

BLOCKCHAIN TECHNOLOGY AND REGULATORY INVESTIGATIONS

As blockchain technology becomes embedded in the finance and financial services industries, cryptocurrencies gain prevalence, and the potential for additional blockchain applications continues to grow, industry participants are likely to face heightened regulatory scrutiny, even as the regulatory landscape shifts and evolves with the technology. Counsel to clients engaged in blockchain-related activities and, in particular, virtual currency transactions, should understand the key aspects of blockchain technology, learn to identify conduct that may be subject to regulation, and follow best practices for counseling a client through a regulatory investigation.



MICHAEL J.W. RENNOCK

PARTNER
STEPTOE & JOHNSON LLP

Michael's practice focuses on mergers and acquisitions, securities offerings,

corporate governance, and various private equity and venture capital transactions. He represents acquirers, sellers, boards of directors and board committees, as well as issuers and investors. Michael also advises companies on their filing obligations under the securities laws.



ALAN COHN

OF COUNSEL
STEPTOE & JOHNSON LLP

Alan advises clients on blockchain technology, cryptocurrency, and cybersecurity issues, as

well as other national security and emerging technology issues. He is a co-chair of the firm's Blockchain and Digital Currency practice and serves as counsel to the Blockchain Alliance, a public-private forum established to provide a platform for the blockchain and cryptocurrency industry to engage with law enforcement and regulators.



JARED R. BUTCHER

ASSOCIATE
STEPTOE & JOHNSON LLP

Jared focuses his practice primarily on complex commercial litigation and international arbitration. He

helps clients navigate the legal and regulatory risks that arise at the intersection of commercial disputes and information technologies such as blockchain, distributed ledger technology, and smart contract systems. Jared also works with the firm's Blockchain and Digital Currency practice to advise clients regarding a wide range of blockchain-related issues.

The rapid growth in the adoption of blockchain technology and the development of blockchain-based applications has begun to revolutionize the finance and financial services industries. Beyond the highly publicized cryptocurrency bitcoin, common blockchain applications range from proprietary networks used to process financial transactions or insurance claims to platforms that can issue and trade equity shares and corporate bonds.

With blockchain use cases and applications expanding in scope and number, regulators around the world, including in the US, Canada, Switzerland, the UK, China, Japan, South Korea, Singapore, Hong Kong, and Australia, have expressed interest in regulating blockchain to protect consumers and the market from fraud and other illegal conduct. As a result, organizations launching blockchain-based systems should be prepared to demonstrate that their blockchain networks comply with applicable industry regulations and guidance to avoid a regulatory investigation.

This article explores the emerging landscape for blockchain technology and virtual currencies, focusing on the regulatory issues and risks facing participants in this space. In particular, it discusses:

- The basics of blockchain technology and its current commercial applications.
- The agencies most likely to investigate and regulate blockchain activities and the types of conduct that can trigger regulatory investigations.
- Best practices for counseling clients through regulatory investigations of blockchain activities.

BLOCKCHAIN BASICS

Distributed ledger technology (DLT) is the foundation of blockchain (see *Box, Blockchain Glossary*). DLT offers a consensus validation mechanism through a network of computers that facilitates peer-to-peer transactions without the need for an intermediary or a centralized authority to update and maintain the information generated by the transactions. Each transaction is validated and, along with a group of validated transactions, is added as a new “block” to an already existing chain of transactions, giving rise to the name “blockchain.” Once a transaction has been added to the chain, it generally cannot be altered or removed. (See *Box, A Visual Representation of Blockchain*.)

There are two types of blockchain networks:

- **Permissioned blockchains.** These networks are proprietary networks that specific individuals or entities use to conduct transactions (such as a group of banks processing financial transactions).
- **Permissionless or public blockchains.** These are open-source networks that anyone can access and use (such as bitcoin users who transact with each other using bitcoin for payment).

Unlike the bitcoin blockchain and other public networks, permissioned blockchain networks are typically developed by companies for their own private commercial use. Organizations

may develop their own network or customize a basic network previously developed by a vendor. In some cases, a group of companies in an industry may collaborate to develop and share a proprietary network to facilitate transactions among them, such as the R3 blockchain consortium, which offers a blockchain system for financial institutions.

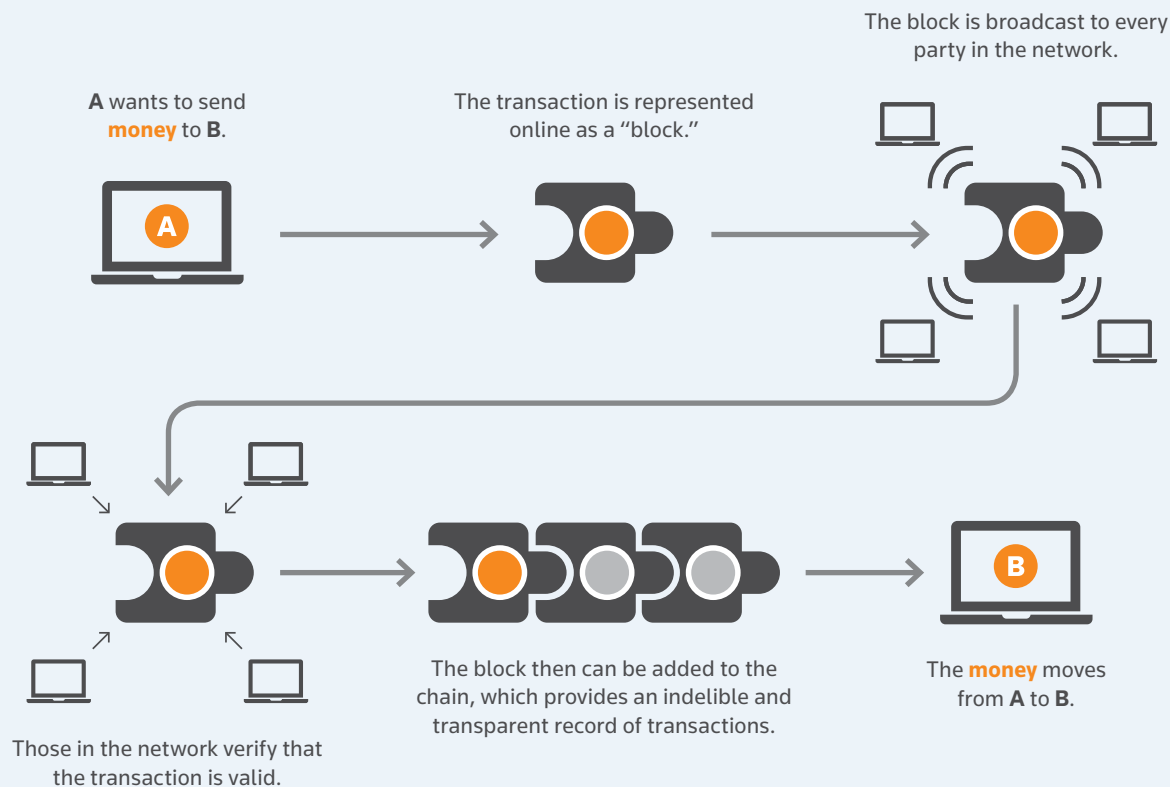
Commercial transactions using blockchain technology share certain key characteristics, including:

- **Real-time records.** Distributed ledgers are updated in real time as transactions and other events occur, with software automating the process. These features ensure that each network participant has its own up-to-the-moment record of transactions, which reduces opportunities for fraud. The automated process and lack of a centralized record keeper also increase efficiencies and generate cost savings.
- **Immutable records.** Blockchain technology enables entities to create permanent, immutable transaction records. This ability offers an obvious commercial benefit, but it can also raise regulatory risk for some parties. Regulators can be given permission to access full transaction histories in the event of an investigation involving transactions recorded to a blockchain, making it more difficult for parties to argue that they lack adequate transaction records (see below *Counseling Clients on Blockchain Investigations*). Additionally, maintaining a permanent record of certain transactions and users through a blockchain can implicate data privacy regulations, particularly as regulators increasingly focus on protecting consumer privacy.
- **Anonymity.** Blockchain technology makes it easier for network users to be pseudonymous, which has ramifications for operators of networks subject to anti-money laundering (AML) and know-your-customer (KYC) regulations (see below *Anti-Money Laundering and Counter-Terrorist Financing Compliance*).
- **Cybersecurity risk.** For a variety of reasons, blockchain networks have proven to be favorite targets for hackers. While no blockchain has been successfully hacked or manipulated, the companies and technology surrounding it have been. Security incidents have ranged from mundane service disruptions to more serious thefts of sensitive data and valuable cryptocurrencies, although the decentralized structure of blockchain networks makes them more resilient against network-wide attacks or tampering.
- **Tax implications.** Blockchain transactions involving virtual currency can give rise to unanticipated tax consequences depending on how the applicable tax authority treats virtual currency. The US Internal Revenue Service (IRS), for example, treats virtual currency as property, which means that a transaction may create the need to recognize a gain or loss on the exchanged cryptocurrency (see below *Tax Treatment of Virtual Currencies*).



Search [Expert Q&A on Blockchain Technology in Banking and Financial Services](#) for more on the implications of blockchain technology for the financial industry.

A VISUAL REPRESENTATION OF BLOCKCHAIN



Source: Financial Times

REGULATION OF BLOCKCHAIN ACTIVITIES

A variety of state and federal agencies and international bodies have shown interest in regulating blockchain-related activities, with a particular focus on virtual currencies. The widespread application and relative novelty of blockchain technology make it difficult to conclusively determine which agencies are likely to investigate any particular blockchain activity. This is largely because the scope of regulatory authority is not yet well-defined in this area and blockchain activities can implicate the jurisdiction of multiple agencies. Most likely, a regulator will investigate any blockchain activity that falls within its traditional jurisdiction.



Search [Virtual Currency Regulation: Overview](#) for more on US regulation of virtual currencies, including federal law, state law, and agency guidance.

Government investigations may be triggered by various blockchain activities. Based on regulatory guidance and enforcement actions to date, counsel should prepare their clients to expect a potential investigation when a blockchain participant:

- Raises capital through an initial coin offering (ICO) (also known as a token sale) or a similar virtual currency fundraising mechanism (see below *Regulation of ICOs and Other Blockchain Investments*).

- Facilitates virtual currency transactions by directly transacting in or issuing virtual currencies, providing or administering a platform for others to transact in virtual currencies, or accepting and transmitting a virtual currency as payment. These transactions can implicate both:
 - AML and counter-terrorist financing regulations (see below *Anti-Money Laundering and Counter-Terrorist Compliance*); and
 - tax compliance issues (see below *Tax Treatment of Virtual Currencies*).

Additionally, though beyond the scope of this article, organizations that collect, store, or use personally identifiable information related to a blockchain network, or suffer a cyber attack or other breach of a proprietary blockchain network, may face regulatory scrutiny over their data privacy and security practices.

Transactions on blockchain networks may also be covered by criminal laws in certain circumstances (see below *Criminal Implications*). For example, criminal securities fraud laws may come into play when companies use ICOs to raise capital by selling a new virtual currency to investors, while the US Department of Justice (DOJ) may find that certain virtual currency transactions raise issues under criminal money laundering, terrorist financing, economic sanctions, and anti-corruption laws.



BLOCKCHAIN GLOSSARY

- **Blockchain.** A blockchain is a peer-to-peer digital ledger of transactions that may be publicly or privately distributed to all users (and therefore is said to be decentralized and distributed). Blockchain technology uses cryptography and a consensus mechanism to verify transactions, which ensures the legitimacy of a transaction, prevents double-spending, and allows for high-value transactions in a trustless environment. A blockchain offers transparency and eliminates the need for intermediaries or third-party administrators.
- **Distributed ledger technology (DLT).** Although it is often used as a synonym for blockchain, DLT generally refers to the distributed, decentralized ledger aspect of blockchain technology. With DLT, a ledger can be maintained, secured, and authenticated by relying on a network of computers (decentralized) rather than a single, centralized authority. As a result, copies of the ledger can be kept and maintained by many individuals or organizations (distributed) and no copy is the master or lead copy.
- **Proof of work.** One of two common consensus validation mechanisms for verifying blockchain transactions. With proof-of-work validation, network participants (known as miners) compete to add the next transaction block to a blockchain by solving a complex cryptographic puzzle, thereby validating prior transactions in the process and earning transaction fees for their work.
- **Proof of stake.** One of two common consensus validation mechanisms for verifying blockchain transactions. With proof-of-stake validation, network participants (known as validators) invest digital coins in the blockchain network, representing their stake in the block. A validator's chance of verifying a block is proportional to its stake in the block.
- **Mining.** The process performed by users (known as miners) to validate transactions on blockchains that use the proof-of-work mechanism for validation.
- **Virtual currency.** A digital representation of value that can be digitally traded and functions as a unit of account or store of value. Virtual currency may come in the form of digital tokens or coins, which are issued by a virtual organization (such as The DAO) or other capital raising entity, and may carry certain rights, such as the right to resell the token or receive a refund (see below *Regulation of ICOs and Other Blockchain Investments*). Virtual currency is not fiat currency (which refers to currency that is recognized as legal tender by a government but is not backed by a physical commodity such as gold or silver (for example, the US dollar)).
- **Virtual currency exchange.** A person or an entity that exchanges virtual currency for fiat currency, funds, or other forms of virtual currency, typically for a fee. Exchanges may also host secondary market trading of virtual currency.
- **Cryptocurrency.** Virtual currency that is secured by cryptography rather than a central system administrator. Popular examples of cryptocurrencies include Bitcoin, Ethereum, Ripple, and Litecoin. Cryptocurrencies are a unit of value used to transact on the underlying blockchain.
- **Token.** Cryptocurrency that is programmed or built on a blockchain to have a range of uses in addition to, or in lieu of, serving as currency both on and off the platform. All virtual currencies and tokens have capital gains potential, particularly if there is a rising demand for the applications and functionalities associated with a particular virtual currency or token.
- **Utility token.** A token that is designed primarily to give the owner access and rights to use a system (like buying tokens at an arcade or tickets at a carnival). Utility tokens typically offer access and functionality features, providing owners with access to a blockchain network and functionalities within that network.

REGULATION OF ICOs AND OTHER BLOCKCHAIN INVESTMENTS

It is difficult to draw a bright line between virtual currencies that function like traditional investments or fiat currencies and those that function as utility tokens, but regulators have shown an increasing interest in bringing regulatory clarity to this area.

The agencies that are most likely to investigate ICOs and other blockchain investments are:

- The Securities and Exchange Commission (SEC).
- The Commodities and Futures Trading Commission (CFTC).
- The Financial Institution Regulatory Authority (FINRA).

SEC

In July 2017, the SEC released an Investor Bulletin that provided recommendations for companies looking to issue tokens through an ICO. Specifically, the Investor Bulletin advised that:

- The SEC will interpret certain ICOs as an offer and sale of securities, requiring the ICO issuer to either:
 - register the tokens with the SEC; or
 - identify an applicable exemption from the registration requirements.
- Where the tokens or coins constitute securities, only registered investment professionals and their firms may sell them.
- If a token sale is described as a crowdfunding contract, it must adhere to Regulation Crowdfunding (17 C.F.R. §§ 227.100-227.503).

- Given the potential for new technology to “perpetuate fraudulent investment schemes,” investors should carefully scrutinize “jargon-laden pitches, hard sells, and promises of outsized returns.”

(SEC, Investor Bulletin: Initial Coin Offerings (July 25, 2017), available at [sec.gov](#).)

Additionally, the SEC recently announced two enforcement proceedings involving blockchain activities. In late 2017, the newly created Cyber Unit of the SEC filed its first action to halt a fast-moving ICO that raised nearly \$15 million in just a few months. In its charges, the SEC alleged that a recidivist Quebec securities law violator, Dominic Lacroix, and his company, PlexCorps, engaged in a fraudulent securities offering by claiming that investment in PlexCoin securities would yield a 1,354% profit in under one month. Before filing the charges, the SEC also obtained an emergency order freezing PlexCorps’s assets. (SEC, SEC Emergency Action Halts ICO Scam (Dec. 4, 2017), available at [sec.gov](#).)

The Cyber Unit also reached a settlement in an administrative proceeding that resolved claims involving the offer and sale of tokens to be issued on a blockchain without being registered as a securities offering. Specifically, Munchee Inc. sold what it represented as a utility token, and which bore no obvious marks of a security because the token did not, for example, carry any equity share, profit share, or dividend. The company conducted a token sale before its platform was operational, yet marketed the tokens as almost assured to give token purchasers an outsized return on secondary exchanges.

In its analysis and order halting the token sale, the SEC made clear that even in a case where the token itself had no outward marks of a security, the lack of a functional platform, combined with the manner in which the tokens were sold, could render the token a security. (SEC, Company Halts ICO After SEC Raises Registration Concerns (Dec. 11, 2017), available at [sec.gov](#).) These actions, and the creation of the Cyber Unit itself, reflect the SEC’s growing focus on ICOs and emphasis on analyzing whether token offerings involve offerings of “securities” that must comply with the same disclosure requirements as other securities offerings.

While senior officials at the SEC have provided some insight into the agency’s views on the regulatory and enforcement landscape for ICOs, their statements underscore the existing uncertainty. For example, Dalia Blass, the Director of the SEC’s Division of Investment Management, stated in a speech that as the SEC receives filings for registered funds that would hold cryptocurrencies, it is considering how the funds fit into the current regulatory scheme and whether differences in the features of cryptocurrencies and other blockchain offerings are important (Dalia Blass, Director, SEC Division of Investment Management, Keynote Address: ICI Securities Law Developments Conference (Dec. 7, 2017), available at [sec.gov](#).)

SEC Chairman Jay Clayton provided some more concrete, if hypothetical, guidance in a recent statement. Chairman Clayton referenced a category of potential tokens that the SEC would not consider securities, for example, a token representing a participation interest in a book club. By contrast, a token

representing an interest in a putative publishing house might merit more scrutiny.

Additionally, Chairman Clayton noted that the SEC would consider it “especially troubling” for promoters marketing an ICO to emphasize the secondary market trading potential (and the tokens’ potential increase in value), suggesting that this type of statement would be a salient factor for the agency when assessing its regulatory scope. (SEC Chairman Jay Clayton, Statement on Cryptocurrencies and Initial Coin Offerings (Dec. 11, 2017), available at [sec.gov](#).)

 Search [SEC and CFTC Issue Statements on Cryptocurrencies and Initial Coin Offerings](#) for more on Chairman Clayton’s statement.

Despite the significant ambiguity that remains, these developments help to define the parameters of the SEC’s regulatory and enforcement practices for ICOs. The enforcement actions and public statements suggest that the SEC may stop short of finding that all ICOs are securities offerings. ICOs that are structured in particular ways and offer tokens carrying specific rights and functionalities may fall beyond the reach of the US securities laws. Additionally, clear regulatory expectations may soon emerge for cryptocurrency and ICO token funds.

CFTC

The CFTC has stated that it considers virtual currency to be a commodity subject to the same regulation and oversight authority as other commodities. However, unlike the SEC, the CFTC remained relatively quiet after opening several investigations of virtual currency exchanges and settling a high-profile enforcement action against virtual currency exchange Bitfinex in 2016 (CFTC, CFTC Orders Bitcoin Exchange Bitfinex to Pay \$75,000 (June 2, 2016), available at [cftc.gov](#)).

That relative quiet ended in 2017 when the CFTC granted LedgerX LLC permission to register as a swap execution facility (SEF) and as a derivatives clearing organization (DCO) for bitcoin-based swaps (see CFTC, CFTC Grants SEF Registration to LedgerX LLC (July 6, 2017) and CFTC Grants DCO Registration to LedgerX LLC (July 24, 2017), available at [cftc.gov](#)). Effectively, these recognitions render LedgerX the first bitcoin options exchange and clearinghouse approved by a US regulator.

 Search [CFTC Registers Digital Currency Trading Platform as Derivatives Clearinghouse](#) for more on the CFTC’s approval of LedgerX’s registration as an SEF and a DCO.

The Chicago Board Options Exchange (CBOE) and the Chicago Mercantile Exchange (CME) began trading bitcoin futures on December 10, 2017. The substantial growth of the trading volume of bitcoin and other virtual currencies seems likely to intensify CFTC attention on these markets with a view toward protecting traders and investors. In turn, this regulatory scrutiny is likely to incentivize market-makers like the CBOE and the CME to develop options for investors, which will in turn elicit more scrutiny.

 Search [CFTC Announces Bitcoin Derivatives Self-Certification Process and New Bitcoin Contracts on Three Futures Exchanges](#) for more on bitcoin futures trading on the CBOE and the CME.

The CFTC has signaled its intention to make its regulatory oversight process the primary vehicle for setting policy for virtual currency and blockchain activities, and to develop a corresponding regulatory framework. These efforts include approval and oversight of virtual currency futures contracts, as well as oversight of virtual currency transactions conducted on margin through virtual currency exchanges.

In a recent joint statement with SEC Chairman Clayton, CFTC Chairman J. Christopher Giancarlo indicated that the CFTC and SEC will work together to bring transparency and integrity to cryptocurrency markets, expressing the agencies' commitment to deter and prosecute fraud and abuse (CFTC and SEC Chairmen in Joint Op-Ed: In Support of Market-Enhancing Innovation, We Will Continue to Bring Transparency and Integrity to Markets (Jan. 25, 2018), available at cftc.gov).

For example, the CFTC recently announced a proposed interpretation defining the "actual delivery" exception of the Commodity Exchange Act (CEA) (7 U.S.C. § 2(c)(2)(D)) in the context of retail commodity transactions involving virtual currencies. The CFTC clarified in this interpretation that under the CEA, covered retail commodity transactions must be traded on a commission-regulated exchange unless the transaction falls within one of the stated exceptions, such as a transaction that results in actual delivery of a commodity within 28 days. The CFTC's proposed interpretation indicates that the actual delivery exception may apply to virtual currency transactions that effectuate a transfer of ownership under the CEA. (Retail Commodity Transactions Involving Virtual Currency, 82 Fed. Reg. 60335-01 (Dec. 20, 2017).)

In practical terms, this indicates that most blockchain networks may be exempt from the CFTC's regulatory requirements because the virtual currency is actually delivered in less than one day after the transaction is executed. However, the exemption would not apply to the CBOE, the CME, or any other party involved in trading virtual currency futures.



Search [CFTC Proposes Legal Interpretation of Actual Delivery Exception for Virtual Currency Regulation](#) for more on the CFTC's proposed interpretation.

FINRA

As a non-profit and non-governmental securities industry regulator, FINRA oversees broker-dealers through a combination of rulemaking and disciplinary actions. FINRA has actively

engaged with individual industry participants to monitor blockchain-related developments and has significant influence over the industry's use of blockchain technology.

In early 2017, FINRA issued a report detailing various ways in which blockchain technology could impact the securities industry. The report focused on the adoption of DLT by market participants themselves, rather than the investment issues that have caught the attention of the SEC and the CFTC (see above *SEC* and *CFTC*).

The report is largely agnostic on industry adoption of blockchain technology, observing that although it offers potential benefits, as with any new technology, blockchain may introduce risks that broker-dealers must take into account. (FINRA, Report on Distributed Ledger Technology: Implications of Blockchain for the Securities Industry (Jan. 2017), available at finra.org.)

Following a comment period for the report, and the launch of a collaborative initiative with industry participants to understand financial technology applications including blockchain (known as the Innovation Outreach Initiative), FINRA held a symposium focusing on potential blockchain applications in the securities industry and the regulatory implications of those applications.

For now, FINRA appears content to follow the course set by federal agencies like the SEC and the CFTC (see Robert Cook, FINRA President and CEO, 2018 Regulatory and Examination Priorities Letter (Jan. 8, 2018), available at finra.org (advising that FINRA will continue to monitor regulatory developments around virtual currencies, and where certain digital assets "are securities or where an ICO involves the offer and sale of securities, FINRA may review the mechanisms ... firms have put in place to ensure compliance with relevant federal securities laws and regulations and FINRA rules"))).

Given the continued emergence of new applications for blockchain technology, it is too early to predict how FINRA ultimately will engage the issue of blockchain-related regulations. However, FINRA seems poised to work with industry participants on finding a workable regulatory and rules-based regime.

ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING COMPLIANCE

Along with their state counterparts, the federal agencies most likely to investigate blockchain transactions for suspected money laundering and counter-terrorist financing activities are:



The CFTC has signaled its intention to make its regulatory oversight process the primary vehicle for setting policy for virtual currency and blockchain activities, and to develop a corresponding regulatory framework.

- The Financial Crimes Enforcement Network (FinCEN).
- The Office of Foreign Assets Control (OFAC).

FinCEN and OFAC are both housed within the US Department of the Treasury.

FinCEN

The regulatory framework underpinning the Bank Secrecy Act (BSA) (31 U.S.C. §§ 5311-5332), which is administered by FinCEN (31 C.F.R. Ch. X), governs US financial institutions. In particular, an individual or organization in the technology sector that facilitates transactions in virtual currency or tokens may constitute a money services business (MSB) if conducted in whole or in part within the US. Guidance issued by, and proposed charging letters settled by, FinCEN regarding administering, exchanging, and using virtual currency have made clear FinCEN's intention to enforce AML requirements against MSBs and money transmitters, and to apply particular scrutiny to virtual currency exchanges and the systems that provide services to those exchanges.



Search [Bank Secrecy Act: Compliance Issues](#) for more on the BSA's regulatory regime.

Counsel to organizations that facilitate virtual currency transactions should become familiar with FinCEN's regulations and guidance so they can provide compliance advice to their clients. One threshold issue counsel should evaluate is whether a client is acting as or has become an MSB as a result of the virtual currency transactions it facilitates.

Under current regulations, an organization qualifies as an MSB if it transmits money or representatives of money, or exchanges money into foreign currency (31 C.F.R. § 1010.100(ff); see also FinCEN, Money Services Business Definition, available at [fincen.gov](#)). The definition is broad enough to encompass more than traditional banks. There is no exemption for transactions below a certain minimum amount, though other exceptions may apply to exempt certain activities from the scope of the MSB rule (31 C.F.R. § 1010.100(ff)(5)(ii)(A)-(F)).

If an organization meets this definition, it may be required to both:

- Register with FinCEN.
- Report suspicious activities by its customers, counter-parties, and personnel.

Additionally, counsel should ensure that their MSB clients have adequate AML compliance programs in place to satisfy FinCEN's requirements regarding internal policies, controls, and training to prevent and detect potential money laundering and terrorist financing.



Search [US Anti-Money Laundering Laws: Key Issues for Financial Institutions](#) and [US Anti-Money Laundering and Trade Sanctions Rules for Financial Institutions](#) for more on the requirements imposed by AML laws and regulations.

In July 2017, FinCEN assessed a civil monetary penalty of over \$110 million against Canton Business Corporation, which

administered a virtual currency exchange called BTC-e, and a \$12 million penalty against Alexander Vinnik, a Russian national who allegedly controlled, directed, and supervised BTC-e's operations, finances, and accounts. This is the first supervisory action against a foreign entity operating as an MSB in the US. FinCEN asserted jurisdiction on the grounds that BTC-e processed substantial transactions (totaling over \$296 million) involving US customers.

FinCEN found a variety of compliance breaches, including BTC-e's failure to:

- Register as an MSB.
- Maintain an effective AML program.
- File suspicious activity reports (SARs).
- Keep transaction records.

These failures resulted in BTC-e maintaining a customer base of criminals who concealed and laundered proceeds from crimes such as ransomware, identity theft, tax fraud, public corruption, and drug trafficking — none of which BTC-e reported to FinCEN or law enforcement. (FinCEN, FinCEN Fines BTC-e Virtual Currency Exchange \$110 Million for Facilitating Ransomware, Dark Net Drug Sales (July 27, 2017), available at [fincen.gov](#).)

The case demonstrates FinCEN's commitment to ensuring that any virtual currency exchange doing substantial business with US customers registers with FinCEN and complies with the BSA and, in particular, the AML regulations.

OFAC

OFAC enforces economic and trade sanctions principally through:

- Comprehensive embargoes against Cuba, Iran, North Korea, Syria, and the Crimea region of Ukraine, and their governments or instrumentalities.
- Its Specially Designated Nationals (SDNs) list, which identifies individuals and entities with whom US citizens and residents are prohibited from doing business.
- Its Sectoral Sanctions Identification (SSI) list, which restricts certain types of new debt and credit activities, principally with persons in Russia and Venezuela.

Although these lists are limited, they change regularly, creating some challenges for US organizations, and those doing business with US organizations, when trying to avoid prohibited activities.

OFAC does not require individuals or organizations to implement any specific compliance programs or conduct "denied party" screening, but its broad prohibition of transactions, when coupled with potentially large civil fines and criminal penalties for violations, makes it advisable for any organizations doing business involving blockchain or virtual currencies to take steps to avoid transactions with sanctioned countries, their governments, SDNs, and persons on the SSI list.

Although OFAC has not yet issued guidance or taken any public enforcement action specific to blockchain technology or virtual currency transactions, organizations and their counsel should proactively evaluate the risk that customers, counter-parties,

and business partners may be subject to economic sanctions. Particularly for organizations that conduct or facilitate transactions involving virtual currencies, it may be difficult to screen participants to determine whether they are located in sanctioned countries or identified on the current SDN and SSI lists, given that potentially anyone with internet access may be able to participate in a transaction.

To mitigate this risk, organizations should consider implementing a KYC program and screening software that can cross-reference transactions for compliance with US sanctions, including by evaluating the participants against the SDN and SSI lists.



Search [Anti-Money Laundering and OFAC Compliance for Financial Institutions: Presentation Materials](#) for a customizable PowerPoint presentation that counsel and their clients can use to educate directors, senior management, and other employees on the obligations and restrictions imposed by US AML laws and OFAC regulations, including more on the SDN list.

TAX TREATMENT OF VIRTUAL CURRENCIES

The IRS and state tax authorities are the primary agencies with jurisdiction over blockchain tax concerns, except where criminal conduct is suspected (see below *Criminal Implications*). While the IRS issued a notice several years ago indicating that it will treat virtual currency as property rather than currency for tax purposes, it has provided little additional guidance (see IRS Notice 2014-21, at A-7 (Apr. 14, 2014), available at [irs.gov](#)).

The IRS assumes that once virtual currency is characterized as property, normal tax consequences flow from that. Although this characterization answers many questions, numerous questions remain unaddressed. For example, the appropriate tax treatment of a token with equity-like or debt-like features, or a virtual currency that undergoes a fork (that is, when the blockchain splits into two branches), remains uncertain.

Instead of providing more guidance and educating taxpayers of their tax obligations relating to virtual currency, the IRS has pursued enforcement actions. Its first action was issuing a “John Doe summons” to the Coinbase virtual currency exchange. The Coinbase summons sought all customer records for a period from 2013 to 2015. This included all records of account activity, including transaction logs and other records. The summons also asked for any correspondence between Coinbase and its users.

After some pushback from Coinbase and its customers, the IRS narrowed the scope of the summons to cover only customers who engaged in transactions of \$20,000 or more. On November 28, 2017, a federal court further limited the information and ordered Coinbase to produce information regarding approximately 14,355 account holders (see *United States v. Coinbase, Inc.*, 2017 WL 5890052, at *6-7 (N.D. Cal. Nov. 28, 2017)).

The Coinbase summons may offer a preview of future enforcement actions, such as the issuance of additional summonses to other virtual currency exchanges and wallets, possibly extending investigations into other virtual currencies. However, it is also possible that the IRS will issue guidance to help taxpayers instead of pursuing an enforcement route.

For now, in the absence of more detailed guidance from the IRS, organizations subject to US tax laws face many unknowns. However, organizations holding virtual currencies or conducting transactions in virtual currencies should, at a minimum:

- Track and report gains and losses to the IRS and any relevant state tax authorities.
- Maintain records adequate to support any reported gains or losses.

Accordingly, organizations that transact business in virtual currencies (including by issuing ICOs or having other involvement in virtual currency investments) should consult with tax counsel to determine whether they should keep records of virtual currency transactions and whether those transactions should be reported to relevant tax authorities.

CRIMINAL IMPLICATIONS

While blockchain activities are not inherently (or even typically) criminal under US law, some law enforcement investigations may target traditional criminal conduct that is facilitated by the use of virtual currencies and blockchain technology.

Perhaps the most infamous case involves the dark web’s Silk Road site, which was the world’s largest platform for the sale of drugs and other illicit goods. Silk Road was primarily enabled by the anonymity of the dark web and the ability of bitcoin to permit trustless transactions between criminals. After an investigation led by the Federal Bureau of Investigation (FBI) and the Drug Enforcement Agency, law enforcement agents shut down the Silk Road site in October 2013 and seized all of its bitcoin assets (then valued at over \$33 million). The creator of Silk Road, as well as several vendors on the site, also faced various criminal charges.

As in the Silk Road case and depending on the conduct at issue, several different agencies, including the DOJ, the FBI, the US Department of Homeland Security (DHS), the Criminal Investigation Division of the IRS, and state law enforcement authorities, may investigate any blockchain activity suspected of violating criminal law. Indeed, last year, the DOJ, FBI, and DHS announced additional steps to combat cyber threats, including the use of blockchain technology to enable anonymity among criminal enterprises (see, for example, DOJ, Colorado U.S. Attorney Creates New Cybercrime and National Security Unit (Feb. 2, 2017), available at [justice.gov](#); DHS, Snapshot: Blockchain Technology Explored for Homeland Security (Jan. 10, 2017), available at [dhs.gov](#); see also *Cryptocurrencies Offer Great Hope, But Present Risks, Says White House*, Financial Express, Dec. 20, 2017, available at [financialexpress.com](#); Wolfie Zhao, *Illicit Cryptocurrency Use Targeted in Proposed 2018 FBI Budget*, Coindesk, June 22, 2017, available at [coindesk.com](#)).

To avoid entanglement with a criminal investigation, counsel should take steps to ensure their clients know the other parties involved in their blockchain activities. This will be easier in some industries than others. For example, a healthcare provider offering a blockchain-based patient monitoring system will likely already know the doctors and patients who participate in that network. This transparency makes it easier for clients to avoid allegations of healthcare fraud.

By contrast, financial institutions may find that blockchain-based transactions make it more difficult to comply with AML and KYC regulations because of the heightened potential for anonymity and the lack of a central authority to monitor transactions. In all cases, clients should be proactive in anticipating and taking steps to prevent criminal activities on their blockchain networks.

COUNSELING CLIENTS ON BLOCKCHAIN INVESTIGATIONS

The procedural steps of a blockchain investigation are likely to be similar to other federal and state enforcement investigations.

As a threshold matter, counsel must learn whether their client has spoken to a regulator about the investigation and, if so, what was discussed. As soon as an investigation begins, counsel should:

- Suspend document destruction procedures for potentially relevant custodians and issue a litigation hold notice that:
 - covers the relevant time period and custodians;
 - is circulated to the appropriate audience;
 - instructs the recipients to keep the matter confidential; and
 - warns that destruction or alteration of documents can carry harsh consequences.

(For more information, search [Litigation Hold Toolkit](#) on Practical Law.)

- attempt to learn as much as possible from the regulator about the investigation; and
- try to narrow the scope of the regulator's document requests.

(For more information, search [Securities Enforcement: Responding to a Regulator's Request for Information and Documents](#) and [Securities Enforcement: A Roadmap of SEC's Investigation and Enforcement Process](#) on Practical Law.)

Investigations into blockchain activities will likely raise unique considerations, requiring counsel to develop strategies that account for:

- **Unsettled laws.** The legal framework governing a client's business may not provide comprehensive guidance specific to blockchain technology. Where there is limited or no relevant guidance, counsel should:
 - consult industry authorities or other persuasive sources that address blockchain issues; and
 - consider all potential legal outcomes given the novelty of the issues raised.
- **Novel technology.** Counsel should assess whether the investigating agency has familiarity with the blockchain technology at issue. If counsel believes that the agency is not sufficiently versed in the applicable technology, counsel





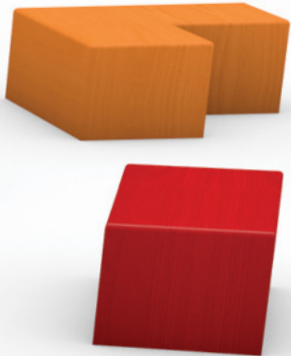
Particularly for organizations that conduct or facilitate transactions involving virtual currencies, it may be difficult to screen participants. To mitigate this risk, organizations should consider implementing a KYC program and screening software that can cross-reference transactions for compliance with US sanctions.



- Conduct an initial factual inquiry, including collecting critical documents and identifying key individuals to interview (for more information, search [Case Assessment and Evaluation](#) and [The Advantages of Early Data Assessment](#) on Practical Law). This may require counsel to learn the transactional history that is relevant to the investigation, which could require technical expertise.
- Determine how to respond to regulators. If a decision is made to cooperate with regulators, counsel should:
 - ensure that the decision is communicated to the regulator promptly;
 - speak with the regulator by telephone;
 - reassure the regulator that the client intends to cooperate;

should discuss with the client whether to educate the agency on the technology. Efforts to educate the agency can be time-consuming and distracting, but can:

- build goodwill with the investigating agency;
 - put the conduct at issue into the proper context; and
 - avoid the appearance that the client has something to hide.
- **Data privacy.** Counsel should consider whether the investigation involves personally identifiable information, trade secrets, or other data that is subject to privacy and confidentiality restrictions. If so, the regulators may focus the investigation on data privacy issues and counsel should make every effort to understand those issues and proactively address any concerns. (For more information, search [Privacy and Data Security Toolkit](#) and [Data Breach Toolkit](#) on Practical Law.)
- 
- 



Counsel should assess whether the investigating agency has familiarity with the blockchain technology at issue. If counsel believes that the agency is not sufficiently versed in the applicable technology, counsel should discuss with the client whether to educate the agency on the technology.

- **Cybersecurity.** If an investigation relates to a threatened or actual security breach, counsel should discuss with the client whether it should implement measures to mitigate the consequences of the breach and enhance security going forward. This type of proactive approach can help avoid unnecessary scrutiny from regulators as well as public relations issues. Additionally, counsel should consider whether the client may be considered the victim of a cyber attack or other cyber crime and, if so, whether the investigating agency is the proper agency to assist the client or whether counsel should notify another agency. (For more information, search [Cyber Attacks: Prevention and Proactive Responses](#) on Practical Law.)
- **Information technology (IT).** A blockchain network presents unique and complex technical issues that may require counsel to collaborate with the client's IT personnel to better understand and explain the blockchain features to regulators. If necessary, counsel may need to advise the client to temporarily halt the practices at issue. Additionally, blockchain users must determine whether their network modifies either the type of data collected or the manner in which the data is used or stored. If so, then further thought may need to be given to compliance with applicable regulations. Counsel should also:
 - consider whether the client should hire an outside consultant to conduct a compliance audit and vulnerabilities testing for its blockchain network;
 - seek assistance from, or pursue a claim against, the third-party technology vendor that developed the client's blockchain network (if applicable); and
 - review with IT personnel (or the technology vendor) any proposed changes to the blockchain network contemplated by a regulatory settlement to ensure the changes are appropriate and effective before finalizing the settlement.

Counsel can work with clients to minimize the likelihood of future blockchain-related investigations by:

- Reviewing and updating compliance policies to address blockchain issues, calling particular attention to unique issues that arise as a result of using a blockchain network.
- Ensuring that employees interacting with a blockchain network receive adequate guidance, including training on:
 - identifying and reporting suspicious activities; and
 - network features and functionalities.
- Monitoring the rapidly evolving regulatory and investigative activities related to blockchain issues, particularly in regulated industries such as finance and healthcare.
- Implementing technical upgrades to enhance the security of blockchain networks.
- Proactively engaging with regulators through industry associations or similar advocacy groups focused on blockchain activities. This type of collaboration with regulators can help clients develop positive solutions designed to limit regulatory infractions.

The authors would like to thank their Steptoe colleagues Jason Weinstein, Lisa Zarlenga, and Jack Hayes for their advice and assistance with this article.



©iStockphoto.com/lucadp