Building Blocks of Blockchain:
A Primer on Cryptocurrency for Estate Planners

Estate Planning Council of North Texas

February 16, 2022

Abigail Earthman
Winstead PC
Dallas, Texas

Abigail Earthman
Winstead PC
Dallas, Texas

Abigail Rosen Earthman is a member of Winstead's Wealth Preservation Practice Group. Abigail handles federal gift and estate tax litigation against the Internal Revenue Service across the country, as well as state fiduciary and probate controversy work in Texas courts. She also counsels clients nationally regarding complex estate administration and litigation and audit risk minimization.

She is a Fellow of the Real Property, Trust and Estate Division of the American Bar Association, where she serves as Chair of the Tax Litigation and Controversy Committee. Abigail received her J.D. from Texas Tech University School of Law and an LL.M in Taxation from Georgetown University Law Center. She has represented clients before the United States Tax Court and United States District Courts in the Northern and Southern Districts of Texas.

TABLE OF CONTENTS

Building Blocks of Blockchain: A Primer on Cryptocurrency for Estate Planners [1]

Austin Bramwell
Milbank, Tweed, Hadley & McCloy
New York, NY

Abigail Earthman
Winstead PC
Dallas, TX

Benetta P. Jenson
J.P. Morgan Private Bank[2] Chicago, IL

Suzanne Brown Walsh
Murtha Cullina LLP
Hartford, CT

I. Introduction

Cryptocurrency has created a lot of buzz – both hype and skepticism. Although cryptocurrency has been in existence since 2008, it is a cutting edge issue in estate planning. Due to its technological, digital nature, cryptocurrency presents interesting and uncertain tax and practical considerations in planning with this special type of asset.

This presentation outline first will provide background on blockchain, the technology underlying cryptocurrencies, and the evolution of cryptocurrencies, such as Bitcoin, in an attempt to demystify the technical features and mechanics of both blockchain and cryptocurrencies, which generally are misunderstood. Even the terminology is confusing so this outline also includes a glossary of the terms used in this area of the tech world which could be viewed as a different language all together.

This outline then addresses planning and specific areas of consideration, such as fiduciary issues related to access to digital assets, transfers, trust funding, custody and titling, which highlight the importance and the need for proper planning and drafting. The characterization of cryptocurrencies as "property" and not currency for purposes of taxation and other regulatory considerations round out the discussion while weaving in areas of planning opportunities and challenges.

II. Background[3]

On May 22, 2010, user "Laszlo" posted on Bitcointalk.org's forum the following: "I'll Pay 10,000 bitcoins for a couple of pizzas . . . like maybe 2 large ones so I have some left over for the next day. I like having left over pizza to

---

[1] These materials are prepared as of November 5, 2018. The author of the various sections of this presentation outline is noted in the appropriate sections, but for the ease of readers, we compiled the sections into one document and Benetta P. Jenson edited throughout. These materials do not constitute, and should not be treated as, legal or tax advice regarding the use of any particular estate planning or other technique, device or suggestion, or any of the tax or other consequences associated with them. Although every effort has been made to ensure the accuracy of these materials and the seminar presentation, none of Austin Bramwell, Abigail Rosen Earthman, Suzanne Brown Walsh, or Benetta P. Jenson, Milbank, Tweed, Hadley & McCoy, Winstead PC, Murtha Cullina LLP, and J.P. Morgan Private Bank assume any responsibility for any individual's reliance on the written or oral information presented during the seminar. Each seminar attendee should verify independently all statements made in the materials and during the seminar presentation before applying them to a particular fact pattern, and should determine independently the tax and other consequences of using any particular device, technique or suggestion before recommending the same to a client or implementing the same for a client.

[2] "J.P. Morgan Private Bank" is a marketing name for private banking business conducted by JPMorgan Chase & Co. and its subsidiaries worldwide. JPMorgan Chase & Co. and its affiliates and/or subsidiaries do not practice law, and do not give tax, accounting or legal advice, including estate planning advice. See further disclaimer at the end of the presentation.

[3] The author of Section II of this presentation outline is Abigail Rosen Earthman.

nibble on later ..... If you're interested please let me know and we can work out a deal."[4] Other forum members replied to Laszlo, some thinking that he was crazy and others believing that Laszlo's offer was fake. User "Jercos" took Laszlo up on the offer, delivering to Laszlo two pizzas and he received 10,000 Bitcoins ("BTC") in exchange. The transaction between Laszlo and Jercos was the first documented purchase made with BTC and, at the time, cost Laszlo about $41 (each BTC being worth less than $0.05).[5] In late December 2017, Jercos's 10,000 BTC were worth more than $197,000,000, when BTC hit a record high. Today, Jercos's BTC are worth approximately $66,000,000. Not a bad return on investment considering Jercos paid Papa John's to cook and deliver the pizzas to Laszlo (whose identity was later revealed as Laszlo Hanyecz), while Jercos (whose identity was later revealed as Jeremy Sturdivant) sat at his computer.

A. Blockchain and Cryptocurrencies – In General

1. Blockchain. Blockchain is the underlying technology of cryptocurrencies, like Bitcoin and others such as Ethereum and Litecoin. Over the past decade and, even more recently, blockchain technology has drawn significant attention from technical developers and financial institutions (among several others), as it has the potential to overhaul almost every interaction, financial or otherwise, in our lives. From wealth management firms to gamers, people are seeking out opportunities to reap the benefits of blockchain technology. As further described throughout this paper, the fundamental components of blockchain technology involve the use of a distributed ledger stored on a highly encrypted, immutable ledger, which is verified by a peer-to-peer network.

2. Cryptocurrencies. New blockchain technology users often ask, why do we care about cryptocurrencies? Why do we need blockchain technology? What problems does it solve? And what is wrong with our current system? Blockchain technology really came to the forefront during the 2008 financial crisis when people began to lose faith in the government and other institutions designed to protect the public's common interests. After 2008, people questioned banking systems' and the government's ability to regulate financial markets. Since then, society's trust in institutions, whether financial, academic, or government, has steadily declined. As further described below, blockchain technology solves many of the problems that institutions currently face and has the potential to restore trust, not only for our regulatory system, but also between and among complete strangers.

So what is wrong with the current banking system? Some perceive the banking system as slow, expensive, and subject to hacking, all problems that, to a certain degree, blockchain technology solves as follows:

a. Faster. In the traditional regime, if Celia who lives in China wants to send $200 to Fisher who lives in Finland, Celia first would need to inform her bank that she would like to initiate a transfer to Fisher. In turn, Celia's bank would verify that she had $200 in her bank account and might charge a fee to convert the currency to Finnish coin and perhaps a second fee for transmitting the payment. Celia's bank then would send a message to Fisher's bank to ensure that he has a valid bank account that could accept Celia's funds. Once confirmed, Celia's bank would update its account ledger to reflect a deduction of $200 from Celia's account and then Fisher's bank would update its account ledger to reflect an addition of $200 to Fisher's account. At best, this process can take a full day, at worst over a week.

If Celia and Fisher were to use blockchain technology, Celia and Fisher would cut out the middlemen (*i.e.*, the banks) and would work directly with each other on a peer-to-peer network. Celia would submit the requested transfer to the blockchain. Computers (sometimes referred to as "miners," as further defined and explained below) would verify that Celia had $200 dollars in her account and that Fisher's account information was valid. Once initially validated, the transaction would be sent to a network of users, and in turn,

[4] For the full post, *See* https://bitcointalk.org/index.php?topic=137.0 (last visited November 5, 2018).
[5] *See* https://www.blockchain.com/btc/tx/a1075db55d416d3ca199f55b6084e2115b9345e16c5cf302fc80e9d5fbf5d48d for the recording of the transaction (last visited November 5, 2018).

each miner also would verify the transaction as valid. The transaction then would be added to every ledger on the network (or "node") and would take only minutes to complete.

b. **Less Costly.** Most banks charge fees to wire funds, convert currencies, effectuate a large transfer, or open an account. Retail stores also pay fees to process credit card transactions. Blockchain eliminates the majority of these fees because there is no central point of processing needed. Instead, users verify others' transactions in exchange for verification and processing of their own transactions. Participating in the network is like participating in a community garden - everyone is in and the community benefits from everyone else's efforts.

c. **More Secure.** Every year we hear about one or more major cyberattacks. The attack on Equifax in 2017 affected 143 million people. The attack on Adult Friend Finder in 2016 divulged the very private information of 412 million people. In 2015, Anthem was attacked and 78 million people had their private health information disclosed. Perhaps the biggest attack occurred in 2013, when the accounts of 3 billion Yahoo users were compromised.

Blockchain technology certainly is susceptible to attacks and malicious use (see "consensus hijacking" below), but in comparison to banks, blockchain technology arguably is more secure. First, the blockchain is secured by multi-layer cryptography that even the best mathematician could not solve without the use of a sophisticated super computer with a high technological function called quantum computing.[6] In addition, each transaction is individually recorded on the blockchain, so if one transaction were hacked, other transactions would be protected.

B. Demystifying Blockchain

What is a blockchain? How was the first blockchain developed? How does blockchain work?

On October 31, 2008, Satoshi Nakamoto[7] published a white paper entitled, "Bitcoin: A Peer-to-Peer Electronic Cash System."[8] The white paper explains both blockchain technology and how cryptocurrencies, such as Bitcoin, work using blockchain technology. Satoshi's paper contains several principles, all of which together form the backbone of a blockchain.

In the paper's abstract, Satoshi asks for "[a] purely peer-to-peer version of electronic cash [that] would allow online payments to be sent directly from one party to another without going through a financial institution." Stating that "a trusted third party" should not be required, Satoshi instead proposes a network of time-stamped transactions (or "hashes") "that cannot be changed without redoing the proof-of-work[9]."

Satoshi further states that "[central processing unit] power is controlled by nodes that are not cooperating to attack the network." In other words, Satoshi's paper calls for a peer-to-peer network, without the use of financial institutions, using cryptography (as security), wherein people trust the network as opposed to an institution.

Satoshi's brainchild was incredibly complicated, which was part of the reason why it has taken the world a long time to venture into these possibilities. The principles of blockchain technology were first applied in the financial sector in January 2009 when the first block (like a page in a ledger and referred to universally

---

[6] For an overview of quantum computers and quantum computing, *see* https://abcnews.go.com/Technology/wireStory/ap-explains-us-push-boost-quantum-computing-58041931.

[7] Satoshi Nakamoto's name is actually a pseudonym. No one has met him or her, and no one has been able to determine who he or she really is. It is even unclear whether he or she is still alive, a fact that adds to the mystique surrounding Satoshi's whitepaper.

[8] A copy of Satoshi's paper may be found at https://bitcoin.org/bitcoin.pdf (last visited November 5, 2018).

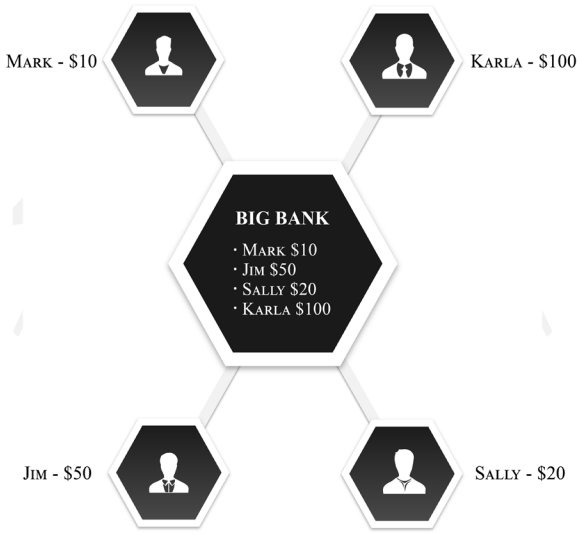
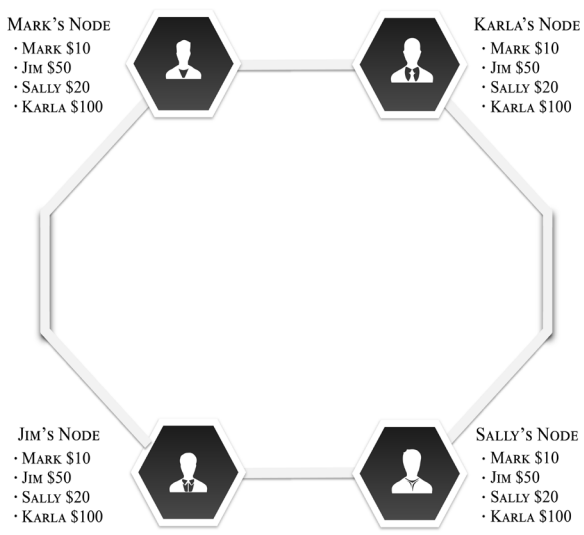
[9] *See* Glossary for definition of "proof-of-work."

as "the genesis block") of the Bitcoin blockchain was formed.[10] Almost ten years later, the Bitcoin blockchain has over 555,000 blocks all linked together, forming a chain. And this number grows every day.

It is important to note that there is no single blockchain, but rather there is blockchain technology and several blockchains. The Bitcoin blockchain is only one example and it is the first of its kind. Other cryptocurrencies have their own blockchain, with varying functions and capabilities. For example, Ethereum has the Ethereum blockchain, which can execute smart contracts, a capability that the Bitcoin blockchain does not have. The essence of blockchain technology, however, is that all blockchains are essentially *distributed ledgers* that record transactions on linked blocks stored on a highly encrypted[11], immutable ledger verified by a peer-to peer network.

C. What is a Distributed Ledger?

A fundamental component of a blockchain is that the ledger or recording of transactions is kept on a *distributed* ledger, as opposed to a *central* ledger. As Satoshi points out in his paper, the problem institutions face is that data is stored in a central location, where consumers must trust a centralized authority to properly maintain and secure a ledger. Blockchain technology's solution is that everyone who is part of the peer-to-peer network will have an exact copy of the ledger, such that each transaction is recorded on each copy of the ledger and peers check one another's changes to the ledger. The theory is that a distributed ledger distributes trust among network participants, as opposed to a central authority, and more participants in the network leads to stronger overall trust.

Centralized Ledger	*Distributed Ledger*
	
• Big Bank has a central ledger that records and accounts for Mark, Jim, Sally, and Karla's individual accounts. • Mark must reconcile his ledger that describes his account against Big Bank's larger ledger and must convince Big Bank that his ledger is correct, if discrepancies arise.	• There is a distributed ledger, and all of Mark, Jim, Sally, and Karla have a copy of it. • Mark, Jim, Sally, and Karla are participants in the network through their computers called "nodes." • All nodes, or participants, agree to a protocol that determines what constitutes the actual ledger at any point in time, which also is referred to as achieving

[10] *See* Glossary for full technical definitions.

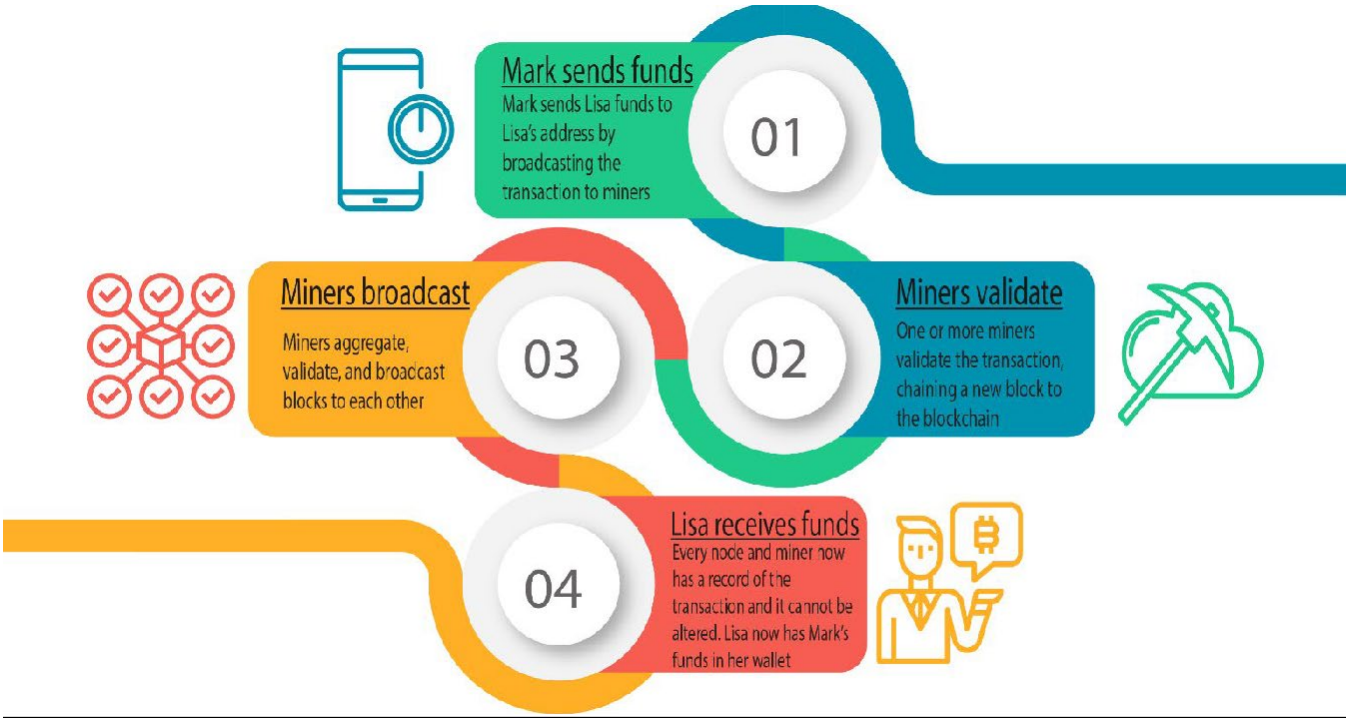
[11] A blockchain uses cryptographic hashing algorithms to secure the transactions on a blockchain. Secure Hash Algorithms ("SHAs") are derived from the United States' National Security Agency which made SHAs publicly available. Blockchains may use other hash algorithms, but they typically use SHA 256. SHAs are highly complex and are outside the scope of this paper.

consensus. Once consensus is achieved, the transaction is permanently recorded.

D. What Does a Transaction on a Blockchain Look Like?

Understanding how a transaction on a blockchain might look provides insight on concepts that are important for planners to know in order to properly advise clients on how to plan using cryptocurrencies:

Mark who lives in Montreal wants to send Lisa who lives in Lisbon 5 Bitcoins for graphic design work Lisa performed. Mark and Lisa are both participants on the Bitcoin blockchain and each have Bitcoin wallets on their computers. Wallets[12] essentially are files that provide access to blockchain addresses and an address is a string of alphanumeric characters. For example, an address might look like the following: 1FcyBEKt5S2GDtv7aQw6rQepAvnsRyHoYM. Each Bitcoin blockchain address holds a balance of Bitcoins.[13]



(1) Lisa might send her address to Mark via a bar code or other digital signature form. Once Mark initiates the transaction on his computer, the four steps outlined above diagram occur within a matter of minutes. Mark's wallet has a cryptocurrency address and a private key, which broadcasts the payment to a Bitcoin miner or miners.

(2) Miners are supercomputers or a pool of supercomputers that bundle transactions over the past 10 minutes or so into blocks. Miners perform the function of "hashing" the transaction or making the transaction secure using cryptography. Simplistically, miners "hash" a transaction by solving a complex math equation, which they are

[12] Wallets can either be stored as "cold" or "hot." Cold storage is a wallet that is held offline usually on a sophisticated USB drive. Hot storage is when the wallet is held online. Cold storage is the safest way to store a wallet because only the physical holder of the wallet/USB drive can access and use the cryptocurrencies stored in the cold wallet. However, if the wallet/USB drive is lost, stolen, or the user fails to remember the passkey, the wallet may be lost in its entirety. Conversely, because a hot wallet is stored online, it is susceptible to hacking or hijacking. For more details, *see* terms "Hot Wallet" and "Cold Storage" in the Glossary.

[13] While some may analogize a blockchain address to an account number at a bank, a blockchain address is different. Participants have the ability to create multiple addresses and often do so for each transaction in order to increase privacy of the transaction. Only those who know the address will have the ability to know the parties to the transaction.

constantly doing. After a short period of time, a miner will take a series of transactions and will complete them, which creates a block. The newest block then is linked to additional blocks in a chain (the number of blocks make up the block height and the full chain is called a distributed ledger).

(3) Miners verify that Lisa and Mark both have valid Bitcoin blockchain addresses and wallets that can send and receive funds. Miners also verify that Mark has 5 Bitcoins in his Bitcoin wallet and that the coins have not been used before, avoiding the "double spend" problem.

(4) Once Mark and Lisa's transaction is on the Bitcoin blockchain, it cannot be altered. It is immutable. Any participant in the network at any time can go back and verify the transaction and copies of the transaction are shared on the distributed ledger, where every node/computer has a copy of the ledger. No central participant controls the entire ledger, making the blockchain more secure than a central database. If one tried to alter a block that contained the transaction (a hard feat itself), they then would need to go into every previous block and change that transaction as well, ensuring that all blocks had the same data, which is nearly impossible.

E. What is the Future of Blockchain?

Most people hear the word "blockchain" and only think of financial transactions. Although blockchain technology is well suited for financial applications, blockchain technology will reach industries and other areas into the future. Two examples of applications of blockchain technology are described below: (1) government elections and (2) estate planning. The reach of blockchain technology certainly is not limited to these other applications, as developers are constantly thinking of new ways to apply blockchain technology.

1. **Government Elections.** In recent years, developers have created technologies that allow them to build programs using blockchain technology as the backbone of an application. Although it might be a long way away for some countries, governments potentially could use blockchain technology to overhaul voting systems. Our current voting system (a) is susceptible to hacking, (b) is generally administered through a central institution, (c) involves a lengthy process of registering, going to polling place, secretly voting, and waiting hours to find out results, and (d) necessitates the use of many people (from an electoral commissioner to identification checkers at polling stations). Our current voting system also relies on the community's trust of the voting system, which may be difficult in countries with large amounts of corruption and dictatorships. By using blockchain technology to change the voting system, many of these countries potentially could have free open elections with less fear of abuse and corruption.

   Blockchain developers currently are working on solving the problems with the existing voting system by using smart contracts along with a distributed ledger, all of which will be housed on a blockchain. Implementing blockchain technology for voting is not a hypothetical anymore. The State of West Virginia contracted the Boston-based company, Voatz, to allow smartphone voting for overseas military personnel during the 2018-midterm elections. Members of the military can cast their vote electronically via their smartphone and the blockchain will anonymously record their votes.[14] While West Virginia piloted the program successfully in two counties in May 2018 for local elections, it still recognized that a change to an online/blockchain-based voting system will not occur overnight, but rather will be a process.

2. **Estate Planning.** There are at least a handful of companies that are exploring using blockchain technology in estate planning. For example, the company, Proof of Existence, allows users to "notarize" documents on a blockchain. There are several other companies who also claim to perform this service already. However, no user would want his or her actual document stored on a blockchain for all to see. Similar to a financial transaction, what is stored on a blockchain is not the identity of the participants in the transaction or the document itself, but rather a cryptographic digest of the information. This cryptographic digest of information is time-stamped on a blockchain and allows a user to later show to others the particular time-stamped place in time that the document existed.

[14] *See* https://money.cnn.com/2018/08/06/technology/mobile-voting-west-virginia-voatz/index.html (last visited November 5, 2018).

Notarizing a document on a blockchain might be an easier feat, of course, than executing a will or trust, but that is exactly what companies such as Will and Testament Coin, Heir (who just launched their initial coin offering, or "ICO"), and Blockchain Apparatus aim to do (all in different ways).[15] These types of companies propose that one day, people will be able to register their will or trust on a blockchain, which would reduce will contests and an array of other issues after death. Additionally, developers propose that by using a smart contract with a specific protocol, trust distributions and payments could happen instantly upon the occurrence of an event (*e.g.*, a trust distribution can be made to a particular beneficiary upon turning age 25). Developing these types of protocols, however, might be many years away, as there are numerous issues still to consider (*e.g.*, how to hold a reserve for taxes, who would be considered the executor or trustee of digital trusts and estates).

F. Glossary

Terminology with respect to blockchain and cryptocurrency is like another language. Many terms and acronyms already have been defined above but for ease of reference, this glossary consolidates those terms and their definitions and includes additional terms.

Airdrop: A term which refers to the distribution of new cryptocurrency to all holders of an existing cryptocurrency.

Altcoin: A commonly used term to refer to a cryptocurrency other than Bitcoin (*e.g.*, Litecoin (LTC), Stellar (XLM), Zcash (ZEC), Monero (XMR)).

Bitcoin ("BTC"): The first open-source, decentralized digital asset or currency that used blockchain technology to operate a global peer-to-peer network without the need for a middleman.

Bitcoin Payments: A peer-to-peer system where transactions occur directly between two users without a central middleman. Network nodes verify each transaction and record each transaction on a publicly distributed ledger or the blockchain. The general public tends to think of Bitcoin payments as the first cryptocurrency, however, other, less sophisticated systems were available prior to Bitcoin. Bitcoin, in 2009, however, became the first decentralized digital currency and remains the largest digital currency in market value, with a total market cap of over $111 billion dollars, as of November 2018.[16]

Block: A verified group of transactions that are permanently recorded on the blockchain. A block is similar to a page in a ledger book. Miners perform the work of building each block and each block references the previous block, creating a chain of blocks in linear sequence.

Blockchain: A series of linked, verified blocks, on a shared ledger that serves as a historical record of all transactions that occur.

Blockchain 1.0: Refers to the use of the blockchain for transactions involving cryptocurrencies as currency in applications such as digital payment systems, remittance, and general banking.

Blockchain 2.0: Refers to the use of the blockchain for use in applications involving contracts, mortgages, lending, title verification, and smart contracts.

Block Explorer: A tool that can be found online that enables a user to view all transactions on the blockchain. The website provides information regarding hash rates, addresses, and transactions. *See* https://blockexplorer.com/ (last visited November 5, 2018).

Block Height: The number of blocks connected on a particular blockchain, starting with Block 0, known as the Genesis Block.

---

[15] *See* https://blockcahinapparatus.com/smart-contracts that states "Blockchain Tech Corp. currently is developing a self-executing will system where the blockchain will automatically check the government's 'Death Master File' maintained by the U.S. Social Security Office and verify that a person did in fact pass. Then, pre-programmed rules setup by the person will automatically distribute their assets to beneficiaries eliminating the need for executors and court battles because the integrity of a will is in question." However, as of November 5, 2018, the website for Blockchain Apparatus has been suspended.

[16] *See* https://coinmarketcap.com/currencies/bitcoin/ (last visited November 5, 2018).

Central Ledger: A ledger maintained by a central agency, such as a bank. Generally, only one or a few copies of the ledger exist.

Cold Storage: The act of moving cryptocurrency offline as a safekeeping measure to prevent hacking or theft. Typical cold storage involves a sophisticated USB drive with multi-layer authentication.

Confirmation: The result that a blockchain has been verified by a consensus of the network through a verification process called mining. Once a transaction has been confirmed it cannot be double spent, reversed, or altered.

Consensus: When a transaction is validated by all users of the blockchain, such that the transaction is recorded and all ledgers are exact copies of each other.

Consensus Hijacking or a 51% Attack: A hypothetical scenario where a miner or miners controlled by a hijacker or a consensus of people controlling multiple miners, control and overtake more than 51% of a network's power to the disadvantage of others. The controller or controllers of the 51%+ may use their power to "double spend" and potentially can break down the network because transactions cannot be verified. A blockchain that has been in existence for a while is less susceptible to a 51% attack, while a younger blockchain is more susceptible to a 51% attack.

Consortium Blockchain: A partly private blockchain where participation in the verification process is limited to a fixed set of nodes. For example, a group of financial institutions might form a consortium blockchain among themselves, requiring 12 of the 15 participants to verify a transaction before a block is valid. Often considered a partially-decentralized system, as the ledger may only be visible to those participants in the consortium.

Cryptocurrency: A digital currency that is secured through cryptography and cannot be unlocked or read without a key. Other terms used synonymously with "cryptocurrency" are "digital currency" and "virtual currency".

Cryptocurrency Address: A string of alphanumeric characters used to send and receive transactions on the Blockchain network.

CryptoKitties: One of the all-time most popular Decentralized APPs ("DAPPs"; see below for definition of a DAPP) thus far and perhaps the most well-known usage of a smart contract, with over 3.2 million transactions, as of November 2018.[17] With a following like that of trading cards, the DAPP allows users to buy, sell, breed, and collect kittens. Interactions with the smart contract are responsible for logging transactions and generating kittens, with the technical details of the smart contract creatively interpreted on a website interface.

Decentralized APP ("DAPP"): An application on the internet that is decentralized and not controlled by a single entity. To be considered a DAAP the application must have four characteristics: (1) autonomous operation, where changes may only occur by a consensus of the users, (2) recording of the application's data must be stored on a blockchain that is decentralized and public, (3) the application must be incentivized using a cryptographic token, and (4) the application must operate according to standard cryptographic protocols that show proof of value.

Decentralized Autonomous Organization ("DAO"): An organization, or product, that operates autonomously and is built on a smart contract or contracts on the blockchain. For example, a person can create a smart contract where 100 Ethereum coins (ETH) are coded and 5 ETH is paid automatically to a specific address each year without allowing anyone to change this direction. This smart contract is a DAO because it can be set up in a way wherein no person can alter it and it is executed automatically until its termination. Many initial coin offerings ("ICOs") use the DAO model to raise initial funds. The funds are escrowed on a DAO contract that pay out funds over time to development teams.

Distributed Ledger: Unlike a centralized ledger that a bank typically uses, a distributed ledger is housed across a network of nodes, each having a copy.

Distributed Network: A network wherein data and processing power or computing power is spread over multiple nodes rather than in one centralized data center.

Double Spend: When a person attempts to spend the same sum of money twice. If this were to occur at a bank, the bank would see the two transactions and cancel one or both transactions. Having no central authority such as a bank, the blockchain cannot do this. That said, the cryptography of the blockchain makes double spending extremely difficult. An attacker would not be able to double spend simultaneously because if an attacker sent out two conflicting transactions the entire network would be

[17] *See* http://dappboard.com/app/application/5a5849635d7064dc7fb37cd0 (last visited November 5, 2018).

able to see both transactions and would invalidate one. Alternatively, an attacker could send one transaction after another, but the blockchain would invalidate the second transaction because it references an amount that had already been spent seconds ago.

Ethereum: The world's second largest cryptocurrency by market cap, with a market cap of over $21 billion, as of November 2018.[18] Vitalik Buterin, a then 19-year old computer programmer, developed the Ethereum blockchain in 2009. Buterin then publicly launched the Ethereum blockchain in 2015, after he successfully crowdfunded approximately $25 million. The Ethereum blockchain, unlike the Bitcoin blockchain, combines both open-source software and smart contracts.

Ethereum Enterprise Alliance ("EEA"): A non-profit organization that is "the industry's first global standards organization to deliver an open, standards-based architecture and specification to accelerate the adoption of the Enterprise Ethereum." *See* http://entethalliance.org (last visited November 5, 2018). Members of the EEA include mostly Fortune 200 companies, such as Hewlett Packard, Toyota, Samsung, Microsoft, Intel, ING, BNY Mellon, J.P. Morgan, and Santander. Law firm members of EEA include BakerHostetler and Pepper Hamilton LLP. Accounting firm members of EEA include Deloitte and Ernst & Young.

Fiat Currency: Legal tender that a government designates as currency.

Genesis Block: The first block in a blockchain, which also is referred to as 0 block.

Giveaways: Transfers of cryptocurrency to those who create an account.

Hard Fork: When one blockchain divides into two separate blockchains. Generally, the result is two competing versions of the split blockchain that have the exact same history up to the point of the split, where the rules of the particular blockchain diverge. With respect to cryptocurrencies, forks generally occur when new governance rules are built into the blockchain's code.

Hash Rate: A term generally used to describe the efficiency of a mining rig, expressed in hashes per second.

Hot Wallet: A cryptocurrency wallet that is connected to the internet. An example of a hot wallet is a wallet held at a cryptocurrency exchange.

***Howey* Test:** A test named after the U.S. Supreme Court case, *SEC.* v. *Howey*, 328 US. 293 (1946), that determines whether a particular transaction qualifies as an "investment contract" for securities law purposes. A transaction is an investment contact, in simplistic form, if the transaction is: (1) the investing of money, (2) the expectation of a profit from the investment, (3) the investment is a common enterprise, and (4) the third party or promoter makes a profit from his or her efforts in promoting the investment. If the transaction qualifies as an investment contract, then the transaction is considered a security and must meet certain disclosure and registration requirements imposed by the Securities Exchange Commission ("SEC"). It is important to note that the SEC argues a very broad definition of the *Howey* Test and has stated that the majority of ICOs are securities.[19]

Initial Coin Offering ("ICO"): During an ICO an entity issues an initial set of tokens or virtual coins to investors to raise capital, similar to an initial public offering or IPO. If a token passes the *Howey* Test, it is treated as a security and subject to SEC restrictions and regulations. As of the end of October 2018, there were 1,160 ICOs with a total capital raised of $7,168,628,996 (compared to 2016 where there were only 29 ICOs with $90,250,273 raised in capital). [20]

Mining: The process of applying high amounts of computing power to solve complex mathematical equations that validate transactions on the blockchain; which is similar to a review process that an auditor typically would perform. As an incentive, miners are rewarded with units of the virtual currency they are mining/validating. Mining usually involves the use of a supercomputer or a collective of supercomputers.

Mining Pool: A collective group of miners that come together to solve complex mathematical equations that validate transactions quicker than a single miner. The mining reward is split among miners according to the contributed processing power of each miner. As a single blockchain gets longer and/or more miners contribute, mining (solving the mathematical equations) becomes more difficult because a single computer will lack the computing power to validate a transaction in a timely

---

[18] *See* https://coinmarketcap.com/currencies/ethereum/ (last visited November 5, 2018).

[19] *See* https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11#_ftnref7 for a Statement on Cryptocurrencies and Initial Coin Offerings by the SEC Chairman Jay Clayton on December 11, 2017.

[20] See https://www.icodata.io/stats/2018 for IPO statistics for 2018 through the end of October 2018 and https://www.icodata.io/stats/2016 for 2016 statistics.

manner. Mining pools work around this problem. Slush Pool is the first and oldest publicly available mining pool. *See* https://slushpool.com/home/ (last visited November 5, 2018).

Node: Any computer that connects to a particular blockchain network that possess a copy of the blockchain. The computer connected to the blockchain network has the ability to see every transaction on the blockchain back to Genesis Block, but would not be able to identify the parties to the transactions without a specific key.

Peer-to-Peer ("P2P"): Decentralized transactions between parties on a highly interconnected network without the use of a single mediation point.

Private Blockchain: A blockchain where network control is centralized. For an example, *see* Ripple (XRP).

Private Key: Similar to a password, a private key is a string of data that allows one to have access to that users' cryptocurrency in a wallet. Private keys typically should be kept offline, as anyone who has access to it could spend all of the cryptocurrency contained in the wallet.

Proof-of-Work ("PoW"): A type of algorithm to validate transactions and achieve consensus. The algorithm rewards miners who solve mathematical problems that validate transactions and those miners then are creators of a new block.

Proof-of-Stake ("PoS"): A type of algorithm to validate transactions and achieve consensus. The algorithm does not provide a reward, but rather the creator of a new block is chosen based on its wealth (*e.g.*, how many coins are held).

Satoshi Nakamoto: The author of the white paper that outlined the basic elements of blockchain technology. Mr. or Ms. Nakamoto is a mysterious person to the blockchain community as no one has ever met or been able to find information on him or her. Satoshi also is responsible for writing the Bitcoin code that launched the Blockchain Network in 2009.

Sharding: The ability to split a blockchain into several partitions, each having their own miners and/or nodes. This is a scaling solution for blockchains. Typically, every node in a blockchain network houses a complete copy of the blockchain. Sharding is a method that allows nodes to have partial copies of the complete blockchain in order to increase overall network performance and consensus speeds.

Smart Contract: A basic building block of the Ethereum blockchain. Agreements that execute on their own based on a set or sets of variables. Advantages of smart contracts include not having to trust a middleman, security (due to the fact one cannot change the terms of the contract once they are placed on the blockchain without changing every block on the chain, which is statistically almost impossible), and speed (a smart contract is considerably faster than executing a contract in a normal fashion).

Soft Fork: A change to protocol that does not require a new version. Some blockchains allow for configurable variables with a simple consensus (*e.g.*, a change to block size). In this scenario, as long as 51% of the miners move to the new protocol, both the new and old protocol will continue to work.

Token Swaps: Decisions by developers of a virtual currency to move to an entirely new protocol, so that existing holders must move to the new protocol or else forfeit their cryptocurrency.

Virtual Currency: Internal Revenue Service ("IRS") Notice 2014-21 defines "virtual currency" as a "digital representation of value that functions as a medium of exchange, a unit of account, and/or a store of value." Cryptocurrency is a form of virtual currency by the IRS definition.

III. Planning with Cryptocurrencies[21]

A. Fiduciary Issues and Considerations. In the past, fiduciaries responsible for managing assets could easily marshal, collect, and manage such assets. Often, the biggest nuisance was convincing a recalcitrant financial institution to honor a power of attorney, and personal representatives and conservators, armed with court decrees, encountered few problems. That landscape has changed with the advent and popularity of digital assets and accounts.

[21] The author of Sections III.A. and III.B. of this presentation outline is Suzanne Brown Walsh. The author of Section III.C. is Austin Bramwell. The author of Section III.D. is Benetta P. Jenson.

1. Fiduciary Access to Digital Assets

a. In general. Marshaling assets is a critical fiduciary duty, as it is impossible to manage a person's assets or estate until the assets are identified and collected. Marshaling traditional assets can be challenging. Digital assets and files, passwords to online accounts, and encryption on locally stored files or assets impose additional barriers to fiduciary access. Federal privacy and anti-hacking laws further impede fiduciary access.

b. Stored Communications Act. The Fourth Amendment to the U.S. Constitution provides citizens with a strong expectation of privacy in their homes. As a result, the government usually cannot search homes without first showing probable cause and obtaining a warrant authorizing a search.

When we use a computer network, we may have the same expectation of privacy. However, because the network is not physically located or even being accessed in our computers or in our homes, it is outside the coverage of the Fourth Amendment.[22] To fill that gap, in 1986 Congress enacted the Stored Communications Act ("SCA") as a part of the Electronic Communications Privacy Act ("ECPA")[23] to respond to concerns that internet privacy poses new dilemmas with respect to application of the Fourth Amendment's privacy protections. The SCA prohibits certain providers of *public* electronic communications services from disclosing the *content* of its users' communications to a government or nongovernment entity (different rules apply to each) except under limited circumstances that are akin to the warrant required under the Fourth Amendment.[24] The SCA regulates the relationship between the government, internet service providers ("ISPs"), and users in two distinct ways.

(1) Limitations on Disclosure of Information on Subscribers. First, the SCA establishes limits on the government's ability to require ISPs to disclose information concerning their subscribers. An ISP may not disclose to the government any records concerning an account holder or the content of any electronic communications in the absence of an applicable exception, such as consent by the account holder.[25]

Providers are permitted, but not required, to divulge non-content, such as the user's name, address, connection records, IP address, and account information to a nongovernmental entity.[26] The subject line of an email has been held to be content protected by the SCA.[27]

(2) Limitations on Disclosure of Content of Communications. Second, the SCA establishes limits on the provider's ability to voluntarily disclose to the government or any other person or entity the content of communications.[28] All

---

[22] *See generally* Orin S. Kerr, *A User's Guide to the Stored Communications Act*, *and a Legislator's Guide to Amending It,* 72 Geo. Wash. L. Rev. 1208 (2004).

[23] Pub. L. No. 99-508, 100 Stat. 1848 (1986). The ECPA is codified at 18 U.S.C. §§ 2510–2522. The SCA is codified at 18 U.S.C. §§ 2701-2711.

[24] *See generally* Kerr, *supra* n. 22, at 1214.

[25] 18 U.S.C. § 2702(a)(1) prohibits voluntary disclosure of the content of an electronic communication to anyone, whereas 18 U.S.C. § 2702(a)(3) prevents the voluntary disclosure of records to the government (although not to others). Depending on the nature of the data, the government must obtain either a subpoena or a warrant, although some exceptions exist in the case of an emergency. 18 U.S.C. § 2702(b).

[26] *Id.* at § 2702(c)(6).

[27] *Optiver Austrl. Pty. Ltd. v. Tibra Trading Pty. Ltd.,* Case No. C 12-80242 EJD (PSG), 2013 U.S. Dist. Lexis 9287 (N.D. Cal. Jan. 23, 2013).

[28] *See* Kerr, *supra* n. 22, at 1212–1213 ("The statute creates a set of Fourth Amendment-like privacy protections"). The 2013 revelations of Edward Snowden provide another angle on the SCA and providers' willingness to disclose. The providers did not want to disclose some information, and the National Security Agency either coerced them to disclose the information or simply took the information without their knowledge. *See e.g.* Ryan Lizza, *The Metadata Program in Eleven Documents*, New

private social media account content (*e.g.*, photos, videos, posts) is protected by the SCA.[29]

A provider of public electronic communications services can *voluntarily* disclose the content of communications, but only if an *exception* to the SCA's blanket prohibition against disclosure applies.[30] The relevant exception for fiduciaries permits (but does not require) a provider to disclose communication content if the provider has the "lawful consent" of "the originator," an addressee or intended recipient of the communications, or the subscriber.[31] There is evidence that Congress intended authorized agents to be able to authorize disclosure of the contents of electronic communications.[32] However, some providers refuse to give executors access to the content of decedents' email accounts without the added assurance of a court order stating that the executor has the user's lawful consent.

On October 16, 2017, the Massachusetts Supreme Judicial Court ("SJC") issued its long-awaited decision in *Ajemian v. Yahoo!, Inc.* ("Yahoo")[33], interpreting the federal SCA to allow Yahoo to divulge the contents of a decedent's email account based solely on the personal representative's consent. Although the decision does not order Yahoo to immediately disclose the emails to the personal representatives, it firmly repudiates the position of the industry that the SCA completely bars such disclosure. As such, it represents a huge victory for fiduciaries and families seeking access to protected communications.

The SJC's decision does not mandate that Yahoo disclose a decedent's email account contents to the fiduciaries; it merely holds that the SCA permits the disclosure. Presumably, the Massachusetts probate court, on remand, will simply issue an order mandating disclosure, now that the SJC has confirmed that Marianne and Robert Ajemian, as Co-Administrators, may provide Yahoo with their late brother's lawful consent under the SCA.

However, what if the probate court, on remand, does not order the disclosure, but instead agrees with Yahoo that its terms of service are binding and allows it to destroy or withhold the emails? Chief Justice Gants, writing separately, indicates that if the trial court were to hold that Yahoo's terms of service agreement were binding and permitted it to destroy the decedent's email messages, the SJC "would surely reverse that ruling." Hopefully that strong signal reaches Yahoo and convinces it to finally give Marianne and Robert Ajemian their late brother's email messages, as they requested more than 10 years ago.

Although the decision is a clear victory for the Ajemians, it still leaves important issues unresolved and important questions unanswered. For example, the Ajemians are still subject to the probate court's future ruling on whether Yahoo's terms of service agreement prevents disclosure. Also, service providers typically interpret the SCA as merely permissive and insist that they are not required to disclose emails, even with the account holder's lawful consent. It therefore will

---

Yorker, https://perma.cc/8R7Y-GBAE (Dec. 31, 2013); Ryan Lizza, *State of Deception: Why Won't the President Rein in the Intelligence Community?* New Yorker, https://perma.cc/F4KK-FVXG (Dec. 16, 2013); Laura W. Murphy, *The NSA's Winter of Discontent*, Huffington Post, https://perma.cc/3V8U-6X6W (updated Feb. 11, 2014).

[29] *See* Rudolph J. Burshnic, *Applying the Stored Communications Act to the Civil Discovery of Social Networking Sites*, 69 Wash. & Lee L. Rev. 1259, 1267–1278 (2012).

[30] 18 U.S.C. § 2702(b).

[31] *Id.* at § 2702(b)(3).

[32] Senate Report No. 99-541 on ECPA, at page 37, which says, "Either the sender or the receiver can directly or through authorized agents authorize further disclosures of the contents of their electronic communication."

[33] SJC-12237 found at https://www.mass.gov/files/documents/2017/10/16/12237.pdf (last visited November 5, 2018).

remain critically important to our clients to monitor case law throughout the States as it continues to develop in these areas.

c. Computer Fraud and Abuse Acts. The Federal Computer Fraud and Abuse Act ("CFAA") criminalizes the unauthorized access of computer hardware and devices and the data stored thereon[34]:

> "(a) Whoever— … (2) *intentionally accesses a computer without authorization or exceeds authorized access,* and thereby obtains— … (C) information from any protected computer … shall be punished as provided in subsection (c) of this section."

The CFAA criminalizes two kinds of computer trespass: (1) accessing a computer "without authorization" and (2) accessing a computer that "exceeds authorized access". The CFAA defines the term "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[35] A related provision of the statute criminalizes the same acts but additionally requires knowledge and intent to defraud.[36].

Unauthorized use includes "obtain[ing] … information" (such as by accessing emails or internet accounts) from a "protected computer," which is defined as any computer connected to a government or financial institution as well as one "used in or affecting interstate or foreign commerce or communication."[37] Because most internet servers are not located in the same state as a website's users, internet use almost always involves obtaining information from a protected computer and therefore implicates the CFAA.[38] The term "computer" includes desktop computers, laptops, notepads, tablets, and smartphones.[39]

Every state has an analogous statute, which varies in coverage, but typically prohibits unauthorized access to computers.[40]

Even though a fiduciary is authorized by the account holder or state law to use a computer or to act on behalf of an account holder, the fiduciary is not necessarily exempt from CFAA prosecution.[41] There is no question that a fiduciary is authorized, in the normal sense of the word, to access an account holder's computer or system that the fiduciary lawfully possesses, controls, or owns by virtue of the proscribed authority of a fiduciary. The analogy is that a fiduciary using, or even hacking into, a computer is no more illegal than a fiduciary using a locksmith (or crowbar) to get into a building owned by an incapacitated person, principal, or decedent. However, accessing a hard drive is technically different from accessing the account holder's digital accounts or assets, which are stored on the provider's server, not the user's. If the fiduciary is violating the account provider's terms-of-service agreement by accessing the account holder's digital accounts or assets online, the fiduciary may be violating the CFAA.[42]

---

[34] 18 U.S.C. § 1030(a)(2)(C)(2012) (emphasis added).

[35] *Id.* at § 1030(e)(6).

[36] *Id.* at § 1030(a)(4). This is the "second prong" of the CFAA.

[37] *Id.* at § 1030(e)(2).

[38] *See Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc.,* 119 F. Supp. 2d 1121, 1127 (W.D. Wash. 2000).

[39] *U.S. v. Mitra,* 405 F.3d 492, 495–496 (7th Cir. 2005).

[40] Natl. Conf. of St. Legislatures, Computer Crime Statutes, http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx (as of June 14, 2018) (last visited November 5, 2018).

[41] *See* James D. Lamm et al., *The Digital Death Conundrum: How Federal and State Laws Prevent Fiduciaries From Managing Digital Property*, 68 U. Miami L. Rev. 385, 399–401 (2014).

[42] Cahn, Naomi and Kunz, Christina L. and Brown Walsh, Suzanne, *Digital Assets and Fiduciaries*, Research Handbook on Electronic Commerce Law, John A. Rothchild, ed., Edward Elger, 2016; GWU Law School Public Law Research Paper No.

d. Revised Uniform Fiduciary Access to Digital Assets Act

The Revised Uniform Fiduciary Access to Digital Assets Act (hereafter, "Revised UFADAA")[43], gives fiduciaries limited, but much needed, access to digital assets, while taking into account the privacy and contractual rights of account holders and compliance with federal and state privacy laws.

Just as with traditional assets, in order to access digital assets held by third-party service providers, in general, fiduciaries first must provide a written request, a copy of the will, trust or power of attorney, and information linking the digital account to the customer (*i.e.*, the decedent or incapable person).

Revised UFADAA's limited default authority over electronic communications content will penalize those who fail to plan for third-party access to their online accounts and digital assets. Likewise, advisors who fail to discuss digital assets and access with their clients will be hard pressed to explain that oversight.

Sections 15(d) and (e) of Revised UFADAA confirm that a fiduciary is an authorized user of the decedent, protected person, principal or settlor's property under applicable CFAA rules and confirms that a fiduciary with authority over devices can access digital assets and files on it and is an authorized user. This clearly authorizes fiduciaries to access private keys stored on electronic devices.

Even when a cryptocurrency owner uses an online wallet instead of storing keys offline in cold storage, access to the account likely will be delayed. Virtual currency wallet/exchange companies are understandably concerned with fraud and theft. Coinbase, the largest commercial online exchange and wallet provider, has posted procedures, requiring a death certificate, last will, probate certificate, government-issued photo ID of the fiduciary, and a letter of instruction before fiduciary access will be granted.[44]

No virtual currency wallet service, as yet, has created online tools (which are akin to designations) by which the user can grant third-party access.

2. Transfers, Trust Funding, Custody and Titling

a. Trust Funding. Ordinarily, it's easy to transfer control over most assets to a trust—not so with virtual currency. There is no legal impediment to funding a trust with virtual currency, but most trustees and many traditional asset custodians are not willing to accept it at this time. One way to transfer the virtual currency to the trustee is to send the virtual currency to the trustee's online wallet account. Another would be to have the Grantor transfer his or her private key to a secure physical device, transfer the device to the trustee, and document the transfer. The former probably will be easier than the latter for a trustee who is not technology-savvy.

Coinbase presently does not support trust accounts.[45] That may be changing as corporate fiduciaries and Coinbase, explore new custody services. For example, Coinbase recently obtained a Limited Purpose Trust Company License from the New York Banking Department.[46] While this type of license allows Coinbase to act as a trustee in New York,

---

2015-18; GWU Legal Studies Research Paper No. 2015-18. Available at SSRN: http://ssrn.com/abstract=2603398 (last visited November 5, 2018).

[43] Natl. Conf. of Comm'rs. on Unif. St. Laws, Revised Uniform Fiduciary Access to Digital Assets Act (2015).

[44] *See* https://support.coinbase.com/customer/en/portal/articles/2321225-how-do-i-gain-access-to-a-deceased-family-member-s-coinbase-account- (last visited November 5, 2018).

[45] *See* https://support.coinbase.com/customer/en/portal/articles/2798697-can-i-create-a-coinbase-account-in-the-name-of-a-trust- (last visited November 5, 2018).

[46] *See* https://blog.coinbase.com/coinbase-custody-receives-trust-charter-from-the-new-york-department-of-financial-services-532c92797215 (last visited November 5, 2018).

Coinbase obtained it in order to act as a "qualified custodian" under the Securities and Exchange Commission's custody rule, which obligates investment advisers to maintain client funds and securities with a "qualified custodian." Apparently, its immediate goal was to provide cryptocurrency custody services for hedge funds, but not act as a New York trustee.

b. **UTMA Accounts**. The Uniform Transfers to Minors Act ("UTMA") defines "custodial property" as any interest in property transferred to a custodian under the Act, so any type of property, including virtual currency, is covered and can become custodial property.[47]

c. **529 Plan Accounts**. IRC § 529[48] requires that contributions to its college savings accounts be made in "cash", and that the qualified tuition program be established and maintained by the state.[49] So, unless the state treasurer's investment options include cryptocurrency investments, virtual currency cannot be held in a 529 account.

d. **UTODSRA Accounts**. The Uniform Transfer on Death Security Registration Act ("UTODSRA")[50], enacted in all states except Texas and Louisiana, applies to a security, which is defined as "a share, participation, or other interest in property, in a business, or in an obligation of an enterprise or other issuer, and includes a certificated security, an uncertificated security, and a security account."[51] This definition is derived from § 8-102 of the Uniform Commercial Code ("UCC") and includes shares of mutual funds and other investment companies.[52] Thus, UTODSRA only applies to tokens which are securities within the meaning of UCC § 8-102.

e. **Joint Transfer-on-Death Accounts**. Normally, payable-on-death and survivorship joint bank accounts are described in the state banking laws, which will not only specify ownership at death but also will clarify that the accounts are not testamentary transfers subject to the statute of wills. Absent a statutory provision that applies to a cryptocurrency account, then, it is likely that a pay-on-death designation will not satisfy the state statute of wills and therefore will fail.[53]

3. **Fiduciary Duties**

a. **Uniform Prudent Investor Act.** The Uniform Prudent Investor Act ("UPIA")[54] was approved in 1994 and is enacted in 44 states (but not in Florida, Georgia, Kentucky, Louisiana, New York and Pennsylvania). The UPIA specifies a trustee's duties to manage trust assets, eliminating all categoric restrictions on investments, so it does not mention virtual currency or any other type of asset class.[55] Trustees must comply with the act unless excused in the trust.[56] The UPIA reflects one of the main themes of modern investment practice: sensitivity to the risk/return curve.[57]

(1) **Prudent Investor Rule.** A trustee shall invest and manage trust assets as a prudent investor would, by considering the purposes, terms, distribution

---

[47] UTMA § 1(6).
[48] References to "IRC §" are to sections of the Internal Revenue Code of 1986, as amended (the "IRC" or the "Code").
[49] IRC § 529.
[50] Natl. Conf. of Comm'rs. on Unif. St. Laws, Uniform Transfer on Death Security Registration Act (1998).
[51] UTODSRA, § 1(9).
[52] UTODSRA, § 1(9), Comment.
[53] *See*, *e.g.*, Uniform Probate Code § 2-502 for the requirements of a valid will.
[54] Natl. Conf. of Comm'rs. on Unif. St. Laws, Uniform Prudent Investor Act (1994).
[55] UPIA, § 2(e).
[56] UPIA, § 1(b).
[57] UPIA, Prefatory Note.

requirements, and other circumstances of the trust. In satisfying this standard, the trustee shall exercise reasonable care, skill, and caution.[58]

(2) **Management.** Under the UPIA, "management" includes the duty to monitor the trust investments.[59]

(3) **Duty to Diversify.** "A trustee shall diversify the investments of the trust unless the trustee reasonably determines that, because of special circumstances, the purposes of the trust are better served without diversifying". [60]

b. **Uniform Prudent Management of Institutional Funds Act.** The Uniform Prudent Management of Institutional Funds Act ("UPMIFA") [61] was approved in 2006 and is enacted in all states except Pennsylvania.

(1) Like UPIA, UPMIFA applies prudent investor standards for the management and investment of charitable funds and for endowment spending.[62]

(2) As under UPIA, there are no prohibited investment classes under UPMIFA, so institutions generally may invest in any kind of property or type of investment, unless prohibited by law other than UPMIFA.[63] However, their duties under UPMIFA require institutions to dispose of unsuitable assets.

(3) While in theory a gift instrument or the governing instruments of an institution can modify most of UPMIFA's duties, the charitable purpose doctrine limits the extent of the modification.[64]

(4) UPMIFA requires institutions to diversify investments, unless due to special circumstances the purposes of the fund are better served without diversification.[65]

(5) In making decisions about whether to acquire or retain an asset, the institution should consider its mission, its current programs, and the desire to cultivate additional donations from a donor, in addition to factors related more directly to the asset's potential as an investment.[66]

B. Importance of Planning and Proper Drafting

1. **Discussion.** It is vitally important to ask clients if they own cryptocurrency and to ask fiduciaries and family members if a there is any evidence or reason to suspect that the decedent or incapable person owned any cryptocurrency. Typically, a lawyer cannot provide adequate estate planning advice without sufficient information regarding the nature, value, and manner in which the client's assets are held.[67] Under the heading "Importance of Facts", the fifth edition of the ACTEC Commentaries on the Model Rules of Professional Conduct states:

---

[58] UPIA, § 2 a.

[59] UPIA, § 2, Comment. **"**Subsections (a) through (d) apply both to investing and managing trust assets. 'Managing' embraces monitoring, that is, the trustee's continuing responsibility for oversight of the suitability of investments already made as well as the trustee's decisions respecting new investments."

[60] UPIA, § 3.

[61] Natl. Conf. of Comm'rs. on Unif. St. Laws, Uniform Prudent Management of Institutional Funds Act (2006).

[62] UPMIFA, § 3.

[63] *Id.*

[64] UPMIFA, § 3, Comment.

[65] UPMIFA, § 3.

[66] *Id.*

[67] Model Rules of Professional Conduct 1.1: Competence; the ACTEC Commentary on Model Rules of Professional Conduct 1.1, including annotations.

> "A lawyer who is engaged by a client in an estate planning matter should inform the client of the importance of giving the lawyer complete and accurate information regarding relevant matters such as the ownership and value of assets and the state of beneficiary designations under life insurance policies and employee benefit plans."[68]

While it seems unlikely that a cryptocurrency owner will fail to provide for access to his or her private keys, we all know that some people steadfastly avoid considering their own mortality. It is incumbent on the estate planner to ask about cryptocurrency and discuss access to it. Access can be provided through a technology-based plan, multi-signature wallets, or a smart contract triggered by death, for example. Or, access can be provided through a non-technology-based plan that relies on private key information that is printed and stored offline in a safe deposit box or another secure location. For those with large holdings, it would be far better to convince the client to identify a trustee or corporate custodian willing to provide custodial services, assuming one is available.

2. **Education.** Family members may not understand that without access to the private key, there is no one who can be compelled by court order to turn the asset over to the fiduciary and that cryptocurrency cannot become unclaimed property. Conversely, if the owner has provided his or her private key and file information to someone other than the fiduciary, probate by computer (the modern version of probate by truck) may be a risk.

3. **Forms and Authority.** Although access provisions sometimes have little to no utility, estate planning documents still should address authority over cryptocurrency, in addition to the dispositive provisions that apply to it.

a. Trustees who will be asked to retain the cryptocurrency for some reason will probably want to use a directed trustee for this purpose, although it may not be prudent to continue to hold cryptocurrency in a trust.

b. At a minimum, documents should include clear authority to retain the cryptocurrency and exonerate the fiduciary for doing so.

C. Taxation and Reporting

1. General Observations

a. Cryptocurrencies are a new and, until recently, unprecedented form of property (or money, depending on one's perspective). But its novelty does not necessarily call for new legal principles. On the contrary, cryptocurrencies are merely "new in the instance." The question is how existing legal principles, including tax and reporting rules, apply to them.

b. That cryptocurrencies do not call for new law is indeed how Treasury and the IRS have approached them, as discussed below.

c. A recurring theme in how to treat cryptocurrency is that the application of general principles to cryptocurrency depends on how it is characterized. For example, is it currency or property? Is it tangible or intangible? Analogies to more familiar concepts are essential to answering these quasi-ontological questions.

2. Cryptocurrency and Tax Fraud

a. Sadly, blockchain technology, because it permits anonymous transactions, also facilitates tax fraud. Perhaps every estate tax attorney has been asked whether one can give valuable tangible property to children just before death so that nobody will know about it. Cryptocurrency makes similar fraud easy and difficult to detect through anonymous

[68] ACTEC Commentaries on the Model Rules of Professional Conduct (2016), pp. 15-16.

transfers on the blockchain. Other frauds involve failing to report gain, compensation, and other income.

b. The IRS has successfully obtained information on Coinbase customers using a John Doe summons. *U.S. v. Coinbase, Inc., et al.*., 120 AFTR 2d 2017-6671 (U.S. Dist. Ct. N.D. CA 2017). In the litigation, the IRS revealed that fewer than a thousand taxpayers reported cryptocurrency gain or loss in each of 2014 and 2015.[69] Stepped-up tax enforcement efforts will continue.

3. Notice 2014-21[70]

a. Notice 2014-21remains, as of the date this outline was written, the only formal guidance issued by Treasury or the IRS on the taxation of virtual currency. However, further guidance may be issued in the near future.[71]

b. Five members of Congress, including Kevin Brady, Chairman of the Committee of Ways and Means, recently wrote a letter to Acting IRS Commissioner Kautter "strongly urg[ing] the IRS to expeditiously issue more robust guidance clarifying taxpayers' obligations" when using virtual currencies.[72]

c. In general, the approach of Notice 2014-21 is to apply "existing general tax principles" to virtual currency transactions. Notice 2014-21 does not suggest that new rules, such as in the form of regulations issued pursuant to IRC § 7805 (which grants Treasury authority "to prescribe all needful rules and regulations for the enforcement" of the Code), are necessary or will be forthcoming.

d. Definition of "virtual currency" and "convertible virtual currency."

(1) Notice 2014-21 defines "virtual currency" as a "digital representation of value that functions as a medium of exchange, a unit of account, and/or a store of value." It does not have "legal tender status in any jurisdiction."

It is unclear what the effects would be if a foreign jurisdiction *did* begin to accept cryptocurrency as legal tender. Conceivably, the foreign currency rules of IRC §§ 985-89 then could apply.

(2) Virtual currency that has an equivalent in real currency (*i.e.*, the coin and paper money of the United States or any other jurisdiction) or that acts as a substitute for real currency, is "convertible."

(3) An example of a *non*convertible virtual currency is the virtual money used in online roleplaying games. For example, in the game Pokémon Go, players acquire Pokécoins. Pokécoins, once acquired (including by paying real currency to the creators of the game), cannot be converted into real currency and therefore are not convertible virtual currency.

(4) Notice 2014-21 only addresses the tax consequences of convertible virtual currencies. When the Notice refers to virtual currency in its guidance, it refers

---

[69] *Id.*; *see also* Roberts, *Only 802 Told The IRS About Bitcoin*, Fortune (March 19, 2017), available at http://fortune.com/2017/03/19/irs-bitcoin-lawsuit/ (last visited November 5, 2018).

[70] Notice 2014-21, I.R.B. 2014-16 (April 14, 2014), www.irs.gov/irb/2014-16_IRB#NOT-2014-21 (last visited November 5, 2018).

[71] Foster, *Guidance on Cryptocurrency Issues Possible This Year*, Tax Notes Today (June 26, 2018).

[72] *See* https://waysandmeansforms.house.gov/uploadedfiles/letter_irs_virtual_currencies.pdf (September 19, 2018) (last visited November 5, 2018).

only to convertible virtual currency (as does this outline, except where otherwise noted).

e. General Rule of the Notice

Notice 2014-21 confirms that virtual currency is treated as property and that general tax principles applicable to property transactions apply to virtual currency transactions.

f. Other Issues Addressed by Notice 2014-21

(1) No foreign currency gain or loss (and thus no *de minimis* gain exception). Virtual currency cannot generate foreign currency gain or loss.

(a) Under IRC § 988(e), individuals may exclude up to $200 of foreign currency gain (per transaction) if it was disposed of in a personal transaction, such as in connection with a vacation abroad. Under Notice 2014-21, this exclusion does not apply to gains from the disposition of virtual currency.

(b) In other words, although not explicitly stated in Notice 2014-21, the IRS will not allow a *de minimis* exclusion of virtual currency gain.

(c) Commenters, including the American Bar Association and the American Institute of CPAs, have called for a *de minimis* exception. However, it does not appear that Treasury currently has the authority to grant one under the Code.

(2) Gross income on receipt, basis, and gain or loss on exchange

(a) Not surprisingly, if a taxpayer receives virtual currency in payment for goods and services, the taxpayer must include in gross income the fair market value of the virtual currency as of the date received.

(b) The basis of the virtual currency received is equal to its fair market value as of the date received.

(c) Fair market value is determined by converting virtual currency into dollars at the exchange rate listed on a virtual currency exchange (such as Coinbase), "in a reasonable manner that is consistently applied."

(d) If a taxpayer exchanges virtual currency for other property, the taxpayer may have gain or loss, depending on the fair market value of the property received versus the basis of the virtual currency exchanged.

(e) Whether gain or loss is ordinary or capital depends on whether the virtual currency is a capital asset.

"Capital asset" is defined in IRC § 1221. Generally, all property is a capital asset unless it meets one of the exceptions listed in IRC § 1221(a). Inventory, for example, or property held primarily for sale to customers in the ordinary course of trade or business, is not a capital asset. The exceptions in IRC § 1221(a) are construed broadly and the general definition is construed narrowly.[73]

Classification of property as a capital asset has two consequences under the Code. First, under I.R.C. §§ 1211(b) and 1212(b), losses on the sale

[73] *Corn Products Refining Company v. Comm'r*, 350 U.S. 46 (1955).

of a capital asset, in the case of the individual, may only offset up to $3,000 of ordinary income, with the excess carried over to future years. Second, if a capital asset is held for more than one year, gain from its sale may qualify for a lower rate under IRC § 1(h).

(f) A taxpayer who "mines" virtual currency (*i.e.*, receives virtual currency in exchange for running a computer to validate transactions and maintain a public ledger) has gross income equal to the fair market value of the mined virtual currency on the date of receipt.

(3) Employment Tax Issues

(a) Individuals engaged in the trade or business of mining virtual currency (other than as an employee) are subject to self-employment tax in addition to income tax.[74] The rates of tax are a combined 15.3% of the Social Security wage base ($128,400 in 2018). For amounts in excess of the Social Security wage base, the tax is 2.9%, plus an extra 0.9% for amounts above $200,000 ($250,000 for joint filers; $125,000 for married taxpayers filing separately).[75]

(b) The fair market value of any virtual currency that is received for services performed as an independent contractor is self-employment income subject to self-employment tax.

(c) Wages paid by an employer in the form of virtual currency are subject to income tax withholding, Federal Insurance Contributions Act ("FICA") withholding, and Federal Unemployment Tax Act ("FUTA") withholding, as well as reporting requirements.

(4) Other Reporting and Withholding Issues

(a) A payment made in the form of virtual currency is subject to information reporting to the same extent as a payment made in property. Notice 2014-21 gives as an example a payment of fixed or determinable income using virtual currency with a value of $600 or more.[76]

(b) A payment made in the ordinary course of business to an independent contractor using virtual currency with a value of $600 or more must be reported on Form 1099-MISC.

(c) Payments made in virtual currency are subject to back-up withholding to the same extent as other payments made in property if the payee's identification number is not obtained.

(5) Miscellaneous

(a) Third-party settlement organizations may be subject to informational reporting. Virtual currency and real currency transactions are aggregated.

(b) Notice 2014-21 confirms that taxpayers, including those who engage in virtual currency transactions, may be subject to various penalties for failure to comply with tax laws.

---

[74] *See* IRC § 1401 et seq.
[75] IRC § 1401(b).
[76] *See* IRC § 6041(a).

4. Foreign Reporting Requirements

a. Private keys can be held in a foreign jurisdiction. Likewise, cryptocurrency can be held through exchanges located offshore. Consequently, foreign cryptocurrency holdings may be subject to reporting as foreign account and asset holdings on Form 114 (Report of Foreign Bank and Financial Accounts) ("FBAR") and/or under Section 6038D (Form 8983). For example, an account with a foreign cryptocurrency exchange should be subject to FBAR reporting.

b. A wallet located abroad should not by itself cause a foreign financial institution ("FFI") or nonfinancial foreign entity ("NFFI") to exist for purposes of the Foreign Account Tax Compliance Act ("FATCA").

(1) Under Treas. Reg. § 1.1471-5(d) and Treas. Reg. § 1.1471-1(b)(80), FFIs and NFFIs are both categories of "entities." An "entity" for FATCA purposes is a person other than an individual.[77] A "person" includes an individual, trust, estate, partnership, association, company, corporation, and persons acting in a fiduciary capacity.[78]

(2) Mere ownership, even co-ownership, does not create a separate entity.[79] Mere agency does not create a person.[80]

(3) Under the foregoing principles, FATCA reporting and withholding requirements should not apply to mere ownership of a wallet located abroad.

5. Tax Consequences of Nonconvertible Virtual Currency

a. Nonconvertible virtual currency is virtual currency that has no equivalent in real currency (*i.e.*, the coin and paper money of the United States or any other jurisdiction) and that does not act as a substitute for real currency. *See* above example of Pokécoins from the Pokémon Go game as nonconvertible virtual currency.

b. The tax consequences of transactions involving nonconvertible virtual currencies have received much less attention than transactions involving Bitcoin and other convertible cryptocurrencies. *See* Notice 2014-21, I.R.B. 2014-16 (April 14, 2014) (declining to offer guidance on nonconvertible virtual currencies).

(1) In almost all cases, the purchase of nonconvertible virtual currency will be a personal expense that is nondeductible under IRC § 262.

(2) Perhaps, however, an individual who is a professional gamer could in some cases write off the cost of acquiring nonconvertible virtual currency as a business expense under IRC § 162.

(3) A taxpayer engaged in the unlawful buying and selling of nonconvertible virtual currency still may have gross income from the unlawful activity. Under *Comm'r v. Tellier*, 383 U.S. 687 (1966), expenses incurred in an unlawful activity still may be deductible, unless deductions are denied by legislation or they fall within a "sharply limited and carefully defined" public policy exception.[81]

---

[77] Treas. Reg. § 1.1471-1(b)(80).

[78] Treas. Reg. § 1.1471-1(b)(100); I.R.C. § 7701(a)(1); Treas. Reg. § 301.7701-6(a).

[79] Treas. Reg. § 1.7701-1(a)(2).

[80] Treas. Reg. § 301.7701-6(b)(2).

[81] *Cf*. IRC § 162(c) (denying deductions for certain illegal bribes and other payments); IRC § 162(q) (denying deductions for certain sexual harassment settlement payments subject to a nondisclosure agreement).

6. Tax Issues Not Addressed in Notice 2014-21

a. Notice 2014-21 provides some helpful guidance but leaves many issues unaddressed.

b. Is cryptocurrency tangible property?

(1) Notice 2014-21 provides that virtual currency is treated as "property" for tax purposes, but is silent on whether it should ever be treated as tangible property.

An underlying assumption of Notice 2014-21 may be that virtual currency is *not* tangible. In particular, Notice 2014-21 concludes that miners of virtual currency realize income as virtual currency is received from the mining activity. An alternative approach, which Notice 2014-21 apparently rejects, would be to require gross income inclusion only when the mined currency is sold, with expenses capitalized rather than deducted.[82]

(2) As discussed at various points below, whether virtual currency is tangible property can have significant effects. Tangible personal property, for example, is subject to the following rules:

(a) The transfer by a noncitizen nonresident of tangible personal property with a situs in the United States is subject to gift or estate tax.[83]

(b) The income tax deduction for a charitable contribution of tangible personal property is generally limited to basis.[84]

(c) A contribution which consists of a future interest in tangible personal property is not deemed made until any non-charitable intervening use has expired.[85]

(d) For gift tax valuation purposes, tangible personal property, if non-depreciable, qualifies for a special exception to the IRC § 2701(a)(2)(a) zero valuation rule for interests retained by the transferor (or applicable family member) in the case of transfers to or for the benefit of members of the transferor's family.[86]

(3) At first blush, it may seem that a thing so abstract and conceptually elusive as cryptocurrency could never be considered "tangible" like a kitchen blender or a Barbie doll. (Then again, "money" is an elusive concept, yet is often considered tangible. *See* Gen. Couns. Mem. 36860 (Sept. 24, 1976).)

(4) Yet cryptocurrency has features that make it highly similar to tangible personal property.[87]

(a) In order to acquire cryptocurrency, one must possess the private key to a public address. The public address is an alphanumeric series of numbers and letters. The private key also is a series of numbers and letters. Everyone can see the public address, but only someone who knows the

[82] *Cf.* IRC § 263A(b) (generally applying uniform capitalization rules to tangible personal property produced by the taxpayer).
[83] *See* Treas. Reg. § 20.2104-1(a)(2); IRC §§ 2501(a)(2), 2511(a); Treas. Reg. § 25.2511-3(b)(1).
[84] IRC § 170(e)(1)(B)(i).
[85] IRC § 170(a)(3).
[86] IRC § 2702(c)(4).
[87] *See generally* Raskin, *Realm of the Coin: Bitcoin and Civil Procedure*, 20 Fordham J. of Corporate & Financial Law 969 (2015).

private key can transfer the units of cryptocurrency associated with that address.

(b) The owner of the private key must take pains to prevent it from becoming known. After all, only persons who know the private key paired with the public address can actually use the units of cryptocurrency associated with that address. Like a hundred dollar bill lying on a sidewalk, if a private key becomes known, the first person who gets it can exploit it for himself or herself, such as converting it into dollars.

(c) A public address is like an unbreakable and immovable but transparent safe. Everyone in the world can see what's in it (*i.e.*, how many units of cryptocurrency it has) but only the person who possesses the private key can access the contents. To everyone else, the contents are totally inaccessible.

(d) In fact, strictly speaking, it is not possible to own Bitcoin or other units of cryptocurrency. A unit of cryptocurrency is simply an entry on a ledger that is accessible to all. The only thing it is possible to own is a *private key* that enables the holder to send cryptocurrency from one address to another.

(e) A private key, once again, is a series of numbers and letters. One way to possess a private key is simply to memorize the numbers and letters. This is known among crypto-enthusiasts as a "brain wallet."

(f) Brain wallets, however, have significant downsides. The most obvious is that one could lose the private key due to memory lapse or death.

(g) Consequently, most participants in cryptocurrency instantiate their private keys in physical form. It is common, for example, to write the private key down on a piece of paper. This is known as a "paper wallet". Other possibilities are to store the private key on a computer hard drive, a phone, or a specially designed piece of hardware. This was described above as a "cold wallet" or "cold storage."

(h) Whatever type of wallet is selected, it necessarily has a *physical location*. Many wallets can be touched, handled, and moved around as much as a kitchen blender or a Barbie doll. In other words, the private key is tangible personal property.

(5) The tangible character of cryptocurrency is demonstrated in other ways.

(a) In shutting down the online black market Silk Road, the FBI was able to "seize[] approximately $18 million worth of Bitcoins" owned by Silk Road mastermind Ross William Ulbright. *U.S. v. Ulbright*, (15-1815-cr) (2nd Cir. May 31, 2017). How were the Bitcoins seized? The answer is by taking possession of Ulbright's laptop, which contained his Bitcoin wallets and, with them, the private keys.

(b) Satoshi Nakamoto defines Bitcoin in a manner that implicitly confirms that it is tangible property. In particular, Satoshi writes:

> "We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership."

The "chain of digital signatures" is publicly distributed. It does not belong to anyone. Owners of private keys, however, can initiate transactions by digitally signing a hash. To access the coin, one must possess the private key.

(c) One way to transfer cryptocurrency to another person is to physically deliver the wallet. For example, if a private key is instantiated on a piece of paper (*i.e.*, a paper wallet), the person holding the paper wallet can deliver it to another. The transfer works mechanically in the same way as a transfer of any other form of tangible property.

(6) Cryptocurrency transfers like tangible personal property transfers.

(a) There are several ways to transfer cryptocurrency.

(b) One way, as noted, is to physically deliver the wallet containing a private key. For example, a person holding a paper wallet can deliver it to another.

(c) Indeed, it is possible to hold cryptocurrency in a form resembling a physical coin. The most well-known is perhaps the Casascius coin, which was manufactured by crypto-enthusiast Mike Caldwell before the Treasury Department's Financial Crimes Enforcement Network (FinCEN) sent him a letter warning that his activities constituted regulated money transmission. Each physical coin contains a piece of paper with a private key.

(d) A second way is to use the private key to initiate a transaction on the distributed ledger and cause units of the cryptocurrency to be sent to a different public address. This type of transfer enriches the holder of the private key to the recipient address. The recipient holder stores the private key in a wallet which, again, is typically in physical, tangible form.

(e) Query whether an incremental enrichment of a piece of tangible property is itself a transfer of tangible property. By analogy, diamonds are rated in part based on clarity; the clearer the diamond, the more valuable it is. Suppose it were possible to transfer clarity from one diamond to another. Would that be a transfer of tangible property? In a sense the answer is yes, because an increase in clarity is a change to the physical characteristics of the recipient diamond. The owner swaps on upgrades a less clear diamond for a clearer one. A cryptocurrency transaction works the same way; essentially the recipient in a cryptocurrency transaction gets an upgrade to his or her wallet. It is possible to conceive of the transaction, in turn, as an upgrade to his or her tangible property.

(f) Another way to transfer cryptocurrency is to use a cryptocurrency exchange, such as Coinbase. When cryptocurrency is transferred to the public address of a Coinbase user, Coinbase holds the private key, but the user does not.

(g) To keep the private keys of their users' public addresses secure, Coinbase employs a "cold-storage technology." Despite the forbidding term "cold-storage technology," all it means is that Coinbase stores

private keys in paper form "in safe deposit boxes and vaults around the world."[88]

(h) Thus, Coinbase customers cannot access their private keys, which explains why Coinbase transactions can take more time than transactions of, say, publicly traded securities. As the Coinbase user agreement provides:

> "Coinbase securely stores all Digital Currency private keys in our control in a combination of online and offline storage. As a result, it may be necessary for Coinbase to retrieve certain information from offline storage in order to facilitate a Digital Currency Transaction in accordance with your instructions, which may delay the initiation or crediting of such Digital Currency Transaction for 48 hours or more. You acknowledge and agree that a Digital Currency Transaction facilitated by Coinbase may be delayed."[89]

(i) A Coinbase account perhaps is best conceived as a bailment. Coinbase customers entrust their private keys to Coinbase, which holds them for customers in order to facilitate exchanges of cryptocurrency.

(j) If an exchange such as Coinbase is a bailment, and ownership of cryptocurrency is essentially ownership of an item of tangible property (*i.e.*, the paper wallets that Coinbase stores in its vaults), then the bailor (*i.e.*, the customer), is the owner of tangible property in the possession of a bailee (*i.e.*, Coinbase). In this view, transactions consummated through Coinbase are transactions involving tangible property.

(k) Coinbase is essentially in the business of holding valuable slips of paper in secure storage facilities for its customers. The slips of paper ultimately belong to the customers even if the system cannot function unless the private keys are hidden. As Coinbase explains, "it's not feasible to provide the private keys to individual wallet addresses; doing so would prevent us from taking advantage of our secure cold-storage technology to protect your funds."[90]

c. Wealth Transfer Tax Issues

Notice 2014-21 says nothing about estate, gift, and generation-skipping transfer tax issues, apart from the general principle that virtual currency is treated as property for tax purposes. These issues are discussed separately below.

d. Charitable Income Tax Deduction Issues

Notice 2014-21 also says nothing about IRC §§ 170 and 642(c) charitable income tax deductions, apart from the general principle that virtual currency is treated as property for tax purposes. These issues are discussed separately below.

---

[88] *See* https://www.coinbase.com/security?locale=en-US (last visited November 5, 2018).

[89] *See* https://www.coinbase.com/legal/user_agreement?locale=en-US (last visited November 5, 2018).

[90] *See* https://support.coinbase.com/customer/portal/articles/1526452-where-can-i-find-the-private-keys-for-my-wallet- (last visited November 5, 2018).

e. Issues Where Confirmation of the Correct Tax Treatment Would Be Helpful

(1) Mining Expenses Deducted as Incurred

(a) Presumably, expenses incurred when mining for virtual currency will be deducted as incurred, given that, under Notice 2014-21, gross income is realized as virtual currency is received.

(b) The alternative approach would be to require mining costs to be capitalized until the virtual currency is disposed.[91]

(c) If virtual currency is properly characterized as tangible personal property, then perhaps capitalization is the better treatment.[92]

(2) IRC § 1031 Like-Kind Exchanges

(a) Under IRC § 1031, for exchanges completed before January 1, 2018, it was possible to defer recognition of gain on the exchange of property held in a trade or business or for investment if the property received was of like kind (and also was held in a trade or business or for investment). Like-kind exchange treatment should be available in the case of pre-2018 exchanges of cryptocurrency for cryptocurrency of like kind.

(b) For exchanges completed after December 31, 2017, P.L. 115-97, also known as the Tax Cuts and Jobs Act, only allows IRC § 1031 like-kind exchange treatment for exchanges of real property. Thus, for post-2017 exchanges, the question of when like-kind exchange treatment is available for cryptocurrency transactions is moot.

(3) Businesses of Buying and Selling Virtual Currency to Customers

Some may be in the business of buying and selling virtual currency to customers. For them, virtual currency is inventory and not a capital asset under IRC § 1221(a). They also should be subject to uniform capitalization rules of IRC § 263A.

(4) Installment Sale Treatment

As with the sale of other forms of property, a sale of virtual currency for at least one payment received after the close of the taxable year of disposition should qualify for installment sale treatment under IRC § 453.

(5) Retirement Account Assets

Individual retirement accounts may hold almost any investment other than certain collectibles under IRC § 408(m). Consequently, it should be possible for an IRA to hold cryptocurrency.

(6) Basis of Virtual Currency Transferred by Gift

(a) If virtual currency is transferred by gift, its basis should be determined under IRC § 1015(a). IRC § 1015(a) provides that the basis of property in the hands of the donee generally is equal to its basis in the hands of the donor. However, if the fair market value of the property at the time of the gift is less than the donor's basis (*i.e.*, the property has declined in

[91] *Cf*. IRC § 263A (setting forth uniform capitalization rules).
[92] *See* IRC § 263A(b)(1).

value), the donee's basis is limited to the property's fair market value for purposes of determining any loss. In other words, the donee can have carryover gain but the donor may not shift unrealized loss to the donee.

(b) It is good practice, when transferring virtual currency by gift, to memorialize the donor's basis at the time of the gift through a contemporaneous memorandum. As blockchain transactions are anonymous, a contemporaneous memorandum is a good idea in general in order to identify the donor and donee.

(c) If property is transferred to a grantor trust, IRC § 1015(a) cannot determine basis, as a grantor trust does not retain its vitality as a separate taxpayer.[93] Exactly how virtual currency can, as a matter of state law, be transferred in trust to begin with is an open question, as discussed elsewhere in this outline. It may be best to conceive of a cryptocurrency wallet as a form of tangible property, which can be held by a trustee, in trust, in the same manner as other tangible personal property.

(7) Non-recognition upon Contributing Cryptocurrency to a Partnership or Corporation

(a) No gain or loss generally is recognized upon the contribution of property to a corporation in exchange for shares in the corporation, provided that, immediately after the exchange, the contributing persons have 80% control of the corporation.[94]

(b) Similarly, no gain or loss generally is recognized upon a contribution of property to a partnership in exchange for a partnership interest.[95]

(c) Both of the foregoing non-recognition rules are subject to an exception if the corporation or partnership is considered an "investment company."[96] The general purpose of the investment company exception is to prevent taxpayers from being able to diversify their appreciated stock and securities holdings tax-free.[97]

(d) Although the term "investment company" is not defined by statute, regulations provide that a transfer will be considered a transfer to an investment company if "[t]he transfer results, directly or indirectly, in diversification of the transferors' interests" – known as the "diversification test" – and the transfer is either to a regulated investment company (a "RIC"), a real estate investment trust (a "REIT"), or to a corporation or partnership "more than 80 percent of the value of whose assets (excluding cash and nonconvertible debt obligations from consideration) are held for investment and are readily marketable stocks or securities, or interests in regulated investment companies or real estate investment trusts." Treas. Reg. § 1.351-1(c)(1).

(e) The Taxpayer Relief Act of 1997 significantly expanded the scope of the investment company exception by deeming certain assets to be "stock

---

[93] Rev. Rul. 85-13; s*ee generally* Bramwell and Vara, *Basis Of Grantor Trust Assets at Death: What Treasury Should Do?*, Tax Notes (August 6, 2018).

[94] IRC §§ 351(a) and 1032(a).

[95] IRC § 721(a).

[96] IRC §§ 351(e) and 721(b).

[97] *See*, *e.g.*, S. Rep. No. 1707, 89th Cong., 2d Sess. 61 (1966); H.R. Rep. No. 2327, 89th Cong., 2d Sess. 9 (1966).

and securities." These listed assets now include "money" and "foreign currency." IRC § 351(e)(1).

(f) Notice 2014-21 provides that virtual currency is "property." Presumably, this means that cryptocurrency is not "money" and therefore is not deemed to be "stock or securities" for IRC § 351(e) or IRC § 721(b) purposes. Thus, cryptocurrency used to fund a corporation or partnership will not count towards the 80% maximum in determining whether the investment company exception applies. However, this conclusion has not been confirmed by the IRS.

f. Issues Where Treasury and/or the IRS Should Issue More Guidance

(1) Valuation based on Exchange Rates

(a) Notice 2014-21 provides that virtual currency is valued based on exchange rates on virtual currency exchanges. Taxpayers may perform the exchange rate conversion "in a reasonable manner that is consistency applied."

(b) Different exchanges often have different trading prices for the same virtual currency. It would be helpful if the IRS could confirm that an average of different exchanges may be used.

(c) It would be helpful if the IRS could confirm that it is acceptable to use the average of the high and low trading prices on the date of the transaction in question.[98]

(d) Virtual currency transactions are unique in that they come with a date and time-stamp. The time-stamp potentially permits more accurate valuation than the traditional method of averaging the high and low publicly traded quoted prices for the day of the transfer.

(e) It is unclear whether different methods may be used for different virtual currencies. Likewise, it is unclear whether different methods may be used for different wallets.

(f) It is unclear whether virtual currency price indexes, which aggregate prices from multiple exchanges, may be used.

(2) Tracking Basis and Issuing Default or Elective Rules

(a) A significant source of uncertainty is how taxpayers who acquire virtual currency at different times and for different costs determine the basis of their virtual currency when they dispose of the virtual currency.

(b) A similar problem arises when a taxpayer acquires stock in a corporation at different times and for different prices. Treas. Reg. § 1.1012-1(c) provides a default rule that the first stock acquired is deemed to be the first stock sold (first-in-first-out or "FIFO").

(c) Given the time-stamps generated for each blockchain transaction, it is in principle possible to trace the basis of cryptocurrency. In practice, however, tracing can be onerous. Consequently, Treasury and the IRS

[98] *Cf.* Treas. Reg. § 20.2031-2(b) (requiring publicly traded securities to be valued for estate tax purposes using the average of the high and low publicly quoted trading prices on the valuation date).

should develop default and/or elective methods of identification. Possibilities include FIFO and cost averaging.

(3) Losses other than from Sales or other Dispositions

(a) Question 6 of Notice 2014-21 confirms that if a taxpayer exchanges virtual currency for other property, the taxpayer may have loss if the fair market value of the property received is less than the basis of the virtual currency exchanged.

(b) If a private key is stolen, a theft loss deduction should be available under IRC § 165, to the extent that the loss exceeds $100 for each theft. IRC § 165(h)(1). The loss is deductible in the year of discovery. IRC § 165(e); Treas. Reg. § 1.165-8(a).

(c) Private keys and wallets also can simply be misplaced or become inaccessible. For example, if a paper wallet is used, the paper could be lost in a fire or otherwise destroyed. Hardware wallets also can be lost or rendered inaccessible if passwords are forgotten. For a harrowing tale, *see* this article: https://www.wired.com/story/i-forgot-my-pin-an-epic- tale-of-losing-dollar30000-in-bitcoin/ (last visited November 5, 2018).

(d) It is unclear whether a IRC § 165 loss deduction is available if private keys are lost or become inaccessible. Under IRC § 165(c), an individual is only allowed a loss deduction for losses (1) incurred in a trade or business; (2) in any transaction entered into for profit; or (3) that arise from fire, storm, shipwreck, or other casualty, or from theft. Under IRC § 641(b), the same limitations on loss deductions apply to trusts and estates.

(e) Under IRC § 165(h)(5), casualty loss deductions, with an exception for losses from a federally declared disaster, are suspended for individuals (and, for trusts and estates, under IRC § 641(b)) through 2025. It is unlikely in any event that a casualty loss deduction would be available for a lost or inaccessible private key, as an event must be "sudden, unexpected, and unusual in nature" for a loss arising from the event to be deductible as a casualty loss. Treas. Reg. § 1.165-7(a)(1).

(f) If an individual's property is destroyed, it is not necessary that the loss result from a casualty event in order to be deductible, so long as the loss was incurred in a trade or business or an activity entered into for profit. Rev. Rul. 87-59 (allowing a deduction for destruction of timber by tree-killing insects over a nine-month period, despite that the loss was not from a casualty); Rev. Rul. 90-61 (allowing a loss for seedling deaths from an abnormal drought, and noting that the loss "need not result from casualty to be deductible under IRC §165). Cryptocurrency normally is acquired for profit. Thus, it would seem that a loss of cryptocurrency could be deducted, even if not from a casualty event.

(g) Under Treas. Reg. § 1.165-1(b), an allowable loss must be evidenced by closed and completed transactions, fixed by identifiable events, and, subject to exceptions, actually sustained during the tax year. In the casualty loss context, a loss has been allowed, and the "closed and completed transaction" requirements apparently satisfied, for the damage or destruction of an engagement ring. *See, e.g., Carpenter v. Comm'r,* T.C. Memo. 1966-228 (upholding a loss deduction for damage to a ring accidentally dropped in a garbage disposal); *cf. White v. Comm'r*, 48 T.C. 430 (1967) (upholding a loss deduction for damage to

a ring caused by accidentally slamming a car door on the wife's hand); but *cf. Keenan v. Bowers*, 91 F. Supp. 771 (E.D.S.C. 1950) (denying a casualty loss deduction for ring accidentally flushed down a hotel toilet).

(h) If a cryptocurrency private key becomes inaccessible because the password has been forgotten, or if the private key is misplaced or destroyed, it is possible, by analogy to the foregoing cases, that the "closed and completed transaction" requirements of Treas. Reg. § 1.165-1(b) would be considered satisfied, so that the loss may be deductible.

(4) Wash Sales

(a) The IRC § 1091 disallowance of losses for wash sales applies only to sales or other dispositions of "stock or securities." It is uncertain whether cryptocurrency is a security for purposes of IRC § 1091. Arguably, cryptocurrency is not a security, and if so, then a loss should not be denied under IRC § 1091.

(b) Even where IRC § 1091 does not apply, an actual loss must be sustained in order for a loss deduction to be allowed. *Schoenberg v. Comm'r*, 77 F.2d 446 (8th Cir. 1935) (denying a loss deduction on substance-over-form grounds, even though sale and reacquisition occurred outside of the then wash-sale window, and the repurchase was made via a separate taxpayer of which taxpayer was a 70% shareholder); *Horne v. C.I.R.*, 5 T.C. 250, 255 (1945) (denying a loss deduction where taxpayer sold a commodities exchange membership certificate and then reacquired another certificate eight days later, even though the predecessor to Section 1091 was held not to apply to the membership certificates).

(c) Treasury and the IRS should confirm that, under general tax principles, artificial losses will not give rise to a deduction, even where IRC § 1091 does not apply. Perhaps, by analogy to IRC § 1091, Treasury and the IRS should create a presumption that a loss is not genuine if sale and reacquisition of substantially the same cryptocurrency occurs within a certain period.

(d) Future legislation also could extend IRC § 1091 to cryptocurrency transactions.

(5) Hard Forks and Other Virtual Currency Events

(a) A blockchain ledger is maintained by a network of computers using open-source software. The network that verifies transactions on the ledger operates by consensus. If the consensus changes, then so does the character of the blockchain.

(b) Each time a blockchain changes character, a potential taxable event occurs, as discussed below.

(c) Types of blockchain changes include:

(i) **Soft Forks.** A soft fork is a modification or software upgrade of an existing blockchain. Similar to an upgrade in a word processing or other software, the new, modified chain still recognizes the old chain as valid.

(ii) **Hard Forks (also referred to as "chain splits").** A hard fork occurs when one network decides to maintain a second ledger

derived from the original ledger, while the original ledger continues to be maintained by a separate network. Holders of cryptocurrency on the original ledger have the option of staying on the old blockchain or transferring to the new one.

(iii) **Airdrops.** The term "airdrops" refers to the distribution of new cryptocurrency to all holders of an existing cryptocurrency.

(iv) **Giveaways.** Giveaways are transfers of cryptocurrency to those who create an account.

(v) **Token Swaps.** Token swaps are decisions by developers of a virtual currency to move to an entirely new protocol, so that existing holders must move to the new protocol or else forfeit their cryptocurrency.

(d) Under the foundational case of *Comm'r v. Glenshaw Glass*, 348 U.S. 426, 431 (1955), "gross income" includes all "undeniable accessions to wealth, clearly realized, and over which the taxpayers have complete dominion." It seems that airdrops and giveaways, because they are bonuses or rewards, should be included in gross income under this *Glenshaw Glass* standard.

(e) A hard fork, because it creates the option to use a new forked blockchain, also is arguably an accession to wealth under *Glenshaw Glass*. Determining the amount of any gross income, however, is difficult. It is unclear at the time of the hard fork how valuable the new blockchain will be; indeed, arguably, the value is initially zero given that the new blockchain is untested and has no discernible value, whether on an exchange or otherwise.

(f) If a hard fork occurs, it is unclear when the realization event occurs (or if the hard fork triggers a realization event to begin with). For example, if one holds cryptocurrency indirectly through an account on an exchange such as Coinbase, a realization event may not occur until the exchange opts to recognize the new blockchain. On the other hand, perhaps the ability to withdraw from the exchange constructively causes the account holder to have access to the new blockchain.

(g) An argument also can be made that a hard fork is not a realization event at all. In this view, the creation of a new blockchain is a change in the form of property rather than a realization of income. The birth of young from pregnant livestock, for example, is not thought to be a realization event. *Gamble v. Comm'r*, 68 T.C. 800 (1977), *acq*. 1986-1 CB 80; *cf. Eisner v. Macomber*, 252 U.S. 189 (1920) (holding that a stock dividend is not income); IRC § 305(a) ("Except as otherwise provided in this section, gross income does not include the amount of any distribution of the stock of a corporation made by such corporation to its shareholders with respect to its stock.").

(h) An analogy can be drawn between a hard fork and a nontaxable corporate reorganization. However, the relevant Code sections (IRC §§ 355 and 368) do not apply.

(i) A significant bitcoin hard fork occurred in 2017 when Bitcoin split into Bitcoin (BTC) and Bitcoin Cash (BTH). To date, the IRS has not issued guidance on the appropriate treatment of this hard fork event.

(j) Token swaps appear to be dispositions triggering gain or loss under IRC § 1001. Perhaps Treasury or the IRS will adopt a more favorable rule, however. If the taxpayer does not acquire cryptocurrency in the new blockchain in time, and the taxpayer's old cryptocurrency becomes worthless, a loss deduction may be available under IRC § 165. IRC § 165 loss deduction rules are discussed in further detail above.

(6) Tax Accounting for Dealers of Cryptocurrency

Some commentators propose that dealers may be able to make a mark-to-market election under IRC § 475 for tax accounting purposes.

(7) Basis of Virtual Currency Acquired from a Decedent

(a) IRC § 1014(a) generally provides that the basis of property acquired or passing from a decedent is equal to its fair market value at the decedent's death, or the alternate valuation date if an alternate valuation date election is made under IRC § 2032.

(b) A decedent's ability to initiate blockchain transactions using his or her private keys passes to whoever becomes entitled to the decedent's wallets at death. The wallet should be considered the property that is acquired or passes from the decedent.

(c) A wallet typically contains multiple private keys. In that case, each private key should obtain a separate basis under IRC § 1014(a). In this view, the wallet is not one item of property but many items for IRC § 1014(a) purposes.

(d) Wallets may be subject to valuation discounts to reflect security risk, as discussed below. Any discount reduces IRC § 1014 basis.

7. Wealth Transfer Tax Issues

a. General Observations

(1) Notice 2014-21 does not explicitly address the gift, estate, and generation-skipping transfer ("GST") tax consequences of virtual currency transactions.

(2) The approach of Notice 2014-21 is to apply "existing general tax principles" to transactions involving virtual currency. Under this approach, existing estate, gift, and GST tax principles apply to virtual currency transactions as much as to any other transactions.

(3) The core announcement of Notice 2014-21 – that virtual currency is "treated as property" for U.S. tax purposes – resolves few, if any, gift, estate, or GST tax issues. Wealth transfer taxes are taxes on certain transfers of property. *See* IRC § § 2103(a); 2501(a)(1); 2612. That virtual currency is property simply confirms that transfers of virtual currency may be subject to wealth transfer tax.

b. Gift Tax Issues

(1) Gifts Where the Donor Retains a Second Copy of the Same Private Key

(a) As discussed, it is possible to cause a cryptocurrency transfer by delivering physical possession of a wallet containing a private key. Suppose, however, that the donor has retained a second copy of the same private key on a different wallet. There are three possible theories for

analyzing the gift in this case, but none of the theories seems fully satisfactory.

(b) The first theory is that the gift is incomplete. Treas. Reg. § 25.2511-2(b) provides that a gift is complete for gift tax purposes "when the donor has so parted with dominion and control as to leave in him no power to change its disposition, whether for his own benefit or for the benefit of another." *See also Estate of Sanford v. Comm'r*, 308 U.S. 39 (1939). According to the incomplete gift theory, by retaining a second copy of the private key, the donor has retained dominion and control over the property transferred, as the donor could, following the transfer, initiate a cryptocurrency transaction using the retained copy of the private key, and thereby deprive the donee of the wealth associated with the private key. The gift would not be complete until the donor either surrenders the second copy of the private key or the donee initiates a transaction using the private key and puts the cryptocurrency beyond the reach of the donor.

(c) The second theory is that the donor has made a completed gift subject to a retained interest. The donor does, after all, relinquish control and dominion over one private key. At a minimum, that key then gives the donee the ability to initiate a cryptocurrency transaction. Thus, in this view, the gift may be complete to at least some extent.

(d) Under the completed-gift-with-retained-interest theory, if the gift is made to or for the benefit of a member of the donor's family within the meaning of IRC § 2704(c)(2), it may be subject to special valuation rules under IRC § 2702. This is because the retained copy of the private key may be treated as a retained life interest for IRC § 2702 purposes. Treas. Reg. § 25.2702-4. As the retained interest is not a qualified interest within the meaning of IRC § 2702(b), it would be valued at zero under IRC § 2702(a)(2)(A).

(e) If the retained interest theory is correct, but the gift is not subject to IRC § 2702 (*e.g.*, for example, because the gift is not to a member of the donor's family), the donor's retained interest still is disregarded if it is "not susceptible of measurement on the basis of generally accepted valuation principles." Treas. Reg. § 25.2511-1(e); *see also Robinette v. Helvering*, 318 U.S. 184 (1943). It may be that the value of the retained interest in such a case – essentially, the ability to use the private key before the donor does – cannot be measured. Thus, just as if IRC § 2702 applied to cause the retained interest to be valued at zero, the value of the gift would be equal to the entire value of the cryptocurrency controlled by the private key.

(f) Note that, under the completed-gift-with-retained-interest theory, there is a potential for doubling of the wealth transfer taxation. Suppose that, under Treas. Reg. § 25.2511-1(e), the donor makes a gift equal in value to the entire value of the cryptocurrency controlled by the private key. The donor still retains the second copy of the private key, which may also be subject to gift or estate tax when it is later transferred.

(g) The third and final theory is that the retention by the donor – or anyone else, for that matter – of a second copy of the same private key is reflected in the value of the gift. In this view, the donor has, by relinquishing possession of one copy of a private key, made a complete disposition *of that copy*. There is no retained interest or retained control over the transferred copy. The value of the gift instead reflects a security

risk discount for the possibility that there could be another person who holds a copy of the same private key.

(h) If the last theory is correct, the results for wealth transfer tax planning with cryptocurrency are explosive. To illustrate, suppose that Father holds two paper copies of a private key associated with $1 million of cryptocurrency. Father gives one copy to Daughter. Clearly, the gift to Daughter (assuming it is complete and Father is not considered to have retained an interest) is worth less than $1 million at the time of the gift. After all, Father could cause Daughter's copy to become worthless simply by initiating a transaction before she does. Perhaps the "security discount" of a poorly secured wallet is 50% or more. If so, Father can make a gift for U.S. gift tax purposes of $500,000 or less. Daughter can nevertheless realize a full $1 million of value.

(i) *See* below for more on security risk discount planning with cryptocurrency.

(j) In principle, there is a fourth theory of how the gift should be treated: the IRS could treat a gift of private key, with a copy of the same key retained by the donor, as an "open transaction" that is not completed until either the donor or the donee uses the private key to initiate a new transaction. In *Estate of DiMarco v. Comm'r*, 87 T.C. 653 (1986), however, the Tax Court refused to apply the open transaction doctrine in the gift tax context. The IRS subsequently revoked the ruling that had adopted an open transaction analysis. Rev. Rul. 92-68 (revoking Rev. Rul. 81-31). Thus, it does not seem that an open transaction approach is viable. *See generally*, Gans, Blattmachr & Bramwell, *Estate Tax Exemption Portability: What Should the IRS Do? And What Should Planners Do in the Interim?*, 42 Real Prop., Prob. & Tr. J. 413 at n. 44 (2007); *cf.* Gans, *Gift Tax: Valuation Difficulties and Gift Completion*, 58 Notre Dame L. Rev. 493 (1983).

(2) Ensuring a Gift of Cryptocurrency Is Complete

(a) As discussed above, there are difficult, unresolved issues with gifts of wallets, including whether a gift of a wallet is complete.

(b) To ensure a completed gift of a wallet, if that is the goal, the donor can represent that he or she has not retained any copies of the private keys (or memorized them), and promise to surrender immediately any others that come into his or her possession.

(c) A gift made by a blockchain transaction also should be considered a completed gift, assuming that the donor does not have a private key to the donee's address. It still is good practice to memorialize the transfer in a contemporaneous instrument whereby the donor represents that he or she does not have the private key to the donee's address. As blockchain transactions are anonymous, it is good practice in any event to memorialize the parties to the transaction when making a transfer by gift.

(d) If the same individual is both the donor and the trustee of a trust that receives the cryptocurrency gift, some practitioners may be concerned that the gift is incomplete, as the donor retains the power to initiate any cryptocurrency transaction. As a long as the transfer is made to an irrevocable trust, the terms of which do not give the donor a power of disposition, the gift should be considered complete. The anonymity of

blockchain transactions makes a breach a fiduciary duty more difficult to detect, but that in itself should not prevent a completed gift.

(e) Those practitioners who are concerned about completed gift issues may nevertheless prefer not to permit the donor to serve as both the donor and the trustee of a trust.

(f) As discussed above, customers of a digital currency exchange, such as Coinbase, do not even have access to the private keys, which Coinbase holds securely for their customers. A transfer using Coinbase, therefore, should not create any incomplete gift issues, as the donor has no power to interfere with the donee's use of his or her cryptocurrency received via Coinbase.

(3) General Valuation

(a) Notice 2014-21, as discussed, provides that if virtual currency is listed on an exchange and the exchange rate is established by market supply and demand, the fair market value of virtual currency is determined "for U.S. tax purposes" by converting the virtual currency into dollars at the exchange rate, "in a reasonable manner that is consistently applied."

(b) Presumably, the position in Notice 2014-21 on valuation also would apply for U.S. gift and estate tax purposes.

(c) Note that, because the conversion of virtual currency into dollars may be made at the exchange rate in "any reasonable manner that is consistently applied," the high/low averaging method that applies to publicly traded securities does not need to be used, although presumably it may be used. Treas. Reg. § 25.2512-2(b)(1) (requiring publicly traded securities to be valued using the average of the high and low publicly quoted trading prices on the date of the gift).

(d) It is possible that cryptocurrency should be valued at a security discount, as discussed below.

(4) Security Discount Planning with Cryptocurrency

(a) Suppose Father holds two copies of the same private key, both stored in the form of paper wallets.

(b) Under the willing-buyer-willing-seller test, "[t]he value of the property is the price at which such property would change hands between a willing buyer and a willing seller, neither being under any compulsion to buy or to sell, and both having reasonable knowledge of relevant facts." Treas. Reg. § 25.2512-1(a).

(c) A willing buyer who is aware of the existence of a second copy of the same private key presumably would pay less for one copy. After all, the value of one copy is only as good as the holder's ability to outrace the other holder to exploit the value of the private key.

(d) Now suppose that Father simultaneously gives one copy of the private key to Son and the second copy to Daughter. The two copies should not be aggregated for valuation purposes. *Cf.* Rev. Rul. 93-12 (holding that, where the donor makes a gift of 20% of the shares in the same corporation to each of five children, the gifts are not aggregated for

valuation purposes and each gift may qualify for a discount for lack of control).

(e) Thus, it seems that multiple copies of private keys could be used as a discount planning device. That Son and Daughter may be able to agree on the use of the private key (*e.g.*, by splitting the cryptocurrency between them), and thereby together receive the entire value of the private key, should not deprive Father of valuation discounts. *Cf. Estate of Bright*, 658 F.2d 999, 1001 (5th Cir. 1981); *Propstra v. U.S.*, 680 F.2d 1248 (9th Cir. 1982) (rejecting the "unity of ownership" principle of valuation).

(5) Cryptocurrency GRATs

(a) A grantor retained annuity trust ("GRAT") works best if the grantor retains an interest for a short period, such as two years (or locks in performance via a substitution of other assets), and the GRAT is funded with volatile assets. If the assets fail to earn returns in excess of the IRC § 7520 rate, they are returned to the grantor in the form of annuity payments. By contrast, if the assets substantially outperform the IRC § 7520 rate, property passes free of gift and estate tax, so long as the grantor survives the fixed term. To maximize short-term upside, more volatility within the GRAT is better. *See* Blattmachr, Bramwell and Zeydel, *Drafting and Administration to Maximize GRAT Performance*, Probate and Property, Vol. 20, No. 6 (November/December 2006).

(b) Cryptocurrencies are volatile and therefore may make good candidates for a GRAT program. For an excellent article on cryptocurrency GRATs, see Birdsall and Taback, *The Bitcoin GRAT*, Trusts & Estates (July 1, 2014).

(6) Non-depreciable Cryptocurrency GRITs

(a) Tangible personal property, if non-depreciable, qualifies for a special exception to the IRC § 2701(a)(2)(a) zero-valuation rule for interests retained by the transferor (or applicable family member) in the case of transfers to or for the benefit of members of the transferor's family. IRC § 2702(c)(4).

(b) The IRC § 2702(c)(4) exception applies in the case of a retained term interest in tangible property, if "the nonexercise of rights under [the term interest] would not have a substantial effect on the valuation of the remainder interest."

(c) Treasury regulations clarify that this exception is limited to tangible property for which no deduction for depreciation or depletion would be allowed, if the property were used in a trade or business or held for the production of income. Treas. Reg. § 25.2702-2(c)(2).

(d) As an example, the regulations cite a trust funded exclusively with a painting. Treas. Reg. § 25.2702-2(c)(2). Other examples of non-depreciable tangible property might include jewelry, other types of artwork, or vacant land. *See* 136 Cong. Rec. S15,682 (Oct. 10, 1990).

(e) A cryptocurrency wallet is an item of tangible property. It is also not subject to wear and tear and is non-depreciable. Thus, it seems that it is possible to avoid IRC § 2702 by making an irrevocable transfer of a

cryptocurrency wallet but retaining the right to the use of the wallet for a period of years.

(f) If a grantor retained income interest trust or "GRIT" is funded with non-depreciable tangible property meeting the requirements of IRC § 2702(c)(4), then the value of the term interest, for gift tax purposes, is the value that the term holder "establishes as the amount for which such interest could be sold to an unrelated third party." IRC § 2702(c)(4).

(g) The holder must be able to reasonably establish the value of the term interest. Treas. Reg. § 25.2702-2(c)(1). Comparable rental values or sales are the best evidence of the value of the term interest, whereas "[l]ittle weight is accorded appraisals in the absence of such evidence." Treas. Reg. § 25.2702-2(c)(3). In addition, the value the retained interest cannot be determined based on the rental value of a comparable item for a period shorter than the term of the GRIT. Treas. Reg. § 25.2702- 2(d)(2), Example 7. Thus, an individual who hopes to reduce the value of his or her gift to a tangible property GRIT must provide evidence of the rental value of comparable property or the prices at which term interests in similar property have exchanged hands.

(h) The value of a given amount of cryptocurrency after a fixed term conceivably could be determined using data from futures markets for cryptocurrency. With that value determined, it should be easy to determine the value of the retained interest.

(i) Thus, it may be possible to avoid IRC § 2702 and create a GRIT funded with a cryptocurrency wallet.

(7) Gifts of Cryptocurrency by Nonresident Aliens

(a) The gift tax does not apply to transfers of intangible property by a nonresident who is not a citizen of the U.S. IRC § 2501(a)(2). The gift tax does, on the other hand, apply to transfers of tangible property situated in the U.S. at the time of transfer. Treas. Reg. § 25.2511-3(a)(1).

(b) The IRS takes the position that currency is tangible property potentially subject to U.S. gift tax if transferred by a nonresident alien. Gen. Couns. Mem. 36860 (Sept. 24, 1976); *cf*. Treas. Reg. § 25.2511-3(b)(4)(iv) (providing that currency is not a debt obligation for gift tax situs purposes). Even a check drawn on a U.S. bank historically has been considered a gift of currency located in the U.S. Gen. Couns. Mem. 36860 (Sept. 24, 1976).

(c) As discussed above, cryptocurrency has features which suggest that it is tangible property. It perhaps resembles tangible property more strongly than fiat currency, most of which is held electronically. Even paper currency purports to be nothing more than a note or evidence of credit from the Federal Reserve (*i.e.*, an intangible debt obligation).

(d) If a nonresident alien wishes to make a gift of cryptocurrency, the prudent course is to make sure that neither the donor's nor the donee's wallet is physically located in the United States. This precaution is similar to standard planning with gifts of currency.

c. Estate Tax Issues

(1) Gross Estate Inclusion of Brain Wallets

As discussed above, it is possible to store private keys in one's memory rather than instantiate them in physical form. Under existing technology, however, your memory dies with you. Thus, it seems that a private key stored in a brain wallet is lost at death and therefore is not included in the gross estate. *Cf. Helvering v. Safe Deposit & Trust Co.*, 316 U.S. 56 (1942) (holding that property was not included in the decedent's gross estate under the predecessor to IRC § 2033, where the decedent had no interest in the property "at the time of his death").

(2) Wallets Lost or Stolen Post-Mortem

(a) A wallet (other than a brain wallet) possessed by a decedent at his or death is includible in the decedent's gross estate under IRC § 2033.

(b) Frequently, however, a wallet will be lost after the decedent's death. This may happen, for example, if a hardware or paper wallet is accidentally discarded. It also is possible to lose access to a hardware wallet.[99]

(c) A wallet may be lost before the value of the wallet can be determined. In that case, it may be unclear what value to assign to the wallet on an estate tax return.

(d) If a wallet is lost, it is unclear whether an offsetting casualty deduction may be claimed under IRC § 2054. See discussion above of whether an income tax loss deduction is available for misplaced or inaccessible cryptocurrency wallets.

(e) Given the overlap between IRC § 2054 and IRC § 165(c)(3) casualty loss provisions, the two Sections generally are read together. *Estate of Meriano v. Comm'r*, 142 F.3d 651 (3d Cir. 1998); *see also Estate of Heller v. Comm'r*, 147 T.C. No. 11 (2016) (citing *John P. White v. Comm'r*, 48 T.C. 430 (1967)). If a wallet is destroyed, depending on the circumstances of the destruction, it is possible that a deduction under IRC § 2054 would be allowed.

(f) IRC § 2054 also will allow a deduction if a wallet is lost in a theft. Whether a theft has occurred is defined by the jurisdiction in which the loss has occurred. *Meriano v. Comm'r*, 142 F.3d 651 (3d Cir. 1998).

(g) No IRC § 2054 deduction is available for losses occurring after distribution to the distributee. Treas. Reg. § 20.2054-1.

(h) If an entity owning cryptocurrency suffers a theft or a casualty loss occurs, an IRC § 2054 deduction may be available to the estate that holds an interest in that entity. *See Estate of Heller v. Comm'r*, 147 T.C. No. 11 (2016).

(i) If a wallet is included in the gross estate, but there is no offsetting deduction under IRC § 2054 or otherwise, an estate tax may be imposed on assets that the beneficiaries do not receive.

[99] *See* https://www.wired.com/story/i-forgot-my-pin-an-epic-tale-of-losing-dollar30000-in-bitcoin/ (last visited November 5, 2018).

(j) If no estate tax deduction is taken or available, it still may be possible to claim an income tax loss deduction. IRC § 642(g). See discussion above of whether an income tax loss deduction is available for misplaced or inaccessible cryptocurrency wallets.

(k) If a wallet is misplaced within six months after the date of death, it is unclear whether the loss can be considered a "disposition" of the cryptocurrency that qualifies for alternate valuation date treatment under IRC § 2032 at the time of the wallet is misplaced. If a private key is rendered inaccessible because the password is forgotten, for example, then a lower valuation may be available for the alternate valuation date six months after the decedent's date of death.

(3) Valuation

(a) Notice 2014-21, as previously discussed, provides that if virtual currency is listed on an exchange and the exchange rate is established by market supply and demand, the fair market value of virtual currency is determined "for U.S. tax purposes" by converting the virtual currency into dollars at the exchange rate, "in a reasonable manner that is consistently applied."

(b) Presumably, the position in Notice 2014-21 on valuation also would apply for U.S. gift and estate tax purposes.

(c) Note that, because the conversion of virtual currency into dollars may be made at the exchange rate in "any reasonable manner that is consistently applied," the high/low averaging method that applies to publicly traded securities does not need to be used, although presumably it may be used. Treas. Reg. § 20.2031-2(b)(1) (requiring publicly traded securities to be valued using the average of the high and low publicly quoted trading prices on the date of the gift).

(d) It is possible that cryptocurrency should be valued at a security discount, as discussed above in connection with gift tax valuation.

(e) It also is possible that a decedent's cryptocurrency should be valued at a discount for lack of access. Ownership of cryptocurrency consists of having access to private keys associated with public addresses. It may not always be possible to access the private keys on a decedent's wallet, even if one has physical possession of the wallet. To take the simplest example, a decedent may have stored paper wallets in a safe, but the combination to the safe may have died with the decedent. The safe and its contents could, perhaps, be valued at a discount to reflect the time, expense, and possible inability to access the contents.

(f) If an estate has physical possession to a wallet but cannot access the wallet's contents, it may not be possible to determine value at all. The value of the wallet seems quite unknowable. It may be that the estate should report only a *de minimis* value. *Cf*. Rev. Rul. 67-370 (holding that the value of a remainder interest that could be revoked by settlor is affected by "its possible curtailment or complete divestment").

(g) Treasury and the IRS should issue guidance on the proper reporting and valuation of missing or inaccessible wallets.

(4) Estate Tax Situs Issues for Nonresident Alien Decedents

(a) A nonresident alien decedent is subject to U.S. estate tax on property which at the time of death is situated (or deemed situated) within the United States. IRC §§ 2101(a); 2103; 2106(a).

(b) Tangible property located in the U.S. is considered to be situated in the U.S. Treas. Reg. § 20.2104-1(a)(2). As discussed above, cryptocurrency has features which suggest that it might be tangible property. To avoid estate tax on cryptocurrency, a nonresident alien decedent's wallet should not be located in the U.S. at death. Nor should a nonresident noncitizen make a transfer of cryptocurrency located in the U.S. at the time of the transfer, if the property transferred will be pulled back into the gross estate, in which case the property will be deemed to have a U.S. situs at the decedent's death. IRC § 2104(b).

(c) The situs for U.S. estate tax purposes of cryptocurrency held in a "web wallet" hosted by a U.S. exchange, such as Coinbase, has not yet been determined. A nonresident alien's account could be considered intangible property situated in the U.S., as the Coinbase account represents a right to private keys physically held by the U.S. exchange. *Cf.* Treas. Reg. § 20.2104-1(a)(4).

(d) Treasury and the IRS should clarify the situs of cryptocurrency held in a web wallet.

(5) Toggling Planning with Cryptocurrency

(a) Given very high estate tax exclusion amounts, almost all wealthy individuals should, when making irrevocable transfers for estate tax planning purposes, make it possible for the transferred property to be pulled back into the gross estate. *See generally* Bramwell and Madden, *Toggling Gross Estate Inclusion On and Off*, Estate Planning, Vol. 44, No. 3 (March 2017).

(b) Toggling planning is especially important with cryptocurrency gifts. The reason is that cryptocurrencies are volatile. Bitcoin, for example, could conceivably be displaced entirely by future improved blockchain technology and drop to zero in value. In that case, it is wise to take steps to effectively restore estate tax exclusion at death by causing transferred cryptocurrency to be pulled back into the donor's gross estate. *See id.*

8. Charitable Income Tax Deduction Issues

a. Substantiation and Valuation

(1) As blockchain transactions are anonymous, with any charitable gift of cryptocurrency it is a good practice to document the gift with a contemporaneous memorandum identifying the donor and donee. The memorandum could be combined with a contemporaneous written acknowledgement meeting the requirements of IRC § 170(f)(8)(B).

(2) If a charitable income tax deduction of more than $5,000 is claimed for a contribution of property, the taxpayer generally must obtain a "qualified appraisal." IRC § 170(f)(11)(C); Treas. Reg. § 1.170A-16(d)(1)(ii); *see also* Form 8283 and instructions available at https://www.irs.gov/forms-pubs/about-form-8283 (last visited November 5, 2018).

(3) The requirement of a qualified appraisal does not apply to a gift of publicly traded securities. Treas. Reg. § 1.170A-16(d)(2)(i).

(4) There is no exception, however, for cryptocurrency, which does not meet the definition of "publicly traded security." *See* Treas. Reg. § 1.170A-13(c)(7)(xi). Consequently, charitable donors of cryptocurrency should obtain a qualified appraisal (and meet other substantiation requirements) in order to claim a charitable income tax deduction under IRC § 170.

(5) However, the price of cryptocurrency often is readily available from exchanges. Treasury and the IRS should permit an exception to the qualified appraisal requirements in the case of gifts of cryptocurrency whose prices are available from exchanges.

(6) As discussed, cryptocurrency may be subject to security risk discounts. Donors should take steps to minimize any discounts, by representing that the donor has not retained copies of the donee's private keys.

b. Split-Interest Rules

(1) Charitable deductions are generally denied if a donor transfers less than his or her entire interest in property to charity. IRC §§ 170(f)(3)(A); 2055(e)(2); 2522(c)(2).

(2) If a donor makes a charitable gift of a private key but retains a copy of the same private key, a deduction could be denied under these rules. Even if a deduction is not denied, the valuation of the gift may be discounted to reflect the security risk of another person using the other copy of the private key.

c. Charitable Income Tax Consequences if Cryptocurrency is Tangible Property

(1) As discussed above, cryptocurrency has features which suggest that it might be tangible property. For example, if cryptocurrency is transferred to charity by handing over physical possession of a wallet holding a private key, then the charitable gift likely is of tangible property.

(2) If cryptocurrency is tangible, then the following consequences would follow:

(a) The charitable income tax deduction would be limited to basis, as the contribution would not (except in, perhaps, some highly unusual cases) be for a related use, as required by IRC § 170(e)(a)(B)(i)(I).

(b) If the gift is to a charitable remainder trust, no deduction would be allowed until the cryptocurrency is sold. IRC § 170(a)(3); *see* PLR 9452026.

(3) Treasury and the IRS should issue guidance on whether and in what circumstances cryptocurrency is considered tangible property for purposes of IRC § 170.

d. Income Tax Charitable Deduction for Trusts and Estates

(1) IRC § 642(c) generally allows a charitable income tax deduction to an estate or trust for any amount of gross income which, pursuant to the terms of the governing instrument, is paid for charitable purposes described in IRC § 170(c). The deduction for a set-aside of gross income is not available to trusts created on or before October 9, 1969. The deduction is in lieu of the IRC § 170(a) deduction available to individuals. IRC § 642(c)(1).

(2) The "gross income" requirement normally prevents a contribution of the full fair market value of the property from being deductible under IRC § 642(c). *Green v. U.S.*., 880 F.3d 519 (10th Cir. 2018). If the property was acquired from gross income, however, a deduction may be allowed to the extent of basis. *Id.* Consequently, as cryptocurrency is treated by the IRS as "property" under Notice 2014-21, deduction under IRC § 642(c) generally will be denied for a contribution of cryptocurrency by a trust or estate, except to the extent that it was acquired from gross income.

(3) The portion of an electing small business trust ("ESBT") that consists of stock in S corporations, by contrast, is allowed a deduction under IRC § 170(a). IRC § 641(c)(2)(E)(i) (overriding IRC § 642(c) and thereby, via IRC § 641(b), putting ESBTs on the same footing as individuals in computing the charitable income tax deduction). Thus, an ESBT may be allowed a charitable income tax deduction under IRC § 170(a) for a contribution of cryptocurrency.

9. State Tax Issues

a. Source of Cryptocurrency Gains

(1) States with income taxes generally tax the income of nonresidents from sources within the state. *See, e.g.*, Cal. Rev. & Tax. Cd. § 17951.

(2) Source income typically includes gains from the sale of tangible personal property located within the state. *See, e.g.*, Cal. Code Reg. 17951-3.

(3) If, as discussed above, cryptocurrency is best conceived as a form of tangible personal property, then gains from the sale of cryptocurrency may be considered source income for purposes of the income tax of the state where the wallet is held.

(4) Even if not considered tangible property, the location of a cryptocurrency wallet within a state may be a sufficient nexus for that state to treat cryptocurrency gains as income sourced in that state.

b. Sales Tax

(1) Sales taxes typically are imposed on the sale of tangible personal property within the taxing state. *See, e.g.*, N.Y. Tax Law § 1105. Sales taxes are "destination taxes" (*i.e.*, the point of delivery controls whether a tax is imposed). *See, e.g.,* N.Y.C.R.R. 525.2(a)(3).

(2) As discussed above, if cryptocurrency is best conceived as a form of tangible personal property, then sales of cryptocurrency to the holder of a wallet located in a particular state may be subject to state sales tax.

(3) Even if not considered tangible property, the location of a cryptocurrency wallet within a state may be a sufficient nexus for that state to tax sales of cryptocurrency to public addresses controlled by the private keys in the wallet.

D. Other Regulatory Considerations

While several regulatory agencies may have concurrent jurisdiction over cryptocurrencies, this outline will cover two of such agencies: (1) the Securities and Exchange Commission and whether cryptocurrency is a "security," and (2) the Commodity Future Trading Commission and whether cryptocurrency is a "commodity."

1. Securities Exchange Commission: Is Cryptocurrency a "Security"?

a. Role of the Securities Exchange Commission. The Securities Exchange Commission ("SEC") is the United States agency that informs and protects investors, facilitates capital formation, enforces U.S. securities laws, regulates securities markets, and provides data.[100] The SEC has issued notices, alerts and guidance regarding cryptocurrency and has been bringing actions related to cryptocurrency offerings against market participants.

b. SEC's Characterization of Cryptocurrency as a Security

(1) SEC Public Statements. In a June 2018 speech at the Yahoo All Markets Summit: Crypto Conference in San Francisco, SEC Director of Corporate Finance William Hinman stated that he did not believe that Bitcoin and Ether, two of the largest cryptocurrencies in terms of market cap, should be treated as "securities" for SEC purposes.[101] One of the factors for treating Bitcoin and Ether as securities is that the control over those two coins is now so decentralized that no one entity has control over the value of the coins. Decentralization is a key factor in defining whether a cryptocurrency is a security under the "investment contract" paradigm, which is described in more detail below. While Director Hinman stated that Bitcoin and Ether are not securities, he indicated that if there is a centralized third party, along with purchases with an expectation of a return, then it is likely a security. Thus, many, but not all ICOs are securities and would come under the regulatory control of the SEC and relevant securities laws.[102] Based on Director Hinman's statements, cryptocurrency can transition at certain points from not being a security to being a security.

(2) Cases

(a) ***Howey*** **Test.** Director Hinman's public statements are in line with the *Howey* test, which is used to identify an investment contract, which is a type of security under securities laws. *See SEC v. W. J. Howey Co.*, 328 U.S. 293 (1946). Under *Howey*:

> An investment contract for purposes of the Securities Act means a contract, transaction or scheme whereby a person [1] invests his money in [2] a common enterprise and is led to [3] expects profits [4] solely from the efforts of the promoter or a third party, … it being immaterial whether the shares in the enterprise are evidenced by formal certificates or by nominal interests in the physical assets employed in the enterprise.[103]

As seen from the factors listed by the court, *Howey* is a facts and circumstances analysis. Until recently, there was not a case on the application of the *Howey* Test to cryptocurrency.

(b) ***U.S. v. Zaslavskiy*** **(September 11, 2018).**[104] On September 11, 2018, the U.S. District Court for the Eastern District of New York denied a motion to dismiss the government's criminal indictment of Maksim Zaslavskiy on the ground that the ICOs at issue in the case did not involve the offer or sale of "securities" as defined under securities laws.

---

[100] *See* SEC website at https://www.sec.gov/ (last visited November 5, 2018).

[101] *See* https://www.cnbc.com/2018/06/14/bitcoin-and-ethereum-are-not-securities-but-some-cryptocurrencies-may-be-sec-official-says.html (last visited November 5, 2018).

[102] *Id.*

[103] *SEC v. W. J. Howey Co.*, 328 U.S. 293 (1946) at 298-299.

[104] *U.S. v. Zaslavskiy*, No. 1:17-cr-00647-RJD-RER, Dkt. No. 37 (E.D.N.Y. September 11, 2018).

Zaslavskiy founded two companies, REcoin Group Foundation, LLC ("REcoin") and DRC World, Inc. (a.k.a. Diamond Reserve Club) ("DRC"). REcoin and DRC engaged in a series of ICOs in which investors purchased cryptocurrency issued by both companies. The marketing materials for each ICO highlighted the potential in the ICO as an investment opportunity, marketed potential returns from the appreciation in value of the investments the companies would make (REcoin was backed by real estate investments while DRC was backed by investments in diamonds), and highlighted the appreciation in value of the digital tokens themselves.

But according to prosecutors, the companies did not have established business operations and did not hire or consult advisors or professionals to facilitate the investments, and the investors did not receive any digital tokens because the companies lacked the technology and expertise to develop and deliver digital tokens.

Zaslavskiy filed a motion to dismiss on several grounds, one of which was that the digital tokens were not "securities" for purposes of securities laws.

The court applied the *Howey* test and held that the indictment alleged sufficient facts to support a conclusion that the digital tokens were securities for purposes of surviving a motion to dismiss. In doing so, though, the court expressly avoided a determination of whether the digital tokens at issue were securities, leaving the ultimate decision for the next proceedings. The court reasoned that a determination would be premature because the analysis is "highly fact-specific."

While the court did not determine whether the particular digital tokens were securities, the case provides a window into how courts may consider the issue and use the *Howey* test in the context of cryptocurrency and ICOs.

(c) **SEC Enforcement Actions.** Also on September 11, 2018, the SEC announced a pair of settled orders against non-issuers participating in the offer and sale of cryptocurrencies the SEC deemed to be unregistered securities. These cases are the SEC's first ever enforcement actions relating to cryptocurrencies.

(i) ***In the Matter of Crypto Asset Management, LP*** **(September 11, 2018).**[105] Crypto Asset Management, LP ("CAM") created a pooled investment vehicle, Crypto Asset Fund, LLC ("CAF"), to invest in digital assets, and CAM marketed CAF as the "first regulated crypto asset fund in the United States." Per the settlement order, CAM's statements were incorrect because neither CAM nor CAF was registered with the SEC. The SEC found that CAF invested more than 40% of its assets in crypto assets, which the SEC deemed to be "securities" and then determined that it was an "investment company" under the Investment Company Act. Because the fund was not registered as an investment company and did not qualify for any registration exemptions or exclusions, the SEC charged CAM with violating the registration provisions of the Investment Company Act. The SEC also charged CAM with violating the

[105] *In the Matter of Crypto Asset Management, LP*, File No. 3-18740 (September 11, 2018).

Securities Act and the Advisers Act for making misrepresentations that it was "regulated."

(ii) ***In the Matter of TokenLot, LLC*** **(September 11, 2018).**[106] The SEC alleged that TokenLot, which described itself as an "ICO Superstore" and sold digital tokens in connection with ICOs and on the secondary market, and TokenLot's owners violated the Securities Act and the Exchange Act by selling securities without registering with the SEC as a broker-dealer. The order concluded that the digital tokens were securities but did not provide any analysis explaining its position that the digital tokens in connection with the ICOs are securities.

c. **SEC Takeaways.** The *Zaslavskiy* case and the SEC's enforcement actions against CAM and TokenLot are examples of the SEC's expanding its enforcement efforts around cryptocurrency transactions. Individuals, funds, or entities that may transact in cryptocurrencies should apply the *Howey* test and determine whether the cryptocurrency or ICO is a "security" for SEC purposes. If so, then they also should understand the disclosure and registration requirements that will apply to be compliant with the securities laws.

2. Commodity Futures Trading Commission: Is Cryptocurrency a "Commodity"?

Regardless of whether a particular cryptocurrency is a "security" for SEC purposes, it could be treated as a "commodity" for purposes of the Commodity Exchange Act ("CEA"), which would subject the cryptocurrency to the jurisdiction of the Commodity Futures Trading Commission ("CFTC") and its regulations, registration, and oversight.[107]

a. **Role of the CFTC.** The mission of the CFTC is to foster open, transparent, competitive, and financially sound markets. By working to avoid systemic risk, the Commission aims to protect market users and their funds, consumers, and the public from fraud, manipulation, and abusive practices related to derivatives and other products that are subject to the CEA.[108]

b. **CFTC's Characterization of Virtual Currency as a Commodity.** Whether a particular virtual currency is a "commodity" is a facts and circumstances determination. The CFTC first found that Bitcoin and other virtual currencies could be properly defined as commodities in 2015 in the CFTC ruling, *In the Matter of Coinflip, Inc. and Francisco Riordan*, CFTC Docket No. 15-29 (September 17, 2015). In the *Coinflip* consent order, the CFTC cited § 1a(9) of the CEA, which defines "commodity" to include, among other things, "all services, rights, and interests in which contracts for future delivery are presently or in the future dealt in."[109] The CFTC noted that this definition of "commodity" is broad.[110]

Coinflip, Inc. was an entity that permitted its users to trade options contracts based on Bitcoin. The CFTC settled its enforcement action against Coinflip, Inc. for violations of the CEA, including trading unregulated options and operating an unregistered swap

[106] *In the Matter of TokenLot, LLC*, File No. 3-18739 (September 11, 2018).

[107] For CFTC resources related to bitcoin and other virtual currency, see https://www.cftc.gov/Bitcoin/index.htm (last visited November 5, 2018).

[108] *See* the CFTC website for CFTC's stated mission and responsibilities, which can be found at https://www.cftc.gov/About/MissionResponsibilities/index.htm (last visited November 5, 2018).

[109] 7 U.S.C. § 1a(9).

[110] *In the Matter of Coinflip, Inc. and Francisco Riordan*, CFTC Docket No. 15-29 (September 17, 2015) at 3; s*ee also, e.g., Board of Trade of City of Chicago v. SEC,* 677 F. 2d 1137, 1142 (7th Cir. 1982).

execution facility. Coinflip, Inc. consented to the CFTC order without admitting or denying the charges.

c. Cases

(1) ***CFTC v. McDonnell*** **(August 23, 2018).** While the CFTC had announced its position that virtual currencies could be commodities in 2015 in *Coinflip*, the case, *CFTC v. McDonnell*, No. 18-cv-0361, Dkt. 29 (E.D.N.Y. August 23, 2018) marked the first court case to weigh in on whether virtual currencies are commodities. In *McDonnell*, a U.S. district court in New York held that virtual currencies are commodities that can be regulated by the CFTC and entered a final judgment ordering Patrick K. McDonnell and CabbageTech, Corp. d/b/a Coin Drop Markets ("CDM") to pay over $1.1 million in civil monetary penalties and restitution in connection with a lawsuit brought by the CFTC alleging fraud in connection with virtual currencies, including Bitcoin and Litecoin. The court found that McDonnell and CDM engaged in a deceptive and fraudulent scheme to induce customers to send money and virtual currencies to CDM, purportedly in exchange for real-time virtual currency trading advice and for virtual currency purchasing and trading on behalf of the customers under McDonnell's direction.

(2) ***CFTC v. My Big Coin Pay, Inc.*** **(September 26, 2018).** On September 26, 2018, the U.S. District Court for the District of Massachusetts entered an order that the CFTC has the power to prosecute fraud involving virtual currency and denying the defendant's motion to dismiss the CFTC's amended complaint.[111]

In January 2018, the CFTC filed a complaint against the defendant, My Big Coin Pay, Inc., which created the My Big Coin ("MBC") virtual currency, for engaging in a fraudulent "virtual currency scheme" in violation of the CEA's ban against fraud or manipulation in connection with the sale of a commodity.

My Big Coin Pay, Inc. pointed to the definition of "commodity" under § 1a(9) of the CEA, which includes agricultural products and "other goods and articles … and all services rights and interests … in which contracts for future delivery are presently or in the future dealt in." My Big Coin Pay, Inc. argued that MBC was not a "commodity" because "contracts for future delivery" are not "dealt in" MBC.

However, the court agreed with the CFTC that the CEA defines "commodity" broadly, "not by type, grade, quality, brand, producer, manufacturer, or form." The court determined both that MBC was a virtual currency and that it was "undisputed" that there is futures trading in virtual currencies (the court pointed to Bitcoin trading), and that, as such, MBC is a "commodity" subject to CFTC jurisdiction.[112]

d. Significance of CFTC Jurisdiction over Virtual Currency. Because cryptocurrency is highly volatile, cryptocurrency investors may use options and other derivative contracts to shift the volatility and hedge the value of the investors' cryptocurrency holdings. If clients are hedging their cryptocurrency holdings or trading, they should determine whether they are subject to CEA rules and whether any registrations or filings are required.

[111] *CFTC v. My Big Coin Pay, Inc.*, No. 18-10077 (D. Mass. September 26, 2018).
[112] *Id.* at 8.

3. Takeaway from Regulatory Considerations

Legal and regulatory authorities have provided some guidance on the treatment, or characterization, of cryptocurrency, but many ambiguities remain and issues continue to emerge as blockchain technology evolves. Planners should be aware of the potential legal and practical implications and oversight in areas beyond taxation that could affect planning with cryptocurrencies.