AMERICAN BANKRUPTCY INSTITUTE

2018 Winter Leadership Conference

Litigating New Financial Industry Issues in Bankruptcy: Cryptocurrency, Blockchain, and Other Breaking News

Hosted by the Bankruptcy Litigation and Commercial Regulatory Law Committees

Dave Berson
Berson Law Group LLP; Overland Park, Kan.

Andrew C. Helman
Murray Plumb & Murray; Portland, Maine

Laura E. Jehl
BakerHostetler; Washington, D.C.

Hon. Stacey G. C. Jernigan
U.S. Bankruptcy Court (N.D. Tex.); Dallas

CONCURRENT SESSION

2018

Litigating New Financial Industry Issues in Bankruptcy: Cryptocurrency, Blockchain, and Other Breaking News

American Bankruptcy Institute – Winter Leadership Conference

December 6-8, 2018
Scottsdale, Arizona

Introductions

Hon Stacey Jernigan
U.S. Bankruptcy Judge
Northern District of Texas

Dave Berson
Berson Law Group LLP
Overland Park, Kansas

Laura E. Jehl
BakerHostetler
Washington, D.C.

Andrew C. Helman
Murray, Plumb & Murray
Portland, Maine

Blockchain and Bitcoin Basics

Blockchain Basics

- "Blockchain" is a technology that creates a public, tamper-proof digital ledger of transactions.
- To access an address on the blockchain, one needs its "key"—a unique string of numbers typically held by the participant on the blockchain or cryptocurrency owner.
- Transactions can be public, pseudonymous or anonymous and recorded with public and private keys.
- Thus anyone can see the address of the transaction but may not know the name of the party involved.

Bitcoin Basics

- Cryptocurrency is a generic term for a wholly digital asset like bitcoin.
- The asset can be used as an investment vehicle or a medium of exchange and payment.
- It is not supported by any physical asset, the full faith and credit of any government, or the creditworthiness of a business.
- Cryptocurrency derives its value from the perception of its worth on the market.

How Does Blockchain Differ from Bitcoin?

- Cryptocurrency is the specific form of a digital asset that is used for investment or as a medium of exchange.
- Blockchain ledger technology is the method by which transactions involving cryptocurrency are recorded or tracked.
- Blockchain is the software on which cryptocurrency runs.
- Transactions are recorded on decentralized ledgers.

How Is Bitcoin Created and Stored?

- Bitcoin is created or obtained by "mining"
- Bitcoin is also obtained by a sale or transfer
  - Initial coin offerings.
  - Peer-to-peer exchanges.
  - Other exchange-based transactions.
- Bitcoin is stored
  - With a digital wallet or
  - By storing a copy of the "private" key in paper or electronic form.

Why Does It Matter?

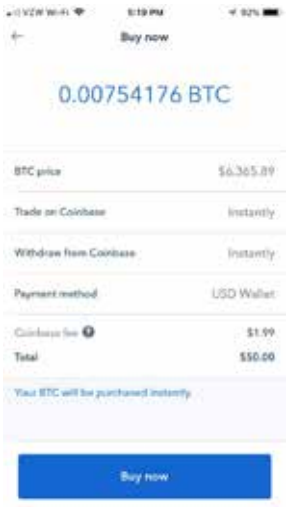
- Cryptocurrency is steadily working its way into the traditional economy as a payment system and investment tool.
- As 2017 closed, 11 percent of Americans surveyed said they currently or previously owned virtual currency, major financial institutions were offering cryptocurrency trading products, and businesses like Dell and NewEgg accepted it for payment.
- Several businesses are now lending against cryptocurrency as collateral.
  - E.g., BlockFi and SALT are lending U.S. currency against cryptocurrency

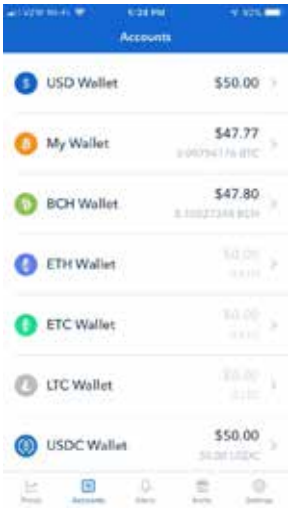
Examples of Useful Cryptocurrency Software and Services

Cryptocurrency Wallet Types

- **Single device software wallet**: You hold the private keys. Wallet is stored on mobile phone, tablet or laptop. Examples: *bitpay.com* and *exodus.io* wallets.
- **Multiple device web wallet**: You hold the private keys. Wallet can be accessed by logging into a website through your web browser or a mobile phone app. Example: *blockchain.com* wallet.
- **Crypto exchange web wallet**: You do *not* hold the private keys, but can immediately sell your cryptocurrency on an exchange. Example: *coinbase.com* wallet.
- **USB hardware dongle wallet**: You hold the private keys and can keep the dongle in a safe deposit box. Example: *trezor.io* wallet.
- **Paper wallet**: You hold the private keys and can keep the paper wallet (with QR codes for the public and private keys) in a safe deposit box.

Buy Cryptocurrency With Your iPhone





BakerHostetler

Hold Multiple Cryptocurrencies in in a Single Wallet

BakerHostetler

Accept Cryptocurrency as Payment

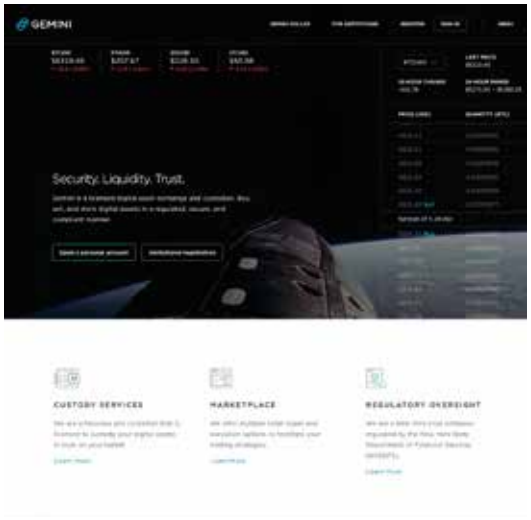
1. Business opens BitPay (*bitpay.com*) account.
2. Business bills customer in U.S. dollars.
3. Business sends a BitPay invoice by email.
4. Customer pays BitPay invoice with cryptocurrency.
5. BitPay converts cryptocurrency into U.S. dollars.
6. BitPay sends ACH of U.S. dollars (after deducting a 1% fee) into checking account of business.

BakerHostetler

Use Cryptocurrency to Load a VISA Debit Card

BakerHostetler

New York Trust Companies: Custody and Escrow Services for Cryptocurrency



BakerHostetler

Cryptocurrency and Regulatory Authorities

BakerHostetler

Cryptocurrency and Regulatory Authorities

- Tax regulation (IRS)
- Securities regulation (SEC)
- Commodities regulation (CFTC)
- Anti-money laundering regulation (FinCEN)
- State money transmitter regulation
- Electronic signature regulation

Tax Regulation

- IRS considers cryptocurrency to be property for tax purposes.

- Taxes owed on realized gains upon the following events:
  - Sale of cryptocurrency for cash.
  - Purchase of goods or services with cryptocurrency.
  - Exchange of one cryptocurrency for another cryptocurrency.

- Ordinary income tax is also owed for the “fair market value” of cryptocurrency mined by a taxpayer.

Securities Regulation

- Securities are regulated by the SEC and state securities commissioners.
- Securities are subject to complex requirements and restrictions on offering disclosure, sale and resale.
- A security includes a digital asset or token that is an "**investment contract**."
- **Definition of investment contract:** An investment of money in a common enterprise with a reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others. *See SEC v. W.J. Howey Co*., 328 U.S. 293, 301 (1946).

Is the Digital Token a Security?

- **Mined cryptocurrencies**: Mined cryptocurrencies, such as bitcoin, are *not* securities.
- **Utility tokens (immediate use):** Digital tokens that are sold for the immediate use of customers to use pre-existing software services are *not* securities. (Note that SEC Chairman Jay Clayton says he has "never seen" a true utility token.)
- **ICO utility tokens (future use):** Digital tokens that are sold by a company to pay for the development of software that will utilize the tokens in the future *are* generally deemed by the SEC to be securities.
- **STO equity tokens**: Digital tokens offering a voting or non-voting equity interest in a company *are* securities.

Securities Issues in Bankruptcy

- Are debts incurred in connection with an initial coin offering nondischargable in bankruptcy?
- Sarbanes-Oxley added Section 523(a)(19)(A) to the Bankruptcy Code. It makes debts arising in connection with a violation of securities laws nondischargable.
- There appears to be some authority for the proposition that a securities law violation by a corporate entity could make a debt of a corporate officer nondischargable if the debt stems from the same securities law violations. *See* Alan Rosenberg, *Are Debts Stemming from ICOs Dischargeable in Bankruptcy?*, XXXVII ABI Journal 8, 30-31, 76-77, August 2018 (discussing theory and providing cases).

Commodities Regulation

- Cryptocurrencies are commodities, subject to CFTC regulation.
- CFTC has the authority to investigate and conduct civil enforcement action against fraud and manipulation in both cryptocurrency derivatives markets and in underlying cryptocurrency spot markets. *See* 7 U.S.C. §§ 9(1), 9(3); *CFTC v. CabbageTech, Corp.*, No. 18-CV-361 (E.D.N.Y. March 6, 2018).
- Any company offering cryptocurrency futures, options or swaps is subject to CFTC registration requirements, unless subject to an exemption.

Anti-Money Laundering Regulation

- A money transmitter must comply with the anti-money laundering regulations of FinCEN.
- FinCEN requires money transmitters to implement a written anti-money laundering compliance program, which includes customer identification, detailed record-keeping and suspicious transaction reporting.
- Since 2013, FinCEN has deemed a "money transmitter" to include (i) a virtual currency exchange and (ii) an administrator of a centralized repository of virtual currency who has the authority to both issue and redeem the virtual currency.

State Money Transmitter Regulation

- In most states, a cryptocurrency exchange is deemed to be a money transmitter that is subject to the same state licensing and regulation requirements as other money transmitters.
- There are only a few cryptocurrency exchanges in the United States, because multi-state money transmitter licensing is *expensive* and *complex.*
- New York also permits the formation of limited purpose trust companies to engage in cryptocurrency exchange, escrow and custody services.

Electronic Signature Regulation

- The federal Electronic Signatures in Global and National Commerce Act (E-SIGN Act), which was enacted in 2000, permits electronic signatures in certain business and consumer contracts to have the same legal enforceability as signed paper contracts.
- The E-SIGN Act defines "electronic signature" as "an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record." 15 U.S.C. § 7006(5).
- This definition is generally considered to be broad enough to include signatures made by cryptographic keys in blockchain-based smart contracts.

Insolvencies Among Cryptocurrency-Related Businesses

MtGox

- MtGox Co., Ltd. was a Japanese company based in Tokyo, formed in 2011, operating one of the earliest exchange sites for bitcoin.
- It became the world's largest exchange until its spectacular demise.
- MtGox filed a Chapter 15 petition in Dallas, Texas, in March 2014, after the filing of its main bankruptcy case in Tokyo in February 2014.
- The impetus for the filing was that 744,408 of bitcoins belonging to customers, plus another 100,000 of MtGox's own bitcoins, collectively valued at $473 million, went missing.
  - This represented 7% of all bitcoin at the time.

MtGox, continued

- Notice issues
  - 120,000 customer/creditors in 175 countries as of the petition date.
  - Trustee could determine the location of 80,000 customers.
  - Email and web-based notice authorized for U.S. proceedings.
- Proof of claim issues
  - Three ways to file proofs of claim: two separate online systems or in writing.
  - Claimants could request distributions in bitcoin or official currency,
  - 23,750 persons filed claims.
  - Claims totaled $2.3 trillion, which were negotiated to about $500 million.

MtGox, continued

- Distributions have not yet been made.
- Bitcoin values have skyrocketed (and then dropped some) during the life of the case
- A creditor sought to initiate a new proceeding in Tokyo to capture the increased value.
- The saga continues . . .

In re Hashfast Technologies, LLC

- This case raised the issue of whether bitcoin is "currency" or other property.
- Hashfast Technologies LLC was a bitcoin mining technology company placed into an involuntary chapter 7 and then converted to a chapter 11.
- An adversary proceeding was filed against a medical doctor paid 3,000 bitcoins to promote the company. The plaintiff sought to avoid this transfer as a preference or fraudulent transfer.

In re Hashfast Technologies, LLC, continued

- At the time of the transfer, the bitcoin was worth $360,000, but it was worth $1.2 million by the time of the litigation.
- A liquidating trustee sought a ruling that the bitcoin was a commodity so it should be valued at $1.2 million, while the transferee argued it was currency and should be valued at $360,000.
- The bankruptcy court ruled that bitcoin was not to be considered U.S. currency in determining its value under section 550(a), but the court declined to decide whether it would order turnover of the asset or its value.
- The case ultimately settled.

Bankruptcy Issues When Individual Owners of Cryptocurrency File

Bankruptcy Issues When an Individual Owner Files

- Cryptocurrency owned by a debtor as of the date a bankruptcy petition is filed would be property of the debtor's estate and must be identified on the debtor's bankruptcy schedules. 11 U.S.C. §§ 521, 541.
- Bankruptcy trustees seeking to identify and liquidate assets will need to rely on an honest debtor to self-report the asset or track down purchases based on a debtor's records.
  - But is this different from a dishonest debtor who hides gold?
- Once identified, the trustee can enforce the bankruptcy estate's rights to obtain a turnover of the property from the party holding it.
  - Caveat: While a U.S. bankruptcy court can claim in rem jurisdiction over property of a debtor's estate—wherever such property is located—an alien individual or business may not recognize the court's authority. 11 U.S.C. § 1334(e).

BakerHostetler

Bankruptcy Issues, Continued

- Trustees and parties-in-interest have many tools available to uncover bankruptcy fraud if there is a reason to believe a debtor is hiding cryptocurrency.
  - 341 meeting.
  - Oral examinations under Bankruptcy Rule 2004.
  - Document production under Bankruptcy Rule 2004
    - Review of credit card and bank statements should reveal cryptocurrency ownership.
- A failure to disclose ownership of cryptocurrency could lead to denial of a discharge or criminal prosecution. 11 U.S.C. § 727(a); 18 U.S.C. §§ 152-57.

BakerHostetler

Bankruptcy and Valuation

- Volatility will likely complicate valuation of cryptocurrency in bankruptcy.
  - Value can vary by the minute or second.
  - A solvent estate could suddenly be insolvent.

- This can pose issues in the following contexts:
  - Valuation of assets in bankruptcy schedules.
  - Valuation of assets at the time of distribution.
  - Valuation of collateral in different proceedings (e.g. claims objection).
  - Valuation in the context of a sale of assets.
  - Litigation strategy for a trustee/DIP seeking recovery of property versus its value under section 550 of the Bankruptcy Code.

Tracing Issues

- Bankruptcy administration may be helped by the traceability of cryptocurrency transactions.

- Section 550(a)(2) of the Bankruptcy Code provides that a transfer avoided under sections 544, 545, 547, 548, 549, 553(b), or 724(a) of the Bankruptcy Code can be recovered from the initial or any subsequent transferee.

- The trustee (or debtor-in-possession) bears the burden to establish that a specific asset is property of the estate. *In re Allou distribs, Inc.*, 379 B.R. 5, 30 (Bankr. E.D.N.Y. 2007).

- Because cryptocurrency transactions are publicly recorded on a blockchain ledger, the trustee/DIP should be able to identify the debtor's cryptocurrency transfers without resort to tracing principles for commingled property.

Cryptocurrency and Article 9

- Uncertainty about the proper classification of cryptocurrency as an asset class under Article 9 means there is also uncertainty about the correct method of perfection.
- In bankruptcy, a trustee or debtor-in-possession has the ability to avoid any transfer subordinate to the rights of a hypothetical judicial lien creditor. 11 U.S.C. § 544(a)(1).
- If a secured creditor has actual control over cryptocurrency (*e.g.*, has the private key), but is not legally perfected, then the trustee can avoid the unperfected lien and preserve its value for the benefit of the estate.
  - In other words, the secured party will be treated as unsecured.

Horrible Hypos

- Assume a company has pledged its general intangibles to secure a loan and then uses bitcoin to buy tickets to an NBA game from a team accepting cryptocurrency as a perk for management or business entertainment.
- Assume a corporate traveler pays for a meal at an airport accepting cryptocurrency (which is owned by the employer).
  - In both examples, the vendor takes the cryptocurrency subject to any security interest.
  - The debtor will have no recognizable "proceeds" for these types of experiential purchases.
  - The vendor could become a litigation target of the secured party.
  - In litigation, the secured party may benefit from the identifiable nature of cryptocurrency and likely would not have to engage in tracing for commingled proceeds of cash.
- Assume the vendor has a secured party with a lien on all assets, including general intangibles, with an "after acquired" clause in its security agreement.
  - Even if the vendor takes the cryptocurrency free of a security interest (because there was none or the disposition was authorized), a further disposition of the cryptocurrency would likely be subject to the security interest of the vendor's lender.

Questions?

Thank You ABI

Litigating New Financial Industry Issues in Bankruptcy: Cryptocurrency, Blockchain, and Other Breaking News

Hon. Stacey G. C. Jernigan
U.S. Bankruptcy Court (N.D. Tex.); Dallas

Andrew C. Helman
Murray Plumb & Murray; Portland, Maine

I. Introduction

This program is designed to help insolvency practitioners gain a working understanding of cryptocurrency, blockchain ledger technology, and the various legal and regulatory regimes governing this new digital asset. Understanding what cryptocurrency is—and what we do and don't know about it—is important as the industry matures and regulatory, insolvency, and litigation issues develop.

II. Blockchain and Bitcoin Basics

A. What is Blockchain Ledger Technology?

Blockchain ledger is a decentralized digital ledger of transactions that can be used to record almost any type of information. It is most well-known for its association with bitcoin and other cryptocurrency and can be thought of as the software on which bitcoin and cryptocurrency run.

One recent article by the co-founder of a blockchain development company described the distributed ledger technology like this:

> In simple terms, a blockchain can be described as an append-only transaction ledger. What that means is that the ledger can be written onto with new information, but the previous information, stored in blocks, cannot be edited, adjusted or changed. This is accomplished by using cryptography to link the contents of the newly added block with each block before it, such that any change to the contents of a previous block in the chain would invalidate the data in all blocks after it.
>
> Blockchains are consensus-driven. A large number of computers are connected to the network, and to reduce the ability for an attacker to maliciously add transactions on the network, those adding to the blockchain must compete to solve a mathematical proof. The results are shared with all other computers on the network. The computers, or nodes, connected to this network must agree on the solution, hence the term "consensus."
>
> This also makes the work of appending data to the ledger decentralized. That is, no single entity can take control of the information on the blockchain. Therefore, we need not trust a single entity since we rely on agreement by many entities instead. The beauty of this construct is that the transactions recorded in the chain can be

> publicly published and verified, such that anyone can view the contents of the blockchain and verify that events that were recorded into it actually took place.

Arthur Linuma, *What Is Blockhain And What Can Businesses Benefit From It?* Forbes.com (Apr. 5, 2018), https://www.forbes.com/sites/forbesagencycouncil/2018/04/05/what-is-blockchain-and-what-can-businesses-benefit-from-it/#6f169a9675fe.

This technology is being used in a number of contexts. For example, banking institutions like JP Morgan are investing resources to use it as a fast, ideally tamper-proof way to record international money transfers. Other companies are using blockchain ledgers to track goods and products, manufacturing, and shipment. It could also be used as to create a ledger of securities transactions or to record transactions involving any other type of information.

B. What are Cryptocurrency and Bitcoin?[1]

Cryptocurrency is a generic term for a wholly digital asset that includes, for example, bitcoin, which is the most well-known type of cryptocurrency. This new digital asset can be used as an investment vehicle or medium of exchange and payment. It is not supported by any physical asset, the full faith and credit of any government, or the creditworthiness of a business. It derives its value solely based on its perception of worth on the market.

Cryptocurrency is based on an application of "blockchain," a computer technology that creates a public, tamper-proof and anonymous digital ledger of transactions with a variety of different uses. Ownership of a cryptocurrency unit—one bitcoin, for example—represents access to a specific digital address on a blockchain ledger. To access the address on the blockchain, you need its "key"—a unique string of numbers typically held by the cryptocurrency's owner. Tis system provides anonymity and transparency—anonymity to the owner of the asset but transparency with respect to the ledger itself. Thus anyone with access to the ledger can see a transaction involving a specific unit of bitcoin, but ownership of the specific bitcoin units may be anonymous.

Bitcoin can be transferred directly in a peer-to-peer transaction or through transactions facilitated by cryptocurrency exchanges, which are able to bring together willing buyers and sellers. Other written materials provided by a panel member provide a discussion of "cryptocurrency wallets," which are electronic or physical ways to store private and public keys.

III. Insolvencies Among Cryptocurrency-Related Businesses

A. Mt. Gox: What Happens When a Cryptocurrency Exchange Fails?

1. Who Was MtGox?

MtGox Co., Ltd., aka MtGox KK ("MtGox") was a Japanese company based in Tokyo, formed in the year 2011, operating what was one of the earliest exchange sites for Bitcoin—

[1] This section is excerpted from a previously published article. Andrew C. Helman and Carl N. Wedoff, *When Blockchain Meets Article 9 And Bankruptcy*, Law360.com (Feb. 9, 2018).

eventually becoming the world's largest Bitcoin exchange, until a spectacular demise. In other words, it became the largest digital marketplace where individuals could buy and sell Bitcoins and also exchange them for foreign currencies like the U.S. dollar. Its website heralded MtGox as the "world's most sophisticated trading platform," for Bitcoin, handling over 80% of all Bitcoin traded worldwide. Its name was an acronym for "Magic: The Gathering Online Exchange" which had originally been a website for a trading card game. MtGox's indirect owner, sole officer and director, Robert Marie "Mark" Karpeles (who was then a 20-something-year-old French software developer), bought the parent company of MtGox in March 2011—approximately two years after the first Bitcoin started being "mined" in 2009. He took the online site (*i.e.,* the software and website and domain name rights) for the trading cards and created the Bitcoin exchange. Once the Bitcoin exchange site for MtGox was up and running, people could go to website, mtgox.com, create an account, and then once registered and given an account number, users/members could trade Bitcoin online using what was supposed to be the Debtor's secure online trading platform. Members could also store Bitcoins in a virtual vault or "wallet" for safekeeping. The "Bitcoin Wallet" was equivalent to a Bitcoin address or set of addresses that could be used to store or transfer user Bitcoins. Basically, there were five steps: (i) opening an account; (ii) verifying an account; (iii) adding funds to an account; (iv) buying and selling Bitcoins; and (v) withdrawing funds. Each customer could view his or her account statement on the website, but MtGox did not deliver paper-based account statements to its customers. MtGox historically communicated in all ways with its customers through email or the website. How did MtGox earn revenue? Whenever it facilitated the exchange of dollars or other fiat currency for Bitcoins or vice versa, it earned a floating rate fee.

2. The Bankruptcy Filing

MtGox filed a Chapter 15 bankruptcy case (*i.e.,* a petition for recognition of foreign proceeding) in Dallas, Texas, USA on March 9, 2014, Case # 14-31229-sgj-15, following the filing of a main bankruptcy case (*i.e.*, a civil rehabilitation proceeding) in Tokyo on February 28, 2014.[2] The impetus for the bankruptcy filing was that 744,408 of Bitcoins belonging to customers, plus another 100,000 of MtGox's own Bitcoins, collectively valued at $473 million at the time, went missing (although, at the time of writing this article, the value would be about 10 times that). At the time, this was about 7% of all Bitcoins in the world. Hacking was suspected—the initial bankruptcy paperwork indicated: "The cause of the theft or disappearance is the subject of intensive investigation. It is believed to have been caused or related to a defect or 'bug' in the bitcoin software algorithm, which was exploited by one or more persons who had 'hacked' the bitcoin network." Apparently, MtGox had experienced numerous security issues since starting operations back in 2011. In any event, MtGox ceased all withdrawals of currency and Bitcoin prepetition on February 7, 2014, while it allegedly tried to get a handle on the missing Bitcoin. It subsequently suspended all trading on February 25, 2014. It was eventually able to recover only about 200,000 of the missing Bitcoin (shortly after filing bankruptcy) from an "offline old-format

[2] The company was initially in a civil rehabilitation proceeding in which management stayed in place and an individual was appointed to be a supervisor and examiner. Then the proceeding was converted to a "provisional administration" and eventually into a proceeding that was more like a Chapter 7 liquidation, and the supervisor/examiner became something like a trustee. MtGox also eventually sought and obtained recognition of their Japanese main case with proceedings in both the UK and Canada. Recently, a new civil rehabilitation proceeding has been commenced (replacing the liquidation) for reasons that will be further explained below.

wallet". Unfortunately for Bitcoin investors, after the MtGox debacle, the price of Bitcoins plummeted, creating a disruptive ripple effect that temporarily devastated the industry.

3. The Founder, Mark Karpeles (a.k.a Magical Tuxedo)

Mr. Karpeles was not at all trusted by the time of the bankruptcy filing. Parties in interest wanted to take his deposition in the U.S. regarding some of the facts he swore to in his Petition for Recognition as the then-Foreign Representative for the company. The U.S. bankruptcy court ruled that he would be ordered to sit for a deposition in the U.S., if Mr. Karpeles wanted to remain as the "Foreign Representative" in the U.S. case. Mr. Karpeles fairly quickly resigned and was replaced by a Japanese attorney, an individual named Nobuaki Kobayashi, as the "foreign representative" in the U.S. case. Mr. Kobayashi was originally a court-appointed examiner in the Japanese case, but his role was expanded to that of a bankruptcy trustee, after the Japanese case went from initially a "civil rehabilitation" case to "provisional administration" (after it became apparent that a viable rehabilitation plan was not possible), then into the equivalent of a liquidation case. Mr. Karpeles was arrested several months later by the Tokyo Metropolitan Police Department on charges of unauthorized creation and use of electromagnetic records and suspicion of corporate embezzlement and (the charges against him were still pending at the time of this article), but he was released from a Tokyo jail on bail on July 14, 2016, after spending over a year in jail. Mr. Karpeles was eventually forced into a personal bankruptcy case in Tokyo. Additionally, on July 26, 2017, the U.S. Department of Justice announced that Alexander Vinnik, a Russian citizen managing another cryptocurrency exchange, was arrested in Greece and extradited to the U.S. and indicted for involvement in money laundering of over 4 billion dollars. The allegations in the indictment suggest that he stole funds by hacking MtGox (and perhaps laundering 530,000 of the stolen MtGox Bitcoins through his own wallets and other accounts).[3] At the time of the writing of this article, it is still unclear what happened, and no more of the Bitcoin that disappeared has been recovered (except for the 200,000 recovered early on).

4. The Purpose for the U.S. Chapter 15 Case and U.S. Assets

The U.S. bankruptcy court has not been called upon to address any "cutting edge" issues such as whether Bitcoin should be regarded as a commodity, currency, or other type of property thus far. As far as U.S. assets, MtGox did not have much—except for some servers in Dallas, Texas. MtGox mainly filed its U.S. bankruptcy proceedings to stay certain litigation against MtGox in the U.S. Specifically, some putative class action plaintiffs in an Illinois federal court action had sued MtGox and Mr. Karpeles on behalf of all persons in the U.S. who had paid a fee to MtGox to buy, sell, or otherwise trade Bitcoin and, also, on behalf of all persons in the U.S. who had Bitcoins or currency stored with MtGox as of February 7, 2014, when MtGox halted withdrawals of currency or Bitcoin (various tort claims were alleged). Second, the company CoinLab was plaintiff in a $75 million federal court lawsuit with MtGox in Washington state, regarding an alleged breach of a certain exclusive license agreement between MtGox and CoinLab for the U.S. and Canada, whereby CoinLab was to have a license to used MtGox technology. A stay of this litigation was urged to be "essential to the efforts" in the Japan Bankruptcy Proceeding. The U.S. bankruptcy court issued the stay of the litigation (as to MtGox) and it remains in effect.

---

[3] Blockchain analysis has suggested that the hacking of MtGox began in autumn 2011.

In addition to the U.S. servers, MtGox had a potential avoidance action against the U.S. government regarding U.S. bank accounts seized prepetition. Specifically, MtGox, Inc. and/or affiliates including Mutum Sigillum LLC ("Mutum"), a Delaware entity, and MtGox North America, Inc., another MtGox subsidiary, had prepetition bank accounts in the U.S. with approximately $5.2 million U.S. dollars in them. The contents of these bank accounts were seized in May 2013 (prepetition) by the U.S. Secret Service and Department of Homeland Security, relating to the Silk Road investigation.[4] The bank accounts were at Wells Fargo, N.A. and Dwolla, an online payment processor for e-commerce (whose funds were actually held in the custody of Veridian Credit Union). The seizures were prompted by the United States government's assertion that MtGox and/or its affiliates operated an unlicensed money transmitting business in the United States in violation of 18 U.S.C. § 1960.[5] The government's assertion was supported by multiple affidavits of government agents, that led a Magistrate Judge in the District of Maryland to find probable cause of this. Specifically, the evidence was that people in the U.S. were purchasing Bitcoin with MtGox by depositing funds with the online payment processor known as Dwolla and then directing that the funds be used to make the purchase from MtGox, which, of course, maintained the registry of ownership of the Bitcoins. Meanwhile the Wells Fargo Bank account in the U.S. would get wires from Sumitomo Mitsui Bank in Japan for MtGox customers that wanted to withdraw funds from MtGox. Then those Wells Fargo funds would be transferred to Dwolla for the benefit of the customers. In summary, the MtGox U.S. affiliates, which were processing funds relating to MtGox's U.S. customers, allegedly violated the money transmitter statutes during the course of MtGox's U.S. bitcoin operations.[6]

MtGox later formed MtGox Inc., a Delaware corporation, in June 2013 (right after the funds seizure). The company was formed to, among other things, facilitate forming banking relationships and obtaining appropriate licenses in the U.S. In June 2013, it had registered with the U.S. Department of Treasury's Financial Crimes Enforcement Network ("FinCen") as a money

---

[4] The Silk Road marketplace was an underground black market that allowed vendors and buyers to conduct illegal transactions over the internet.

[5] Money transmitting businesses are required by 31 U.S.C. § 5330 to register as such with FinCen. A violation of 18 U.S.C. § 1960 occurs when a person or entity "conducts, controls, manages, supervises, directs, or owns all or part of an unlicensed money transmitting business" 18 U.S.C. §1960(a), with the term "'unlicensed money transmitting business' mean[ing] a money transmitting business which . . . (B) fails to comply with the money transmitting business registration requirements under section 5330 of United States Code, or regulations prescribed under such section . . . ." 18 U.S.C. § 1960(b)(1)(B). On March 18, 2013 FinCen issued guidance on the application of FinCen's regulations to bitcoin operations, stating that an administrator or exchanger of virtual currencies is a money transmitter under FinCen's regulations and must register. See FIN-2013-G001, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," March 18, 2013. 18 U.S.C. § 981 provides that any personal property involved in a transaction or attempted transaction in violation or 18 U.S.C. § 1960 is subject to forfeiture to the U.S. See 18 U.S.C. § 981.

[6] Mutum was used for the processing of funds relating to MtGox's U.S. customers to and from the Bitcoin exchange through an online payment processor, Dwolla, which was located in Iowa. In order to facilitate trades on the MtGox exchange, Mutum funded its Dwolla account from its Wells Fargo account. Additionally, MtGox would transfer, by international wire transfer, funds from Sumitomo Mitsui Bank in Japan in the name of Mt. Gox Company Ltd. for the benefit of the Mutum Wells Fargo account. After the funds were credited to the Mutum Wells Fargo account, they were frequently disbursed to the Dwolla account to purchase Bitcoins, which would then be registered on MtGox's Bitcoin registry.

transmitter business. It had been in the process of seeking to obtain state money transmitter business licenses at the time of the filing. MtGox Inc. apparently never conducted any business operations.

The U.S. Attorney ultimately agreed to return half of the seized funds (approximately $2.6 million), pursuant to a motion to compromise approved by the U.S. bankruptcy court.

5. The Japanese Main Case

Most of the activity of the MtGox bankruptcy case has been in Tokyo, Japan—which was determined to be the center of main interests. The bankruptcy process in Japan is, not surprisingly, quite different than U.S. bankruptcy proceedings. Japanese bankruptcy trustees are required to occasionally meet and confer with the judge (which meetings occur behind closed doors as opposed to open court on the record), and trustees issue periodic written reports to creditors and have periodic creditor meetings. There do not seem to be as many court hearings on the record as what U.S. practitioners are used to. In any event, it was fairly quickly determined by the Japanese Trustee/Foreign Representative appointed that trading/operations on the MtGox exchange would never be resumed. Thus, the case revolved mostly around forensic investigations, locating and marshalling assets, efforts to sell assets, and the gargantuan issue of claims allowance/disallowance and the payment process.

The Trustee first began a process of attempting to preserve electronic data on the Debtor's servers and computer systems and then identifying and transferring the Debtor's cash into the Bankruptcy Trustee's account located in Tokyo. The Trustee retained Deloitte Touche Tohmatsu LLC (and affiliates) and ReEx Accounting Firm to engage in forensic investigations of missing Bitcoin. The Japanese Trustee engaged early on in discussions with various potential buyers of MtGox assets. Mr. Kobayashi received several proposals from parties that were interested in acquiring the exchange and restarting it. Mr. Kobayashi and his team underwent due diligence with respect to those proposals and eventually announced that they had reached a deal with a third party named Payward Japan, KK (as a supporting party)—the operator of a Bitcoin exchange named "Kraken," with offices and users around the world (and which also is a founding member of several Bitcoin self-regulatory organizations, namely the Digital Asset Transfer Authority and the Japan Authority of Digital Assets.). The deal was approved by the Tokyo court and contemplated that Payward would purchase the hard assets (servers and PCs located in Japan, after data was extracted), for monetary consideration of 30 million Yen, which equaled $250,000 U.S. currency. But, perhaps more importantly, Payward would provide nonmonetary consideration in the form of support to the Trustee as follows: (a) Payward would provide 500 hours of free consulting in connection with analyzing the lost Bitcoin; (b) Payward would assist with an online proof of claim system through the MtGox website; and (c) Payward would provide unlimited assistance to Trustee in distributing Bitcoin if that form of distribution were to be chosen.

6. MtGox's Assets Being Administered in Tokyo

As far as assets in Japan and other non-U.S. locations, MtGox had servers and PCs located in Japan, and data thereon. There were also some servers in Europe in various countries.[7] It was also determined that MtGox had 43 bank accounts at 14 different banks (holding, in the aggregate, $4.9M in fiat currency, measured in U.S. Dollars), 39 of which accounts were in Japan. Other accounts were in the Caribbean, Europe, and Australia. The Trustee continued throughout the case to collect/repatriate funds from the various accounts around the world—early reports indicated that he had collected 1.5B yen total (*i.e.,* fiat currency), which is equivalent to $12.2M U.S. dollars, but the gross amount increased over time. And, the Trustee had 200,000 of Bitcoin on hand (*i.e.,* the 200,000 of missing Bitcoin that was recovered early on) to manage. The Debtor's primary bank for business activities was the Japan Net Bank, Limited. MtGox also had significant receivables owing from its parent company (Tibanne) and other affiliates including K.K. Shade 3D, K.K. Bitcoin. Café, and Mr. Karpeles.

7. MtGox Creditors (Mostly Exchange Users/Customers)

The Japanese Trustee/Foreign Representative reported in the U.S. bankruptcy case that there were 120,000 customers in 175 countries with balances on the MtGox website exchange as of the Petition Date. He had information on the location for about 80,000 customers: 30,701 were in the U.S.; 6,103 were in the U.K.; 5,921 were in Germany; 2,458 were in Canada; 2,416 were in France; 2,284 were in China; 1,095 were in Japan. Other than customers, the company had only around ten trade creditors, spread out between Japan, the U.S., the U.K., Poland, and India. There was no secured debt. In the U.S. there were (as earlier mentioned) certain litigation claimants. There was also one large U.S. depositor, in particular, claiming to have had 40,000 Bitcoin on deposit at the time of the bankruptcy filing.

8. Notices

As far as the U.S. case, the U.S. bankruptcy court approved a three-fold notice to the U.S. creditors as to the request for and hearing on recognition (that is, the court's consideration of whether the U.S. Chapter 15 case should go forward). One was through an e-mail to customers, basically advising them of the recognition hearing. Second was through a posting of a notice on the MtGox Website. The third was a posting of a notice on a blog on Reddit, which is frequented by tech users. Hard copies were made available to anyone who filed a notice of appearance or who otherwise requested hard copies. The court declined a request of the U.S. Trustee to require publication notice in the Wall Street Journal and Financial Times, since the court was convinced that the electronic notices were sufficient for this high-tech type of creditor. To be clear, given the online nature of the Debtor's business, and the fact that the Debtor had historically communicated and interfaced with its customers and creditors worldwide through electronic means, and in particular the MtGox website –http://www.mtgox.com—the court thought electronic notices were reasonable and adequate in the case.

---

[7] MtGox never had its own employees. Its workforce was supplied by its parent company, Tibanne, which employed 29 employees as of the bankruptcy filing under a Services Agreement and also had contract workers in the U.K., India, and one in Peru.

As far as notice of the Japan proceedings, when the MtGox exchange was shut down and the Japan Petition was filed in February 2014, the Debtor continued to use the Website to communicate with customers, creditors and other parties. On February 28, 2014, the Debtor posted to the Website a notice regarding the filing of the Japan Petition. That notice listed the Tokyo address of the Debtor's Headquarters. It also communicated that the Debtor had established a call center with a Tokyo telephone number and directed all inquiries to be made to that number (the "Call Center"). Subsequent to the February 2014 Notice, the Debtor published additional notices regarding the Japanese proceedings that identified both the Tokyo address of the Headquarters and details regarding the Call Center. The Japanese Trustee thereafter continued with the Debtor's prior practice of communicating to customers, creditors and other parties through the company Website. He would post such things as "FAQ notices."

9. Proof of Claim Process

With regard to the proof of claim process, it has been much slower than is typical in the U.S.—however, the most recent delays have been due to (ironically) maneuvers of creditors to capture a significant increase in value of Bitcoin in recent months.

The proof of claim deadline established, a few months into the case, was May 29, 2015 (15 months after Japan case filed). And it was not until April 2015 that the Japanese Trustee/Foreign Representative filed a "Notice of Filing of Proof of Claim Documents in Japanese Bankruptcy Proceeding" notifying parties of the deadline and explaining the Proof of Claim procedures. Such Notice was attached to a "Report to Creditors" (and posted on the MtGox website). The Notice provided that there were three ways to file a Proof of Claim. First, there was a "System" in place at https://claims.mtgox.com for former users of the MtGox exchange to file a bankruptcy claim online (utilizing a customer's user name in the MtGox system and email address and password registered in the system). Second, there also was a system to file a proof of claim through the Payward/Kracken online system set up for this purpose. Third, people had the option of filing their claims in writing. There were 400,000 former exchange users or customers for which emails were available and they were sent by email notice of the proof of claim procedures. In theory, contact information should have been available for all customers, since when customers creates a MtGox account, they were required to verify it by providing such information as the user's full name, date of birth, country of birth, physical address, and proof of identity such as a government issued identification card. After the deadline, the Trustee would decide what claims to allow or not allow by September 9, 2015. On the proof of claim form, creditors were to indicate whether they preferred distributions on their claims in Bitcoin or fiat cash.

The last report the U.S. bankruptcy court received regarding the proof of claim process was as follows: There were 24,750 persons who filed bankruptcy claims as asserted customers of the MtGox exchange, 6,642 of which were U.S. customers. The total amount of claims that were filed was, using a conversion to U.S. dollars, equal to $2,320,632,367,562. The Trustee had negotiated these claims down to just under $500 million, last check.

10. Timing of Distributions?

The timing of distributions (more than four years after the bankruptcy proceedings were first initiated) is still uncertain. For one thing, the Japanese Trustee is still selling the Bitcoin of MtGox that he manages. He is apparently known in crypto currency circles as the "Tokyo Whale" because of the large amount of Bitcoin he controls. Additionally, the Japanese Trustee is apparently still considering distributions in Bitcoin. Finally, the Tokyo proceedings have morphed over time. First, there was a civil rehabilitation proceeding (something like a reorganization chapter). Then there was a conversion to a liquidation proceeding. Recently, the case has been superseded with another rehabilitation proceeding, in a slightly unusual turn of events.

11. The Surge in Bitcoin Prices and the Newest Rehabilitation Proceedings for MGox

On November 24, 2017, one of the creditors of MtGox holding Bitcoin-based claims (the "Petitioning Creditor") essentially filed a new bankruptcy case—*i.e.,* filed an involuntary petition for commencement of civil rehabilitation proceedings in the Tokyo Court (the "Second Civil Rehabilitation Petition"). In response to the Second Civil Rehabilitation Petition, the Tokyo Court appointed an examiner, Mr. Hisashi Ito, to examine whether there were any grounds to dismiss the Second Civil Rehabilitation Petition. ***The Petitioning Creditor sought to superseded the existing liquidation case with a new civil rehabilitation proceeding in order to capture the increase in value of Bitcoin from April 2014 to November 2017 and to avoid having MtGox's ultimate equity owner, Mr. Karpeles (who remains charged with embezzlement and data manipulation with respect to the Debtor), capture that increase of value through an equity dividend***. In a Japanese bankruptcy proceeding, the Trustee and Debtor are constrained by Japanese law to valuing the claims of creditors who held Bitcoins as of April 24, 2014, the date of the commencement of the Japan liquidation proceedings. On April 24, 2014, the market price of Bitcoin was $483 U.S. dollars. In other words, the maximum amount to be distributed from the Debtor's estate to a Bitcoin holder who deposited one Bitcoin with the Debtor would be $483 U.S. dollars – even if the market price of one Bitcoin at the date of distribution was (for example) $10,000 U.S. dollars. By comparison, on November 24, 2017, the date of the filing of the Second Civil Rehabilitation Petition, the market price of Bitcoin was $8,201.46 U.S. dollars.

Under Japanese law, civil rehabilitation proceedings do not constrain a debtor or trustee to value Bitcoin-based claims at a certain point of time. While the amount of claims will be valued on the date of the commencement of the civil rehabilitation proceedings for the purpose of determining the amount of voting rights each creditor has to vote on any plan of rehabilitation, there is flexibility on how to distribute and allocate value upon a debtor's exit from such proceedings. In summary, the Petitioning Creditor sought to avail itself of this flexibility to avoid the rigid valuations impressed on its claims under the Japan Bankruptcy. The thought was there would be either a revaluing claims as of the date of commencement of the rehabilitation (which is permissible under Japanese law) or through a confirmed rehabilitation plan which would recognize the dramatic increase in Bitcoin market price and allocate value to Bitcoin creditors accordingly—including through a distribution of Bitcoin in kind. Absent the institution of a civil rehabilitation proceeding, Mr. Kobayashi and the Tokyo Court would be constrained by Japanese law in the Japan Bankruptcy to provide Mr. Karpeles, after, inter alia, the payment of creditors' claims, with

the residual value created by the increase in the market price of Bitcoin, rather than to the Bitcoin creditors themselves.

On February 28, 2018, Mr. Ito, the examiner appointed by the Tokyo Court, submitted a report in which he concluded that there were no grounds to dismiss the petition to commence the Second Civil Rehabilitation Proceedings – provided that certain measures were implemented to protect the interests of "bankruptcy creditors" (*i.e.,* creditors who filed proofs of claims in the earlier-filed bankruptcy liquidation case, including creditors with non-bitcoin claims). Specifically, it was suggested that these claims should essentially have priority over claimants surfacing upon the commencement of the Second Civil Rehabilitation Proceedings. Put differently, Mr. Ito did not recommend commencement of civil rehabilitation proceedings unless, among other things, proper reserves were established by Mr. Kobayashi, as the Bankruptcy Trustee, to fund all non-Bitcoin claims that had not been disallowed by the Tokyo Court in the first case, including with interest. The Tokyo Court accepted the report and, thus, the bankruptcy liquidation proceeding is now stayed and was replaced by a civil rehabilitation proceeding effective June 22, 2018 (with the same individual, Mr. Kobayashi serving as Civil Rehabilitation Trustee). A new proof of claim bar date of October 18, 2018 was established.

So the saga continues. To more clearly understand this, some stark numbers should be considered, as noted in a recent Fortune magazine article:

"Between the time MtGox shut down and when it entered liquidation in April 2014, the price of Bitcoin had plummeted more than 20% to $483. It would be over two and a half years before Bitcoin would regain its previous high—long enough that many MtGox victims didn't even bother filing a claim for what they considered an insignificant sum. Then early last year, Bitcoin finally broke its old record. By late May, it was trading at nearly $2,200, making MtGox's remaining Bitcoins—202,185 to be exact—worth more than everything it owed in claims. When the Bitcoin price peaked at $20,000 in December, the value of MtGox's assets (by then including Bitcoin derivatives such as Bitcoin Cash) ballooned to $4.4 billion—nearly 10 times the amount MtGox said it lost in the first place. The fact that you have a bankruptcy where the only asset that it owns goes up by 5,000%, that's pretty unprecedented."[8]

B. In re Hashfast Technologies LLC: Is Bitcoin Currency or Other Property?

1. Who was Hashfast?

Hashfast Technologies LLC was a Bitcoin mining technology company that was founded in 2013, based in San Jose, California, that was placed into an involuntary Chapter 7 bankruptcy case (consented to by the company and converted to Chapter 11) in the Northern District of California in 2014. Case # 14-30725. The company described itself in bankruptcy filings as being engaged in the manufacture and sale of special purpose computers systems and computer chips designed for processing and analyzing Bitcoin transactional information or "Bitcoin mining." The Debtors' assets fell into two categories: inventory and intellectual property. The inventory consisted mainly of ASIC chips (in wafer form or in various stages of completion), mining boards,

[8] *J. Wiecczner, Mt.Gox and the Surprising Redemption of Bitcoin's Biggest Villain*, FORTUNE (Apr. 19, 2018).

as well as various other system components used in the Bitcoin mining business. The intellectual property consisted of some patents, mask works, and design specifications useful in designing current and future chips, boards, and systems for Bitcoin mining. The Debtor also held two Bitcoin wallets that, in the aggregate, as of June 3, 2014, held 0.062052 Bitcoins. The company had no secured lenders. Its cash came from presales of its manufacturing equipment and funds obtained through the liquidation of Bitcoin holdings it had.

Starting in late 2013, the company began experiencing difficulties in their ability to produce the ASIC chips and other hardware in a timely manner. Those difficulties included ASIC chip and board design errors that required additional effort and time to correct. As a result of those delays, the company failed to meet certain delivery deadlines that had been set by their customers, all of whom had prepaid for product. Those failures led to refund demands and litigation, all of which exacerbated the cash flow problems the company was already experiencing.

The company eventually confirmed a plan of liquidation. The company ended up selling its inventory in the ordinary course of business.

2. Adversary Proceeding Addressing the Nature of Bitcoin (sort of)

An adversary proceeding was filed during the case by the debtor against a medical doctor who had been paid 3000 Bitcoin in 2013 by Hashfast to promote Hashfast's Bitcoin business. The debtor sought to avoid this prepetition transfer under wither preference or fraudulent transfer theories. The 3,000 Bitcoin had a $360,000 value at the time of the transfer in 2013, but had appreciated to a $1.2 million value by 2016. The Liquidating Trustee (who stepped into the shoes of the debtor, post-confirmation) urged the court to rule that the Bitcoin was a commodity that should be valued at its current value of $1.2 million. The recipient of the 3,000 Bitcoin wanted the court to rule that Bitcoin was currency that should be valued at the original $360,000. A motion for partial summary judgment was filed—asking for a ruling only on the section 550 aspect of the original complaint. Specifically, section 550(a) of the Bankruptcy Code, of course, permits a trustee, once a transfer has been avoided, to recover, for the benefit of the estate, either the property transferred or the value of the property. Typically, when currency is transferred, there is no question over the form of recovery: avoidance of a $100 transfer leads to a $100 recovery. However, when other types of property are transferred, the form of recovery becomes relevant, since the property could increase or decrease in value following the transfer. The Liquidating Trustee, thus, argued that the Bitcoin were property and that the estate was entitled to recover either the 3,000 Bitcoin or their current appreciated value of $1.2 million. Specifically, the Liquidating Trustee argued that Bitcoin are a commodity, like gold, silver or pork bellies, that fluctuates in price based upon market conditions—making the point that this was the position of the U.S. Commodity Futures Trading Commission ("CFTC"), which had recently issued an order finding that Bitcoin are a commodity covered by the Commodity Exchange Act and the Internal Revenue Service ("IRS"), which had likewise issued a formal notice stating that Bitcoin are property, not currency, with the result that taxes must be paid on gains arising from the sale of Bitcoin. The defendant, in turn, argued that Bitcoin were not property for purposes of Section 550(a) but rather the equivalent of U.S. dollars that retained their lower "face" value.

On February 22, 2016, Bankruptcy Judge Montali issued an order that stated that Bitcoin was not to be considered U.S. currency in determining its value under 11 U.S.C. § 550(a). The court held as follows: "The court does not need to decide whether bitcoin are currency or commodities for purposes of the fraudulent transfer provisions of the bankruptcy code. Rather, it is sufficient to determine that, despite defendant's arguments to the contrary, bitcoin are not United States dollars. If and when the Liquidating Trustee prevails and avoids the subject transfer of bitcoin to defendant, the court will decide whether, under 11 U.S.C. § 550(a), he may recover the bitcoin (property) transferred or their value, and if the latter, valued as of what date." Thus, the court was only minimally holding that Bitcoin were property that could be subject to an avoidance action.

IV. Bankruptcy Issues When and Individual Owner of Cryptocurrency Files[9]

A. Overview

Insolvency practitioners may begin to see cryptocurrency-related issues in bankruptcy cases. While cryptocurrency is a new form of digital property, the issues for practitioners should largely be familiar. They raise questions about disclosure, valuation, and related litigation and evidentiary issues.

B. How Does a Trustee get Information About Cryptocurrency?

To begin with, like all other forms of property, cryptocurrency owned by a debtor as of the date a bankruptcy petition is filed is included in the broad scope of property of a debtor's estate and must be disclosed in a debtor's schedules of assets and liabilities with a debtor's estimation of value. 11 U.S.C. §§ 521, 541.

Bankruptcy trustees seeking to identify and administer a debtor's assets will need to rely on an honest debtor to self-report ownership of cryptocurrency or track down the asset based on the debtor's records. This is no different from what is expected of any debtor, and a failure to disclose ownership of cryptocurrency could lead to denial of a discharge or criminal prosecution. 11 U.S.C. § 727(a); 18 U.S.C. §§ 152-57.

The primary tools available to a bankruptcy trustee are 341 meetings, oral examinations of a debtor or another party under Rule 2004, and document production under Rule 2004. A review of credit card and bank statements should reveal ownership of cryptocurrency. Barring that, a trustee may want to consider searching known e-mail accounts for key terms that could indicate a cryptocurrency account at a known exchange.

Once identified, a bankruptcy trustee can enforce a bankruptcy estate's rights to obtain turnover of cryptocurrency from any party holding it. However, while a U.S. bankruptcy court can claim *in rem* jurisdiction over property of a debtor's estate—wherever such property is located—an alien individual or business may not recognize the court's authority. 11 U.S.C. § 1334(e).

---

[9] Portions of this section are adapted or excerpted from a previously published article. Andrew C. Helman and Carl N. Wedoff, *When Blockchain Meets Article 9 And Bankruptcy*, Law360.com (Feb. 9, 2018).

Bankruptcy administration may be helped by the traceability of cryptocurrency transactions. Sections 550(a)(2) of the Bankruptcy Code provides that a transfer avoided under §§ 544, 545, 547, 548, 549, 553(b), or 724(a) of the Bankruptcy Code can be recovered from the initial or subsequent transferee. The trustee (or a debtor-in-possession), however, bears the burden to establish that a specific asset is, in fact, property of the estate. *In re Allou Distribs., Inc.* 379 B.R. 5, 30 (Bankr. E.D..N.Y. 2007).

Because cryptocurrency transactions are publicly recorded on a blockchain ledger, the trustee/DIP should be able to identify the debtor's cryptocurrency transfers without resort to tracing principles for commingled property. In other words, one group of cryptocurrency does not appear to be fungible and interchangeable with another group of cryptocurrency due to the fact that all are uniquely identifiable and a record of related transactions exists.

This raises strategic issues in the context of fraudulent transfer litigation strategy. State and federal fraudulent transfer and bankruptcy law allow a plaintiff/creditor to recover **either** the value of property transferred **or** the property itself. *E.g.*, 11 U.S.C. § 550; UFTA § 7; UVTA § 7. The question for a plaintiff is whether they want the cryptocurrency itself or its value—at what time—and how will value be proved when value can change by the second?

As already discussed, a number of these issues were raised in the *Hashfast Technologies* case. In that case, a trustee brought an action to avoid and recover the transfer of 3,000 Bitcoins on a fraudulent transfer theory. The value at the time of the transfer was about $363,000, but the value at the time of the lawsuit was about $1.3 million. The trustee filed a motion for summary judgment arguing he was entitled to the Bitcoins or their current value, because they are a commodity and not currency. The case settled without resolving this issue.

C. Who Has An Interest in Cryptocurrency and How Are These Interests Classified Under Article 9?

As use of cryptocurrency increases, disputes will inevitably arise about the way this new form of digital property should be treated under Article 9. As commercial and insolvency lawyers know, there are recognized forms of collateral under Article 9, and they are subject to different rules for perfection of security interest.

On one end of the spectrum are specifically enumerated classes of collateral including, for example, everything from accounts receivable, to inventor, goods, instruments, investment property and money. UCC §§ 9-102(a)(2), (44), (47), (48), (49), (c); 1-201(24). On the other end is the catch-all "general intangible," which, subject to a few exceptions, includes "any personal property" of a debtor that does not fall within a specifically enumerated class of collateral. UCC § 9-102(42).

Cryptocurrency will likely be classified as a "general intangible" because it does not fall within any of the other specifically enumerated classes of collateral. There are several reasons for this.

To begin with, as several early writers on cryptocurrency and the UCC have noted, cryptocurrency almost certainly is not "money" within the meaning of the UCC.[10] The UCC defines "money" as a "medium of exchange currently authorized or adopted by a domestic or foreign government[.]" UCC §1-201(b)(24). It does not appear that the federal government has authorized or adopted cryptocurrency as a medium of exchange or with any other government.[11]

Moreover, cryptocurrency also does not fit neatly within many of the other categories of collateral recognized under Article 9. As one writer noted:

> Bitcoins are not "instruments" under Article 9 because by definition instruments only exist in written form and involve the payment of money. Bitcoins are not "inventor" under Article 9, because inventory (a sub-type of goods) is limited to items that have a tangible, physical existence. Accounts in which bitcoin are held are not "deposit accounts," because only accounts maintained by a bank are included within that defined term.[12]

Similarly, cryptocurrency is not "investment property" because it is not a "security." *See* UCC §§ 8-102(12), 9-102(49).

There are three reasons why classifying cryptocurrency as a general intangible, as opposed to money, for example, is significant.

First, a security interest in a general intangible can be perfected by filing a financing statement in the jurisdiction where the debtor is located rather than by obtaining possession (e.g., money) or control (e.g., deposit account) over the property. UCC § 9-301(a), 9-310(a), 9-312(b). (Generally speaking, an individual is located at his or her principal place of residence, a single-site business is located at its place of business, and a multisite business is located at its chief executive office. UCC § 9-307.)

Second, once perfected, "[a] security interest . . . continues in collateral notwithstanding sale, lease, license, exchange or other disposition thereof unless the secured party authorized the disposition free of the security interest[.]" UCC § 9-315(a)(1). In other words, a security interest will remain attached to and perfected in cryptocurrency even after a vendor accepts it as payment, as long as the secured party did not consent to a transfer of its collateral free of the security interest.

---

[10] *See* George K. Fogg, *The UCC and Bitcoins: Solutions to Existing Fatal Flaw,* Electronic Commerce & Law Report, BNA/Bloomberg Law (Apr. 1, 2015), https://www.bna.com/ucc-bitcoins-solution-n17179924871/.

[11] There are, however, two recent decisions from the Southern District of New York in which the federal courts have held that cryptocurrency transactions can give rise to money laundering or unlicensed money transfer claims under federal law, though a state court reached the opposition conclusion. *See* Alan Rosenberg, *The Cryptocurrency Craze*, Vol. XXXVII Am. Bankr. Inst. J. No. 2 (Feb. 2018) (discussing *U.S. v. Ulbricht*, 31 F.Supp. 2d 540 (S.D.N.Y. 2014); *U.S. v. Murgio*, 209 F.Supp. 3d 698 (S.D.N.Y. 2016); *State of Fla. v. Michell Abner Espinoza*, Case No. F14-2923, in the Eleventh Judicial Circuit in Miami-Dade County, Fla.)).

[12] *See* Fogg, *The UCC and Bitcoins*, *supra* n. 9, (*citing, inter alia*, UCC §§1-201(a)(24) (money), 9-102(47) instruments), 9-102(a)(48) (investment property), 9-102(a)(44) (deposit accounts)).

Third, a security interest in one form of collateral will ordinarily attach to and be perfected in "proceeds" of the collateral—virtually anything received for a disposition of the collateral—for at least 20 days, and perhaps longer, depending on certain criteria. UCC §§ 9-102(64), 9-315(e). So, for example, a lender with a blanket security interest in all accounts receivable of a debtor will ordinarily be perfected in any cryptocurrency obtained with proceeds of accounts receivable, even if general intangibles were not expressly considered as part of the lender's collateral package at the time of the loan origination.

An example or two makes the point: Suppose a company has pledged its general intangibles to secure a loan and then uses bitcoin to buy tickets to an NBA game from a team accepting cryptocurrency as a perk for management or for business entertainment.[13] Or suppose a corporate traveler pays for dinner and a glass of wine with cryptocurrency owned by the traveler's employer while traveling through the Australian airport that has announced it will accept cryptocurrency as payment.[14]

What happens to the cryptocurrency in the hands of the vendor? Because of the fact that a security interest continues in general intangibles following a disposition (unless otherwise authorized by the secured party), the vendors will likely be holding the lenders' collateral, while the debtor will have no recognizable "proceeds" from these types of "experiential" purchases. This sets the stage for a dispute between the secured party and the vendor. Unlike tracing commingled proceeds of cash, however, the secured party my benefit from the publicly verifiable nature of cryptocurrency transactions when trying to locate specific cryptocurrency subject to its security interests, like a certain bitcoin unit. This may avoid the need for cumbersome state-law-tracing analysis that could be required with commingled funds in a deposit account.

V. Conclusion

It is not yet clear what the long-term role for cryptocurrency will be in our economy—and litigation is likely needed to answer a number of important factual and legal questions. This makes it important for commercial and bankruptcy lawyers to be familiar with what cryptocurrency is and how it operates, the way that it is regulated, and the way that it interacts with commercial and insolvency law.

---

[13] Catherine Clifford, *Billionaire Mark Cuban says the Dallas Mavericks will accept bitcoin next season*, CNBC (Jan. 17, 2018), https://www.cnbc.com/2018/01/17/mark-cuban-nbas-dallas-mavericks-will-accept-bitcoin-next-season.html (NBA team announcing plans to accept bitcoin).

[14] Chris Leadbeater, *Australian airport becomes the first to accept Bitcoin*, The Telegraph (Feb. 1, 2018), http://www.telegraph.co.uk/travel/news/brisbane-becomes-worlds-first-airport-to-accept-bitcoin.

Bloomberg Law®

Blockchain Primer

Laura E. Jehl
Partner
Baker & Hostetler LLP

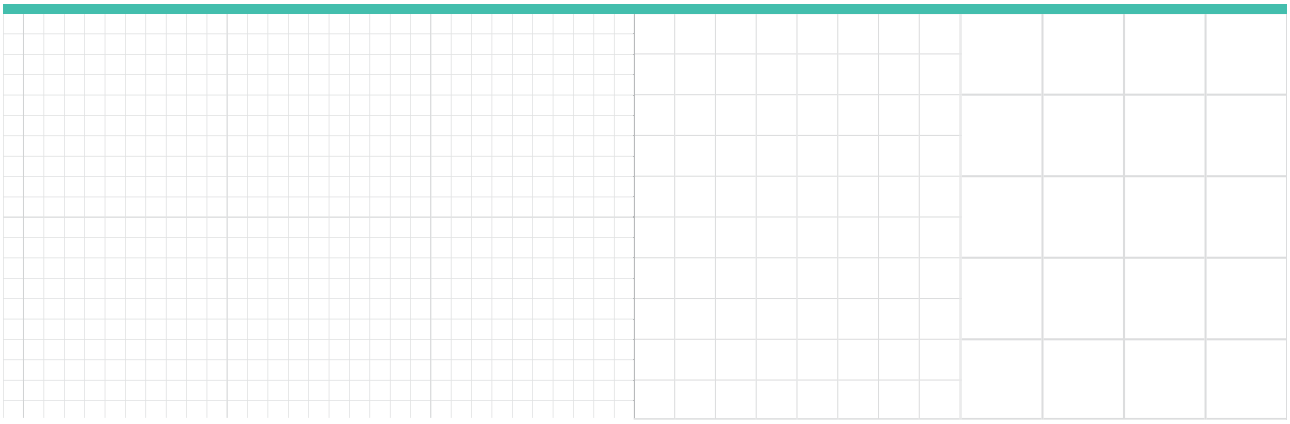


Table of Contents

Laura Jehl, a partner in the Washington office of Baker & Hostetler, focuses her practice on privacy and data security, counseling multinational companies on privacy and data protection issues related to cybersecurity and data breach matters, as well as U.S. and international data privacy and big data issues. Laura also advises clients regarding privacy and security issues related to digital currencies and blockchain technologies.

An Introduction to Blockchain Technology

By Laura E. Jehl
Baker & Hostetler LLP

What is blockchain technology? How does it work?

Blockchain is a decentralized distributed ledger. What does that mean? Envision a standard business ledger, like your bank statement, credit card bill, or a local tax bill. The ledger records transactions, usually transfers or exchanges of assets, into or out of a particular "account," and is compiled by a central authority such as a bank or government agency. A standard ledger system requires that the central agent be trusted: if a bank verifies an electronic funds transfer, for example, that transfer is deemed to have been made even if one party or the other contends that it did not.

A decentralized ledger is a database that is synchronized across a peer-to-peer network of computers. The ledger permanently records changes to the database using cryptographic hash-linked "blocks." When a transaction occurs, a block is added to the ledger, forming a sequential chain with previous transactions, thus the name blockchain. Each block contains data from the previous block, so each transaction can be validated by computers and viewed and affirmed by consensus among the participants in the network. No single party controls the data or the information. Every party can verify the records on the ledger directly, without reliance on any central authority.

What are the advantages of blockchain?

Blockchain technology offers greater efficiency, transparency and security than centralized, trust-based systems and processes.

Centralized systems can be slow and expensive, as middlemen and verification processes clog the pipes. Suppose you want to send money to a family member abroad. If you wire the funds via an intermediary (e.g., your bank or Western Union), the transfer will be subject to fees for electronic funds transfer, currency exchange and more. The transaction will also likely be delayed, often several days, by mandatory waiting periods and settlement times, regulatory oversight, and will be vulnerable to diversion or corruption along the way. In contrast, anyone with a digital currency "wallet" (easily available online) can transfer bitcoin or another virtual currency from anywhere using a smartphone app. The bitcoin is sent directly to the intended recipient's wallet, pseudonymously (if the sender wishes) and without incurring fees, and the amount and addresses will be recorded on a public ledger, adding blocks to the chain. While blockchain transactions are not instantaneous, they usually take several minutes, rather than several days for standard bank transactions.

Every transaction on the blockchain is visible to anyone in the computer system. Each user (known as a node) on the blockchain has a unique alphanumeric address, and everyone on the network can monitor each transaction.

Distributed ledger transactions also offer security advantages over those enabled by a central authority. Because the ledger is chronologically ordered and stored on many computers across the network, a "hack" of a distributed ledger would require simultaneous changes to data on all systems. The algorithm behind the blockchain has (thus far) been very secure. While there have been highly-publicized thefts of digital currency, those incidents involved the compromise of internet-connected digital currency organizations or exchanges, not of the blockchain itself.

What's the difference between blockchain and Bitcoin?

Bitcoin was the first use of blockchain/distributed ledger technology, and the first cryptocurrency or virtual currency. Bitcoin has real monetary value, but it only exists in the ledger. It was born out of the 2008 financial crisis, and was intended to create a mechanism for anonymous online payments without need for a central authority. Although Bitcoin has been embraced as a payment method by many legitimate businesses and individuals, its relative anonymity has also led to widespread use for criminal activities such as money laundering and ransomware payments. After Bitcoin, a number of other cryptocurrencies were launched, most notably Ethereum, which created both a platform for digital currency and an engine for other applications, including so-called "smart contracts." Many – but not all – of the newer cryptocurrencies permit or require proof of a user's identity.

What are some non-currency applications of blockchain technology?

New applications for blockchain technology are growing explosively across industries as diverse as financial services, venture funding, manufacturing, real estate, Internet of Things and government agencies. A few of the most promising use-cases to date include:

"Smart contracts" (which, it has been said, are neither smart nor contracts) embed code in the blockchain network which defines the conditions to which all parties to the contract agree. When, and if, required conditions of the contract are met, the contract self-executes. If a contract for the shipment of goods requires that the goods reach a destination by a certain date, when the goods are confirmed to have arrived on time the code will trigger an automatic payment. Smart contracts eliminate the costs and delays associated with middlemen.

"Provenance." Blockchain provides a secure and immutable way to establish "provenance" – where something came from and where it's been since. Questions of provenance are at the core of many legal issues – verification of title to real estate; the origin and receipt of shipped goods; ensuring the authenticity of luxury goods, art and expensive wine; or being able to identify "conflict diamonds " – to name a few. The immutable mechanisms of blockchain eliminate the need for costly audits, registrations and validation.

"Self-sovereign identity." Several promising projects are exploring the use of blockchain technology to create a "self-sovereign identity" – a single, secure and immutable identity record for each person, which is portable, cannot be taken away, and does not depend on any centralized authority. These digital identity projects offer significant opportunities to improve and streamline identification processes by creating, in effect, a permanent and secure "identity card" for everyone, including both "the undocumented" – refugees and migrants who have lost their records, as well as people from undeveloped regions with no formal identity document process to begin with – and even replacing paper passports.

Closer to home, countless data breaches at companies and government agencies holding vast databases of consumers' personal information have broken the current "user name and password" scheme for online identification. Self-sovereign identity may offer a new model: one in which the individual would control access to his or her personal data, which could be used across the internet to verify access to websites and conduct business, and could limit the use of that data to only the "minimum necessary" for each interaction. Verification of identity would become automatic for all websites rather than requiring an ad hoc procedure that must be repeated each time the user logs in.

Blockchain – The Future of Digital Identity?

By Laura E. Jehl
Baker & Hostetler LLP

A New Paradigm for Proof of Identity

Government agencies, prominent tech companies, startups and newly-created foundations are all working to develop a new paradigm for proof of identity based on blockchain technology. Known as "digital identity," "decentralized identity," or "self-sovereign identity," it would allow individuals to control their own digital identities, limit access to personal data, and provide a much-needed, secure replacement to the current username and password system for access to websites. Digital identity also holds promise for the more than one billion people worldwide who lack officially recognized proof of their existence and, as a result, are deprived of protection, access to banking, education and basic rights.

What is Digital, or Self-Sovereign, Identity?

Digital identity is, essentially, a means of decentralizing identifying information so that individuals have control over their own data. For digital identity to meet the needs of governments, individuals, and businesses, it must be *personal, persistent, portable,* and *private:*

- **personal:** unique to only one person;
- **persistent:** remaining with the individual from birth to death;
- **portable:** accessible from anywhere; and
- **private:** only the individual can grant permission to use or view this data.

Blockchain's distributed ledger technology, combined with encryption, offers the possibility of creating immutable digital identity records that can only be linked to transactions or other data with the explicit authorization of the user. Most blockchain-based ID systems rely on decentralized identifiers ("DIDs"), which hold unique metadata that proves ownership of a particular identity. This distributed, decentralized architecture—with data spread across millions of devices rather than centralized in valuable "honeypots" that attract hackers—provides far greater security against cyberattacks, data breaches, and data corruption than the current system of centralized data repositories.

In addition, because the individual controls access to the data, the individual can share only the "minimum necessary" data for each transaction, and prevent the collection and storage of vast amounts of personal information by each business or organization with which the individual interacts. As a simple example, when an individual walks into a bar and orders a drink, the individual can provide access only to confirmation of legal drinking age, instead of handing over a driver's license containing name, address, birthdate, height, weight, vision and other information. The bartender receives only the information needed to comply with legal age restrictions, and the individual can enjoy a drink without revealing sensitive personal information.

Why Do We Need Digital Identity?

Digital identity has the potential to solve a wide range of pressing problems in both the developed and the developing world.

In the developed world, the current username-and-password identity scheme used to conduct transactions over the internet is becoming more insecure and may not be tenable long-term. The internet's address system is based on identifying and validating communications between

endpoints—computers—on a network. Because that architecture has no way to verify the identification of the people behind those endpoints, each website or application must develop its own system of identifying users, leading to a proliferation of usernames and passwords that is inherently insecure. Each app or website also collects its own trove of personal data, creating huge and redundant volumes of user data. These inefficiencies result in huge costs—arising from identity assurance processes, expensive and ongoing data security efforts, regulatory compliance and potential liability—for the organizations who hold personal data. For individuals, the costs are measured in time spent entering and re-entering the same data, and choosing—and forgetting—multiple usernames and passwords. And, after a seemingly endless series of data breaches, it's clear that the current system is inadequate to protect the security of sensitive personal information, including traditional forms of identity such as Social Security numbers.

The developing world, on the other hand, faces a different kind of identity crisis. Approximately one-sixth of the world's population lacks any form of officially recognized identification. Without proof of identity, individuals are often unable to vote, gain access to healthcare, buy a mobile phone, open a bank account, or enroll in school, and are at greater risk of trafficking. Persons without official identity also cannot obtain passports, register for refugee status, or register the births of their own children. Without accurate population records, public and private organizations struggle to deliver aid and services, and to verify the identities of millions of refugees and displaced persons worldwide. Recognizing these costs, a United Nations-led global partnership of governments, non-governmental organizations, and technology companies has undertaken an effort, known as ID2020, to accelerate access to digital identity.

Self-sovereign identity also promises to eliminate middlemen and streamline bureaucratic processes such as background checks, passport controls and immigration systems. When an identity is verified on a blockchain network, the verifying party can see other trusted sources—like banks, universities, or government agencies—who have verified the same data. The validation itself can be shared without revealing any of the underlying data.

What's Next?

Self-sovereign identity has the potential to reconfigure the relationship between governments and individuals, placing control of identity data in the hands of citizens and raising many new questions:

- Will governments and organizations who currently serve as "identity providers" become "identity verifiers," since identities will still have to be originally proven in some form, such as a birth certificate?
- Despite the reduced risk of loss or theft of digital identities, will there still be a need for "identity-proofing"—checks to ensure that individuals are who they say they are, whether online or in the real world?
- Since there are multiple digital identity projects and proofs-of-concept underway, will DIDs be standardized so that the systems are interoperable and identities portable from one system to another?
- And how will existing regulations—such as the EU's new General Data Protection Regulation—interact with this new technological approach to data privacy and security?

Despite these and other unresolved issues, widespread adoption of digital identity appears inevitable. Stay tuned for developments in this fast-moving area.

Blockchain 'Smart Contracts' – A New Transactional Framework

By Laura E. Jehl, and Brian Bartish
Baker & Hostetler LLP

With the growing buzz around blockchain technology, many organizations are in a race to position themselves as early adopters and leaders in the space. For these organizations, one of the more exciting blockchain applications is the promise of increased efficiency and reduced costs in the transacting process through so-called "smart contracts" – which are actually neither "smart" nor necessarily true legal contracts. Smart contracts are automated programs that encode transactional logic for self-execution and rely upon decentralized cryptographic methods to effectuate enforcement. Regardless of one's opinion of their name, or their legal status, smart contracts are garnering a significant amount of attention and investment due to their ability to radically transform the way parties transact with one another.

What are smart contracts?

Smart contracts actually predate the creation of blockchain technology, as the term "smart contracts" was first coined by computer science and legal researcher Nick Szabo in the mid-1990s. Szabo defined a smart contract as "a set of promises, specified in digital form, including protocols within which the parties perform on these promises." He offered an analogy of the vending machine to illustrate his premise that the entire environment of the transaction could be created within the purview of a machine. In stocking the vending machine, the owner has created an offer, which is accepted when a buyer inserts cash and makes a selection. The code running the machine then takes over to perfect performance by verifying the currency input, dispensing the buyer's selection, and returning any required change. While Szabo's initial vision of smart contracts promised modest gains in transactional efficiency through automation, the advent of blockchain technology has created a number of significant new benefits, perhaps chief among them the ability to create trust between parties operating in a trustless environment that does not rely on a centralized institution, government, or other middleman.

How do smart contracts operate?

Smart contracts rely on code deployed on a blockchain to automatically execute the terms of an agreement. This is where smart contracts begin to depart from traditional contracts, i.e., agreements embodying certain terms to be fulfilled by parties and given the force of law to incentivize performance. In contrast, smart contracts can be viewed as "autonomous agents" designed to execute the logic of an agreement through code that responds to specific messages or transactions. In computational terms, smart contracts are programs that can execute an arbitrary, or open-ended, array of user-specified state transition functions, including performing calculations and storing information. These alter the collective status, or state, of the underlying system, which embodies the entire history of preceding events and the way those events bear upon circumstances such as the ownership of outstanding currencies, the location of goods in transit, or the status of voting rights. The programs function as cryptographic "boxes" that contain value or information and that can only be unlocked in response to certain predefined conditions. Smart contracts, therefore, aren't truly smart, but rather deterministic.

While not as "smart" as advertised, blockchain-based smart contracts represent an evolution of the underlying bitcoin technology, requiring more powerful platforms and more robust programming languages. The Ethereum Virtual Machine, or simply Ethereum, is the best-known of these

platforms. Ethereum emerged with its own programming language, Solidity, specifically designed to encode logic into smart contracts. Ethereum and Solidity offer important advancements over the bitcoin architecture, as both were designed to be "Turing-complete," meaning that they can encode any computation that can be conceivably carried out, including infinite loops. This capability becomes important as the complexity of smart contracts increases, particularly when a smart contract calls on another smart contract as an independent data source or a verifier of real-world events (often referred to as an "oracle"). For example, smart contracts involving financial derivatives may rely on an external source of data, such as the value of the dollar or the Nasdaq index, which can be fed to the derivatives contract through a separate smart contract deployed specifically for calculating those functions. The fact that Solidity is Turing-complete, however, may expose users to infinite loops in contract execution that can cause significant delays and waste both computational and financial resources. Ethereum attempts to manage this type of "denial of service" threat through its transaction structure. Each Ethereum transaction consists of:

- the message recipient;
- the cryptographic signature of the sender;
- an amount of ether (the cryptocurrency used on Ethereum) to transfer;
- an optional data field;
- a "startgas" value, which represents the maximum number of computational steps that a transaction can take when executing; and
- a "gasprice" value, which represents the price per computational step that the sender pays to the miner in order to publish the transaction to the blockchain.

In the event that a transaction "runs out of gas" before completing its execution, the participating nodes and the entire blockchain revert to their previous states, but the miner (i.e., the node that earns the right to publish the block containing the transaction) still collects the gasprice transaction fee. This design, however, is not foolproof against all malicious attacks and still presents some significant risks due, in part, to simple programming error.

Another risk was exemplified by the so-called Decentralized Autonomous Organization (DAO), where a number of Ethereum users joined together to create a sort of crowd-funded venture capital fund where members could vote to invest the DAO's funds in a number of projects. This early attempt at an organization managed entirely through smart contracts ended in ignominy, however, as an attacker exploited flaws in the logic of the underlying smart contracts to siphon off nearly $50 million in ether. The funds were recovered, but only after Ethereum leaders convinced a majority of nodes on the platform to implement a "hard fork" – essentially an operation that reverted the state of the network to what it was prior to the theft. This hard fork, however, required the users to abandon the original network, which still exists under the name Ethereum Classic. The DAO hack served as a lesson that many of the purported strengths of the blockchain architecture, such as its immutability, may be detrimental in certain contexts. Users should therefore carefully consider whether the blockchain will increase the efficiency of transactions or subject them to heightened or unnecessary risks.

Smart contract use cases

Despite the risks, smart contracts offer a number of exciting potential use cases. The developers of Ethereum envisioned a broad array of uses, such as financial derivatives for crop insurance, savings wallets, wills, employment contracts, and peer-to-peer gambling. Smart contract use cases extend beyond the purely financial, as they offer a potential solution to coordination failures among transacting parties. They also offer avenues for experimentation with decentralized governance structures for software development, project management, and entire business organizations.

Unlike the early days of Ethereum, corporations are now investing in smart contract pilots and setting up joint ventures to work on the technology. In 2017, AIG partnered with IBM to create a smart contract multinational insurance policy for Standard Chartered Bank PLC. The policy operates through multiple smart contracts, covering a main policy for Standard Chartered's U.K. headquarters and local policies for affiliates in the U.S., Singapore, and Kenya, which communicate to share data and documents. Also in 2017, French insurer AXA started testing Fizzy, a flight-delay insurance product that leverages smart contracts on the Ethereum blockchain. The smart contracts are connected to global air traffic databases so that as soon as a flight is delayed more than two hours, the smart contract triggers compensation to the insured traveler.

One of the most oft-cited implementations of a smart contract is supply chain management, in which a contract or series of contracts is part of a system that automatically controls the shipment of goods and payments through all stages of the logistics cycle. IBM recently announced a new joint venture with Danish firm A.P. Moller-Maersk – the world's largest container shipping firm, handling roughly one in seven containers shipped globally – that will implement smart contracts as part of a comprehensive strategy to digitize the global supply chain. Their goal is to drive down expenses and increase the speed of the end-to-end shipping process by using smart contracts to automate costly customs clearance and approval requirements.

Beyond the corporate world, governments are also experimenting with the technology. Sweden's land registry authority, the Lantmäteriet, is testing a system for real estate transactions and mortgage deed processes. This would allow buyers and sellers to strike a deal using a smart contract connected to a private blockchain, which reduces the need for paperwork and provides greater transparency in chain of title. One of the hurdles in the Lantmäteriet's road map is a legal issue: validity of digital signatures for real estate contracts. Elsewhere around the globe, Dubai is undertaking a comprehensive digital transformation that would migrate all visa applications, bill payments, and license renewals to blockchain technology by 2020.

While blockchain-based smart contracts are still in a state of infancy and their risks are not always fully anticipated, the interest in their applications to the commercial sector has intensified development efforts. Hyperledger, Project Accord, and the Enterprise Ethereum Alliance have already gained a number of influential supporters from various fields.

Hyperledger is a membership-based organization with the objective of advancing cross-industry blockchain technologies. It incubates and promotes a number of tools including Hyperledger Burrow – a smart contract machine contributed by smart contract startup Monax and co-sponsored by Intel – which executes Ethereum smart contract code on a permissioned virtual machine. Hyperledger has more than 100 members, from tech companies to banks and academic institutions to commercial industry groups.

The Accord Project is an open source software initiative established with Hyperledger, the International Association for Contract & Commercial Management, and the W3C, a web standards body. One of its projects, Cicero, aims to provide lawyers and business professionals with a system for turning paper-based, legally binding agreements into legally binding smart contracts. The Accord Project's membership consists of big law firms, startups, venture capital firms, and other organizations.

More than 150 organizations from a range of industries – including software, infrastructure, financial services, manufacturing, and law – signed on to the Enterprise Ethereum Alliance, launched in February 2017. Formed with the goal of connecting business leaders, startups, academics, and vendors with Ethereum subject matter experts to establish a road map for enterprise adoption, the Ethereum Enterprise Alliance counts Microsoft, JPMorgan Chase, Mastercard, BP, ING, and Deloitte among its members.

Propelled by the strong interest of these well-funded industry leaders, smart contracts are increasingly appearing on legislative agendas. Arizona and Nevada have recently passed laws that promote the legal enforceability of smart contracts, and Florida appears poised to do the same. Much like smart contracts themselves, the gears of progress propelling these efforts appear poised to self-execute.

A Guide to U.S. Regulation of Cryptocurrencies and Cryptocurrency Exchanges

By Laura E. Jehl and Melonia Bennett
Baker & Hostetler LLP

I. Introduction

Blockchain technology is a ledger system with a list of records, called blocks, which are linked and secured using cryptography. The purpose of a blockchain is to serve as "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way."[1] Information recorded on a blockchain's distributed ledger is inherently resistant to modification.

Blockchain technology underlies cryptocurrencies—digital assets that function as a medium of exchange using cryptography to secure transactions.[2] Bitcoin was the first cryptocurrency to use blockchain technology for its distribution, and it remains widely used as a unit of exchange. To exchange Bitcoins, individuals use public and private keys; a public key is used to receive Bitcoins, and a private key is used to allow withdrawals. Transactions take place between users directly (without an intermediary), are verified by the network, and are recorded on a publicly distributed ledger. Bitcoin is just one of many cryptocurrencies that use blockchain technology, including Ethereum, XRP, and Litecoin.

Individuals may use the services of an exchange to buy and sell cryptocurrencies. Exchanges will typically convert cash, bank wires, or ACH transfers into cryptocurrency, based on the current exchange rate. For many cryptocurrencies, exchange rates fluctuate widely—for example, the exchange rate for Bitcoin has fluctuated between about $900 and $19,000 in the past year alone.[3]

The proliferation of Bitcoin and other cryptocurrencies has raised many questions about the legal status of these technologies and financial instruments and how their exchange should be regulated under federal and state money transmitter laws. The classification and regulation of cryptocurrency exchanges is evolving quickly, and navigating the regulatory guidance requires careful consideration of both the guidance and the exchanges' business models. Cryptocurrency exchanges are regulated at the federal level under the Bank Secrecy Act (BSA) as money service businesses (MSBs) and at the state level as money transmitters. As new cryptocurrency exchanges launch and expand the services they offer, institutions that understand the regulatory landscape and can quickly adapt to changing rules will be in the best position to benefit from the massive growth of the cryptocurrency industry.

---

[1] Iansiti, Marco and Karim R. Lakhani. "The Truth About Blockchain." *Harvard Business Review*, Harvard University, Jan. 2017.

[2] There are many, many definitions of digital currencies, virtual currencies, and cryptocurrencies. Generally, cryptocurrencies are considered to be a subset of virtual currencies. However, all of the currencies and tokens discussed, infra, function at least in part as cryptocurrencies. For additional definitions of virtual currencies, see FIN-2013-G0001, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, Mar. 18, 2013; "Virtual Currencies, Key Definitions and Potential AML/CFT Risks." *Financial Action Task Force*, Jun. 2014, http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

[3] "Bitcoin, Ethereum, and Litecoin Price." *Coinbase*, https://www.coinbase.com/charts?locale=en-US.

II. Federal Law – Money Service Business Registration and Criminal Implications

Since the enactment of the Money Laundering Suppression Act of 1994, MSBs have been required to register with the Financial Crimes Enforcement Network (FinCEN) of the United States Treasury Department on a biannual basis.[4]

In 2001, in an effort to thwart terrorist funding, the USA PATRIOT Act expanded federal regulation of MSBs by making it a federal crime to operate a money transmitter business without a money transmitter license in any state that required such a license.[5] The USA PATRIOT ACT revised 18 U.S.C. § 1960 to make it a crime to "knowingly conduct, control, manage, supervise, direct, or own all or part of an unlicensed money transmitting business." This includes operating an MSB without a license in a state that requires a business to be licensed, failing to comply with the FinCEN registration requirements, or knowingly transmitting money derived from or intended to finance criminal activity. Violation of these criminal provisions is a felony punishable by imprisonment of up to five years, fines, and possible forfeiture.

The Money Laundering Suppression Act and the USA PATRIOT Act inadvertently set the stage for the civil and criminal regulation of cryptocurrency exchanges. Arguably, the first-ever virtual currency case brought under these laws was against e-gold. Launched in 1996, e-gold was a digital gold currency and alternative payment system backed by gold reserves.[6] At its peak in 2006, e-gold was processing more than $2 billion worth of transactions per year.[7]

E-gold's creators failed to foresee how criminals would exploit their payment systems, including money laundering, fraud, and hacking incidents. In an effort to put a stop to the criminal abuse of e-gold's system, in 2007, the U.S. Department of Justice (DOJ) brought an indictment against e-gold and its directors under Section 1960 for operating as an unlicensed money transmitting business.[8] As part of these criminal proceedings, the court entered an order adopting the Treasury Department's expansion of the definition of money transmission to include not "only transmissions of actual cash or currency" but also "a transmission of the value of that currency through some other medium of exchange."[9] In July 2008, e-gold and its directors pled guilty to conspiracy to engage in money laundering and the operation of an unlicensed money transmitting business and agreed to pay a $3.7 million fine.

The federal government soon found, however, that requiring MSB registration and criminalizing unlicensed MSBs was not sufficient to protect the public from criminal cryptocurrency activities. The invention of Bitcoin in 2009, and the subsequent profusion of alternative blockchain-based cryptocurrencies, expanded both the usefulness of these assets and the criminal appetite to exploit them. In reaction, on March 18, 2013, FinCEN issued an interpretive guidance for virtual currency exchanges (the "FinCEN Guidance")[10] that closely tracked the positions taken by the DOJ in the e-gold case.

---

[4] *See* 31 U.S.C. § 5330.

[5] Pub. Law 107-56, 115 Stat. 272 (2001).

[6] Dixon, Julie. "The e-gold story." *DGC Magazine*, Jun. 27, 2013, http://dgcmagazine.com/the-e-gold-story/.

[7] *Id.*

[8] *See United States v. e-gold*, No. 1:07-cr-00109 (RMC) (D.D.C. Apr. 24, 2007).

[9] Memorandum Decision, *United States v. e-gold*, 550 F. Supp. 2d 82, 94 (D.D.C. May 8, 2008) (emphasis in original).

[10] See FIN-2013-G0001, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, Mar. 18, 2013.

The purpose of the FinCEN Guidance was "to clarify the applicability of the regulations implementing the BSA to persons creating, obtaining, distributing, exchanging, accepting, or transmitting virtual currencies." It defined two categories of cryptocurrency industry participants: "exchangers" and "administrators." An exchanger is a person or entity "engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency." An administrator of virtual currency is a person or entity "engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency."[11]

The FinCEN Guidance concluded that the definition of a money transmitter does not distinguish between "real" and "virtual" currencies. "Accepting and transmitting anything of value that substitutes for currency makes a person a money transmitter under the regulations implementing the BSA."[12] Therefore, exchangers and administrators are money transmitters that must register as MSBs (unless they fall under an exception). As registered MSBs, these businesses are subject to certain additional requirements under the BSA and its implementing regulations and are required to develop robust anti-money laundering ("AML") compliance programs.

The federal government is currently relying on authority pursuant to 18 U.S.C. § 1960 and the FinCEN guidance to go after cryptocurrency exchanges that it believes are engaged in illegal behavior. In the past two years, there has been an increasing number of criminal complaints for the operation of unlicensed MSBs related to cryptocurrencies in violation of Section 1960. The DOJ has brought cases in Arizona, Colorado, Maine, Missouri, New York, and Ohio.

III. What Is Reasonable Compliance for MSB Cryptocurrencies?

Since the 2007 indictment of e-gold, federal regulators and the DOJ have continued to investigate cryptocurrency companies. The most infamous investigation involved the Silk Road, a dark website that served as a marketplace for illegal drugs, stolen identities, and other criminal activities. Buyers and sellers conducted all transactions on the site using Bitcoin. In 2013, the DOJ shut down the Silk Road and charged its owner, Robert Ulbricht, with narcotics conspiracy, conspiracy to commit computer hacking, money laundering conspiracy, and running a criminal enterprise. The DOJ seized 173,991 Bitcoins in connection with this case, then valued at about $33.6 million.[13]

As public interest in cryptocurrencies and other tokens has grown, so too has the interest of federal regulators and the DOJ in cryptocurrency organizations. Recently, federal regulators and the DOJ have investigated and charged another major cryptocurrency exchange, BTC-e. Federal regulators have also looked at other kinds of cryptocurrency business and their market impact, including the Decentralized Autonomous Organization (known as "The DAO"). As explained more fully below, the resulting civil and criminal investigations, reports, complaints, indictments, and settlements have provided the cryptocurrency world with better insight into what is required of a cryptocurrency MSB and what kind of BSA/AML compliance is required. The settlement agreements and consent order in the BTC-e case, and the Securities and Exchange Commission's (SEC) report on The DAO, in particular, provide insight into what is considered a reasonable compliance for cryptocurrency exchanges.

---

[11] *Id.*

[12] *Id.*

[13] Press Release, "Manhattan U.S. Attorney Announces Seizure Of Additional $28 Million Worth Of Bitcoins Belonging To Ross William Ulbricht, Alleged Owner And Operator Of 'Silk Road' Website." *Department of Justice*, Oct. 25, 2013, https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-seizure-additional-28-million-worth-bitcoins-belonging.

A. The DOJ's and FinCEN's Response and the Impact of BTC-e

Canton Business Corp. (also known as BTC-e) was an Eastern European cryptocurrency exchange that conducted substantial business and maintained servers in the United States. Starting in 2011, BTC-e served approximately 700,000 customers and conducted more than $296 million in transactions of Bitcoin alone.[14] Many of these transactions supported criminal enterprises. For example, according to a 2017 research report by Google, Chainalysis, and others, BTC-e processed 95% of ransomware payment proceeds.[15]

On July 26, 2017, the DOJ brought a 21-count indictment against BTC-e and its alleged head of operations and finance, Alexander Vinnik, for operating an unlicensed MSB, operating an international money laundering scheme, and laundering funds from the hack of another cryptocurrency exchange, Mt. Gox.[16] In addition, FinCEN assessed a $110 million civil penalty against BTC-e for willfully violating AML laws. Vinnik was also individually assessed a $12 million penalty for his role in the violations.

Although BTC-e claimed it had instituted a "Know Your Customer" ("KYC") program, the DOJ indictment accused BTC-e of faking the program. The DOJ and FinCEN charged BTC-e with failing to comply with numerous requirements under the BSA, including critically that BTC-e was not registered with FinCEN and did not have an AML compliance policy. The DOJ indictment [17] and the FinCEN penalty assessment[18] firmly established that BSA requirements for MSBs apply equally to any cryptocurrency exchange that does business in the United States or with U.S. persons, regardless of the nationality of its ownership or its physical location.

---

[14] Press Release, "FinCEN Fines BTC-e Virtual Currency Exchange $110 Million for Facilitating Ransomware, Dark Net Drug Sales." *FinCEN*, Jul. 26, 2017, https://www.fincen.gov/sites/default/files/2017-07/BTC-e%20July%2026%20Press%20Release%20FINAL1.pdf.

[15] Bursztein, Elie, Kylie McRoberts, and Luca Invernizzi. "Tracking desktop ransomware payments." *Research at Google*, https://www.blackhat.com/docs/us-17/wednesday/us-17-Invernizzi-Tracking-Ransomware-End-To-End.pdf.

[16] BTC-e processed transactions involving funds stolen from the Mt. Gox exchange between 2011 and 2014. Most of the charges (19 of the 21) against Vinnik were for his attempts to launder these proceeds of the Mt. Gox theft.

[17] https://www.scribd.com/document/354823899/Vinnik-Superseding-Indictment-Redacted-0.

[18] Assessment of Civil Money Penalty, *In the Matter of BTC-E a/k/a Canton Business Corporation and Alexander Vinnik*, FinCEN No. 2017-03 (Jul. 26, 2017).

Summary of Charges Against BTC-e	
DOJ Indictment: The DOJ indictment provides for multiple failures by BTC-e.	**FinCEN Assessment:** The FinCEN assessment provided additional details of BTC-e failures.
• It failed to register as an MSB with FinCEN.	**• It failed to register as an MSB with FinCEN.** It also failed to register as a U.S. agent.
• It did not have a KYC or customer identification process: BTC-e did not ask for identifying information or documents, only username, password, and e-mail address. Further, it allegedly made false public statements about its KYC policies, including that it required scanned copies of IDs and utility or bank statements.	**• It did not have a KYC or a Customer Identification Program:** BTC-e failed to collect and verify even the most basic customer information needed to comply with the BSA—name, date of birth, and address. BTC-e implemented policies to verify customer identification in May 2017 but stated that compliance with those policies was "optional."
• It did not have an AML program or policies.	**• It did not have a written, implemented AML program:** BTC-e needed, at a minimum, a written program that (a) incorporates policies, procedures, and internal controls reasonably designed to assure ongoing compliance; (b) designates an individual responsible to assure day-to-day compliance with the program and BSA requirements; (c) provides training for appropriate personnel, including training in the detection of suspicious transactions; and (d) provides for independent review to monitor and maintain an adequate program. BTC-e also failed to have a training program and did not designate an AML compliance officer, as required by BSA/AML regulations.
• It purposefully obscured and anonymized transactions: Customers could not fund BTC-e accounts directly but had to wire funds to a BTC-e shell or affiliates. BTC-e made false public statements about refusing international wire transfers.	**• It did not have internal controls:** BTC-e lacked adequate internal controls to mitigate virtual currency risks. It failed to conduct appropriate risk-based due diligence to address anonymizing features and decentralized mixing services used in its transactions. BTC-e attracted and maintained a customer base that included known criminals and criminal enterprises, and allowed these criminals to conduct transactions through its platform.
• BTC-e and its leadership were allegedly aware BTC-e was being used by criminal enterprises to launder money: BTC-e's customers had criminally suggestive usernames; known ransomware schemes deposited funds with BTC-e; funds stolen from Silk Road and Mt. Gox were deposited with BTC-e; and BTC-e shared customers and conducted transactions with Liberty Reserve.	**• It did not have suspicious activity reports (SARs):** BTC-e processed thousands of suspicious transactions, including transactions with customers "widely reported as associated with criminal or civil violations of U.S. law," without ever filing an SAR.
	• It did not comply with recordkeeping requirements: BTC-e's transactional records for transmittals of funds in amounts of $3,000 or more lacked required information including name, address, and account numbers.

B. The SEC's Response

1. The DAO Investigation

On July 25, 2017,[19] the SEC issued The DAO Report[20] about the tokens offered as part of an initial coin offering (ICO) by The DAO, a decentralized autonomous organization and venture capital fund based on Ethereum.[21] In April 2016, the DAO token ICO raised about $120 million[22] from more than 11,000 investors. Shortly thereafter, in June 2016, hackers exploited The DAO's code problems and stole one-third of the tokens – worth about $50 million.[23]

The DAO Report concluded that DAO tokens sold on the Ethereum blockchain constituted "securities" under the Securities Act of 1933 and the Securities Exchange Act of 1934 ("Exchange Act") and that possible securities violations had occurred.

The DAO Report also concluded that the web-based platforms that traded DAO tokens, which were registered with FinCEN as MSBs, should have registered as exchanges pursuant to the Exchange Act.[24] The SEC explained that these platforms provided customers with a system that "matched orders from multiple parties to buy and sell DAO Tokens for execution based on non-discretionary methods," and that they therefore satisfied the SEC's test of whether a trading system constitutes an "exchange." This conclusion serves as a warning to other MSB-registered exchanges that the sale of ICO-type tokens on their own platforms may trigger additional SEC registration and reporting requirements.

2. *Ongoing SEC Actions*

The DAO Report was just the beginning. Since then, the SEC has taken additional actions against other companies engaging in ICOs. For example, in December 2017, the SEC entered an agreed order with Munchee Inc., a California company, to stop its ICO.[25] Munchee attempted to raise $15

---

[19] The SEC's Office of Investor Education and Advocacy also issued an investor bulletin educating investors about ICOs: https://www.investor.gov/additional-resources/news-alerts/alerts-bulletins/investor-bulletin-initial-coin-offerings.

[20] SEC Release No. 81207, "Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO." *Securities & Exchange Commission*, Jul. 25, 2017, https://www.sec.gov/litigation/investreport/34-81207.pdf.

[21] *Id.*; Siegel, David. "Understanding The DAO Hack for Journalists." *Medium*, Jun. 19, 2016, https://medium.com/@pullnews/understanding-the-dao-hack-for-journalists-2312dd43e993.

[22] Waters, Richard. "Automated company raises equivalent of $120M in digital currency." *Financial Times*, May 15, 2016.

[23] Price, Robert. "Digital currency Ethereum is cratering because of a $50 million hack." *Business Insider*, Jun. 17, 2016, http://www.businessinsider.com/dao-hacked-ethereum-crashing-in-value-tens-of-millions-allegedly-stolen-2016-6.

[24] *See* 15 U.S.C. § 78e. According to the DAO Report:

> Exchange Act Rule 3b-16(a) provides a functional test to assess whether a trading system meets the definition of exchange under Section 3(a)(1). Under Exchange Act Rule 3b-16(a), an organization, association, or group of persons shall be considered to constitute, maintain, or provide "a marketplace or facilities for bringing together purchasers and sellers of securities or for otherwise performing with respect to securities the functions commonly performed by a stock exchange," if such organization, association, or group of persons (1) brings together the orders for securities of multiple buyers and sellers, and (2) uses established, non-discretionary methods (whether by providing a trading facility or by setting rules) under which such orders interact with each other, and the buyers and sellers entering such orders agree to the terms of the trade.

[25] Order, In re Munchee, Inc., Adm. Pro. No. 3-18304 (SEC Dec. 21, 2017), https://www.sec.gov/litigation/admin/2017/33-10445.pdf.

million for its restaurant review iPhone app, in part by selling tokens. Relying on The DAO Report, the SEC found that Munchee was engaged in unregistered securities offers and sales in violation of the Securities Act. Instead of imposing a penalty, the SEC and Munchee agreed that Munchee would immediately end its ICO and return all the proceeds raised as part of its token sale.

Not all companies engaged in ICOs have escaped federal intervention as easily as Munchee. In another example, AriseBank, a Dallas company claiming to be the "world's first decentralized bank" with "one of the largest cryptocurrency platforms ever built,"[26] has come under SEC scrutiny. As part of its ICO, AriseBank claimed to have raised more than $600 million, with a goal of $1 billion by February 2018. It marketed its ICO through various social media accounts, video and radio interviews, and even an endorsement by former professional boxer Evander Holyfield.

The SEC intervened in January 2018, filing a complaint in federal court claiming that AriseBank's ICO was a fraud and an illegal securities offering in violation of the Securities Act and the Exchange Act. The SEC complaint alleged that AriseBank had not filed a registration statement, that there was no applicable exemption, and that it had made "materially false statements and omissions to induce investment in the ICO." These allegedly included false statements that AriseBank had purchased an FDIC-insured bank to enable it to offer customers FDIC-insured accounts and that it would offer customers an AriseBank-branded Visa card to use with more than 700 cryptocurrencies.[27]

To date, the court has granted the SEC's request to freeze AriseBank's assets and has appointed a receiver for its digital assets.[28] The SEC's action is ongoing, and it is not the only regulatory agency interested in the actions of AriseBank. Also in January 2018, the Texas Department of Banking issued a consumer alert and a cease-and-desist order for AriseBank, stating that it was not licensed to operate in Texas.[29] States have played an active role in cryptocurrency regulation, as discussed in the next section.

IV. State Money Transmitter Licensing Laws

In addition to FinCEN-imposed federal registration requirements on MSBs, nearly all states require money transmitters to be licensed by the state. But state regulation is highly uneven,[30] and New York is the only state requiring a license specifically for virtual currency. The current patchwork of regulatory requirements has triggered the need for a model law—the Uniform Regulation of Virtual Currency Businesses Act—discussed below.

A. New York's Bitlicense

While nearly all states issue money transmitter licenses (that may or may not cover the activities of cryptocurrency businesses), to date only New York has required a specific virtual currency license.

---

[26] Complaint, *SEC v. AriseBank, Jared Rice Sr., and Stanley Ford*, No. 3:18-cv-00186 (N.D. Tex. Jan. 25, 2018), ECF No. 2 at 1.

[27] *Id.*, Amended Complaint, ECF No. 21 at 2.

[28] *SEC v. AriseBank, Jared Rice Sr., and Stanley Ford*, No. 3:18-cv-00186 (N.D. Tex.), ECF Nos. 6, 27.

[29] "Consumer Alert." *Texas Department of Banking*, Jan. 5, 2018, http://www.dob.texas.gov/public/uploads/files/news/press-releases/2018/01-05-18pr.pdf; Press Release, "Texas Department of Banking Commissioner Issues Cease & Desist Order Relating to AriseBank." *Texas Department of Banking*, Jan. 26, 2018, https://www.dob.texas.gov/public/uploads/files/news/press-releases/2018/01-26-18bpr.pdf.

[30] Consult Bloomberg Law's interactive map of state money transmitter laws to view the current status of licensing requirements: https://www.bloomberglaw.com/product/bankfinance/bf_fintech/page/bf_tracker_digitalcurrency.

Known as a Bitlicense, and offered by the New York Department of Financial Services ("NYDFS"),[31] the Bitlicense requires exchange companies to be licensed to operate in New York. It also has specific compliance obligations, including AML program requirements and cybersecurity program requirements, as well as complaint processes, business continuity plan requirements, record keeping, marketing, and consumer protection. The AML program requirements largely overlap with the federal AML requirements for MSBs:

Summary of New York Anti-Money Laundering Programs Requirements (23 N.Y.C.R.R. § 200.15)
• Conduct an initial risk assessment.
• Create a written AML program that provides internal controls, policies, and procedures for ongoing compliance; independent testing for compliance; a designated, qualified AML compliance individual; ongoing AML compliance training; and board of director approval of the policy.
• Maintain records of all virtual currency transactions, with identity and physical addresses of the party or parties, amount or value, method of payment, dates, and description.
• Report to NYDFS all transactions in an aggregate amount that exceed $10,000 in one day that are not subject to federal currency transaction reporting requirements.
• Maintain policies and procedures to block or reject specific or impermissible transactions that violate federal or state laws, rules, or regulations.
• Conduct suspicious activity monitoring and reporting.
• Maintain a customer identification program, including establishing a customer's identity when an account is opened and verifying the identity with name, physical address, and other identifying information; and check customers against the Specially Designated Nationals list maintained by the Office of Foreign Asset Control (OFAC).
• Ensure enhanced due diligence measures for high-risk customers, high-volume accounts, accounts on which an SAR has been filed, or accounts involving foreign entities.
• Verify identification of any account holder initiating a transaction with a value greater than $3,000.
• Maintain risk-based policies, procedures, and practices to ensure, to the maximum extent practicable, compliance with applicable regulations issued by OFAC.

Perhaps because of these stringent standards, only a handful of licenses have been issued to companies since they were introduced in 2015. Bitlicensed entities include Ripple Labs' affiliate XRP II LLC and Coinbase Inc.[32]

[31] 23 N.Y.C.R.R. pt. 200.

[32] *See* Virtual Currency Licensing. *N.Y. Department of Financial Services*, http://dfs.ny.gov/banking/virtualcurrency.htm.

While New York is the pioneer, it is unlikely to remain the sole state enacting new laws and regulations to govern cryptocurrency companies.

B. New Model Law – the Uniform Regulation of Virtual Currency Businesses Act

To date, only a handful of states have clearly defined "virtual" or cryptocurrency or have issued specific guidance for cryptocurrency exchange companies regarding their money transmitter license.[33] However, this space is evolving, and many more states are likely to enact specific regulation of cryptocurrency businesses. For instance, the Uniform Regulation of Virtual Currency Businesses Act ("URVCBA"), a model law approved by the Uniform Law Commission in 2017,[34] has the goal of providing states with a framework for the regulation of all persons engaged in a "virtual currency business activity."[35]

The URVCBA provides a licensing structure to companies engaged in exchanging, storing, or transferring virtual currencies. Unlike most states' money transmitter licensing laws, the URVCBA provides detailed definitions for these terms, providing more certainty to cryptocurrency companies to encourage innovation. The idea is that only exchanges and wallet providers are regulated by the URVCBA. The model act purposely does not attempt to regulate people or companies that use cryptocurrencies on their own behalf because its goal is to regulate only the consumer-facing portions of the industry. It also has regulatory requirements similar to those of FinCEN, thereby creating a uniform regulatory approach for all players in the cryptocurrency industry.

The URVCBA includes requirements for monitoring compliance, anti-fraud, and cybersecurity programs. It requires robust consumer and insurance coverage disclosures. The URVCBA attempts to resolve some of the difficulties facing companies hoping to operate nationwide, as it contains provisions designed to encourage the use of reciprocal licensing among the states.[36]

To date, the URVCBA has been introduced in two states[37] and is expected to be considered by many more state legislatures in the next few years. The cryptocurrency marketplace is evolving, and states and the federal government will likewise continue to evolve their regulatory oversight of the industry.

---

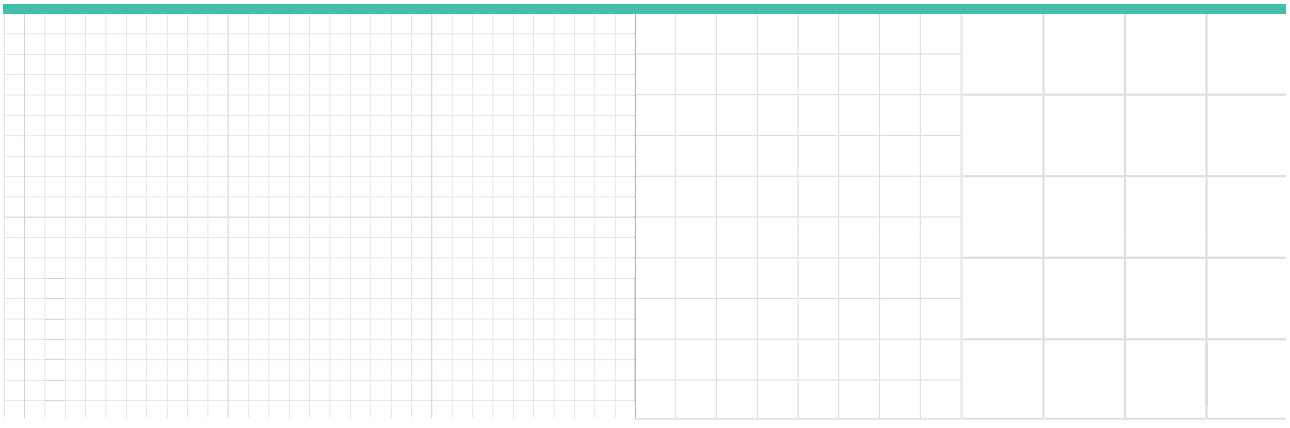
[33] For example, see Connecticut (Conn. Gen. Stat. § 36a-596), Illinois (Digital Currency Regulatory Guidance), Kansas (Regulatory Treatment of Virtual Currencies Under the Kansas Money Transmitter Act), and Texas (Supervisory Memorandum 1037: Regulatory Treatment of Virtual Currencies Under the Texas Money Services Act).

[34] "Final Uniform Regulation of Virtual-Currency Businesses Act," http://www.uniformlaws.org/shared/docs/regulation%20of%20virtual%20currencies/URVCBA_Final_2017oct9.pdf.

[35] *Id.*

[36] Uniform Regulation of Virtual-Currency Businesses Act § 204.

[37] Hawaii and Nebraska, *see* http://www.uniformlaws.org/Act.aspx?title=Regulation%20of%20Virtual-Currency%20Businesses%20Act.



CRYPTOCURRENCY AND DIGITAL ASSET REGULATION

by

Dave Berson
Berson Law Group LLP
Overland Park, Kansas
banktaxlaw.com

The ownership and sale of cryptocurrency and other digital assets is subject to a complex patchwork of federal and state laws and regulations. This document summarizes some of the significant areas of law. Additional information about U.S. blockchain law can be found at the website: ***blockchainlawguide.com.***

BACKGROUND ON CRYPTOCURRENCY WALLETS

There are wide range of cryptocurrency wallets that are available at this time The current types of cryptocurrency wallets include: (i) a single device software wallet in which you hold the private keys (examples: wallets by Bitpay (*bitpay.com*), Exodus (*exodus.io*), and Jaxx (*jaxx.io*)), (ii) a multiple device web wallet in which you hold the private keys (example: Blockchain wallet (*blockchain.com*)), (iii) a multiple device web wallet in which you do not hold the private keys (example: Coinbase wallet (*coinbase.com*)), (iv) a USB hardware dongle wallet in which you hold the private keys (examples: wallets by Trezor (*trezor.io*) and KeepKey (*keepkey.io*), and (v) a "paper wallet" in which the private keys and public keys are written down (which can be later loaded into a software wallet of your choice to be spent).

Instructions with respect to transferring custody of cryptocurrency, in the case of a will or living trust, need to be written in a manner that is easily understandable for individuals who are not familiar with cryptocurrency. For example, in the case of a single device software wallet, instructions should include (i) a description of the name and version of the wallet software, (ii) a description of the name and version of the operating software system of the wallet device (i.e., iOS, Android, MacOS, Windows or Linux), (iii) a description of the types of virtual currency held by the wallet, (iv) either the long-form private and public keys for the wallet or the 12 word "seed" recovery phrase for the wallet, and (iv) step-by-step instructions (which may include screenshots) showing how the wallet can be restored onto a new device, if the current wallet device cannot be accessed.

TAX REGULATION

The Internal Revenue Services ("IRS") considers "virtual currency," such as bitcoin, ethereum tokens, and other cryptocurrency, as "property" for tax purposes, with taxes owed if there is any realized gain on sale. *See* IRS Notice 2014-21, *Guidance on Virtual Currency* (March 25, 2014). For an individual filing a federal income tax return, the gains or losses from a sale of virtual currency that was held as a "capital asset" (i.e., for investment purposes) are customarily reported on Schedule D of IRS Form 1040, and Form 8949 (Sales and Other Dispositions of Capital Assets).

For an individual filing a federal income tax return, the gains or losses from a sale of virtual currency that was held as a "capital asset" (i.e., for investment purposes) are reported on (i) Schedule D of IRS Form 1040 and (ii) IRS Form 8949 (Sales and Other Dispositions of Capital Assets). Any realized gains on virtual currency held for more than one year as a capital asset by an individual are subject to capital gains tax rates. Any realized gains on virtual currency held for one year or less as a capital asset by an individual are subject to ordinary income tax rates. The IRS requires, on Form 8949, for each virtual currency transaction, the following information be disclosed: (i) a description of the amount and type of virtual currency sold, (ii) the date acquired, (iii) date the virtual currency was sold, (iv) the amount of proceeds from the sale, (v) the cost (or other basis), and (vi) the amount of the gain or loss. It should be noted that the record keeping requirements of IRS Form 8949 can be particularly onerous for those who have used cryptocurrency to make numerous small purchases of goods or services throughout the year.

Any realized gains on cryptocurrency held for more than one year as a capital asset by an individual are subject to capital gains tax rates. Any realized gains on cryptocurrency held for one year or less as a capital asset by an individual are subject to ordinary income tax rates.

For 2018, federal income taxes are owed on any realized gains in the value of cryptocurrency upon the following events:

- Sale of cryptocurrency for cash.
- Purchase of goods and services with cryptocurrency .
- Exchange of one cryptocurrency for another cryptocurrency.

Ordinary income tax is also owed for the "fair market value" of any cryptocurrency that has been mined by the taxpayer. If the mining is done as a hobby activity, then the value of the cryptocurrency on the date of mining would be reported in the "other income" line of the taxpayer's Form 1040.

The IRS has not yet provided specific guidance as to whether or not it is a taxable event for a taxpayer to retrieve, through wallet software, a free "fork" or "airdrop" of cryptocurrency. For example, individuals who held bitcoin (BTC) in certain types of software wallets, as of August 1, 2017, are able to use software to retrieve an equal amount of bitcoin cash (BCH). If the IRS specifically determines that cryptocurrency retrieved from a fork is not a taxable event, then taxable gain will not be realized until the forked cryptocurrency has been sold or exchanged. If the IRS determines that cryptocurrency received from a fork or airdrop is a taxable event, it is possible that the IRS could deem ordinary income to be realized for the "fair market value" of the coin on the date of retrieval of the cryptocurrency.

SECURITIES REGULATION

The Securities and Exchange Commission (the "SEC") has regulatory authority over the issuance or resale of any token or cryptocurrency that has the characteristics of an "investment contract". Under Securities Act § 2(a)(1) and Securities Exchange Act § 3(a)(10), a security includes "an investment contract." *See* 15 U.S.C. §§ 77b-77c. An "investment contract" has been defined by the U.S. Supreme Court as an investment of money in a common

enterprise with a reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others. *See SEC v. Edwards*, 540 U.S. 389, 393 (2004); *SEC v. W.J. Howey Co.*, 328 U.S. 293, 301 (1946).

In making a determination as to whether a token is an "investment contract," both the SEC and the courts look at the substance of the transaction, instead of its form. In 1943, the U.S. Supreme Court determined that "the reach of the [Securities] Act does not stop with the obvious and commonplace. Novel, uncommon, or irregular devices, whatever they appear to be, are also reached if it be proved as matter of fact that they were widely offered or dealt in under terms or courses of dealing which established their character in commerce as 'investment contracts,' or as 'any interest or instrument commonly known as a 'security'." *SEC v. C.M. Joiner Leasing Corp*., 320 U.S. 344, 351 (1943). In 1990, the U.S. Supreme Court determined that "Congress' purpose in enacting the securities laws was to regulate investments, in whatever form they are made and by whatever name they are called." *Reves v. Ernst & Young*, 494 U.S. 56, 61 (1990).

The Chairman of the SEC has taken the position that even if a cryptocurrency token issued in an initial coin offering ("ICO") has "utility," the token can be still be deemed to be a security that is regulated under the Securities Act. On February 6, 2018, in written testimony to the U.S. Senate Banking Committee, the Chairman of the SEC stated as follows: "Tokens and offerings that incorporate features and marketing efforts that emphasize the potential for profits based on the entrepreneurial or managerial efforts of others continue to contain the hallmarks of a security under U.S. law."

On September 11, 2018, the U.S. District Court for the Eastern District of New York held that a digital token can be deemed to be a security under the Howey test. *See U.S. v. Zaslavskiy*, No.17- CR-647(RJD) (E.D.N.Y. September 11, 2018).

If an ethereum token or other digital asset is a security (because it is an "investment contract"), then the issuer must issue the security by means of either a registered securities offering or an exemption from securities registration requirements. The definition of issuer is broadly defined to include "every person who issues or proposes to issue any security" and "person" includes "any unincorporated organization." 15 U.S.C. § 77b(a)(4).

Securities broker-dealers and exchanges are subject to (i) the regulatory and enforcement authority of the SEC and (ii) the licensing, examination and enforcement authority of the Financial Industry Regulatory Authority ("FINRA"). FINRA is a private, non-profit corporation that acts as a self-regulatory organization for securities broker-dealers.

On March 7, 2018, the SEC provided the following guidance: "If a platform offers trading of digital assets that are securities and operates as an 'exchange,' as defined by the federal securities laws, then the platform must register with the SEC as a national securities exchange or be exempt from registration." SEC Public Statement, *Potentially Unlawful Online Platforms for Trading Digital Assets* (March 7, 2018). The SEC further stated that "investors should use a platform or entity registered with the SEC, such as a national securities exchange, alternative trading system ("ATS"), or broker-dealer."

An ATS is a trading system that meets the definition of "exchange" under federal securities laws, but is not required to register as a national securities exchange, pursuant to the exemption provided under Rule 3a1-1(a)(2) of the Securities Exchange Act. To operate under this exemption, an ATS must (i) register as a broker-dealer, (ii) file an initial operation report with the SEC on Form ATS prior to commencing operations, (iii) comply with FINRA reporting requirements, and (iv) comply with the additional requirements of SEC Regulation ATS.

On July 6, 2018, FINRA published Regulatory Notice 18-20, *FINRA Encourages Firms to Notify FINRA if They Engage In Activities Related to Digital Assets*. The notice stated, in part: "FINRA is monitoring developments in the digital asset marketplace and is undertaking efforts to ascertain the extent of FINRA member involvement related to digital assets. To supplement FINRA's efforts to date, FINRA is issuing this Notice to encourage each firm to promptly notify FINRA if it, or its associated persons or affiliates, currently engages, or intends to engage, in any activities related to digital assets, such as cryptocurrencies and other virtual coins and tokens."

COMMODITIES REGULATION

On September 17, 2015, the Commodities Futures Trading Commission (the "CFTC") ruled that "virtual currencies" are commodities subject to CFTC regulation. The Commodities Exchange Act ("CEA") provides the CFTC with enforcement jurisdiction to investigate and conduct civil enforcement action against fraud and manipulation in both cryptocurrency derivatives markets and in underlying cryptocurrency spot markets. *See* 7 U.S.C. §§ 9(1), 9(3).

On October 4, 2017, the CFTC stated that "virtual tokens may be commodities or derivatives contracts depending on the particular facts and circumstances." The CFTC stated that it "looks beyond form and considers the actual substance and purpose of an activity when applying the federal commodities laws and CFTC regulations." The CFTC noted that examples of prohibited digital currency activities include (i) price manipulation of a virtual currency traded in interstate commerce, (ii) pre-arranged or wash trading in an exchange-traded virtual currency swap or futures contract, (iii) a virtual currency futures or option contract or swap traded on a domestic platform or facility that has not registered with the CFTC as a SEF or DCM, and (iv) "certain schemes involving virtual currency marketed to retail customers, such as off-exchanged financed commodity transactions with persons who fail to register with the CFTC." *CFTC Primer on Virtual Currencies*, at p. 13 - 14 (October 4, 2017).

On March 6, 2018, a U.S. District Court upheld the authority of the CFTC, under 7 U.S.C. § 9(1) to take enforcement action against a contract of sale of a virtual currency in interstate commerce. See *CFTC v. CabbageTech, Corp*., No. 18-CV-361 (E.D.N.Y. March 6, 2018).

ANTI-MONEY LAUNDERING REGULATION

Under the Bank Secrecy Act (the "BSA"), a money services business ("MSB") is subject to the federal anti-money laundering regulations of FinCEN. In addition, the

Internal Revenue Service (the "IRS") has the authority to examine MSBs with respect to their compliance with FinCEN's anti-money laundering regulations. A "money transmitter" is a type of MSB that is regulated by FinCEN.

On March 18, 2013, FinCEN deemed a "money transmitter" to include (i) a virtual currency exchange and (ii) an administrator of a centralized repository of virtual currency who has the authority to both issue and redeem the virtual currency. FinCEN issued guidance that stated as follows: "An administrator or exchanger that (1) accepts and transmits a convertible virtual currency or (2) buys or sells convertible virtual currency for any reason is a money transmitter under FinCEN's regulations, unless a limitation to or exemption from the definition applies to the person." *See* FIN-2013-G001, *Application of FinCEN's Regulations to Person's Administering, Exchanging or Using Virtual Currencies* (March 18, 2013). PDF

An MSB that is money transmitter must conduct a comprehensive risk assessment of its exposure to money laundering and implement an anti-money laundering ("AML") program based on such risk assessment. FinCEN regulations require MSBs to develop, implement, and maintain a written program that is reasonably designed to prevent the MSB from being used to facilitate money laundering and the financing of terrorist activities.The AML program must: (i) incorporate written policies, procedures and internal controls reasonably designed to assure ongoing compliance; (ii) designate an individual compliance officer responsible for assuring day to day compliance with the program and Bank Secrecy Act requirements; (iii) provide training for appropriate personnel, which specifically includes training in the detection of suspicious transactions; and (iv) provide for independent review to monitor and maintain an adequate program. *See* 31 U.S.C. §§ 5318(a)(2), 5318(h); 31 C.F.R. § 1022.210. FinCEN requires a money transmitter's anti-money laundering program to identify its customers, report suspicious activities for transfers in amounts of $2,000 or more in a day, retain detailed records for transfers by a single customer in one day of $3,000 or more, keep records for at least five years, and file a Currency Transaction Report for single customer transactions that are more than $10,000 a day.

STATE MONEY TRANSMITTER REGULATION

Currently, in most states, a cryptocurrency exchange is deemed to be a money transmitter that is subject to the same state licensing and regulation requirements as other money transmitters. In certain states (such as Colorado and Kansas), businesses engaging in certain types of cryptocurrency sales are exempt from state licensing requirements. Montana is currently the sole state that has no licensing requirements for money transmitters. New York currently has the most onerous money transmitter licensing and compliance requirements for a cryptocurrency exchange.

A cryptocurrency exchange that desires to be licensed in all 50 states is subject to the following expensive licensing requirements: (i) minimum surety bond requirements that range from $1,000 to $500,000 per state, (ii) application fees that range from $0 to $5,000 per state, (iii) licensing fees that range from $0 to $3,750 per state, and (iv) minimum net worth requirements that range from $5,000 to $1,000,000. In addition, a money transmitter is required

to comply with the financial disclosure and consumer compliance requirements of each state in which it does business.

The New York State Department of Financial Institutions currently permits the formation of New York limited purpose trust companies to engage in cryptocurrency exchange, escrow and custody services. This type of trust company charter provides the advantages of (i) being exempt from the money transmission licensing requirements of most states in the United States, (ii) being able to conduct a broad range of fiduciary services related to cryptocurrency assets, (iii) providing reassurance to customers that data security, operations and personnel are subject to bank-grade supervisory and examination standards, and (iv) being able to sell ethereum-based tokens that have a pegged value of $1.00 per token and are fully collateralized by FDIC-insured deposits. The New York trust company charter has the disadvantages of having higher minimum capital requirements and a significantly higher level of compliance costs related to more stringent regulatory oversight and examination. Two limited purpose trust companies that engage in the virtual currency business have been chartered: Gemini Trust Company, LLC and Paxos Trust Company, LLC (which has a trade name of “itBit Trust Company”).

ELECTRONIC SIGNATURE REGULATION

The federal Electronic Signatures in Global and National Commerce Act ("E-SIGN Act"), which was enacted in 2000, permits electronic signatures in certain business and consumer contracts to have the same legal enforceability as signed paper contracts. The E-SIGN Act states that "with respect to any transaction in or affecting interstate or foreign commerce (1) a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form; and (2) a contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation." 15 U.S.C. § 7001(a).

In addition, the E-SIGN Act states that "If a statute, regulation, or other rule of law requires a signature or record relating to a transaction in or affecting interstate or foreign commerce to be notarized, acknowledged, verified, or made under oath, that requirement is satisfied if the electronic signature of the person authorized to perform those acts, together with all other information required to be included by other applicable statute, regulation, or rule of law, is attached to or logically associated with the signature or record." 15 U.S.C. § 7001(g).

The E-SIGN Act does not apply to certain types of contracts and documents. The E-SIGN Act does not apply to wills, trusts, matters of family law, or commercial business transactions subject to the Uniform Commercial Code. *See* 15 U.S.C. § 7003(a). The E-SIGN Act also does not apply to (i) court documents, (ii) notices of cancellation or termination of utility services, (iii) a default under a credit or rental agreement for a primary residence of an individual, (iv) the cancellation or termination of health or life insurance benefits (excluding annuities), (v) a notice of a material failure or recall of a product that risks endangering health and safety, or (vi) any document required to accompany any transportation or handling of hazardous materials, pesticides or other toxic or dangerous materials. *See* 15 U.S.C. § 7003(b).

The broad definition of "electronic signature" in the E-SIGN Act includes signatures made by cryptographic keys in blockchain-based smart contracts. The E-SIGN Act defines "electronic signature" as "an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record." 15 U.S.C. § 7006(5). The E-SIGN Act defines ‘‘record’’ as "information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form." 15 U.S.C. § 7006(9).

The District of Columbia and 47 states (excluding Illinois, New York and Washington) have enacted the Uniform Electronic Transactions Act ("UETA"). UETA is a more comprehensive statute than E-SIGN, and includes additional provisions governing such as issues as (i) the attribution of a signature to an individual, (ii) the effect of mistakes in electronic communications, and (iii) the admissibility of electronic records into evidence.

Instead of enacting UETA, Illinois has enacted the Electronic Commerce Security Act (5 ILCS 175/1). New York has enacted the Electronic Signatures and Records Act (N.Y. Stat Tech L §§ 301-309). Washington has enacted the Electronic Authentication Act (R.C.W. ch. 19.34).