Bloomberg Law Tech & Telecom

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

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

This article, the fourth in a series, explores applications of blockchain technology.

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

[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.

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.

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.

---

[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).

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.

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.

---

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

[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.

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."

[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).

• **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 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.

---

[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.

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. 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

---

[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.

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

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]

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

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

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.

