be guaranteed to get exactly $36 in return. You could buy $1 of every cryptocurrency and they might all end up worthless."[14]

Under the prior prudent person rule, a trustee could not invest in cryptocurrency, absent express permission in the trust, because of this risk. How-ever, under the Uniform Prudent Investor Act effective in most states, trustees must make investment decisions "in the context of the trust portfolio as a whole and as part of an overall investment strategy having *risk* and return objectives reasonably suited to the trust."[15] Accordingly, a trustee needs to determine with respect to each trust whether

investment in cryptocurrency is allowed or perhaps even required. The author's anecdotal conversations with corporate trustees reveal a tremendous hesitancy to invest in cryptocurrency without express permission in the trust instrument from the settlor, a release by the beneficiaries, or authorization in a court order.[16]

Although management of cryptocurrency poses risks for the fiduciary, including the inherent volatility of the underlying asset itself, there are vehicles that can ease the burden of management upon a fiduciary. A grantor retained annuity trust (GRAT) created to hold cryptocurrency, opened consecutively with a standard bank account for the GRAT at the time of its funding, "can [allow the fiduciary to]use the power of substitution to exchange the cash in the bank account for cryptocurrency in the GRAT that has appreciated significantly, thus locking in the increased value of the cryptocurrency."[17]

Taxation and Classification of Cryptocurrency

Digital currencies have value, and so legally they must be reported in the valuation of an estate. In 2014 the IRS indicated that cryptocurrency is "property" rather than currency.[18] Accordingly, cryptocurrency is subject to capital gains tax rules. The fair market value of cryptocurrency is to be calculated "by converting the virtual currency into U.S. dollars ...at the exchange rate, in a reasonable manner that is consistently applied."[19] There are sources that keep historical records of the value of a cryptocurrency as of a certain date, such as Poloniex and Coinmar-ketcap.com. These resources enable users to access crypto currency records much as they can access historical records of stock. A fiduciary should be aware of these basis rules, as there are situations where it could be more advantageous to purchase either with cash or with cryptocurrency depending on its impact on the taxpayer's basis.[20]

Further, there is the potential for scenarios beneficial to the decedent's beneficiaries to arise because of this distinction by the IRS. Because the property is not treated like a fiat currency, "certain planning techniques can maximize the 'step-up' in tax basis that occurs at death for certain assets. This planning may later reduce the inheriting owner's tax burden significantly if, for example, the inheriting owner were to sell assets after the death of the originalowner."[21] The basis of a unit of cryptocurrency fora person acquiring it from a deceased owner will be the fair market value as of the date of the owner's death. [22]

Taxpayers who are engaged in the mining of cryptocurrency must compute their taxable gross income based on the fair market value of the cryptocurrency on the date received. The initial meta-physical quandary of taxing digital mathematical creations is explained by characterizing mining as the reception of existing virtual currency in exchange for computer services.

A significant issue left unaddressed by Notice 2014-21 is whether the property classification applied to cryptocurrency falls under the tangible or intangible property distinction. Some commentators have recognized that the Notice's treatment of miners' realized income from mining activity inherently rejects a tangible personal property approach.[23] Another commentator has acknowledged that cryptocurrency does have characteristics making it amenable to a tangible personal property characterization.[24] These distinctions are important, particularly in the context of charitable deductibility and transfer by a noncitizen nonresident if the situs of the crypto-currency is in the United States.25Although multiple professional interest groups, such as the American Institute of Certified Public Accountants (AICPA)and the American Bar Association's Tax Section, have approached the IRS with requests for additional guidance, only guidance on the relatively narrow treatment of "hard fork" and "airdrop" occurrences has been issued as of late 2019.[26]

Additional considerations apply for states that impose an income tax and, if the cryptocurrency is considered tangible, taxes on the sale of tangible personal property. For Internet sales tax purposes, "the location of a cryptocurrency wallet within a state may be a sufficient nexus for that state to tax sales of cryptocurrency" that occur for a particular wallet.[27]

The question of whether cryptocurrency can be classified as a "security" and thus fall under the jurisdiction of the Securities and Exchange Commission (SEC) increasingly is being answered in the affirmative. In a June 2018 speech, SEC Director of Corporate Finance William Hinman expressed that although Bitcoin and Ether specifically were not securities "if there is a centralized third party, along with purchases with an expectation of a return, then it is likely a security."[28] Additionally, enforcement actions have proceeded along similar lines, applying the *Howey* test for a general determination of a security in an admittedly "highly fact-specific"inquiry.[29] It is more clear that cryptocurrency may be classified as a "commodity" for the purposes of the Commodity Exchange Act (CEA) and be subject to the jurisdiction of the Commodity Futures TradingCommission.[30] Citing the definition of commodity in the CEA, the CFTC noted it encompassed abroad inclusion of "among other things, 'all services, rights, and interests in which contracts for future delivery are presently or in the future dealt in.'"[31] Estate planners should seek advice from qualified professionals if these complicated scenarios should

arise in their practice.

CONCLUSION AND RECOMMENDATIONS

As time marches by, an increasing number of your clients will own cryptocurrency. Only with proper planning, however, will the value of this property be available to the client's successors in interest. Here is a summary of the key steps that an estate planner should take.

- Early in the estate planning process, via client intake forms, questionnaires, or interview questions, as certain whether your client owns (or plans to acquire) cryptocurrency.
- A cryptocurrency-owning client needs to keep detailed records of the date of each virtual currency purchase and the amount so that capital gains income tax planning can be accomplished effectively, such as (1) selling and paying the tax (or taking a loss) now, (2) gifting with a carryover basis, or (3) allowing it to pass at death to give the beneficiary a stepped-up basis.
- If the client owns cryptocurrency stored in a software wallet not connected to an exchange, it is essential to make arrangements to protect and then transfer the private key or seed phrase to the person whom the client wishes to own the virtual currency after the client's death. Storing the key or phrase in a safe-deposit box is a frequently used technique. If the client owns cryptocurrency stored on an exchange, then protection, storage, and transfer of the username, password, and security question information are needed. In addition, some exchanges use two-factor authentication. For example, after entering the user name and password on the exchange's website log-in page, the exchange sends a numerical code to the owner's cell phone, which the user must then enter to access the owner's account. If this is the case, the cell phone itself and how to access it also must be protected.
- If the client owns cryptocurrency stored on a hardware wallet (flash drive), arrangements to reveal to the intended beneficiary both the drive's location and the keys, phrases, or codes needed to access it must be made. As with software wallets, keeping the device and phrase in a safe-deposit box is often an effective protection method.
- The estate planner needs to ascertain whether the client wishes to make a specific gift of any crypto-currency upon death (either to a person or to a trust) or whether it is merely to become part of the decedent's general estate. If a specific gift is intended, the gift provision needs to be drafted carefully so as to transfer the cryptocurrency but not contain the private key, see phrase, password, or other access information. Instead, the will should describe how he beneficiary (or trustee, if the transfer is to a trust) may obtain this information, such as on a flash drive in a safe-deposit box or from a trusted individual.
- After a person has died, search diligently for the existence of digital currency. If the decedent used an exchange to purchase the cryptocurrency, the exchange account typically will be linked to a bank account or credit card, so the decedent's bank records or emails may provide a clue that the account exists. Signs of cryptocurrency also can be spotted on the decedent's phone, tablet, or computer, if a mobile wallet or offline wallet were used. Another, albeit much rarer sign, would be a room filled with high-end computers, which could indicate that the decedent was a miner.
- If cryptocurrency is located, the executor or administrator will need to deal with it appropriately. The property is just like any other estate asset. It needs to be preserved as much as possible if it is subject to a specific bequest in the decedent's will. If itis not, the personal representative will need to decide whether to retain the cryptocurrency or liquidate it for United States currency. As discussed above, this will require the executor or administrator to act as a reasonably prudent investor.
- For inventory and transfer tax purposes, the value of the cryptocurrency is the fair market value at the date of death. Several websites maintain historical exchange rate records such as Poloniex, Bittrex, and Coinmarketcap.
- A trustee should not invest in or retain cryptocurrency without settlor, beneficiary, or court authorization.

*Governor Preston E. Smith Regents Professor of Law, Texas Tech University School of Law, Lubbock, Texas. Prof. Beyer holds a J.D. summa cum laude from the Ohio State University and LL.M. and J.S.D. degrees from the University of Illinois. As a state and nationally recognized expert in estate planning and a frequent contributor to both scholarly and practice-oriented publications, Prof. Beyer was inducted into the National Association of Estate Planning Councils' Estate Planning Hall of Fame in November 2015. He is a member of the Order of the Coif, an Academic Fellow and Regent of the American College of Trust and Estate Counsel, and a member of the American Law Institute.

The author expresses with gratitude the assistance of Kurt Brown, 2021 J.D. Candidate, Texas Tech University School of Law, in the preparation of this Study.

FOOTNOTES

1. Jake Frankenfield, *Virtual Currency*, INVESTOPEDIA (Aug.17, 2019), https://www.investopedia.com/terms/v/virtualcurrency.asp.
2. Alexander George, *Did You Miss the Cryptocurrency Boat?,* POPULAR MECHANICS, Apr. 2018, at 16, 17.
3. *See* Prypto, *Bitcoin Public and Private Keys—Dummies*,www.dummies.com (last visited Dec. 31, 2018).
4. Sean Williams, *Cryptocurrencies Explained, in Plain English*, THE MOTLEY FOOL (Jan. 22, 2018), https://www.fool.com/investing/2018/01/02/cryptocurrencies-explained-in-plain-english.aspx.
5. Jonathan Ore, *How a $64M Hack Changed the Fate of Ethereum, Bitcoin's Closest Competitor*, CANADIAN BROADCASTING CORPORATION (Aug. 28, 2016), https://www.cbc.ca/news/technology/ethereum-hack-block-chain-fork-bitcoin-1.3719009.
6. *United States v. Coinbase*, Inc., No. 17-cv-01431-JSC, 2017 U.S. Dist. LEXIS 196306 (N.D. Cal. Nov. 28, 2017).
7. Jeff John Roberts, *Only 802 Told the IRS About Bitcoin*, FORTUNE (March 9, 2017), https://fortune.com/2017/03/19/irs-bitcoin-lawsuit.
8. *See* Stephen Shankland, *UK Man Tries to Retrieve $7.5Million in Bitcoins from Dump*, CNET (Nov. 29, 2013),https://www.cnet.com/news/uk-man-tries-to-retrieve-7-5-million-in-bitcoins-from-dump/.
9. James Rogers, *$190 Million Gone Forever? CryptoBoss Dies with Passwords Needed to Unlock Customer Accounts*, FOXNEWS (Feb. 4, 2019), https://www.foxnews.com/tech/cryptocurrency-exchange-chief-dies-with-passwords-needed-to-unlock-customers-190m-re-ports-say.
10. Adam Hayes, *Stablecoin*, INVESTOPEDIA (Sept. 1, 2019), https://www.investopedia.com/terms/s/stablecoin.asp.
11. Rebecca Patterson, *The Hype and Hope of Bitcoin and Blockchain*, Bessemer Trusts, Second Quarter 2018, at 1, 3.
12. Saifedean Ammous, *Can Cryptocurrencies Fulfill the Functions of Money?* 10 (Columbia University Center on Capitalism and Society Working Paper No. 92, Aug.2016), https://capitalism.columbia.edu/files/ccs/workingpage/2017/ammous_cryptocurrencies_and_the_functions_of_money.pdf.
13. Federal Deposit Insurance Corporation: FDIC Mission (last visited Oct 3, 2019), https://www.fdic.gov/about/strategic/strategic/mission.html; Federal Reserve Bank: About the Fed (last visited Oct. 3, 2019), https://www.federalreserve.gov/aboutthefed/pf.htm
14. Alexander George, *Did You Miss the Cryptocurrency Boat?,* POPULAR MECHANICS, April 2018, at 16, 17.
15. UNIF. PRUDENT INVESTORACT§2(b) (emphasis added).
16. *See also* Suzanne Walsh, *Every Day is Bitcoin Pizza Day: What Clients and Estate Planners Need to Know about Cryptocurrency*, LEXOLOGY.COM (Sept. 6, 2017), https://www.lexology.com/library/detail.aspx?g=26ec7aff-527b-4fcf-8b22-f6d48527fe64.
17. Parker F. Taylor, Vanessa A. Woods & Jack Tanenbaum, *Estate Planning with Cryptocurrency*, PROB. & PROP., Jul.–Aug. 2019, at 28.
18. I.R.S. Notice 2014-21, https://www.irs.gov/businesses/small-businesses-self-employed/virtual-currencies (last visited Oct 5, 2019).
19. Walsh, *supra* note 17.
20. Sasha A. Klein & Andrew R. Comiter, *Bitcoin: Are You ready for This Change for a Dollar?,* Probate & Property March/April 2015 11, at 13.
21. Geoffrey S. Kunkler, *Preparing for the New Frontier in Trusts & Estates: Blockchain and Cryptocurrency, Incorporating Cryptocurrencies into Estate Planning*, 29 OHIOPROB.L. J.5 (2018).
22. IRC § 1014(a)(1) (2018).
23. Sasha A. Klein & Andrew R. Comiter, *Bitcoin: Are You Ready for This Change for a Dollar?,* PROB. & PROP.11, (Mar.–Apr. 2015).
24. Max I. Raskin, *Realm of the Coin: Bitcoin and Civil Procedure*, 20FORDHAMJ.OFCORP. &FIN.L.969 (2015).
25. Austin Bramwell, Abigail Rosen Earthman, Benetta P. Jenson, & Suzanne Brown Walsh, *New Kids on the Block (chain): Planning with Bitcoin and Cryptocurrency*, 53 HECKERLINGINST.ONEST. PLAN.14 (2019).
26. I.R.S. News Release IR-2019-167 (Oct. 9, 2019); see also Parker F. Taylor, Vanessa A Woods & Jack Tanenbaum, *Estate Planning with Cryptocurrency*, PROB. & PROP.23, (Jul.–Aug. 2019).
27. Bramwell et al., *supra* note 26, 42.
28. *Id.*at 43.
29. *United States v. Zaslavskiy*, No. 17CR647 (RJD), 2018U.S. Dist. LEXIS 156574 (E.D.N.Y. Sep. 11, 2018) (applying SEC v. W. J. Howey Co., 328 U.S. 293 [1946] at 298-99).
30. Jenson et al., *supra* note 26, 45.
31. *Id.*