Part I: U.S. Crypto Regulations — Federal Regulators & Corresponding Regulations

1. Overview

During the so-called Initial Coin Offering (ICO) boom of 2017-18, the global blockchain-cryptocurrency sector was highly unregulated. Consequently, the industry was a breeding ground for 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. The Securities Exchange Commission or SEC intervened to remedy the situation, thus bringing cryptocurrencies under the regulatory purview in the United States of America. Though the overall framework covers both Federal and State laws, this report shall focus only on the former.

The SEC is the primary regulatory body governing cryptocurrencies in the US, as per the tenets of the Securities Act of 1933. The Framework for Digital Assets (henceforth, the Framework) facilitates the identification of digital assets as 'securities' and is a central cogwheel of SEC's machinery for regulating digital assets and cryptocurrencies. Drawing precedence from the US Supreme Court's ruling in the SEC v/s WJ Howey Co. case of 1946, the Framework deems 'investment contracts' as securities, based on parameters elaborated later in this report.

At the outset, it's worth mentioning that the US 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. Therefore, in addition to the SEC, the US employs institutions like the Commodity Futures Trading Commission (CFTC), Financial Crimes Enforcement Network (FinCEN), Internal Revenue Service (IRS), and the Office of the Comptroller of the Currency (OCC) to formulate and enforce cryptocurrency regulations.

The CFTC regulates the overall commodity derivatives market in the US, 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 virtual assets under its purview. In other words, everything that isn't a security as per SEC's definition is a commodity for the CEA.

FinCEN is a subsidiary of the US 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 substitute for currency' are also considered 'money transmitters' and must be registered with the FinCEN. However, Decentralized Exchanges (DEXs) and software wallet providers are exempt from the FinCEN guidelines under normal circumstances.

The IRS, for its part, strives to curtail tax evasions 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 chartered banks to offer custodial services for crypto-assets, subject to nuanced safeguards.

2. Securities Laws (SEC)

In a public statement from 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 US, 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 rampant 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 US regulatory landscape. And in fulfilling this purpose, the SEC refers to the Securities Act of 1933.

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. The purview of 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). Apparently, the SEC allocates the majority share of its budget and workforce to the enforcement division. The allocation witnesses a significant uptick in the aftermath of the global financial crisis of 2007-2008, and furthermore 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.
- On July 25, 2017, the SEC published its Report of Investigation on The DAO's initial coin offering and eventual hack. Besides involving 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.

Security Token Offering (STO): 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 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.*"

Gensler also realises 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.

2.1. Securities Act of 1933

The Securities Act, often known as the "Truth in Securities" law, originally governed traditional stocks, bonds, equity, and so on. Safeguarding the interests of investors is the primary motive behind this Act, achieved through the fulfilment 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 themselves 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 US-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.

2.2. 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 so-called Howey test.

In a 1946 ruling, the US 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 US 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 the federal law. On this note, we may elaborate the four prongs of the Howey test, thus highlighting their implications.

2.2.1 Investment of Money

Although significant, the first prong is somewhat obvious 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.

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

2.2.2 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 two requirements — "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.

2.2.3 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) **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 party (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.

2.2.3.1 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.

Besides 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’ investment proposition.

2.2.3.2 Derived from the efforts of others

Besides being reasonable in above terms, the expectation of profit must be objectively derived from the efforts of the AP(s). The said 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 such efforts of the AP, either fully or partially.

Purchasers may rightfully expect the AP to perform tasks essentially 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.**

2.2.3.3 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.

2.3 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 fulfilment of conditions stipulated in the commission's statement from 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 the 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.

3. Commodity Exchange Act (CFTC)

Originally restricted to traditional markets alone, the CTFC currently regulates digital assets as commodities, per 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 in the proliferating blockchain-cryptocurrency industry.

According to LabCFTC, a digital asset is "anything that can be stored and transmitted electronically, and has associated ownership or use rights." On the other hand, a smart contract "is a set of coded computer functions," as defined in the LabCFTC primer. Based on these definitions, the CTFC regulates, primarily, the crypto-derivatives market in the U.S., aiming to "*protect market users and their funds, consumers, and the public from fraud, manipulation, and abusive practices.*"

Therefore, besides its oversight on derivatives exchanges, CFTC's authority has two major aspects: anti-manipulation and anti-fraud. Accordingly, the institution stipulates the following regulatory guidelines:

- Transparency, resilience, and safety are necessary for the desired functioning of digital asset markets.
- Ensuring market integrity should be a key governance motive for 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.

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 USA PATRIOT Act. However, according to the Joint Statement 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 said holding 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 CTFC's view. Moreover, though the CFTC regulation primarily involves "retail commodity transactions," its implication can be extended to other regulatory domains.

4. 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**. On the other hand, a "virtual" currency is similar to its "real" counterpart, but has limited scope. Furthermore, a "convertible virtual currency" is one whose value correlates to another "real" or "virtual" currency.

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.

4.1.1 BSA Obligations for Money Transmitters

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 the management and staff 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.*" Due 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.

4.2 FATF Recommendations

As an independent, inter-governmental body, the Financial Action Task Force (FATF) is responsible for combating money laundering and terrorist financing. The FATF Recommendations is currently accepted as the global standard for Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT). In a draft Guidance published in 2019, the FATF proposed a 'risk-based' approach to virtual currencies. In June 2020, however, the FATF further clarified its definitions and scope, through its 12-Month Review.

According to the FATF, a Virtual Asset (VA) "*is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes.*" The current definition of VA excludes "*digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations.*"

On the other hand, a Virtual Asset Service Provider (VASP) is "*any natural or legal person who is not covered elsewhere under the Recommendations*" but provides services that are otherwise subject to FATF regulations. According to the Review mentioned above, VASPs provide the following services, either immediately or on behalf of another legal person:

- Facilitating conversions from virtual assets to fiat currency and vice-versa.
- Facilitating conversions between different forms of virtual assets.
- Transact virtual assets (on behalf of another legal person).
- Offer custodial services for virtual assets, thereby retaining control over them.
- Provide financial services corresponding to "an issuer's offer and/or sale of a virtual asset."

5. 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 a 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 US Infrastructure Bill, 2021

In the recent $1 trillion infrastructure bill proposed and passed in the US Senate, the current Joe Biden administration strives to infuse substantial public investments to developing 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 fulfil their tax-report 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 the parliament 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.

6. OCC Regulations for Cryptocurrencies

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 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.

7. Conclusion

Blockchain technology is often touted as one of the most promising innovations since the Internet, and with good reason. By enabling cryptocurrencies, for one, 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 so-called 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. Federal authority has arguably been the most meticulous and persistent globally.

The U.S. has one of the most complex and multi-tiered regulatory frameworks in the world, concerning digital assets and cryptocurrencies. Besides the Securities and Exchange Commission (SEC), which is the primary regulatory authority in this regard, the U.S. federal machinery involves the CFTC, FinCEN, IRS, and OCC. Legitimising the said authority and defining its scope, the U.S. has statutes like the Securities Act of 1933, the Commodities Exchange Act (CEA) of 1936, and the Bank Secrecy Act (BSA). On this note, the Framework enabling regulators and businesses to identify crypto-based securities (as distinct from utilities) is the SEC's greatest contribution towards cryptocurrency regulations, not just in the US but also globally.

The global cryptocurrency market is expected to reach $4.94 billion by 2030, with a CAGR of 12.8% for the current decade. As a major breeding ground for blockchain-cryptocurrency innovations, the US contributes significantly to this growth, akin to its role in the evolution of the Internet. Therefore, to summarize and conclude this paper, we must reiterate the progressive stance of the current regulatory regime in the US, prioritizing regulations over prohibition. Through an integrated machinery, federal cryptocurrency regulations in the US fosters innovation, while restricting fraudulent activities. Though legitimate businesses can proliferate unhindered, the said regulations protect consumers, and particularly investors who often have immense financial stakes. As the industry matures, there will be further increase in the demand for accountability and stability, conditions that robust and inclusive regulations imply. And in the process, it shall be necessary for federal regulators to sustainably strengthen and refine their approach vis-a-vis the dynamic and burgeoning blockchain-cryptocurrency sector.