MERKLE SCIENCE

A Guide to U.S. Cryptocurrency Regulations

Part I: Federal Regulators & Corresponding Regulations

Table of Contents

Overview

During the Initial Coin Offering (ICO) boom of 2017-18, the global blockchain-cryptocurrency sector was thought to be largely unregulated. Consequently, the industry was plagued with hackers, frauds and pump-and-dump schemes. According to a study by Statis Group, nearly 80% of the ICOs conducted in 2017 were scams, causing investors to lose over $1.4 billion. While FinCEN and the IRS previously issued guidance on digital assets, the U.S. Securities and Exchange Commission (SEC) did not issue its first guidance on crypto assets until July 2017, with the release of its DAO Report. The SEC also clarified that cryptocurrencies meeting the definition of "security tokens" would fall under the SEC's regulatory purview. Though the overall framework covers both Federal and State laws, this report will focus only on the former.

The U.S. has one of the most complex regulatory frameworks in the world, particularly concerning digital assets. The infrastructure comprises multiple tiers of regulatory bodies that govern specific aspects of crypto-based market interactions. On the Federal level, the SEC, the Commodity Futures Trading Commission (CFTC), Financial Crimes Enforcement Network (FinCEN), the Internal Revenue Service (IRS), and the Office of the Comptroller of the Currency (OCC) work together to formulate and enforce cryptocurrency regulations.

Per the tenets of the Securities Act of 1933, the SEC is one of the primary regulatory bodies governing cryptocurrencies. The Framework for Digital Assets (henceforth, the 'Framework') deems certain digital assets that have the requisite features of "investment contracts" as securities, placing them under the SEC's purview.

Digital assets that do not fall under the categorization of securities fall under the purview of the CFTC. The CFTC regulates the overall commodity derivatives market in the U.S., under the Commodity Exchange Act (CEA) of 1936. Following the incorporation of the Dodd-Frank Wall Street Reform and Consumer Protection Act in 2010, the CFTC's domain was expanded to cover the Swaps market. The CEA defines 'commodity' to include currencies, interest rates, or any contract that stipulates future delivery, thus bringing digital assets under its purview. FinCEN is a subsidiary of the U.S. Treasury Department, whose primary function is to regulate and restrict the use of cryptocurrencies for financial crimes. According to its guidelines, services transmitting 'other value that substitutes for currency' are also considered "money service businesses" and must be registered with FinCEN.

The IRS, for its part, strives to curtail tax evasion through the use and sale of cryptocurrencies. Despite having issued multiple iterations of its 2014 guidelines, the IRS has persistently defined virtual assets as property, therefore subject to federal tax laws. Although crypto-based payments and purchases have implications for taxation according to the IRS, they aren't treated as foreign currencies, unless issued officially by a sovereign nation.

Finally, the OCC also explores questions relating to cryptocurrencies vis-a-vis the banking sector, and thereby formulates regulatory guidelines. In a major development of recent times, the OCC has allowed its federal chartered banks to offer custodial services for crypto-assets, subject to nuanced safeguards.

The U.S. Treasury Department is set to release a report on stablecoins in late October 2021. On December 23, 2020, the U.S. President's Working Group on Financial Markets released an initial assessment on certain key regulatory and supervisory considerations surrounding stablecoins. According to the statement released by the Treasury Department, U.S. authorities will assess the technological and market landscape as well as the regulatory framework for oversight of stablecoin arrangements to ensure responsible innovation while addressing risks to the financial system. Further, the Treasury Department also stated that — depending on the stablecoin's design

and other factors such as functions, activities, and risks attached — a stablecoin can be security, commodity, or derivative. In this case stablecoins themselves, transactions related to stablecoins, and participants involved in the stablecoin arrangement will fall under the ambit of the U.S. securities law and/or the Commodity Exchange Act.

In addition, stablecoin participants have to meet all the applicable anti-money laundering and sanctions legislation obligations such as registration requirements, recordkeeping reporting requirements, and implementing risk-based compliance programs before bringing their products to the market. Stablecoin participants will have to put additional safeguards in situations where stablecoins are adopted at a large scale and are primarily being used for retail payments. The Treasury encouraged participants who are engaged in the design of stablecoins and their function operations, risk management, and transactions to align with seven key principles:

- ***Facilitating Financial Stability:*** Stablecoins should be designed to address potential financial stability risks such as large scale potentially disorderly redemptions and general business losses. Stablecoin participants are required to integrate appropriate systems, controls and practices to manage the risks surrounding stablecoins.
- ***Facilitating End User Protection:*** Stablecoin arrangements should provide enforceable direct claims by holders against the issuer or the reserve assets to exchange their stablecoins for the underlying fiat currency. These rights should be disclosed to the stablecoin holders, establishing claims procedure to minimize counterparty risks to the stablecoin holder.
- ***Ensuring Market Integrity:*** Stablecoin arrangements must meet all the applicable AML/CFT and sanctions obligations.
- ***Facilitating Operational Resilience:*** Stablecoin arrangements are required to put a robust risk management framework in place. The aim is to ensure a high degree of security and operational reliability including cybersecurity and business continuity management.
- ***Facilitating Well Functioning Payments and Trading Markets:*** Stablecoin arrangements should put data management systems in place to record and safeguard data and information collected and produced in their operations.
- ***Facilitating Macroeconomic and International Monetary Stability:*** This includes not undermining the domestic fiat currency and imposing additional limitations on certain stablecoins.
- ***Facilitating Comprehensive Cross-border Supervision:*** In situations where the stablecoin arrangements operate in multiple different jurisdictions, they are required to provide necessary information to all relevant national authorities.

Securities Laws (SEC)

In a public statement on November 16, 2018, the SEC emphasized the need for "market participants" to comply with the "well-established and well-functioning federal securities law framework" even while dealing with "securities" that leverage innovations in blockchain technology. Setting the tone for cryptocurrency regulations in the U.S., the statement anticipated the Framework for "Investment Contract" Analysis of Digital Assets, published by the SEC on April 3, 2019.

The Framework arrived in the aftermath of the 2017-18 ICO boom, whereby numerous scams and hacks caused massive losses for investors. Insofar as it governs the identification of digital "securities" for the enforcement of federal securities laws, the Framework is pivotal to the U.S. regulatory landscape. And in fulfilling this purpose, the SEC refers to the Securities Act of 1933.

Definition of digital asset securities under the SEC
Under the definition of the SEC, not all digital assets are considered securities. The "Howey Test" is the standard used to ascertain which digital assets are securities. Under that definition, almost all ICOs are considered securities. BTC, however, is not considered to be an "investment of money in a common enterprise with a reasonable expectation of profits to be derived from the efforts of others". But while BTC is not a security, Bitcoin exchange-traded funds (ETFs) are considered securities. The SEC has the power to approve or reject new digital asset products. On October 15, 2021, the SEC approved the first Bitcoin futures ETF, opening up crypto to a wider audience.

Market participants under the SEC
Market participants that fall under the purview of the SEC include trading platforms and exchanges that trade registered securities, as well as qualified custodians. Specifically when it comes to digital asset exchanges, many of them are offering digital asset trading and refer to themselves as "exchanges." However, platforms that offer to trade in digital asset securities and operate as "exchanges" (as defined by federal securities laws) must register with the SEC as a national securities exchange or obtain an exemption.

Should such platforms not offer to trade in digital assets that are considered securities — per the definition above — they will likely be registered as money transmission services (MTSs) instead. MTSs are money transfer or payment operations that are primarily subject to state rather than federal regulations. These platforms will also have to register with FinCEN and are subject to certain reporting requirements.

2.1 SEC's Enforcement Authority & Actions

One of the primary functions of the SEC is to enforce statutes like the Securities Exchange Act of 1934 (commonly known as the Exchange Act), the Securities Act of 1933, the Trust Indenture Act of 1939, the Investment Company Act of 1940, and the Investment Advisers Act of 1940, among others. These statutes, particularly that of the securities laws, covers both criminal and civil violations. However, in and of itself, the SEC is "responsible only for civil enforcement and administrative actions," according to an official report published in 2005.

Functioning within this scope, the Division of Enforcement serves as an investigative and enforcement wing, commonly known as the SEC Enforcement. It can initiate civil action in any U.S. District Court or facilitate administrative hearings under any independent Administrative Law Judge (ALJ). In the aftermath of the global financial crisis of 2007-2008, there has been a significant uptick in the budget and workforce allocated to the enforcement division, and even more so since the emergence of digital currencies.

Notable Enforcement Actions

In 2013, the SEC undertook its first crypto-related enforcement action, according to a comprehensive report by Cornerstone Research, titled *SEC Cryptocurrency*

Enforcement: Q3 2013—Q4 2020. In this case, the defendants—Trendon T. Shavers and his company, Bitcoin Savings & Trust—were accused of running a Ponzi scheme to defraud investors. The SEC's enforcement drive peaked amidst the ICO bubble of mid-2017, and during the period analyzed in the above report, the SEC has initiated 75 enforcement actions. Forty-three of these were litigated in district courts, and the majority of these litigations involved unregistered securities offering and fraud. Against this backdrop, the following are some of SEC's most notable enforcement actions vis-a-vis cryptocurrencies:

- On June 3, 2014, the SEC charged Erik T. Voorhees, the co-owner of SatoshiDICE and FeedZeBirds, for selling shares and soliciting investors online without due registration with the SEC. Voorhees paid over $50,000 in fines to settle the SEC's charges.
- On July 11, 2016, SecondMarket and Bitcoin Investment Trust (BIT) agreed to settle charges laid against them by the SEC, following a three-year-long administrative proceeding. According to the SEC, the entities failed to comply with Rules 101 and 102 of Regulation M, under the Exchange Act. Regulation M prohibits certain types of trading activities that can potentially raise the price of a security offering or create a false appearance of active trading in the market by investors. Rule 101 in particular, prohibits any "distribution participant" and any of its affiliates from directly/indirectly bidding or inducing (or attempting to induce) any person to bid/purchase security during the distribution period. In March 2014, BIT announced a redemption scheme for shares purchased within a year. Subsequently, through its affiliate SecondMarkets, BIT began accepting orders to redeem shares from BIT shareholders, Between April 2 and September 14 BIT's active participant (as defined in section 2.3.3) purchased 85,621 BIT shares from the shareholders and earned redemption fees, thereby violating Rule 101.
- On July 25, 2017, the SEC published its Report of Investigation on The DAO's initial coin offering and eventual hack. In addition to being one of the most infamous cryptocurrency hacks, this case became a milestone in SEC's regulation and enforcement concerning digital assets. In the report, the co-directors of SEC's Enforcement Division at the time, Stephanie Avakian, stressed the point that innovativeness "does not exempt securities offerings and trading platforms" from the obligations of the existing regulatory framework.
- On November 29, 2018, the SEC settled charges against celebrities Floyd Mayweather Jr. and DJ Khaled when they failed to disclose earnings for promoting the ICO by Centra Tech Inc.
- On October 11, 2019, the SEC initiated emergency enforcement actions against Telegram Group Inc. and its subsidiary TON Issuer Inc. to prevent them from "flooding the U.S. markets" with unregistered and unlawful digital tokens.
- On May 28, 2020, the SEC charged BitClave PTE Ltd. for offering unregistered securities. Later that year, computer programmer John McAfee was also charged with similar allegations, and so was Ripple Labs Inc., among several others. Notably, 2020 was the year of skyrocketing interest in novel crypto-assets like NFTs.
- On September 1, 2021, BitConnect, along with its founder Satish Kumbhani and U.S. associates, was charged for its unregistered coin offering. According to the SEC, the accused had defrauded retailers for over $2 billion. The SEC charged Defendants with lying about BitConnects's ability to make a profit, violating the anti-fraud and registration laws put in place to protect retail investors. This court action joined another parallel case filed by the SEC in May 2021 against five other promoters that are tied to BitConnect. According to the SEC, the five promoters, known as Arcaro Promoters, falsely advertised the merits of investing in BitConnect's lending program to prospective retail investors without being registered as broker-dealers.
- On August 6, 2021, the SEC sued Blockchain Credit Partners and two of its executives for illicitly offering securities through its DeFi money market platform from February 2020 to February 2021.

Security Token Offerings (STOs): Emergence & Regulation

In a statement published in 2018, the SEC recognized the significant advancement of technologies like blockchain and their impact on securities markets. However, the regulator also highlighted the challenges posed by the emergence of blockchain-based assets and financial products. Particularly in light of enforcement actions undertaken during 2017-2018, the perils of unregulated markets became apparent on both sides of the table. Consequently, industry practitioners adopted a revised understanding of Initial Coin Offerings, replacing them increasingly with Security Token Offerings (STOs).

Among other outcomes, the shift underlines the broad acceptance of the fact that several, if not all, digital currencies are securities of some form or another. Furthermore, it represents a mature stance towards legitimate regulatory compliance within the U.S. Federal laws. In other words, businesses conducting STOs realize the need to register with the SEC for conducting public sales or duly apply for exemptions in the case of private offerings. For public offerings or IPOs, the entity must provide complete financial and non-financial disclosures, besides meeting the requirements for electronic filing. Similarly, exchange platforms must also register with the SEC as national securities exchanges, unless they are eligible for exemptions under the ATS framework (discussed later).

STOs may be of several kinds depending on initiating company and its asset type, but in general, they are of three kinds:

- Public Offering or IPO
- Private Offering
- Regulation Crowdfunding

Issuing No-Action Letters

The SEC is stringent, both in terms of investigations and enforcement. However, there is substantial scope for relief and exemption for eligible blockchain-cryptocurrency businesses, which is necessary for supporting innovations. On this note, businesses may request the SEC to issue Staff No-Action letters, given that the former meets certain conditions.

In 2019, for example, TurnKey Jet Inc. received such a letter, the first of its kind blockchain-based markets. Besides not using sales proceeds for platform upgrades, the letter required TurnKey to make tokens immediately usable after sale. Recently, the IMVU also received a no-action letter for its VCOIN offering, subject to similar conditions as TurnKey. However, unlike TurnKey's tokens, VCOIN could be transacted on and off IMVU's platform.

In 2020, the SEC issued a no-action (explanatory) letter to FINRA, marking a significant milestone in the U.S. regulatory landscape. Responding to FINRA's query about the Joint Staff Statement from 2019, the SEC highlighted the four-step Alternative Trading Systems (ATS) framework in this letter, besides providing other clarifications. Eventually, in 2021, the ATS framework and other definitions provided in the letter served as the foundation for SEC's Safe Harbor discussed in a later section.

Notably, the issuance of no-action letters to blockchain-cryptocurrency firms resonates with the positive but cautious stance of the current SEC Chairman, Gary Gensler. Though Chairman Gensler called for cracking down on the 'wild west' of cryptocurrencies, he regards crypto as a 'catalyst for change' in need of better regulatory oversight. According to him, *"We just don't have enough investor protection in crypto finance, issuance, trading, or lending...This asset class is rife with fraud, scams, and abuse in certain applications. The crypto area is trying to stay outside of investor protection...We can do better."*

Chairman Gensler also recognizes the need for greater clarity in terms of how the federal regulatory framework responds as a whole to cryptocurrencies. The ATS framework facilitates this purpose to a great extent. Nevertheless, despite conflicts with the radicals of the crypto-industry, Gensler is reportedly against banning cryptocurrencies in the U.S.

2.2. Securities Act of 1933

The Securities Act, often known as the "Truth in Securities" law, originally governed traditional stocks, bonds, equities, and other financial instruments that are considered securities. Safeguarding the interests of investors is the primary motive behind this Act, achieved through the fulfillment of two fundamental objectives:

- In any public securities sale, investors must receive complete and verifiable information, financial or otherwise, to enable informed decision-making and investments.

- Through transparent information sharing, the Act intends to restrict misunderstandings and to prohibit frauds, scams, and similar acts of deception.

To sell securities legally under this Act, entities must disclose necessary and relevant information by registering with the SEC. In this regard, the following are some of the broad categories of information sought from the registering company:

- Details of business holdings and properties;
- Details of the security being sold;

- Details of the company's management;
- Financial audit reports from independent agencies.

Besides access to the above information, investors are entitled to various redressals in the event of loss due to inadequate or misleading disclosures. For U.S.-based companies, the said information is available on EDGAR. However, the Act exempts private or limited-size sales, intra-state offerings, and government-issued securities. Fostering financial inclusion is among the primary motives of this exemption.

2.3. The Framework & "Howey" Test

Bringing crypto-assets under the purview of the Securities Act was the point of departure for the SEC regulations. Consequently, stipulating the parameters for proper identification of "securities" was the primary rationale behind the Framework. And to achieve this purpose, the SEC implements the Howey test.

In a 1946 ruling, the U.S. Supreme Court defined the parameters to determine which financial exchanges qualify as investments. According to the ruling, an "investment contract" entails: **(a) the investment of money, (b) in a common enterprise, (c) with a reasonable expectation of profits to be derived from the efforts of others**. These parameters represent the three 'prongs' of the Howey test, based on which the Framework defines certain securities as investment contracts.

The SEC's Report of Investigation, published on July 25, 2017, was the first significant instance of implementing the Howey test for cryptocurrencies. The publication investigated the infamous DAO Attack where investors lost 3.6 million ETH, equivalent to nearly $70 million at the time. According to this report, the SEC found the DAO (Stork.it) in violation of the U.S. federal securities law, though it refrained from pursuing enforcement action.

In the detailed explanation of the Framework published two years after the investigation, the SEC clarified its approach further. As noted in this publication, *"The focus of the Howey analysis is not only on the form and terms of the instrument itself (in this case, the digital asset) but also on the circumstances surrounding the digital asset and the manner in which it is offered, sold, or resold (which includes secondary market sales)."*

Furthermore, according to the SEC, *"[Issuers] and other persons and entities engaged in the marketing, offer, sale, resale, or distribution of any digital asset will need to analyze the relevant transactions to determine if the federal securities laws apply."* In other words, the Framework requires businesses to share the responsibility of identifying whether its offering counts as securities under federal law. On this note, we may elaborate the four prongs of the Howey test, thus highlighting their implications.

2.3.1 Investment of Money

"Investment of money" is the first prong of the Howey test and is "typically satisfied in an offer or sale of a digital asset" as it necessarily involves an exchange of value, in one form or another — it does not literally require money.

Because of its broad interpretation, the clause applies to purchases or investments using crypto-assets like bitcoin and isn't limited to conventional currencies. Furthermore, offerings like bounty programs and airdrops also become subject to the Howey test.

2.3.2 Common Enterprise

The Framework doesn't elaborate the second prong of the Howey test, though it provides some insight into the matter through end-text notes. In this section, the SEC stipulates one of two requirements (or both) — "horizontal commonality" and "vertical commonality" — to satisfy this aspect of the test.

- **Horizontal Commonality:** Entails the fact that each investor's fortune is horizontally tied to the fortunes of other participating investors, due to the pooling of assets and pro-rata profit distribution.
- **Vertical Commonality:** Focuses on vertical promoter-investor relationship, wherein the fortune of the investor is related to the efforts and success of the promoter. In this scenario, the inter-investor relationship is mostly irrelevant.

The platform or network on which the sale and purchase of digital assets occur may, in light of the above insights, represent the common enterprise. Moreover, the proceedings of the SEC vs Int'l Loan Network, Inc. case visibly exemplified the existence of either of the two forms of commonality in any digital asset investment.

2.3.3 Reasonable Expectation of Profits, Derived from the Efforts of Others

According to the Framework, "Usually, the main issue in analyzing a digital asset under the Howey test is whether a purchaser has a reasonable expectation of profits (or other financial returns) derived from the efforts of others." Because of its broad scope and ambiguity, the third prong is more complicated than the other two. Consequently, the SEC describes this at length, highlighting several conditions for determining each of its aspects: (a) a reasonable expectation of profit and (b) derived from the efforts of others.

In this context, the Framework defines an 'Active Participant' (AP) as 'a promoter, sponsor, or other third parties (or affiliated group of third parties)' which 'provides essential managerial efforts' (as opposed to simply ministerial ones) to ensure the enterprise's success. The 'economic reality of associated transactions and the commercial 'character of the instrument' are essential factors for consideration in this regard. Furthermore, it's necessary to objectively analyze the offering, in terms of its nature and approach.

2.3.3.1 Reasonable expectation of profit

Purchasers may reasonably expect 'capital appreciation on their initial investment, either through 'participation in earnings' or the development of the business enterprise. However, purely market-driven price appreciation is not 'profit' in the context of the test. Among the several satisfying conditions outlined in the Framework, the following are some of the most significant:

- The digital asset represents a stake (ownership) in the enterprise, thus promising a share in revenue and profit.
- The offered asset is tradable on secondary markets, either at the time of sale or in the future.
- The digital asset is distributed through public sales, and not simply to potential users as a means to access utilities on the network.
- The offering price and the market price of the network's utilities are uncorrelated.
- The trading volume of the digital asset and the quantity of the underlying goods or services are uncorrelated.

In addition to the above points, the AP's role is of paramount importance for determining reasonable expectations of profit. The primary considerations here are whether the AP has raised funds in excess of what is required for establishing the network and whether it continues to expend funds from proceeds or operations to meet this purpose. Furthermore, the expectation is reasonable if the enterprise's marketing efforts promoted the 'expertise' of the AP and/or indicated the asset's investment proposition.

2.3.3.2 Derived from the efforts of others

Besides being reasonable in the above terms, the expectation of profit must be objectively derived from the efforts of the AP(s). The efforts must be essentially managerial, insofar as they determine the enterprise's success in the long run. In other words, the success or failure of the enterprise depends on the efforts of the AP, either fully or partially.

Purchasers may rightfully expect the AP to perform tasks essential for the enterprise to achieve its intended purpose, particularly if the latter is "responsible for the development, improvement (or enhancement), operation, or promotion of the network." This consideration is of greater significance when the project is still in its developmental phase, awaiting completion at the time of the offering. However, the purchaser's expectation isn't valid if it relates to the efforts of the "decentralized" or dispersed user's community.

The AP's managerial efforts may also involve its role in creating and/or sustaining markets for the offered digital asset. According to the Framework, this applies to situations where the AP: (i) controls the asset's supply, through its creation and issuance, and (ii) can influence its market price by 'limiting supply or ensuring scarcity' through buybacks, 'burning', and/or other means.

2.3.3.3 Other considerations and the scope for reconsideration

In addition to the above aspects, the following are some additional considerations relating to the Howey analysis:

- The developmental and operational phase of the digital asset and its underlying distributed ledger network.
- The utilitarian nature of the offering vis-a-vis its speculative aspects.
- The sustainability and consistency of the value proposition.

- The ability to immediately make payments or redeem the underlying goods or services using the offered asset.

Having outlined the necessary and sufficient conditions in detail, the Framework also stipulates the grounds for reconsideration of an asset's status. In other words, the purchaser may, over the course of time, stop expecting profits from the efforts of others. For instance, the AP may have already fulfilled its promised role, thereby facilitating complete decentralization of the network and its assets. Furthermore, the manifestation of direct correlations between the asset's value and its market dynamics or the quantity of redeemable goods and/or services. Basically, the criteria for meeting the Howey test are dynamic, meaning that digital assets are subject to revaluation at any phase of their evolution.

2.4 SEC Safe Harbor

To foster innovations while upholding the Consumer Protection Rule (Rule 15c3-3), the SEC exempts certain "broker-dealers" from the regulatory obligation for registration. The said exemption, however, is not exclusive but rather contingent on the fulfillment of conditions stipulated in the commission's statement, as laid out in the SEC's safe harbor in December 2020 and published in April 2021.

The following are some of the parameters validating reliance upon the safe harbor provided by the SEC:

- The broker-dealer meets the fundamental obligation of securing excess margin digital asset securities and has access to this fund at all times.
- The broker-dealer's business deals exclusively in digital asset securities, and its traditional securities positions, if any, are purely for hedging or meeting minimum net capital requirements per Rule 15c3-1.
- The broker-dealer maintains written and auditable documentation to facilitate the Howey analysis of its digital asset offerings if and when required.
- The broker-dealer doesn't acquire custody of purchasers' funds despite the existence of known security or functionality loopholes in its system.
- The broker-dealer provides detailed documentation on how it plans to mitigate and resolve common attack vectors, such as 51% Attacks, for instance.
- The broker-dealer makes public disclosures of its digital asset securities holdings and informs potential users of all associated risks, financial or technical.
- The broker-dealer enters into separate written agreements with each individual customer.

The rule is currently valid for a 5-year period, effective from April 27, 2021. During this tenure, the SEC seeks comments from the industry's stakeholders, in an attempt to promote participation and diversity.

Commodity Exchange Act (CFTC)

Originally restricted to traditional markets alone, the CTFC currently regards digital assets as commodities within the meaning of the Commodity Exchange Act (CEA) of 1936. In its attempt to foster innovation and enhance regulatory experiences, the CFTC-subsidiary research wing, LabCFTC, published detailed primers on digital assets and smart contracts. The primary motive behind these primers was to educate common users about the crucial elements of the blockchain-cryptocurrency industry.

According to the CFTC, a digital asset is anything that can be stored and transmitted electronically and has associated ownership or use rights. Based on the design, function, and use, a digital asset may be characterized differently. Both virtual currencies and digital tokens fall within the definition of digital assets.

As per the CFTC, virtual currencies – sometimes called "coins," "native tokens," or "intrinsic tokens" — act as a medium of exchange and play an important part of the digital asset landscape, which includes markets overseen by the CFTC. Virtual currencies are native assets of specific blockchain protocols, such as ETH and BTC. Bitcoin and Ether are considered commodities under the CEA.

On the other hand, digital tokens are units of value that blockchain-based projects develop on top of an existing blockchain. While ETH is the virtual currency (as explained above), there are many other digital tokens builton the Ethereum blockchain such as DAI or COMP. DAI, for instance, is a stablecoin issued by MakerDAO, an Ethereum-based lending protocol. COMP is a governance token issued on Compound, an interest rate DeFi protocol built on top of Ethereum. Utility tokens would also fall under the digital token category, enabling token holders future access to products and services offered by an organization.

Other than its oversight on derivatives exchanges, the CFTC has two major priorities: anti-manipulation and anti-fraud. It is important to note that beyond instances of fraud or manipulation, the CFTC does not oversee "spot" or cash market exchanges. It also does not oversee virtual currency transactions that do not utilize margin, leverage, or financing. Accordingly, the institution stipulates the following guidance:

- Transparency, resilience, and safety are necessary for the desired functioning of digital asset markets.
- Ensuring market integrity should be a key governance motive for all digital asset platforms.
- The CTFC prohibits and engages with market manipulation and deceptive sales practices, as well as 'pump-and-dump' or other fraudulent schemes.

The CFTC Has Both Enforcement and Regulatory Authorities

Enforcement Authority — The CFTC can take robust enforcement action to prosecute fraud, abuse, manipulation, or false solicitation in markets for virtual currency derivatives and spot trading. Since 2018, with the formation of the Virtual Currency Task Force, enforcement actions by CFTC on crypto platforms have gone up significantly. The CFTC enforcement actions can be classified in the following manner:

- Fraudulent Schemes
- Price manipulations
- Failure to register
- Illegal off- exchange transactions
- AML/CFT violations

Notable Enforcement Actions Taken by the CFTC on the Crypto Industry

- On October 15, 2021, the CFTC issued an order fining Tether for making untrue and misleading statements about Tether's stablecoin. According to CFTC, from June 2016 to late February 2019, Tether made misleading or untrue statements about whether it held sufficient U.S. dollar reserves to fully back up its USD-tethered token. Tether has agreed to pay $41 million in fines.

- In a separate order, CFTC ordered Bitfinex to pay $1.5 million in civil monetary penalty. The Bitfinex order finds that from at least March 1, 2016 through at least December 31, 2018, Bitfinex offered, entered into, executed, and confirmed the execution of illegal, off-exchange financed retail commodity transactions with U.S. persons that were not eligible contract participants (ECPs) under the CEA. Further, Bitfinex illegally engaged in retail commodity transactions without registering as a futures commission merchant (FCM).
- On September 28, 2021, the CFTC issued an order, filing and settling charges against crypto exchange Kraken for offering margined retail commodity transactions in cryptocurrency including bitcoin between June 2020 and June 2021. Kraken did not register as an FCM or a Designated Contract Market (DC) before offering margined retail commodity transactions to U.S. customers. Kraken agreed to pay a $1.25 million civil fine.
- CFTC ordered crypto exchange Coinbase to pay a $6.5 million fine for making misleading claims about its trading volume. As per the order, between January 2015 and September 2018, Coinbase recklessly delivered false, misleading, or inaccurate reports concerning transactions in digital assets, including Bitcoin, on the GDAX electronic trading platform it operated.

Regulatory Authority — The CFTC's regulatory authority includes registration requirements, day-to-day oversight, and principle-based regulations. The CEA accords the CFTC powers to regulate all participants in the future/derivatives market such as crypto exchanges, intermediaries, as well as entities who fund or provide derivatives trading advice. While registration types under the CFTC continue to evolve as financial instruments change and develop, some common types of registrations seen in the crypto industry include:

- ***Designated contract markets license (DCM):*** A DCM is a trading platform that facilitates futures trading. DCMs are designated by the CFTC under the CEA and involve the use of contracts for the sale of a digital asset for future delivery. A DCM can allow both institutional and retail participants to participate on the platform. An example of this would be the Chicago Mercantile Exchange, which enables trading and clearing of Bitcoin futures.
- ***Futures commission merchants license (FCM):*** An FCM is an intermediary entity that solicits or accepts orders to buy or sell futures contracts, options on futures, etc. An FCM accepts money or other types of assets from customers in order to support such orders. Examples of FCMs are entities that provide derivatives trading advice, such as advisors and funds.
- ***Swap execution facility registration (SEF):*** An SEF is a platform that matches counterparties — buyers and sellers — in swap transactions, such as an OTC desk. As per the Dodd-Frank Act, an SEF provides multiple buyers and sellers the opportunity to directly execute or trade swaps (including options and forward on commodities such as Bitcoin) by accepting bids and offers. Platforms like LedgerX LLC were granted a SEF registration in 2017 by the CFTC.

CFTC Advisory on Designated Contract Markets, Swap Execution Facilities, and Derivative Clearing Organizations (DCOs):

In 2018, the CFTC released a staff advisory that set out guidance for CFTC-registered entities seeking to list or clear virtual currency derivatives products. According to the advisory, in order to list or clear virtual derivative products, trading platforms and clearing houses have to ensure the following:

- Partner with spot market platforms that follow KYC/AML rules;
- Have information-sharing agreements with spot market platforms;
- Monitor price settlement data from spot markets and identify/investigate anomalies and disproportionate moves;
- Set large trader reporting thresholds at five bitcoins or less;
- Regularly coordinate with CFTC surveillance staff and provide trade data; and
- Allow CFTC staff to review initial and maintenance margins for virtual currency futures.

CEA provides that designated contract markets (DCM) and swap execution facilities either have the option to (a) submit a certification to CFTC or (b) submit the contract for commission approval. DCMs/SEFs bring the vast majority of new products to market through the certification process. When a DCM/SEF certifies a new contract, it must determine that the offering complies with the CEA and Commission regulations, including that

the new contract is not readily susceptible to manipulation.

Virtual Currency Self-Certifications and "Heightened Review"

According to the provisions of the CEA, after submitting the certificate, which states that all the requirements laid down by CEA regarding future contracts have been duly met (self-certifying), a futures exchange can list a new product. For example, TeraExchange became the first exchange to self-certify and list Bitcoin non-deliverable forwards on September 12, 2014.

Additionally, depending on risk matrices, the CFTC may also institute the practice of "heightened review" wherein it may request voluntary compliance by applicants before self-certification, which includes several important criteria such as "substantially high" initial and maintenance margins, information sharing agreements, and coordinating product launches with the CFTC's market surveillance branch to enable the CFTC to monitor "minute by minute developments."

3.1 Prohibited Activities

The LabCTFC primer on Smart Contracts highlights certain examples of prohibited activities, particularly in relation to the use of derivatives contracts. The following are its main points:

- Contracts' execution must not enable fraud or manipulation;
- Contracts must not be executed or traded on unregistered or inappropriately registered platforms;
- Contracts must not violate existing CEA or CFTC regulations, such as disruptive trading practices, non-maintenance of proper compliance records, and inefficient network supervision;
- Contracts must not be in violation of the Bank Secrecy Act (BSA) or the U.S. PATRIOT Act. However, according to the joint Statement made by the CFTC, SEC, and FinCEN, entities registered with these institutions will be subject to specialized BSA norms, rather than the ones applying to MSBs in general.

3.2 The "Actual Delivery" of Digital Assets

The notion of "actual delivery" introduces ambiguities in relation to digital assets, and was therefore clarified by the CFTC in 2020. In this regard, two factors are the most worthy of consideration:

- The customer has, (a) possession of and complete control over the whole of the purchased commodity, and (b) can exhaustively use the commodity freely in commercial arrangements;
- The seller does not retain any legal right or ownership claim for the sold commodity, after a 28-day period from the transaction date.

In cases where the promoter or seller can restrict the user's access to the platform or digital assets, the latter doesn't exercise meaningful control in the CTFC's view. Moreover, though the CFTC regulation primarily involves "retail commodity transactions," its implication can be extended to other regulatory domains.

Bank Secrecy Act (FinCEN)

In 2013, the FinCEN published the first consolidated guideline for implementing the Bank Secrecy Act (BSA) in relation to cryptocurrencies. In doing so, FinCEN distinguishes between "real" currencies and "virtual" currencies. According to this classification:

- "Real" currencies are (a) issued by a sovereign nation, (b) functions as a legal tender, (c) circulating and customarily accepted as a medium of exchange within the issuer's jurisdiction.
- A "virtual" currency is similar to its "real" counterpart. It operates like a currency in some environmentsbut does not have all the attributes of real currency. In particular, virtual currency does not have legal tender status in any jurisdiction.
- A "convertible virtual currency" (CVC) is an unregulated digital currency that does not have the status of legal tender, but can nonetheless be used as a substitute for real and legally-recognized currency. Convertible digital currencies are easily exchanged for fiat currencies such as dollars via cryptocurrency exchanges. Examples of this include BTC, ETH, and XRP.

The first iteration of FinCEN's regulations applied to "administrators" and "exchangers" of virtual currencies, identified as "money transmitters" as a whole. According to FinCEN, *"An administrator is a person 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." On the other hand, "an exchanger is a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency."*

However, the regulation doesn't apply to individual users, as they do not qualify as Money Services Businesses (MSBs) per the FinCEN's view. In other words, the regulation applies only to the providers of "money transmission services" and not otherwise. On this note, services pertaining to e-currencies, e-metals, centralized virtual currencies, and decentralized virtual currencies fall under FinCEN's regulatory purview.

4.1. Revised FinCEN Guidelines

In May 2019, FinCEN issued a revised set of regulatory guidelines, which currently oversees the implementation of the BSA vis-a-vis virtual currencies. Though the guideline was meant to "consolidate" existing regulations rather than implementing a new framework, it expanded FinCEN's scope to cover emerging "business models" or "the subset of key facts and circumstances" that enable the regulator to determine whether the BSA applies to a particular entity. Besides identified MSBs, the regulation also applies to banks and credit unions dealing in virtual currencies.

According to the FinCEN guideline, any "person" — legal or natural, temporal or non-temporal, licensed or unlicensed — is a money transmitter insofar as they receive from one person (in any form) and transmit the same to another (in the same form or another). Therefore, almost every person facilitating financial transactions between counterparties is subject to BSA, as per FinCEN's approach. However, a person may be exempt from these regulations if the above definition doesn't apply to their "activity", irrespective of their status as a business.

Considering the broad definition of MSBs under FinCEN, the scope for exemption from the BSA is determined subjectively at times, based on the business model defined above. Notwithstanding, the following are certain "persons" to whom exemptions from BSA clearly apply:

- Banks, either national or foreign.
- Persons registered with and regulated by the SEC or CFTC.
- Foreign financial agencies participating in the U.S. markets, under the SEC or CFTC's jurisdiction.
- Natural persons offering MSB-like services on an irregular basis and not for profit or gain.

Furthermore, in the U.S., the FATF recommendations are implemented through BSA and FinCEN at the federal level.On May 9, 2019, FinCEN issued an advisory on illicit activity involving convertible virtual currency. FinCEN issued this advisory to assist FIs in identifying and reporting suspicious activities concerning how criminals and other bad actors exploit CVCs.

4.1.1 BSA Obligations for Money Service Businesses

The updated FinCEN guidelines imply the following obligations for MSBs and other entities subject to the BSA regulatory framework:

- Financial institutions are expected to promote a 'culture of compliance' and adapt the norms of behavior, transparency, and knowledge accordingly. Holding management and staff of the financial institutions accountable is the primary motive in this regard.
- MSBs must "develop, implement, and maintain an effective written anti-money laundering program" to prohibit money laundering and terrorism financing on their platforms.
- MSBs should adopt a risk-based approach towards structuring their programs, prioritizing the ease of compliance. A robust risk assessment mechanism is integral to this infrastructural requirement.
- Persons who are NOT exempt from the 'MSB Rule' must register with FinCEN within 180 days of their incorporation. Furthermore, they must *"comply with the recordkeeping, reporting, and transaction monitoring obligations set forth in Parts 1010 and 1022 of 31 CFR Chapter X."* Filing of Currency Transaction Reports and Suspicious Activity Reports are mandatory under this framework.
- The established "Funds Transfer Rule" and "Funds Travel Rule" also apply to MSBs.
- Irrespective of an MSB's structural and technological framework, it must submit the necessary regulatory information to FinCEN, prior to or at the time of beginning transmittal.

FinCEN Requirement for Certain Transactions Involving Convertible Virtual Currency or Digital Assets

On December 23, 2020, FinCEN published a notice of proposed rulemaking suggesting requirements for banks and money services businesses ("MSBs") related to certain transactions involving convertible virtual currency or digital assets with legal tender status (The Proposed Rule). On January 15, 2021, FinCEN re-opened the comment period for its recently proposed rulemaking for an additional 15 days.

FinCEN extended the comment period on the proposed reporting requirements regarding the information on CVC or LTDA transactions greater than $10,000 — or aggregating to greater than $10,000 — that involve unhosted wallets or wallets hosted in jurisdictions identified by FinCEN.

Additionally, FinCEN also provided an additional 45 days for comments on the proposed requirements that banks and MSBs report certain information regarding counterparties to transactions by their hosted wallet customers, and on the proposed recordkeeping requirements.

Reporting Requirement

FinCEN proposed a new rule seeking to bring CVC and LTDA within the existing anti-money laundering (AML) and "know your customer" (KYC) regulatory framework under the Bank Secrecy Act (BSA).

The proposed rule requires banks and MSBs to report transactions in CVC and LTDA exceeding $10,000 in a "one-day" period involving (a) unhosted wallet or (b) hosted walled within jurisdiction identified by FinCEN (Otherwise Covered Wallet).

The otherwise covered wallet is a wallet that is held at a financial institution that is not subject to the BSA and is located in a foreign jurisdiction identified by FinCEN on the "list of foreign jurisdictions", which FinCEN is proposing to establish. This list would initially comprise of jurisdictions designated by FinCEN as jurisdictions of primary money laundering concerns such as Myanmar, Iran, and North Korea.

Further, the rule defines "one day" as a 24-hour period. Under the rule, banks and MSBs are required to document the method used to identify the fair market exchange rate (Prevailing Exchange Rate) at the time of each transaction to determine whether the value of the CVC/LTDA meets the $10,000 threshold.

If the $10,000 threshold is met, banks and MSBs will need to file CVC/LTDA Transaction Reports. The proposed rule requires CVC/LTDA Transaction Reports to be filed

with FinCEN, unless otherwise specified, on a form prescribed by the Secretary of Treasury. The report must be filed within 15 days of the reportable transaction(s) using a Value Transaction Report Form.

For the purpose of the proposed rule, CVC and LTDA must be aggregated from all offices and records within the financial institution, but are not required to be aggregated with other currency transactions such as fiat currency.

If a counterparty's wallet is hosted by a BSA regulated MSB, the banks and MSBs will have to ensure that such other MSB is also registered with FinCEN. If the counterparty's wallet is with a foreign institution, then the Banks and MSBs to ensure that such institution is not located in a jurisdiction which is on the 'List of Foreign Jurisdictions'. Additionally, they will also have to ensure that the foreign institution is compliant with the applicable registration and other requirements by adopting a risk based approach.

The reporting requirement would apply regardless of whether the banks/MSBs customer acts as:

- The sender or recipient of the transaction
- The user of an unhosted wallet and otherwise covered wallet is the customer for whom the bank/MSB holds a hosted wallet.
- A participant of a transaction where even one participant holds an unhosted wallet or otherwise covered wallet

A value transaction report would require following information:

- The CVC or LTDA type used in the transaction
- The transaction amount
- The assessed transaction value (in USD)
- Date and time of transaction
- The transaction hash
- CVC or LTDA addresses involved in transaction, and if they are hosted or unhosted
- The name and physical address of each counterparty to the transaction

Exception: The proposed rule exempts reporting of transactions with wallets hosted by a BSA regulated institution or financial institution located in a jurisdiction that is not in the list of foreign jurisdictions. Additionally, banks and MSBs would be required to have a reasonable basis to apply such exceptions.

CVC/LTDA Record-Keeping Rule

Under the proposed rule, Banks and MSBs are also required to keep records of transactions, including the identity of the customer and any other parties to the transaction if parties involved use an unhosted or otherwise covered wallet for transactions of $3000 or more.

Banks and MSBs are required to collect both the name and physical address for the counterparties to the transaction(s), as well as any additional information the Secretary of the Treasury may prescribe for CVC/LTDA Transaction Reports.

In order to calculate the $3,000 value, banks and MSBs are required to use the Prevailing Exchange Rate at the time of the transaction, consistent with the CVC/LTDA Transaction Reporting requirement.

If enacted, the proposed Rule would mandate that CVC/LTDA transaction records be maintained electronically and retrievable by customer name, customer account number, or counterparty name. The proposed rule also requires banks and MSBs to keep similar information for transactions greater than or equal to $3000 between their customer and a counterparty using an unhosted or otherwise covered wallet.

Under the proposed rule, banks and MSBs are required to collect the name and address of each counterparty to the transaction as well as other counterparty information prescribed by FinCEN. Banks and MSBs have to also put risk based procedures in place in order to determine whether to collect additional information about their customers' counterparties or take steps to confirm the accuracy of counterparty information.

Exception: Like reporting requirements, the proposed rule similarly exempts transactions involving wallets hosted by BSA-regulated institutions or foreign financial institutions located in a jurisdiction that is not on the List of Foreign Jurisdictions. However, the bank or MSB applying for this exception should have a reasonable basis for doing so.

FinCEN's National Priority List

The United States Financial Crime Enforcement Network (FinCEN) issued its first government-wide list of priorities for Anti Money Laundering and Countering the Financing of Terrorism National Priorities (Priority List) on June 30,

2021. The Priority List, coupled with the Department of the Treasury's Illicit Finance Strategy 2020 and National Risk Assessment Priority List 2018, aims to help the covered institutions assess their risks, tailor their AML programs, and prioritize their resources in line with the key AML/CFT threats identified by FinCEN. As per FinCEN, covered institutions are those financial institutions that are required by the Bank Secrecy Act to maintain an AML Program. Covered Institutions include both banking institutions and non-financial banking institutions such as mutual funds, banks without a Federal functional regulator, and money service businesses (MSBs) amongst others.

As per the FinCEN official press release, the Priority List identifies and describes the most significant AML/CFT threats currently faced by the United States, which include: corruption, cybercrime, domestic and international terrorist financing, fraud, transnational criminal organizations, drug trafficking organizations, human trafficking, and human smuggling, and proliferation financing. FinCEN also announced that it will issue additional regulations later this year as required by the Anti Money Laundering Act 2020. These regulations will provide more specific guidance to covered institutions so that they can "review and incorporate, as appropriate, each Priority based on the institution's broader risk-based program."

Within the section 'Cybercrime, including relevant Cybersecurity and Virtual Currency Considerations', FinCEN notes that the Department of Treasury is particularly concerned about "cyber-enabled financial crime, ransomware attacks, and the misuse of virtual assets that exploits and undermines their innovative potential, including through laundering of illicit proceeds." Further, FinCEN also pointed out that CVC have become "currency of preference in a wide variety of online illicit activities." This was, no doubt, spurred by the recent wave of crypto-related ransomware attacks, such as the Colonial Pipeline ransomware attack. In fact, FinCEN specifically stated, "ransomware is a particularly acute concern, as criminals increasingly use sophisticated attacks to target various sectors, including government, finance, education, energy, and health care."

FinCEN added that cryptocurrencies are often used to layer transactions in order to hide the origin of money derived from illicit activities. Criminals often leverage tools such as mixers and tumblers in order to break the connection between the sender address and the receiver address. FinCEN recommends that covered institutions should focus on identifying and reporting suspicious AML/CFT activities as per the provisions of FinCEN Advisory 2019.

Internal Revenue Code (IRS)

According to the IRS, "Virtual currency transactions are taxable by law just like transactions in any other property. Taxpayers transacting in virtual currency may have to report those transactions on their tax returns." The IRS borrows its definition of virtual currencies from FinCEN, although its scope is usually limited to convertible virtual currencies.

In an information bulletin from 2014, the IRS clarified its treatment of virtual currencies as property, and therefore subsumed them into the general principles of federal taxation. Consequently, individuals and merchants receiving payments in virtual currencies must declare their 'fair market value' as part of their gross income. Except foreign currency gains or losses, every norm governing conventional taxation also applies to virtual currencies under the IRS.

5.1. The U.S. Infrastructure Bill, 2021

In the recent $1 trillion infrastructure bill proposed and passed in the U.S. Senate, the current Biden administration strives to infuse substantial public investments to develop and repair the nation's infrastructure. From roads to clean drinking water and high-speed internet, the bill allows for a wide scope according to its proponents. However, though apparently unrelated, the bill has implications for crypto-based transactions.

As a means to generate funds to support its agenda, and to enhance the overall tax compliance in cryptocurrency markets, the bill requires crypto-brokers to duly fulfill their tax-reporting obligations. The process inherits the reporting framework for traditional stockbrokers but includes specifications for the novel crypto industry.

According to some estimates, enforcing the bill could accrue over $28 billion in crypto-tax revenues over the next ten years. However, despite its success in Congress so far, the bill has been criticized heavily by a section of crypto-industry stakeholders. The primary concern, in this regard, is that the regulation imminently threatens the fundamentals of the blockchain-cryptocurrency domain, namely financial privacy and autonomy. The situation, therefore, is somewhat dilemmatic at the time of writing.

OCC Regulations for Cryptocurrencies

As of July 2020, the Office of the Comptroller of the Currency affirmed its legal interpretation allowing federally chartered banks to provide custodial services for crypto assets — opening the door to industry disruption and development of new digital asset protection services and solutions. Banks looking to decide which digital assets to custody need to assess the different types of risks that each digital asset carries.

In January 2021, amidst the global emergence of Central Bank Digital Currencies (CBDCs), the OCC allowed national banks and federal savings associations to participate in Independent Node Verification Networks (INVN) and use stablecoins for "bank-permissible" functions.

According to the then Acting Comptroller of Currency, Brian P. Brooks, *"The President's Working Group on Financial Markets recently articulated a strong framework for ushering in an era of stablecoin-based financial infrastructure, identifying important risks while allowing those risks to be managed in a technology-agnostic way. Our letter removes any legal uncertainty about the authority of banks to connect to blockchains as validator nodes and thereby transact stablecoin payments on behalf of customers who are increasingly demanding the speed, efficiency, interoperability, and low cost associated with these products."*

Courtesy of this development, the entities mentioned above will be able to validate, store, and record stablecoin-based transactions on their customers' behalf. In doing so, the participating bank or associations must comply with the regulatory framework of the Bank Secrecy Act, as described earlier. Therefore, the existing AML/CFT standard and tax-reporting rules also apply in this regard. And finally, the facilitating institutions must assume the responsibility of conducting thorough risk-assessment and mitigation strategies.

regard, is that the regulation imminently threatens the fundamentals of the blockchain-cryptocurrency domain, namely financial privacy and autonomy. The situation, therefore, is somewhat dilemmatic at the time of writing.

Conclusion

Blockchain technology is often touted as one of the most promising innovations since the Internet, and with good reason. By enabling cryptocurrencies, it has unfurled hitherto inaccessible ways of transacting, investing or speculating, and bootstrapping capital for business. However, despite its nascency, the industry has already witnessed the perils of unregulated and "permissionless" marketplaces. Although rightly deemed as a catalyst for change across sectors, crypto-based innovations have been disturbingly susceptible to frauds and imposters. Particularly so during the ICO Craze of 2017-18, when thousands of blockchain and cryptocurrency businesses solicited investments for groundbreaking solutions running on "decentralized networks" and platforms. Though many of these businesses are genuinely cutting-edge, the amount of value lost to scams, frauds, and hacks has also been staggering. And in this context of safeguarding the broader interests of consumers and investors, the U.S. regulators have arguably been the most meticulous and persistent globally.

When it comes to digital assets and cryptocurrencies, the U.S. has one of the most complex and multi-tiered regulatory frameworks in the world. Besides the Securities and Exchange Commission (SEC), other U.S. federal regulators include: the CFTC; FinCEN; the IRS, and the OCC. Cementing its authority and defining its scope, the U.S. has, in its regulatory arsenal, statutes such as the Securities Act of 1933, the Commodities Exchange Act (CEA) of 1936, and the Bank Secrecy Act (BSA). This Framework enables regulators and businesses to identify crypto-based securities (as distinct from utilities) and is the SEC's greatest contribution to cryptocurrency regulations, not just in the U.S. but also globally.

According to CoinMarketCap, the global cryptocurrency market cap has exceeded $2.6 trillion as of October 21, 2021. As a major proving ground for blockchain-cryptocurrency innovations, the U.S. contributes significantly to this growth, akin to its role in the evolution of the Internet.

With the attention placed on the crypto industry of late, U.S. regulators are keenly focused on the potential of crypto technology, as well as cryptocurrency as a highly desirable asset class. In order to maintain its domineering position in emerging technologies, the U.S. crypto industry and federal regulators must develop proactive and collaborative stances in order to bridge the gap between supporting innovation and investor protection.

Merkle Science believes that — in order to promote mainstream adoption of cryptocurrency and to ensure consumer protection — it is necessary to put in place a safe and proportionate regulatory framework that fosters innovation and fair competition. The industry must come together and propose technical solutions to regulatory problems. On the other hand, regulators must not default to trying to fit cryptocurrency into existing frameworks; they may have to reimagine the way they approach this bold new asset class.

How Merkle Science Can Help

Merkle Science provides blockchain transaction monitoring and intelligence solutions for cryptoasset service providers and financial institutions to address their risk exposure to virtual currency-related crime in accordance with FCA AML/CTF compliance requirements.

Our Blockchain Monitor enables compliance teams to go beyond using a database of bad addresses and configure custom risk rules to identify and detect high-risk transactions or addresses. The following are a few ways through which compliance teams can customize risk parameters:

- Detect direct or indirect interactions with high-risk entities (such as coin-mixers, darknet marketplaces), ransomware addresses, scam addresses, theft and hack addresses, the U.S. OFAC list, and other sanctioned or criminal addresses

- Set specific parameters related to frequency, size of transactions, and custom patterns to flag otherwise concealed criminal activity on the blockchain. (See FATF's Virtual Asset Red Flag Indicators of Money Laundering and Terrorist Financing for more information)

- Test and optimize risk rules within a "sandbox" environment before implementation to avoid false positives and too many/few relevant risk alerts.

For more information about how Merkle Science could help your firm comply with FCA virtual currency requirements reach us at contact@merklescience.com.

About the Author

Mary Beth Buchanan

President, Americas & Global Chief Legal Officer

Merkle Science

Mary Beth Buchanan is the President Americas and Global Chief Legal Officer at Merkle Science, where she leads the company's expansion into the Americas and directs the company's global legal, regulatory and government affairs efforts. Mary Beth is also currently a Member of the Board at the Cardano Foundation. Mary Beth brings over three decades of deep expertise at the intersection of federal law enforcement, global interagency cooperation, corporate compliance, digital assets, and emerging regulatory frameworks. Prior to joining Merkle Science, Mary Beth was the Chief Legal and Compliance Officer at Menai Financial Group, the Global Chief Legal Officer at Bitstamp and the General Counsel at Kraken.

Having been active in the digital currency space since late 2013, Mary Beth is dedicated to education efforts with regulators and policy makers on the potential of blockchain and cryptocurrency technology. Throughout her career, she has seen first-hand both the key role that clear regulations can play in supporting innovation and entrepreneurship, as well as the difficulties faced by digital asset startups in meeting their new compliance mandates.

Mary Beth also served for eight years as the Presidentially appointed United States Attorney for the Western District of Pennsylvania. Early in her career, Mary Beth was an Assistant United States Attorney, with a focus on financial crimes, often working in parallel with the SEC, CFTC, IRS, and state regulators. Mary Beth also served as the United Nations' Ethics and Reputational Risk Officer, leading the United Nations' first ethics and reputational risk assessment for UN Peacekeeping and Special Political Operations.

Mary Beth holds a Juris Doctorate from the University of Pittsburgh School of Law and a Bachelor of Science from the California University of Pennsylvania.

Contact Us

contact@merklescience.com