MERKLE SCIENCE

Merkle Science RegWatch: 2021 Global Cryptocurrency Regulatory Review



Table of Contents

Crypto Regulatory Roundup: The Global Landscape

1. Overview **01**

2. Global Scenario: Financial Action Task Force (FATF) **02**

2.1 The Second 12-Month Review

2.2 The Updated Guidance On VAs & VASPs

2.2.1 The Modified Definition

2.2.2 The Travel Rule & P2P Interactions

2.2.3 Stablecoin Classification

3. The United States of America: Federal & State Legislation **06**

3.1 Federal Regulations

3.1.1 The Bipartisan Infrastructure Deal

3.1.2 OFAC's Updated Advisory On Ransomware

3.1.3 The U.S. Treasury Department's Stablecoin Report

3.1.4 Rep. Don Beyer's New Digital Assets Bill

3.1.5 FinCEN's National Priority List

3.1.6 Crypto ETFs

3.1.7 Crypto Policy Sprint

3.1.8 National Cryptocurrency Enforcement Team

3.1.9 Notable Enforcement Actions

3.2 State Legislation

3.2.1 DAOs As LLCs: Wyoming

3.2.2 Uniform Money Services Act Amendment: Arkansas

4. Canada **14**

4.1 Staff Notice 21-329: Guidance & Regulatory Requirements For CTPs

4.2 Staff Notice 21-330: Guidelines For Advertisement, Marketing, & Social Media Use By CTPs

4.3 Ontario

4.4 British Columbia

Table of Contents

5. United Kingdom (U.K.) **17**

5.1 The Financial Services Act 2021

5.2 FCA's Consumer Research Note 2021 & Temporary Registrations Regime Extension

6. European Union (EU) **19**

6.1 Package Of Legislative Proposals: Strengthening AML/CFT Controls

6.2 ESMA Report on Trends, Risks, and Vulnerabilities

6.3 EU Digital Finance: MiCA and DORA Proposals

7. Switzerland **22**

7.1 Phase I: Enabling Ledger-Based Securities

7.2 Phase II: Bringing the DLT Act Fully into Force

8. Singapore **24**

8.1 The Independent Reserve's In-Principle Approval

8.2 DBS Vickers' In-Principle Approval

8.3 Investor Alert For Binance

9. South Korea **25**

9.1 Act on Reporting and the Use of Specific Financial Transaction

9.1.1 Travel Rule Requirements

10. Japan **27**

10.1 Travel Rule Requirement

10.2 Crypto Derivatives

10.3 Tax Plan 2022

10.4 Stablecoin Law

10.5 Japan's Central Bank Digital Currency (CBDC)

11. Hong Kong **29**

11.1 Legislative Proposals to Enhance Anti-Money Laundering and Counter-Terrorist Financing Regulation

12. Australia **31**

12.1 Treasurer of Australia Announces New Crypto Regulatory Regime

13. Conclusion **32**

Overview

The blockchain-cryptocurrency market boomed in 2021, growing exponentially to peak at $3 trillion in global valuation. It was the year when Bitcoin and Ethereum, among others, achieved new all-time highs, both in terms of price and adoption. Emerging blockchains have also become increasingly popular. The market cap of Solana (SOL), which is often dubbed the "*Ethereum Killer*", grew by 400% in mid-2021, continuing steadily upwards thereafter.

Decentralized Finance or DeFi has been a major catalyst to this growth. Its market cap had risen by 382% since the beginning of the year to reach $95.7 billion by August 2021. And in January 2022, it is over $160 billion with more than $99 billion in total value locked (TVL) according to DeFi Pulse.

Four factors have contributed significantly to DeFi's steady growth since Q1 2021. First, the price of the governance tokens of leading decentralized exchanges rose during the so-called altcoin season. Second, the supply and scope of stablecoins increased, while their market cap grew 18x over the year. Third, DeFi protocols saw massive increase in capital inflow due to strengthening investors' confidence and interest. To this end, leading DeFi innovators like Chainlink have endeavored to identify persistent risks, promote best security practices, and develop mitigating solutions. Fourth, traders have followed the cue of rising investor participation, which led to a surge in decentralized trading volumes.

However, there's also been a flip-side to this success—the rise in criminal activities. As more money flowed into DeFi, crimes like ransomware and hacks increased. Consumers lost substantial sums to continued attacks on the hot wallets and smart contracts, while scams targeted investors globally. According to industry reports, there have been over 169 blockchain-related hacks in 2021, draining about $7 billion through November. And thus, to re-establish order and safety, regulators have issued several updated guidelines and requirements.

Safeguarding consumers and investors is the primary goal of crypto-regulations, but the need for regulatory clarity extends beyond that. It enables businesses and other stakeholders to properly classify tokens and make well-informed decisions. For example, a derivatives platform needs to know which tokens to include in its services and which to exclude. Similarly, those intending to bootstrap liquidity for their projects need to understand the difference between utilities and securities. Moreover, sound and fair regulatory insights help minimize risks concerning money laundering, terrorism financing, technological flaws, and cybersecurity.

Therefore, it's worthwhile to review and sum up the global regulatory landscape as it stands at the outset of 2022. In this report, we will be highlighting the changes that have occurred in 2021 within key organizations and jurisdictions, including the Financial Action Task Force (FATF), the United States, Canada, the United Kingdom, the European Union, Switzerland, Singapore, South Korea, Hong Kong, Japan, and Australia.

Global Scenario: Financial Action Task Force (FATF)

The FATF is an autonomous, intra-governmental organization and a key player in the global financial regulatory landscape. It promotes policy-making to combat money laundering, as well as the financing of terrorism and the proliferation of weapons of mass destruction.

In recent years, the FATF's oversight has become increasingly relevant for the cryptocurrency and virtual assets sector. Because these assets transact quickly, are globally accessible (borderless), and most importantly are pseudo-anonymous, they are highly conducive to the variety of financial crimes and money laundering, thus falling under the FATF's purview. The organization therefore makes several efforts to mitigate crypto-related financial crimes at the international level.
The 4th FATF Plenary was one such effort, convened in June 2021, where delegates from the organization's global network met virtually amidst the pandemic. The Plenary discussed several aspects of a risk-based approach to prevent financial crimes and terrorist financing. As a part of this discussion, it finalized the Second 12-Month Review of the implementation of its revised standards concerning Virtual Assets (VAs) and Virtual Asset Service Providers (VASPs).

2.1 The Second 12-Month Review

The FATF published this review in July 2021, based on the outcomes of public consultation and a survey of the FATF Global Network conducted from March to April that year. Merkle Science was one of the proud contributors of this survey, where one of the primary agendas was to identify whether the FATF needs to update its revised standards to address peer-to-peer (P2P) transactions specifically. However, due to inconsistencies in the overall data received in this regard, the FATF concluded that there wasn't enough evidence suggesting the need to directly address P2P transactions in its guidelines.

In general, the review found that nearly 50% of reporting jurisdictions—58 out of 128—have introduced legislation to implement the Revised FATF Standards. A majority of these (52) have permitted VASPs to function in compliance with the said standards, while 6 of them have imposed prohibitions. Nevertheless, much progress remains to be made in this regard, especially among FATF-Style Regional Bodies (FSRBs), as 70 FATF jurisdictions are yet to implement necessary laws. On the bright side, 26 of these 70 jurisdictions have begun relevant legislative processings. However, a noteworthy point with regard to this report is that it's an outcome of self-reporting by participating jurisdictions—the FATF analyzed the information, but not their accuracy or validity.

Closing the implementation gap is crucial from the viewpoint of establishing global safeguards against illicit activities, money laundering, terrorist financing, and other ways of misusing VASPs. Moreover, there's much evidence to show that robust AML/CFT regulations fosters business development and adoption at the international level. For example, the regulatory clarity of Singapore was a great boon for the DBS Digital Exchange (DDex) while launching its $15 million digital bond, as the esteemed panelists observed during a session of Merkle Science RegWatch.

According to the review, the conundrum concerning the Travel Rule is a major obstacle for uniform implementation of FATF Standards. The rule is similar to the Travel Rule of the U.S. Banking Privacy Act, requiring financial institutions and crypto-companies to share/ receive customers' information for domestic wire transfers and cross-border transactions exceeding 1000 USD or EUR. The Bank Secrecy Act (BSA) Travel Rule is nevertheless distinct insofar as it has a higher threshold and applies to transactions equal to or over $3000.

However, a majority of jurisdictions are yet to comply with this rule, blaming the private sector for the lack of a unified technological framework. Only 10 of the reporting jurisdictions actively enforce the Travel Rule, while 12 more have introduced regulations that are yet to be

enforced—none of these is aware if any VASP is in full compliance with the said rule. And because inadequate implementation in turn disincentivizes the private sector from innovating the necessary solutions, it leads to a vicious circle. Thus it is also the case that technological innovation can play a major role in enhancing the efficiency and effectiveness of risk-based AML/CFT procedures at the international level.

2.2 The Updated Guidance On VAs & VASPs

In October 2021, FATF published its updated guidance on VAs and VASPs. It incorporates the feedback received through public consultation for the Second 12-Month Review. The primary goal here is to provide a clearer framework for determining whether an entity is a VASP, particularly concerning DeFi protocols.

A draft updated guidance was published in March 2021 when it received much attention from industry stakeholders by expanding the scope of VASP's definition. However, it also became fairly confusing by including non-custodial wallets, multisig protocols, and decentralized exchanges under its purview. According to the draft, any entity that (a) provides DeFi services directly or indirectly and (b) has no traditional financial counterparty is a VASP, even though (c) it may not earn directly or generate profits. This definition was subject to criticism with good reason.

It was extremely difficult to specifically identify activities or roles that qualified as VASPs under this definition. Consequently, it imposed regulatory obligations on entities like web developers, coders, etc., who do not have access to the resources and degree of control necessary for enforcing AML/CFT procedures. DeFi protocols are usually non-custodial and don't have control over customers' assets, unlike custodial financial intermediaries. This forecloses their ability to comply with the FATF's recommendations, particularly those requiring protocol owners to freeze users' assets for legal purposes. And thirdly, the reasons why centralized VASPs aren't able to implement the Travel Rule also apply to DeFi protocols.

The FATF's stance while formulating this definition was that no technology is completely decentralized. Its claim was that *someone must be providing* the financial services that a DeFi protocol offers. And this facilitating entity was to be regulated as a VASP. However, the argument misses the point that most DeFi protocols eliminate centralized intermediaries or facilitators by using self-executing smart contracts. DeFi protocols decision-making procedures are also community-oriented and are not controlled by any singular entity. Moreover, compelling decentralized protocols to collect and hold massive amounts of user-generated data on-chain could ironically amplify the risks of hacks and breaches. It thus became necessary to harmonize AML/CFT compliance with users' privacy.

2.2.1 The Modified Definition

Reflecting upon the above concerns, the FATF duly modified the definition in the updated guidance. It now states that *"creators, owners, and operators or some other persons who maintain control or sufficient influence in the DeFi arrangements, even if those arrangements seem decentralized, may fall under the FATF definition of a VASP where they are providing or actively facilitating VASP services."*

To ensure clarity, the FATF also explained the scope of this modified definition with regard to specific financial activities. Summarily, VASPs include:

- virtual asset exchanges and transfer service providers;
- custodial wallet service providers that retain control over their consumers' (natural or legal persons) virtual asset wallets and/or private keys;
- financial service providers offering their platform for the issuance or sale of virtual assets, either for launching projects through ICOs, IDOs, etc., or otherwise;
- other potential business models that fulfil any or all of these criteria.

However, it's interesting to note that the definition appears to exclude multisig wallets where the consumer "maintains unilateral control of their assets at all times", as long as the wallet's developers don't "actively facilitate" the transaction. It is nevertheless unfortunate that the FATF does not still clarify the intended meaning and scope of active facilitation.

The guidance also introduces an owner/operator test to ease the process of identifying decentralized VASPs. Per this test, entities that "maintain control or sufficient influence" over the protocol are deemed its owners and are thus required to comply with AML/CFT regulations.

Although the meaning of "sufficient influence" remains vague, the FATF has provided a non-exhaustive list of parameters and activities to help nations assess control. Whether the entity is able to set or modify the rules of the protocol and the existence of business relationships between providers and consumers are crucial points of consideration in this regard. Moreover, the test also inquires whether any particular entity profits by offering a service in DeFi.

DeFi applications, however, are not to be considered VASPs as per the updated guidance, thus reflecting FATF's technology-neutral stance. In other words, the FATF Standard doesn't apply to technology per se but rather to its operators, if any. Developers are also exempt from the rule as a result, unless they specifically offer their applications as a part of some business venture. Similarly, individuals who hold governance tokens of decentralized protocols are also not VASPs. However, they might qualify for the owner/operator test in some situations.

Furthermore, the Updated Guidance sets out measures that countries can adopt based on their risk assessment, including:

- requiring VASPs to facilitate transactions only to/from addresses or sources that are acceptable in line with their risk-based assessment;
- requiring VASPs to facilitate transactions only to/from VASPs and other obliged entities, and/or additional AML/CFT requirements (such as enhanced recordkeeping) for those who allow transactions to/from non-obliged entities;
- requiring VASPs to file reports (such as currency transaction reports) when their customers transact with unhosted wallets; and
- conducting enhanced regulatory scrutiny of VASPs that enable customers to transact with unhosted wallets.

2.2.2 The Travel Rule & P2P Interactions

The FATF considers VASPs that don't implement the Travel Rule as higher-risk entities. It moreover requires VASPs to collect the information necessary for AML/CFT regimes while interacting with unhosted wallets. And to eliminate uncertainties for smoother implementation, the updated guidance explains certain aspects of the rule. For example, it states that recipient VASPs are not subject to the rule in scenarios where originator VASPs are automatically refunded for sending more than the actual amount of VA.

VASPs are also required to perform counterparty due diligence for Travel Rule compliance, ensuring the recipients legitimacy before transacting. The screening process must be continuous to remain updated with regard to sanctions imposed on a given counterparty. To ensure optimal data security, the updated guidance advises VASPs to share customer information only with reliable and trustworthy counterparties. VASPs thus need to assess the counterparty's AML/CFT controls and gauge its ability to transmit sensitive data securely. Moreover, the FATF clarifies that transactions between VASPs and unhosted wallets needn't comply with the Travel Rule, thereby excluding the fees paid to miners and validators.

Similar to the Travel Rule, regulating peer-to-peer (P2P) interactions has been a significant challenge for the FATF as there are no obligated intermediaries responsible for enforcing compliance. Its initial stance was that VASPs interacting with unhosted or private wallets should effectively be banned. However, the updated guidance retracts from this position, recognizing that unhosted wallets are in fact borderless and decentralized, meaning they cannot be banned. Rather it recommends the private sector to collaborate with regulators for the purpose of training, investigations, and enforcements. VASPs may thus use blockchain analytics tools for risk analysis and management.

2.2.3 Stablecoin Classification

The FATF's approach towards stablecoins is more nuanced in the updated guidance. It now recognizes that stablecoins may be centralized or decentralized, and thus have different structures. These differences relate to how particular stablecoins are accessed and governed (i.e. whether the stablecoin can be transferred to and used by an unhosted wallet).

One or more legal persons constitute the governance body of centralized stablecoins. They control the rules of the network and its decision-making procedure. And thus they are either financial institutions or VASPs as per the updated guidance. This also subjects them to proper ML/TF risk assessments prior to launching. Decentralized stablecoins must also undergo similar pre-launch assessments, even if there's no identifiable VASP in their case.

2.2.4 Clarifications Regarding CBDCs and NFTs

The Updated Guidance excludes CBDCs, arguing that they are digital representations of national fiat currencies and not VAs. Nevertheless, it does recognize the fact that CBDCs may have associated ML/TF risks distinct from those relating to VAs. The FATF therefore recommends effective risk analysis and management strategies in this regard, while stipulating that the general regulations applicable to fiats issued by central banks also apply to CBDCs.

The FATF also takes due cognisance of a rapidly emerging asset type, namely Non-Fungible Tokens or NFTs. Per the Updated Guidance, these assets, "*depending on their characteristics, are generally not considered to be VAs under the FATF definition.*" However the determination rests on the actual features and functioning of a given NFT, and those facilitating payments or involving some form of investment proposition are to be regulated as VAs. Moreover, certain NFTs may represent underlying assets that already fall under the FATF's regulatory purview. Therefore, in effect, only those NFTs that are purely "collectibles" may be relieved of regulatory obligations, and countries must determine the same on a case-to-case basis.

The United States of America: Federal & State Legislation

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 U.S. Securities and Exchange Commission (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. Moreover, there are specific state-level regulators, such as the Department of Financial Services, New York.

The Securities Act of 1933 is the primary statute for regulating cryptocurrencies and other digital assets in the U.S., and it posits the SEC at the head of the regulatory framework. Some of the other prominent laws include the Commodity Exchange Act (CFTC), the Bank Secrecy Act (FINCEN), the Internal Revenue Code (IRS), and the Uniform Commercial Code (State of Wyoming).

Enforcement actions based on the above laws is currently the predominant method for crypto regulations in the U.S. Notably, the frequency of such actions have increased significantly in the recent past, particularly since Gary Gensler became Chairman of the SEC. According to Gensler, crypto markets are akin to the "wild west" in need of greater regulatory insight. His concerns stem mainly from the lack of investor protection in crypto which inevitably leads to frauds, scams, and abuses. *"The crypto area is trying to stay outside of investor protection...We can do better"*, Gensler says.

In view of these concerns, Gensler recently appointed Corey Frayer as his senior advisor for crypto policy. Given Frayer's experience and track record, this could be seen as a move towards more robust crypto regulations, especially because Gensler has variously expressed the need for it. On this note, the possibility of unifying the framework by establishing a single regulator for cryptocurrencies remains. However, there's an ongoing and noteworthy internal debate in this regard.

According to Commissioner Hester Pierce, for example, *"typically in Washington, when you build another regulator, all you get is the existing regulators plus one."* She, for one, has been consistently vocal about the coming together of traditional and crypto-based finance in harmony. Pierce is in agreement with Gensler on the point of greater regulatory clarity, and the need for collaborating with industry stakeholders, especially exchanges. However, for her, it's necessary for the SEC *"to work at building something that makes sense in terms of regulatory clarity, instead of always just falling back on enforcement."*

3.1 Federal Regulations

Bearing the above context in mind, we may now discuss the recent updates concerning cryptocurrency regulations in the U.S.

3.1.1 The Bipartisan Infrastructure Deal

President Joe Biden signed the $1.2 trillion U.S. Infrastructure Bill into law on November 15, 2021. Though not directly related, the law has significant implications for the crypto industry, particularly in terms of its reporting requirements for taxation.

According to the law, platforms such as Coinbase must track and report transactions to the IRS from 2023 and onwards. The information to be shared not only includes financial data but also personal data, including the user's name, address, telephone number, and so on. The obligation is similar to the one imposed on brokers and exchanges in traditional stock markets. Nevertheless, it is highly concerning from the viewpoint of consumers' privacy and data security.

There's a more specific issue here as well, concerning how the law defines crypto brokers without providing much clarity. It has been variously pointed out that the

definition is too wide and includes entities like miners and software developers. They are thus being asked to report information that they don't possess or have access to in the first place. Moreover, compelling exchanges to report in the manner that the law stipulates could foster the risk of surveillance and selective discrimination. Besides stifling innovation, this could deprive many Amerians of their financial rights.

Additionally, the language in the original bill also caused concern that it may push crypto businesses and trading overseas, potentially damaging blockchain innovation in the U.S. and its position in the global blockchain race.

Senators like Cynthia Lummis, Ron Wyden, and Ted Cruz had proposed amendments to the bill while it was being debated in the House, but without much success. They have thus introduced standalone bills to rectify the law's definition of a digital assets broker. Cruz's bill goes a step further, proposing to altogether repeal the section of the law dealing with crypto.

On December 14, 2021, senators Rob Portman (R-Ohio), Mark Warner (D-Va.), Mike Crapo (R-Idaho), Kyrsten Sinema (D-Ariz.), Pat Toomey (R-Pa.), and Cynthia Lummis (R-Wyo.) issued an open letter to the Secretary of the U.S. Treasury Department, Jannet Yellen, to further address concerns regarding the definitional scope of the Infrastructure Bill. The letter highlights that the Bill's definition of a "broker" is too wide and includes entities responsible merely for validating transactions or developing hardware. And in view of this concern, the authors of the letter have sought necessary clarification and guidance from the U.S. Treasury Department.

3.1.2 OFAC's Updated Advisory On Ransomware

The U.S. Treasury Department's Office of Foreign Assets Control (OFAC) issued the Updated Advisory on ransomware in September 21, 2021, where it highlighted *"the sanctions risks associated with ransomware payments in connection with malicious cyber-enabled activities and the proactive steps companies can take to mitigate such risks, including actions that OFAC would consider to be 'mitigating factors' in any related enforcement action."*

Ransomware attacks have increased significantly in the post-COVID scenario. There's been a 21% rise in cases from 2019 to 2020, amounting to a 225% rise in associated losses, imploring the U.S. government to adopt holistic counter measures. The Updated Advisory is a step in this direction, and it *"strongly discourages all private companies and citizens from paying ransom or extortion demands and recommends focusing on strengthening defensive and resilience measures to prevent and protect against ransomware attacks."* The OFAC is of the view that it's not advisable for companies and institutions to facilitate ransomware payments on behalf of victims because it encourages similar attacks in the future. Moreover, by doing so, the facilitator could also be in violation of OFAC regulations, per the Advisory.

Over the years, the OFAC has designated and sanctioned various malicious actors for conducting or facilitating ransomware attacks. Some of the prominent names on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List) include Evgeniy Mikhailovich Bogachev (Cryptolocker), the Lazarus Group (WannaCry 2.0), and Evil Corp (Dridex). In September 2021, SUEX OTC, S.R.O. became the first virtual currency exchange to make it to this infamous list. Nearly 40% of all transactions on this platform are related to illicit activities, as the Advisory duly notes.

Through its Advisory, the OFAC urges companies to engage ransomware victims to adequately implement sanctions compliance programs, assessing and mitigating the risks of interacting with SDNs, blocked persons, or embargoed regions. To this end, companies must also consider their regulatory obligations under the FinCEN. They may accordingly have to file Suspicious Activity Reports (SARs) or register as Money Service Businesses (MSBs). Adopting the defensive measures highlighted in Cybersecurity and Infrastructure Security Agency's (CISA) Ransomware Guide (2020) is also recommended.

Furthemore, the Advisory clarifies OFAC's scope for enforcement actions under the authority of the International Emergency Economic Powers Act (IEEPA) or the Trading with the Enemy Act (TWEA). The guideline stipulates the following as considerable factors for enforcements:

- Did the victim have a sanctions compliance program? What was its nature and adequacy?
- Did the victim follow CISA's Ransomware Guide to take measures like offline backups, updating the antivirus and antimalware programs on their system,

authenticating employees, and so on?
- Did the victim collaborate with enforcement authorities, promptly providing the information and technical details necessary for retribution? That is to ask whether the victim expressed "full and ongoing cooperation" through their actions.

The Updated Advisory specifically states that a significant mitigating factor in its enforcement response against companies will be the whether the company has adopted robust cybersecurity practices, referred in the guidance as "defensive and resilience measures. OFAC mentioned certain practices highlighted in the CISA ransomware guide.

The Advisory ultimately implies that there's no *safe harbor* for ransomware and that *paying up* and *forgetting* isn't the proper way around the problem. It thus promotes resilience over relenting to perpetrators, and works towards the wider goal of disrupting financial criminals and their networks for stronger national security.

3.1.3 The U.S. Treasury Department's Stablecoin Report

On November 1, 2021, the President's Working Group on Financial Markets (PWG) released a much-anticipated report on stablecoins, jointly with the Federal Deposit Insurance Corporation (FDIC) and the Office of the Comptroller of the Currency (OCC). The report recommends the Congress to promptly formulate and *"enact legislation to ensure that payment stablecoins and payment stablecoin arrangements are subject to a federal prudential framework on a consistent and comprehensive basis."*

According to Janet L. Yellen, Secretary of the U.S. Treasury Department, "Stablecoins that are well-designed and subject to appropriate oversight have the potential to support beneficial payments options. But the absence of appropriate oversight presents risks to users and the broader system." She further notes the inconsistencies in the current regulatory oversight and its fragmented nature, which effectively enable unregulated stablecoins. And thus the need for collaborative legislation, as mentioned above.

The report recommends several general measures, such as respecting market integrity, boosting investor protection, and curbing illicit activities. But more importantly, it stipulates three specific guidelines for stablecoins:

- **Safeguards against loss of value:** In the event that a substantial number of holders lose confidence in a particular stablecoin, its value could dwindle as investors sell out rapidly. This could also happen if the stablecoin's reserve asset is breached somehow or if the redemption process is unclear to consumers. To safeguard users against such losses, the report recommends legislation to require stablecoin issuers to be *insured depository institutions*. Thus, by requiring private issuers of stablecoins to become chartered institutions with the OCC, the recommendation fosters innovation and technological advancement while ensuring optimal risk assessment. Moreover, regulating stablecoin issuers as FDIC-insured depository institutions would subject them to consolidated supervision and prudential standards, including obligations for leverage and risk-based capital, limited affiliations with commercial entities, and other restrictions. However, it's important to note that stablecoin issuers must not be regulated as traditional banks, for that will obstruct innovation and effectively ban the stablecoin industry altogether, as Flavia Navis warned during a Merkle Science webinar on this subject.
- **Safeguards against payment risks:** Similar to legacy finance, stablecoin-based payments are prone to multiple risks concerning credit, liquidity, settlement, and governance. But no single entity is responsible for mitigating such risks for stablecoins, due to their decentralized nature. Per the report, it's thus necessary to bring custodial stablecoin wallets under the federal regulatory oversight to ensure optimal risk-management standards.
- Safeguards against systemic risks and monopoly: Increasing demand will motivate stablecoin providers to scale their offering which in turn poses systemic risks. There will be a significant impact on the markets if a big stablecoin suddenly breaks down. Unchecked affiliations between stablecoin issuers and commercial entities could lead to monopoly and contract free market principles. Thus the report recommends legislation to curtail the scope for such affiliations. Promoting interoperability and collaboration is also advisable.

In addition to the above guidelines, the report also identifies and addresses certain other important risks concerning stablecoins.

- **Illicit Financing Risks:** Stablecoins also pose illicit finance concerns and risks to financial integrity, including concerns related to compliance with rules governing AML/CFT activities.
- **DeFi Risks:** Digital asset trading platforms and DeFi arrangements present risks of particular focus to the agencies, and most notably to the SEC and CFTC. Among others, these risks include increased reliance of stablecoin arrangements on digital asset trading platforms and vice versa. Potential AML/CFT risks and risks may arise from unique aspects of distributed ledger-based arrangements. These include governance issues, interoperability, scalability, protocol and smart contract vulnerabilities, cybersecurity, and other operational issues.

However, although the report calls for regulatory oversight on stablecoins, it does not specify which organization must assume this role. Nevertheless, it does note that the SEC and CFTC have "broad enforcement, rulemaking, and oversight authorities" to address the concerns mentioned above. Moreover, the Treasury Department promises to continue working closely with the FATF to implement robust AML/CFT regimes for stablecoins, both nationally and internationally. And to this end, the Congressional Hearing on Stablecoins provides certain noteworthy insights.

For one, the U.S. Congress strives to hone its understanding of stablecoins, as to whether these assets are *"similar to notes or instruments issued by Wildcat Banks before the standardization of American currency, or whether they're just product innovation."* Members of the Congress are generally concerned about the prudential risks that stablecoins pose, including liquidity and operational risks. There's moreover the awareness that the overall growth of DeFi, as well as of stablecoins, is an imminent threat to the sovereign governing entity for any given nation. Economic policy-making is the most at risk in this regard.

Furthermore, the overdependence of stablecoin arrangements on digital asset trading platforms and vice-versa potentially threatens the smooth functioning of these platforms, especially in cases where the stablecoin falters or collapses. Thus it becomes increasingly necessary for regulators like the SEC and CFTC to oversee the safety and soundness of fiscal policy apparatus like stablecoins, as well as the novel threats they pose. The Congress is also equally concerned about the general risks of market integrity and consumer protection. Besides the possibility of fraud, these risks include acts of misconduct in digital asset trading: market manipulation, front running, and the lack of transparency in pricing.

3.1.4 Rep. Don Beyer's New Digital Assets Bill

According to Congressman Don Beyer (D-VA), *"digital assets and blockchain technology hold great promise, and it is clear that assets like Bitcoin and Ether are here to stay. Unfortunately, the current digital asset market structure and regulatory framework is ambiguous and dangerous for investors and consumers. Digital asset holders have been subjected to rampant fraud, theft, and market manipulation for years, yet Congress has hitherto ignored the entreaties of industry experts and federal regulators to create a comprehensive legal framework. Our laws are behind the times, and my bill would start the long overdue process of updating them to give digital asset holders and investors basic protections."*

Rep. Beyer believes that innovation in digital assets could result in massive job-creation for ordinary Americans, besides offering them new goods and services. Yet, on the contrary, there's a rising number of crimes in the domain which threatens users. He thus introduced the Digital Asset Market Structure and Investor Protection Act of 2021 to *"promote innovation and US jobs by providing legal and regulatory certainty for digital assets, provide fundamental investor protections to U.S. retail investors and other consumers, improve trade reporting and transparency, strengthen the Bank Secrecy Act requirements related to the treatment of digital assets, and protect U.S. investors in the digital asset sector."*

The comprehensive bill covers nearly every aspect relevant to regulating cryptocurrencies and other digital assets in U.S. markets. Some of its key points include:

- Definitions for digital assets and digital asset securities to foster clarity and streamline the regulatory procedures.
- Legal and regulatory certainty for top assets through a joint legislation by the SEC and CFTC.
- Reporting requirements for private digital asset

transactions within 24 hours of finalization.
- Explicit authority to the Federal Reserve for the issuance of digital U.S. Dollars.
- Clarifications about stablecoins, that they aren't legal tenders in the U.S., while authorizing the Treasury Department to veto their issuance.
- Directives for the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), and the Securities Investor Protection Corporation (SIPC) to clearly communicate that their policies do not cover stablecoins.
- Requisitions for regulatory and definitional clarity from the FinCEN, SEC, and CFTC, particularly concerning their registration requirements.

The first section of the bill provides a definition for "digital asset securities", and if passed, will bring such securities under the oversight of the SEC and the Securities Exchange Act, 1934. More importantly, the Sec 103 of the bill contains provisions for desecuritization, and explains how tokens classified as digital asset securities may become cryptocurrencies that aren't regulated as securities. In doing so, the bill reflects SEC Commissioner Hester Peirce's longstanding efforts to create a safe harbor for crypto projects to get off the ground. The updated status will put these assets under the purview of the CFTC.

However, a point of concern with the bill is that it provides the U.S. Treasury Department with the power to veto stablecoin issuance. This move could potentially hamper innovation and trading in stablecoins, as they will constantly need permission and approval from the Treasury Department. It thus remains to be seen how this aspect of the bill will eventually be enforced, especially in relation to algorithmic stablecoins.

3.1.5 FinCEN's National Priority List

The Financial Crimes Enforcement Network (FinCEN) issued the first National AML/CFT Priorities List in September 2021, along with accompanying statements. The list covers the leading risks facing Americans, including corruption, cybercrime, domestic and international terrorist financing, fraud, transnational criminal organizations, drug trafficking organizations, human trafficking and human smuggling, and proliferation financing.

According to Acting Director Michael Mosier, *"[the] publication of government-wide AML/CFT Priorities is a significant milestone in FinCEN's efforts to improve the efficiency and effectiveness of the nation's AML/CFT regime and to foster greater public-private partnerships."*

Regulations for implementing the National Priorities, which the FinCEN promises to publish within 180 days from the announcement. It has thus advised institutions to be prepared but not to amend their existing risk-based AML/CFT programs prior to the regulations. The Priorities aren't meant to amend the BSA either, though banks and non-bank financial institutions may update their regulations according to the list.

Virtual Currency Considerations is One of the Top Priorities for the FinCEN

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 Convertible Virtual Currencies (FinCEN's term for cryptocurrencies) 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."

The 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

Regulations of Bank Secrecy Act to be Updated

Along with the Priority Lists, the Federal Banking Agencies (FBAs), which include the Federal Reserve Board, the

FDIC, FinCEN, the National Credit Union Administration, the Office of the Comptroller of Currency, State Bank and Credit Union Regulators, issued an interagency statement to provide financial institutions with additional clarity regarding the effects of the AML/CFT priorities. According to the statement, the FBAs plan to revise BSA regulations to address "how the AML/CFT Priorities will be incorporated into banks' BSA requirements."The FBAs also clarified that the newly published AML/CFT priorities will not take effect until the effective date of final updated BSA regulations.

Lastly, FinCEN issued related statements to both financial and non-bank financial institutions, offering them key advice stating that "in preparation for any new requirements when those final rules are published, covered institutions may wish to start considering how they will incorporate the AML/CFT Priorities into their risk-based AML programs, such as by assessing the potential related risks associated with the products and services they offer, the customers they serve, and the geographic areas in which they operations."

3.1.6 Crypto ETFs

October 19, 2021 became a landmark in the history of cryptocurrencies when the first-ever, regulated futures-backed Bitcoin Exchange Traded Fund (ETF) started trading on the New York Stock Exchange (NYSE). ProShares received the license to launch this product from the SEC, following almost two years of communications to and fro. The product had a record-breaking debut, reaching $1 billion AUM in just two days from launch.

Other futures-backed ETFs have followed suit, such as the Valkyrie Bitcoin Strategy ETF (Nasdaq) and VanEck Bitcoin Strategy ETF (CBOE). Though their launch was equally significant from a broader perspective, their debuts were quite humble in comparison to ProShares' ETF.

However, physically-backed or spot Bitcoin ETFs are yet to convince the SEC about their ability to safeguard investors. Consequently, the SEC has rejected several such filings recently, including those by Valkyrie, VanEck, and Kryptoin. The proposals by several others, such as First Trust, Skybridge, Fidelity, and Invesco, are awaiting SEC's decision, due around mid-to-end of January 2022.

Concerns about price manipulation is the major reason behind SEC's rejection of spot Bitcoin ETFs. Futures-backed ETFs, on the contrary, are more compatible with existing investor protections, as Gensler himself noted in an interview with CNBC. He further pointed out that the Chicago Mercantile Exchange (CME) has already been dealing in Bitcoin Futures since 2017, under the regulatory oversight of the CFTC.

3.1.7. Crypto Policy Sprint

In view of the increasing institutional participation in crypto-markets, the Federal Reserve System, the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC) issued a joint statement in November 2021.

The agencies summarized their "policy sprints" through this announcement to provide a comprehensive roadmap of future actions and ensure greater regulatory clarity. The overall purpose here is to facilitate safer and more secure crypto-markets with effective customer protection and optimal compliance. To this end, the agencies have based their recommendations on the major issues facing banking institutions dealing in digital crypto-assets.

Developing a common vocabulary is a primary agenda for these sprints, besides assessing the relevance and applicability of existing regulations to emerging crypto-assets. Moreover, the agencies have identified the following areas where the broader public requires clarity:

- Traditional custodian services
- Safekeeping services for crypto-assets
- Purchase and sale of crypto-assets
- Crypto-collateralized lending and borrowing
- Stablecoins, their issuance and distribution
- Accounting and balance sheet maintenance for crypto-assets

Furthermore, evaluating how bank capital and liquidity standards may apply to crypto-based interactions is also a part of the agencies' plan. They will work with the Basel Committee on Banking Supervision (BCBS) which is currently the leading body for setting prudential regulation standards at the global level.

3.1.8 National Cryptocurrency Enforcement Team

On October 6, 2021, the U.S. Department of Justice (DoJ) formed a National Cryptocurrency Enforcement Team

(NCET), as Deputy Attorney General Lisa O. Monaco announced. It's a task force combining the expertise of the DoJ Criminal Division's Money Laundering and Asset Recovery Section (MLARS) and Computer Crime and Intellectual Property Section (CCIS), among others. Representatives from the U.S. Attorney's office will also join the team.

The primary goal of the NCET is to investigate and prosecute complex cases involving the criminal use of cryptocurrencies and other digital assets. The task force will particularly look into crimes committed by crypto-exchanges, mixing and tumbling services, and money launderers.

The increasing use of crypto-assets for online crimes and in so-called darknet marketplaces that list everything from drugs to child pornography is one of DoJ's main concerns. Ransomwares are a considerable menace as well. And thus the task force will also assist victims of such crimes, ensuring adequate and prompt retribution.

According to Monaco, *"if cryptocurrency exchanges want to be the banks of the future, we need to make sure people can have confidence in these systems."* To this end, the NCET will foster proactive collaborations between the government and industry stakeholders, particularly concerning monitoring for illicit activities. Identifying criminals promptly will also go a long way in enhancing the crypto sector's overall reliability among investors and consumers. Moreover, the task force will oversee the creation of better-educated regulators, who are genuinely competent to address the needs of a dynamic and budding industry.

3.1.9 Notable Enforcement Actions

In addition to the several policy changes and inclusions that we have discussed so far, there have been many notable enforcement actions in the recent past. The following are some of the most prominent ones in this regard:

- **Chatex:** The OFAC designated and sanctioned Chatex, a virtual currency exchange, on November 8, 2021, for facilitating multiple ransomware-related transactions. The exchange was found to have direct ties with SUEX OTC, which was similarly sanctioned in September 2021. The current enforcement actions also designated IZIBITS OU, Chatextech SIA, and Hightrade Finance Ltd for providing material support to Chatex. The OFAC identified the Sodinokibi/REvil ransomware as a part of this process, designating Ukrainian Yaroslav Vasinskyi and Russian Yevgeniy Polyanin for their enabling involvement in the project.
- **Blockchain Credit Partners:** The SEC penalized the Blockchain Credit Partners and its owners Gregory Keough and Derek Acree for raising $30 million through unregistered and fraudulent offerings under the name of DeFi Money Market (DMM). Undertaken on August 6, 2021, this was the first-of-its-kind enforcement action involving a DeFi protocol. The company sold so-called mTokens and DMG governance tokens with the promise of investing them in 'real-world' assets like car loans to generate passive income for token holders. However, the owners soon realized the impracticality of the plan, but concealed the information from token holders. Instead, they channelized personal funds, as well as those from other companies, to keep up the facade while updating their website with false information.
- **Poloniex LLC:** The SEC charged Poloniex LLC on August 9, 2021, for operating an unregistered digital asset exchange. The accused agreed to pay over $10 million for settling the case. The exchange operated from July 2017 to November 2019, dealing in unsolicited utilities and securities during that time. In a drive to increase its market share, Poloniex "aggressively" entered the market without proper licenses, despite qualifying as an exchange under the U.S. Securities Law. Moreover, several of its offerings qualify as securities under the Howey Test. And despite full knowledge of these classifications, the company attempted to bypass the SEC's regulatory regime.
- **Kraken:** The CFTC charged Payward Ventures, Inc. on September 28, 2021, for illegally offering margined retail commodity transactions through the Kraken Exchange. Moreover, the exchange failed to acquire licenses necessary for such offerings, and was thus asked to pay $1.25 million in fines.
- **Tether & Bitfinex:** The CFTC charged Tether (Tether Holdings Limited, Tether Limited, Tether Operations Limited, and Tether International Limited) and Bitfinex (iFinex Inc., BFXNA Inc., and BFXWW Inc.) on October 15, 2021, ordering them to pay a total of $42.5 million in fines. Tether was accused of misleading consumers by claiming that its stablecoin was fully-backed by the U.S. Dollar. Bitfinex, on the other hand, was deemed

guilty of illegal operations and violation of previous CFTC orders.

3.2 State Legislation

Alongside the happenings at the federal level, as we have been discussing so far, there have been some major developments at the state level as well.

3.2.1 DAOs As LLCs: Wyoming

Mark Gordon, Governor of the State of Wyoming, signed Bill 38 into law on April 21, 2021, thus recognizing Decentralized Autonomous Organizations (DAOs) as Limited Liability Companies (LLCs). Wyoming became the first state to pass such a legislation, according to which a DAO *"is a limited liability company whose articles of organization contain a statement that the company is a decentralized autonomous organization."*

To facilitate proper identification, the law stipulates two kinds of DAOs: *member managed and algorithmically managed*. However, it requires DAO LLCs to be domiciled in Wyoming which could be a source of much confusion, given the borderless and online-native nature of several DAOs. Nevertheless, the law enables easier business processing for existing and upcoming DAOs, particularly by relieving any single entity from being liable for the DAO's actions. Rather than being sued as general partnerships in the event of conflicts, the law will serve to preserve the rights of DAOs as legal persons.

3.2.2 Uniform Money Services Act Amendment: Arkansas

On May 4, 2021, the State of Arkansas passed a proposed amendment to its Uniform Money Services Act to include virtual asset transactions under its regulatory purview. Incidentally, the said act is the state's statute for money transmissions. Following this enactment, virtual asset service providers will be required to meet certain reporting and bookkeeping requirements. Licensing obligations will also apply to such entities.

Canada

Regulations on virtual assets came early in Canada, when they were brought under the oversight of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) in August 2014. The Canadian Securities Administrators (CSA) further extended its regulatory scope in August 2017 by issuing a staff notice to bring cryptocurrencies under the purview of its securities law.

The Canadian regulatory framework relies on the definition of virtual currencies provided by the nation's financial intelligence unit, namely the Financial Transactions and Report Analysis Center of Canada (FINTRAC). Per this definition, a virtual currency is *"a digital representation of value that can be used for payment, investment or retail activities such as buying and selling of goods and services."*

FINTRAC's regulatory oversight extends over crypto-asset trading platforms or CTPs which the PCMLTFA deems as Money Service Businesses (MSBs). Such MSBs are usually domiciled in Canada, but may also be foreign entities (FMSBs). The FINTRAC also issued guidelines for establishing robust KYC procedures, primarily for AML/CFT purposes, that came into effect from June 1, 2021.

Besides the FINTRAC, the Canada Revenue Agency (CRA) regulates crypto-based taxations under the Income Tax Act. Moreover, the CSA defines securities and requires business dealing in these assets to acquire a license (receipt) from the securities regulatory authority.

Merkle Science elaborated on each of these aspects in its publication—*A Guide To The Canadian Regulations For Cryptoasset Businesses*. Readers may refer to this for a comprehensive view of the regulatory framework in Canada. And thus, we currently only briefly discuss some of the high-points of Canadian crypto regulations from 2021.

4.1 Staff Notice 21-329: Guidance & Regulatory Requirements For CTPs

The Investment Industry Regulatory Organization of Canada (IIROC) collaborated with the CSA to issue Staff Notice 21-329 on March 29, 2021, clarifying the application of securities legislation to CTPs. The IIROC is a self-regulatory body of the Canadian Federal Government, and is responsible for overseeing investment dealers and trading activities.

Per the notice, CTPs are entities that enable trading in crypto-assets that are (a) securities under CSA's definition, and (b) are not securities but fall under CSA's purview as crypto-asset contracts. Either of these asset types are regulated under the securities laws, and their providers are required to duly register with the CSA. They may also face enforcement actions by failing to do so. Moreover, the CSA defines the conditions for partial exemption for existing regulatory obligations.

The notice further distinguished between two kinds of CTPs: Dealers and Marketplaces. Dealer Platforms are those where buy and sell orders do not interact directly, but are always intermediated by the dealer. The regulation allows these platforms to distribute and trade security tokens, enter into crypto-contracts with accredited investors only, and offer margin or leveraged securities subject to due registration and IIROC membership.

Marketplace Platforms, on the other hand, serve as a common intermediary for multiple parties trading tokens or crypto-contracts. Besides providing a market or platform for the interaction of buyers and sellers of security tokens, marketplaces are allowed to intermediate trades and facilitate peer-to-peer securities exchange on their platform.

The registration process and its requirements are different for each of these types of CTPs, as elaborated in the guide mentioned above.

4.2 Staff Notice 21-330: Guidelines For Advertisement, Marketing, & Social Media Use By CTPs

On September 23, 2021, the IIROC and CSA jointly issued Staff Notice 21-330 to advise CTPs on regulatory requirements concerning advertising, marketing, and social media use. To this end the notice applies to both registered and prospective CTPs.

The notice guides CTPs regarding fake or misleading advertisements by providing a non-exhaustive list of examples. In general, sanctions may apply to statements that (a) falsely suggest the CTP's registration under securities law, (b) suggest that regulatory authorities have endorsed the CTP, its products, offers, disclosures, or representations, and (c) provide false or misleading information on matters that relevant to investors while choosing the CTP's offerings.

Moreover, the CSA and IIROC staff express their concern over 'gambling-style' promotions that involve challenges, contests, bonus offers, and so on. In the notice, they note how such schemes feed on the consumer's fear of missing out, often driving them to make rash and risk-prone decisions.

The notice duly reminds CTPs that they are "gatekeepers of the integrity of capital markets" and must not engage in actions that bring disrepute to these market arrangements. Contrary to this obligation, misleading advertisements fail to provide fair treatment to market participants and consumers.

CTPs are also advised to comply with existing regulations while using social media platforms, especially with those concerning proper bookkeeping and documenting business activities. To this end, they must design databases with retrieval capacities. Determining the extent of legitimate supervision is also necessary, for which CTPs may adopt a risk-based approach. And finally, CTPs must acquire adequate legal consultation and develop systems to comply with the general tenets of the securities law.

4.3 Ontario

The Ontario Securities Commission (OSC) has a state-level regulatory framework, consistent with the federal framework comprising CSA and IIROC. An OSC staff notice from March 2021 required CTPs to comply with Ontario Securities Law, failing which they could face enforcement actions. Per the notice, CTPs that currently offered derivatives trading services to individuals and companies based in Ontario had to reach out to the OSC by April 19, 2021. The notice also highlighted the OSC's awareness of platforms aspiring to become *"reporting issuers"* through IPOs, reverse takeover, etc., and asked them to contact the OSC staff.

Poloniex, a digital assets trading platform incorporated under Polo Digital Assets, Ltd. in the Republic of Seychelles, faced such enforcement actions in May 2021. The OSC published a Statement of Allegations to announce the proceedings when the CTP failed to comply with regulatory obligations. Following this enforcement, the OSC added Poloniex to its Investor Warning List, which the organization constantly updates.

4.4 British Columbia

The British Columbia Securities Commission (BCSC) clarified its regulatory scope and the requirements thereof, in accord with CSA-IIROC Joint Staff Notice 21-329. Per this notification published on April 7, 2021, CTPs based in British Columbia are required to engage with the BCSC for authorization. Earlier, in January 2021, the BCSC had issued another notification advising consumers to be cautious while dealing with unregistered CTPs, such as Mercury Crypto Invest.

4.5 Ongoing Monitoring Requirements

On June 1, 2021, FINTRAC's Ongoing Monitoring Requirements came into effect, applicable to all reporting entities that are subject to the PCMLTFA, including MSBs. All reporting entities thus had to develop review and compliance procedures to detect suspicious transactions, as well as for client identification and continuous risk assessment. The FINTRAC provided due guidance and explanations in this regard.

Following the initial publication, the regulator also issued additional guidelines over the year to clarify and assist the implementation of specific aspects of the requirements. In September 2021, it issued guidance on reporting *large virtual currency transactions*. And in November 2021, the updated guidance on reporting terrorist property was published, which replaced *"Guideline 5: Submitting Terrorist Property Reports to FINTRAC."*

The updated guidance for combatting terrorist financing subjected MSBs to Section 83.1 of the Criminal Code or Section 8 of the Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism (RIUNRST), requiring them to disclose terrorism-related transactions and to submit a Terrorist Property Report (TRP). To ensure effective compliance, the FINTRAC additionally recommended existing and aspiring MSBs to remain duly acquainted with the tenets of the Criminal Code and the RIUNRST.

United Kingdom (U.K.)

The UK has enforced various steps to prevent and prohibit money laundering for over thirty years now. The current iteration of its Money Laundering Regulations (MLRs) came in January 2020, when the Money Laundering and Terrorist Financing (Ammendment) Regulations 2019 was further amended into the Money Laundering and Terrorist Financing (Amendment) (EU Exit) Regulations 2020.

Besides implementing updated FATF Standards, the purpose of such amendments is to keep the UK's regulatory framework updated to meet latest threats and concerns. And thus, in view of the rapid industry changes in 2021, the HM Treasury launched a consultation seeking the public's views on proposed amendments to the current MLRs. Some of the broad agendas of these amendments are as followed:

- Modifying the scope of MLRs to incorporate changes in risk assessment methods and observations thereof.
- Clarifying changes to better regulatory clarity and stronger supervision.
- Expanding certain MLRs to align them with updated FATF requirements, thus ensuring UK's position at par with international standards.
- Collecting and sharing information.
- Implementing FATF recommendations concerning crypto-asset transfers to mitigate ML/TF risks.

According to the consultation paper, *"the government's approach to implementation is guided by the principle that the application of the FATF's Recommendation 16 aka the 'Travel Rule,' and it should be consistent across the financial services industry, regardless of the technology being used to facilitate transfers, unless there is a compelling reason to adopt a different approach."*

The consultation, however, also takes into account the private sector's contribution in development of Travel Rule solutions and notes that *"the government has been kept informed of technological developments, such as the development of common data standards and the progress of a large number of software solutions, and considers that the time is now right to begin planning for the implementation of the Travel Rule."*

These requirements, when enacted, will apply to crypto asset exchange providers and custodian wallet providers, as defined in The Money Laundering and Terrorist Financing (Amendment) Regulations 2019, which are carrying on business in the UK. Moreover, for bank transfers, R.16 was implemented in the UK via the Funds Transfer Regulation (FTR), which now forms part of retained EU law. The government believes that the requirements set out in the FTR remain the right way to implement R.16. The proposal seeks to replicate the FTR's requirements for the crypto asset sector as much as possible. However, the proposal does not seek to expand the scope of the FTR to include crypto asset firms but to adapt certain necessary provisions of FTR. Crypto businesses will be given a grace period to integrate the amendment which will be made to the Money Laundering Regulation.

The consultation was open from July 22, 2021 to October 14, 2021, and the feedback is currently under review. Earlier, in January 2021, the HM Treasury had released another consultation seeking feedback on the UK's overall regulatory approach. Merkle Science discussed the scope and agendas of this consultation in its publication, A *Guide To The UK Regulations For Cryptoasset Businesses.*

Summarily, the January 2021 consultation paper sought to (a) protect financial stability and market integrity, (b) deliver robust consumer protections, and (c) promote competition and innovation, while supporting UK-based fintech firms. The paper also proposed several regulatory changes to strengthen the regime against illegal use of cryptocurrencies while making it agile and flexible to keep pace with the changing landscape. There's also a proposal to transfer the responsibility of detailing firm requirements from the HM Treasury to UK's financial service regulators who function on behalf of the

government. However, similar to the July 2021 consultation, the feedback for this one is also under review as of January 3, 2022.

5.1 The Financial Services Act 2021

On April 29, 2021, the Financial Services Act 2021 (FS Act) received Royal Assent to become the first law to implement a post-Brexit revamp of the UK's financial services framework. The goal of this act is to make the UK a progressive financial center, backed by technological advancements and green industries.

According to John Glen, Economic Secretary of the Treasury, *"For the first time in decades, the UK has full control of its own financial services regulation. This Act will protect people who rely on financial services day-to-day and boost the competitiveness of our dynamic global financial centre. It marks a major milestone in our plans to develop a regulatory regime that works for the UK and helps us seize new opportunities in the global economy."*

The primary implications of the FS Act for cryptocurrencies and digital assets concern updates to MLRs. By amending the Proceeds from Crime Act 2002 (POCA), the Act brings digital payments and payment service providers within the scope of the threshold amount provisions. Institutions are allowed to have certain interactions with criminal property without commiting an offence, as long as the value remains under the stipulated threshold amount.

The Act also amends the Crime and Security Act 2001 to provide regulators the authority to freeze digital currency accounts in genuinely applicable cases. Moreover, it amends the Sanctions and Anti-money Laundering Act 2018, enabling the government to enforce regulations on cross-border applications and overseas trustees.

5.2 FCA's Consumer Research Note 2021 & Temporary Registrations Regime Extension

Based on quantitative research conducted in phases since October 2018, the UK Financial Conduct Authority (FCA) published a report in June 2021. Its primary agenda is to analyze risks and benefits for consumers who interact with cryptoassets. The report mostly focuses on unregulated cryptocurrencies, such as Bitcoin, Ethereum, Ripple, and so on.

The report statedly follows increasing public and institutional interest in cryptoassets, as well as the growth in their market capitalization and prices. Ownership and awareness have also risen during the period of the research, and so have governmental focus along various flanks.

However, the overall level of understanding has been found to decline, implying that consumers are buying into crypto without much idea about what they are getting. According to FCA's observations, a majority of crypto users are middle-aged men, above 35 years of age. Some of the other key findings of the report are as follows:

- 78% of adults have some awareness about cryptoassets
- 38% of people are less likely to consider cryptocurrencies as a gamble and more likely to view them as alternative investments
- 29% of crypto holders regularly check their balances
- 46% of crypto users are not fully sure about the benefits

Besides publishing the Consumer Research Note, the FCA has been involved in another prominent regulatory event in 2021. On June 3, it announced the decision to extend the last date of the Temporary Registrations Regime (TRR) from July 9, 2021 to March 31, 2022.

The TRR's purpose is to provide temporary trading licenses to firms that have already filed for registration but are awaiting confirmation. However, the FCA notes in its announcement that several projects are withdrawing their applications as they fail to meet the standard of current MLRs. AML/CFT controls are a crucial point of consideration in this regard.

European Union (EU)

As of January 2022, the status quo for crypto regulations in the EU is that member countries individually legislate regulatory regimes, while following certain overarching guidelines. The FATF's intragovernmental standard for VASPs is one such guideline. The other is AMLD5, an EU directive issued in 2020 requiring VASPs to register with local regulatory authorities. However, neither of the two are statutes per se but are goals instead. The EU thus currently lacks a comprehensive regulatory framework binding on all of its twenty-seven members.

Taking cognisance of this situation, Markets in Crypto-Assets (MiCA) is formulating a regulatory package to be ratified soon, by 2023. The framework puts much emphasis on 'asset-referenced tokens' which is a variety of stablecoins backed by a 'basket' of multiple commodities, fiats, and/or crypto-assets. They are quite unlike the usual dollar-pegged stablecoins in this regard and resemble the concept that Facebook's infamous Libra token (now, Diem) originally adopted. So much so that according to Patrick Hansen, EU's RegTrax contributor, the proposal was in fact entirely designed with Libra (or its likes) in mind. Moreover, the proposed framework somewhat underplays the role and significance of DeFi, which is being held to its discredit.

Nevertheless, MiCA's package is expected to significantly enhance the ease of doing crypto-based business in the EU. To this end, it introduces a unified licensing procedure so that acquiring a license from any member-country suffices for the eligibility of operating in the others. In other words, licenses would be 'passportable' under MiCA's regime.

The MiCA framework thus contributes to the EU's overall strategy for Digital Finance, preparing it for the so-called digital age. And in all of this, MiCA relates to three types of assets: asset-referenced tokens, e-money tokens like USDT or USDC, and utility tokens like the Basic Attention Token (BAT). Furthemore, issuers of these tokens are required to publish and share their white papers to a local regulatory body for its approval. In view of this process, analysts like Hansen have claimed that compliance will be easy for VSAPs, but not cheap—white papers involve substantial investments, for one. Although plausible, these are speculative observations after all, and what comes of MiCA in reality remains to be seen.

6.1 Package Of Legislative Proposals: Strengthening AML/CFT Controls

On July 20, 2021, the European Commission announced a package of four legislative proposals aimed at reinforcing the EU's AML/CFT regime.

First, the package proposes a *"regulation of the European Parliament and of the Council establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) 1094/2010, (EU) 1095/2010."* This constitutes the Anti-Money Laundering Authority (AMLA) regulation whose prime objective is to establish a new, pan-EU regulatory authority. Besides coordinating national authorities, the AMLA will assist EU Financial Intelligence Units (FIUs) for better analytics and enforcements. Moreover, it will also be responsible for overseeing some of the riskiest financial institutions operating across the EU.

Second, the Commission calls for a "regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing." Known as the New Regulation on AML/CFT, this rule will unify the various AML/CFT regimes existing across the EU and implement stricter AML requirements. It will thus formulate comprehensive regulations for more granular methods of customer due diligence and legal person identification. The proposal also strives to clarify the powers and scope of supervisors and FIUs. Moreover, it defines certain provisions for 'obliged entities' through the following amendments:

- Including those crowdfunding service providers that existing regulations don't cover.
- Including mortgage and retail creditors, as well as non-financial or non-credit intermediaries.
- Including the legal representatives of third country nationals.
- Excluding retail commodity traders.

Additionally, the New Regulation on AML/CFT will explain and clarify the definition of *"Politically Exposed Persons"* (PEPs). It also intends to streamline and update the beneficial ownership requirements to include new provisions for nominees and foreign entities. Doing so will allow the Commission to ensure optimal regulatory transparency across the EU, while mitigating risks that commonly shelter criminals at the intermediate level. The proposal also provides for a clearer recording of suspicious transactions, while clarifying potential red flags. However, it does not alter the existing disclosure requirements and the method of private-to-private information sharing.

Third, it includes a "directive of the European Parliament and of the Council on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849." This is the 6th AML Directive (AMLD 6) that replaces the current AMLD 4 regime while transferring certain provisions to national laws. For example, currency exchanges, cheque cashing offices, and gambling service providers will be regulated by individual member countries. However, such regulations will come under the AMLA's oversight and standards.

Fourth, the package proposes a *"regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets (recast)."* The goal of this Revised Regulation on Transfers of Funds is to enhance the traceability of crypto-assets, besides limiting large cash payments. It has therefore introduced a limit of €10,000 on large cash payments, which is high enough not to put into question the euro as legal tender and recognises the vital role of cash while making it harder for criminals to launder dirty money. In addition, providing anonymous crypto asset wallets will be prohibited, just as anonymous bank accounts are already prohibited by EU AML/CFT rules. Through this proposal, the Commission brings Crypto-Asset Service Providers or CASPs under the purview of Regulation 2015/847. Moreover, it incorporates FATF's Updated Guidance into the EU's regulatory framework. And to this end, CASPs will be required to comply with the Revised Regulations by reporting for every transaction (a) the originator's name, (b) their account number, and (c) their address or customer ID.

The legislative package is under review at the time of writing, with the AMLA expected to be functional by 2024.

6.2 ESMA Report on Trends, Risks, and Vulnerabilities

On November 2, 2021, the European Securities and Market Authority (ESMA) released a comprehensive report analyzing the current risks and trends in the EU. According to this publication, the region's financial markets improved steadily since early-2021, often surpassing pre-COVID levels in terms of their valuation. Simultaneously, however, there's been a significant rise in risk-taking behaviors, leading to increased volatility in equities and crypto-assets.

The ESMA expects such risks to continue, particularly threatening institutional and retail investors, which calls for resilience and positive risk assessments. To this end, the report holds upcoming MiCA regulations in high regard due to its ability to enable interconnected risk analysis and management. But beyond that, the MiCA framework is significant also because of the high volatility associated with crypto-assets, particularly for those currently existing outside the EU's regulatory framework.

6.3 EU Digital Finance: MiCA and DORA Proposals

Earlier, we mentioned the EU's holistic strategy for Digital Finance. Now we elaborate on this aspect briefly, particularly focusing on MiCA and DORA proposals. The EU Council declared its position on these proposals on November 24, 2021, which is now its mandate for negotiations with the European Parliament.

DORA stands for Digital Operational Resilience, and it comprises the Digital Finance package along with MiCA and a Distributed Ledger Technology (DLT) proposal. Ensuring a robust and expansive regulatory framework that is also innovation-friendly is the primary goal of this package.

Slovenia's Minister of Finance, Andrej Šircelj, succinctly summarizes the scope and vision of the Digital Finance package. He says, *"Digital finance is an increasingly important part of Europe's economic landscape. It is essential to create a stimulating environment for innovative businesses while mitigating the risks for investors and consumers. I think today's agreement strikes the right balance between the two. Both files are a priority for the Presidency and we now hope for a quick agreement with the European Parliament on these proposals."*

The package is currently awaiting a political agreement between its negotiators. The EU Council and European Parliament will formally adopt the regulations once that is achieved.

Switzerland

Switzerland has one of the most favorable regulatory regimes in the world for crypto-assets and digital currencies. The Financial Market Supervisory Authority (FINMA) applies a 'same business, same rules' principle, thus focusing more on the type of business than the underlying technology. In 2021, FINMA moved to further enhance the Swiss regulatory framework, while the Federal Council legislated the Federal Act on the Adaptation of Federal Law to Developments in Distributed Ledger Technology, commonly known as the DLT Act. The law came into force in two phases—partly in February 2021, and the rest in August 2021—and it amended certain aspects of the existing Swiss law. Moreover, FINMA retained the token classification provided in its 2018 ICO Guidelines and applied them to the DLT Act.

- Amendments in February came into force first, as they enable the creation of ledger-based securities (uncertificated securities).
- The remaining provisions of the DLT Act concerning - the amendments to the Swiss banking regulation, financial market infrastructure regulation, and the anti-money laundering regulation entered into force on 1 August, 2021. These amendments created a new financial market infrastructure to enable multilateral trading of uncertificated securities.

Phase I: Enabling the Issuance of Ledger-Based (Uncertified) Securities

In the first phase, the Swiss Parliament enacted amendments to the Code of Obligations, the Federal Intermediated Securities Act (FISA), and the Federal Act on International Private Law. The main agendas for this phase was to lay the groundwork for ledger-based securities and to clarify the scope for ombudsman affiliations.

The DLT Act modified Article 973d et seq. of the Swiss Code of Obligations (CO) to include DLT Rights as a new asset-class. These rights are similar to certified or uncertified securities in traditional markets, and they apply to asset or utility tokens that imply claims against a certain issuer or third party. The Act, however, limits DLT Rights to particular ledgers and does not allow their interoperability. Both fungible and non-fungible contracts may be represented by these rights. Membership rights also fall in the domain of DLT Rights, but not cryptocurrencies and other factual assets.

The Act requires DLT Rights to be registered on the underlying ledger, which in turn must meet certain eligibility criteria. For one, the rights must be disposed only to the original holder and not to debtors. It must also protect the integrity and immutability of these rights through the use of resilient technology and organizational measures. The terms of DLT Rights must also be publicly accessible on the ledger's network.

DLT Rights are also consistent with the bindings of FISA, and can thus be utilized for creating book-entry securities. These may in turn be deposited with custodians who may credit rights to multiple accounts. However, the Act requires custodians to essentially freeze such securities, transferring them only in compliance with FISA.

As for ombudsman affiliations, the DLT Act relieves from this requirement entities that solely interact with institutional or professional counterparties. Similarly, financial institutions don't have to be affiliated to an ombudsman as long as they don't offer retail financial services.

Phase II: Bringing the DLT Act Fully into Force

The Parliament brought the remainder of the DLT Act into force on August 1, 2021, besides enforcing the associated blanket ordinance. The key point of this phase of implementation was to introduce a licensing regime for DLT Trading Facilities, which in turn brings forth financial markets for DLT Securities. To this end, the DLT Act amends the Financial Market Infrastructure Act (FinMIA) to include DLT Trading Systems as a new form of financial market infrastructure. It also formulates a new license

category for distributed ledger-based securities.

One of the most distinguishing features of the DLT Act is its provision for crypto-asset segregation in the event of bankruptcy. Claims over bankruptcy proceedings are justified when the debtor has a contractual obligation to make assets readily available, and the custodian has exclusive powers for the assets' disposal. They are also justified when a third-party has a clearly identifiable share of community assets. The DLT Act amends the Federal Act on Debt Collection and Bankruptcy to enable this provision.

Moreover, it amends the existing Swiss Banking Act (SBA) to accommodate the implications of the bankruptcy provision, besides expanding the standing scope of the Fintech license. On this note, it's worthwhile to note that the Swiss National Bank supervises DLT Trading Systems under the statute of the National Bank Act.

Finally, the DLT Act adapts the Swiss Anti-Money Laundering Act (AMLA) and the Anti-Money Laundering Ordinance (AMLO) to ensure robust AML/CFT controls for crypto-based platforms and businesses. Moreover, as per FINMA's standing ordinance, the Travel Rule applies to financial intermediaries and the blockchain-based transactions they facilitate. The AMLA involves a non-exhaustive list enumerating instances and activities to be considered intermediation, which allows for greater regulatory clarity.

Singapore

Singapore has a robust yet progressive regulatory framework, similar in character to that of Switzerland. The Island nation is gradually transforming itself into a Smart Financial Center, thus emerging as a leader in the global fintech revolution. The Payment Services Act of 2019 (PSA) is Singapore's primary statute for crypto-assets, duly implemented by the Monetary Authority of Singapore (MAS). Businesses dealing in crypto-assets can function smoothly and freely within this framework, which is a significant catalyst for innovation.

Merkle Science recently elaborated on these above aspects, and more, in its *Guide to the Singapore Regulations for Cryptoasset Businesses*. This publication serves to provide a regime's comprehensive view to its readers. And thus, we currently focus only on the prominent events that have occurred since this guide.

8.1 The Independent Reserve's In-Principle Approval

The MAS provided in-principle approval to Independent Reserve, Australia's leading crypto-exchange, on August 2, 2021. Thanks to this approval, the exchange platform will be able to offer digital payment services in compliance with the PSA.

Interestingly, Independent Reserve became the first VSAP to acquire in-principle approval in Singapore. Per the current regime, adequate due diligence, effective solicitation, and optimal risk assessment are key determining factors for approvals and licensing. As Adrian Przelozny, Independent Reserve's CEO, puts it, *"To be one of the first cryptocurrency exchanges to be notified by MAS of our in-principle licencing approval is a reflection of the robustness of the policies, procedures and risk management systems that we have put in place to guide our day-to-day operations."*

8.2 DBS Vickers' In-Principle Approval

On October 1, 2021, the MAS formally approved DBS Vickers (DBSV) to serve and assist asset managers and businesses to trade digital payment tokens on the DBS Digital Exchange (DDex). DBSV is the brokerage arm of the DBS Bank, and following the approval, is to be reckoned a Major Payment Institution in Singapore.

The DDex originated as a member-only exchange in December 2020, when it garnered substantial interest among its user base which included corporate actors and institutional investors. Thanks to the approval, the platform now expects to grow at 20-30% per annum over the next three years.

In the words of DDex's Chairman, Eng-Kwok Seat Moey, *"Having received formal regulatory approval from MAS, DBSV is now in a better position to support institutional and corporate investors in tapping into the growing potential of digital assets as an investment class. This marks another significant milestone in our ability to provide integrated solutions across the digital asset value chain, from deal origination to tokenization, listing, trading and custody. We believe that DBSV's licence, coupled with recent enhancements to DDEx such as round-the-clock operations since August, could add to DDEx's volumes in the coming months and accelerate growth momentum for DBS' digital asset ecosystem."*

8.3 Investor Alert For Binance

Binance made it to MAS's Investor Alert List, joining other unregulated exchanges that have the deceptive appearance of being licensed or regulated in Singapore. By offering its services in Singapore, Binance was also deemed to have violated the PSA, and was thus received the order to stop the concerned operations.

The listing happened in September 2021. However, earlier, in July 2021, MAS had announced that Binance's license application was under review and that the regulator would 'follow up' with the exchange. Agreeing to work closely with MAS, Binance subsequently appointed experts like Richard Teng to spearhead its operations and regulatory procedures in Singapore.

South Korea

9.1 Act on Reporting and the Use of Specific Financial Transaction

On March 25, 2021, South Korea enforced the amendments to the Act on Reporting and the Use of Specific Financial Transaction. The amendment imposes information-reporting and anti-money laundering obligations on VASPs.

The amendment applies to VASPs who engage in one or more of the following commercial activities or procedures:

- The purchase and sale of virtual assets
- Transfer of virtual assets
- Safekeeping and administration of virtual assets
- Intermediation or brokerage of virtual asset transactions
- Exchanges between virtual assets
- Other activities specified by the enforcement degree

Under the amendment, VASPs have to establish robust AML/KYC procedures using a risk-based approach, which includes conducting customer due diligence and suspicious transaction reporting. VASPs are also required to implement a technical solution, which permits the exchange of their identifying information with the counterparties involved in a transaction.

Further, VASPS have to acquire the Information Security Management System (ISMS) certification from the Korea Internet & Security Agency (KISA). The ISMS certification is given by KISA to those VASPs who meet the government standards for the protection of the personal information of their users.

The amendment mandates VASPs to secure a contract with local banks to provide withdrawal and deposit accounts for their users, under their real names. Those VASPs owners, who do not have an authorized bank account, will either have to pay a 50 million South Korean won fine or face a 5-year prison sentence.

Additionally, individuals holding an executive position at a VASP must not have any financial crime-related charges in their background within the past five years.

9.1.1 Travel Rule requirements

Both domestic and foreign VASPs have to register with FIU and comply with the Travel Rule requirements by March 25, 2022. To get their registration approved, VASPs are also required to submit certain details to the FIU such as the official name of the VASP, location, and place of business, contact information, and bank account details.

The threshold for the Travel Rule compliance is one million South Korean won. Under the Travel Rule requirement, VASPs have to collect, identify, and verify the following identifying information of the customer for due diligence:

- Name
- Identification number
- Address and contact information
- Nationality

In August 2021, Korea's three top cryptocurrency exchanges — Bithumb, Coinone, and Korbit —launched a joint venture to co-develop solutions for the Travel Rule system known as Connect Digital Exchanges (CODE). Additionally, to ensure compliance with the Travel Rule requirements and to reduce the risk of money laundering, in December 2021, Coinone announced that it would reject deposits from unverified private wallets starting January 24, 2022. Twenty other Korean exchanges including Upbit, Bithumb, and Korbit, \are expected to implement similar or identical measures.

Barring the Travel Rule requirements, VASPs had to become fully compliant with all the other provisions of the amendment by September 2021. Only four major exchanges — Upbit, Bithumb, Coinone, and Korbit — were able to fully comply with the new regulations. Around 36 exchanges were shut down, while 25 other exchanges that had acquired the ISMS certification but not the

real-name bank account contract were granted leeway to continue operation; however, these exchanges could provide only token-to-token exchange and not fiat-to-crypto services, while the FIU reviewed their reports. Finally, the FIU approved 16 exchanges — 4 fully functioning exchanges and 12 token-to-token exchanges — while 13 exchanges without the bank partnership await their result.

Japan

10.1 Travel Rule Requirement: Japan's Financial Services Agency (FSA) announced on March 31, 2021, that it will implement FATF's Travel Rule. The Travel Rule will be enforced in Japan from April 2022.

Japan Virtual Currency Exchange Association (JVCA) — a self-regulatory body charged with creating rules and policies applicable to crypto exchanges in Japan — is responsible for implementing the Travel Rule regulation. On March 31, 2021, the FSA issued a Request for Notification of Originator and Beneficiary Information upon Crypto Assets Transfer to JVCA, requesting JVCA to enact rules for enforcing the Travel Rule Regulations. These rules will require the originator's crypto-asset exchange providers (CESPs) to collect identifying information of the originator and beneficiary upon the transfer of virtual assets and give notice of such information to the beneficiary's CESP. Hence, CESPs in Japan will have to share user date with each other but not with the regulators.

10.2 Crypto derivatives: In October 2021, crypto exchange Huboi 's Japanese Subsidiary — Huboi Japan, Inc — received approval from FSA to offer crypto derivatives. Presently, only 7 out total 34 crypto exchanges have received such approval from the FSA.

In order to operate a trade, underwrite, and manage crypto derivatives and operate as a derivative trading system, CESPs have to register as a Type I Financial Instruments Business with the FSA, as designated under the Financial Instruments and Exchange Act. This essentially means that the CESPs have to fulfill the same stringent regulatory requirements as financial institutions. To register, firms must have a stated capital of at least 150 million yen($466,000), net assets of at least 50 million yen, and a capital-to-risk ratio of over 120%. Without this license, the cryptocurrency exchanges may only offer limited spot trading services of cryptocurrencies for customers.

10.3 Tax Plan 2022: On December 10, 2021, Japan's ruling coalition — Liberal Democratic Party and Komeito coalition — approved the official tax plan for the 2022 fiscal year. Under the tax plan, the token listing including the listing of crypto assets will continue to be taxable. Post the listing of tokens on an active market, token issuers will be required to pay taxes on all listed tokens even those tokens which are not sold.

A project that lists some of its tokens on exchanges and keeps the rest in its treasury, will also have to pay taxes held in the treasury if the market value of the tokens go up. If a project is unable to pay the required taxes it will be forced to sell more of its token to the public market, adversely affecting both the token price on the one hand and the profitability and growth of the project on the other hand. As a result, a number of crypto platforms, including Astar Network — a multi-chain Decentralized Application —have dissolved their entities in Japan and moved to other countries.

10.4 Stablecoin Law: According to news reports, the FSA will introduce new legislation in 2022, which will limit the issuance of stablecoins to banks and wire transfer companies. The FSA is also all set to toughen regulations meant to prevent money laundering. Under the new regulations, intermediaries like wallet providers involved in stablecoin transactions and management will be brought under the agency's oversight. They will also be required to meet obligations under the Act on Prevention of Transfer of Criminal Proceeds, these obligations include verifying user identities and reporting suspicious transactions. The new legislation is being enacted to protect consumers from potential risks surrounding asset-backed stablecoins.

10.5 Japan's Central Bank Digital Currency (CBDC): A consortium of 74 Japanese firms is working towards issuing digital yen, according to the white paper and progress report published by DeCurret — the consortium's secretariat. The Consortium is supervised by the Bank of

Japan, the FSA, and three other ministries.

The members of the consortium include banks such as MUFG Bank, Sumitomo Mitsui Banking Corp., Mizuho Bank, Japan Post Bank, and industry leaders ike the Nippon Telegraph & Telephone Corp., East Japan Railway, and Mitsubishi Corp., as well as local governments. The consortium is proposing a model similar to bank deposits for digital yen. The digital yen will be issued by banks as their liability, thus, ensuring the stability of the digital currency. Further, the consortium will also be releasing a beta version of the digital currency marketplace for non-fungible tokens (NFTs) by 2022.

Hong Kong

11.1 Legislative Proposals to Enhance Anti-Money Laundering and Counter-Terrorist Financing Regulation

Following the public consultation conducted by the Hong Kong Financial Services and Treasury Bureau (FTSB) from November 2020 to January 2021 outlining the legislative proposals to enhance AML/CFT regulation in Hong Kong, on May 21, 2021, the FTSB published a consultation conclusion on the Legislative Proposals to Enhance Anti-Money Laundering and Counter-Terrorist Financing Regulation.

Under the proposed framework, VASPs will only be allowed to offer their services to professional investors. Professional investors are defined as individuals with a portfolio of over HK$8 million (US$1 million) or companies with more than $5 million in total assets. Other than professional investors, Hong Kong's Securities and Futures Commission (SFC) regulated fund managers can invest up to 10% of their gross asset value in crypto and can apply for a special license if they wish to invest more.

The SFC also seeks to establish a new licensing regime for certain types of VAs falling under Hong Kong's Securities and Futures Ordinance — an ordinance that consolidates and amends the law relating to financial products and the securities and futures market.

The proposed framework covers, *"any person seeking to engage in the business of operating a virtual asset exchange in Hong Kong".* In essence, it applies to any crypto business that performs the following commercial activities:

- The selling or buying of cryptocurrencies
- Facilitating the transfer and exchange of crypto

The proposed framework mandates crypto businesses to acquire the SFC license, those crypto businesses that are unable to obtain the said license on time will be prohibited from actively marketing themselves to the public. To obtain an SFC license, crypto businesses must fulfill the following three conditions, firstly, they must be incorporated in Hong Kong. Secondly, they should meet the requirements of the 'fit and proper test that involves criminal background checks, AML/CFT performance history, and financial standing and lastly, they have to appoint at least 2 officers who will be responsible for overseeing compliance.

The proposed framework allows crypto businesses to cater only to certain types of customers such as professional investors; however, before providing the services they have to meet certain regulatory requirements such as implementing robust AML/CFT measures, record-keeping rules, a mechanism for reporting suspicious transactions, and conducting

Offense	Punishment
Operating without a license	• Fine: up to $5,000,000 • The senior management can also face imprisonment up to 7 years • In case of a continuing offense, an additional fine of $100,000 for each day the offense continues
Provision of false, deceptive, or misleading statements about a business's compliance status when filing a license application	• Fine: up to $1,000,000 • Senior management may face imprisonment up to two-year
Violation of AML/CFT requirements	• Fine: up to $1,000,000 • Senior management may face imprisonment up to two year

customer due diligence. Additionally, they also have to follow certain regulations related to the management of financial resources, for example, financial reporting and prevention of market manipulation. To ensure market integrity and ensure investor protection, crypto businesses will also have to comply with present and future SFC guidelines. They will have to introduce strict criteria for deciding, which VAs can be traded on their platform.

If a crypto business fails to meet the requirements set out in the proposed framework, it may either be liable to pay a certain fine or face imprisonment or both.

It’s expected that the new licensing regime for crypto businesses will be introduced in the 2021-22 legislative sessions, which runs from October 2021 until the summer recess in July 2022.

Australia

In October 2021, the Australian Senate on — Australia as a Technology and Financial Centre — recommended a set of new rules to establish a regulatory framework for crypto assets.
The Senate, in the proposed framework, made some key recommendations including:

- Establishing a market licensing regime for Digital Currency Exchanges (DCE), including capital adequacy, auditing, and responsible person tests under the Treasury portfolio.
- Establishing a custody or depository regime for digital assets with minimum standards under the Treasury portfolio.
- Conducting a token mapping exercise in order to categorize various types of crypto assets and other digital tokens
- Establishing a new Decentralised Autonomous Organisation (DAO) company structure.This new legal structure will give DAOs a separate legal identity, with DAO token holders given limited liability
- The senate will also clarify the AML/CFT regulations to ensure that they are adequate, do not undermine innovation, and give consideration to the driver of the Financial Action Task Force 'Travel Rule'.
- In order to increase certainty and transparency around de-banking, the Australian Government will develop a clear process for businesses that have been de-banked.

12.1 Treasurer of Australia announces a new crypto regulatory regime

- In December 2021, Australian treasurer Josh Frydenberg announced new payment systems regulations. These new regulations seek to broaden the definition of services and products that can be regulated — crypto assets will now be regulated as payment systems. To ensure consumer protection, crypto platforms that facilitate buying and selling of crypto assets will have to get licensed with Australian financial regulatory authorities. The government will release a new licensing plan for crypto exchanges in 2022. In addition, the treasury will also join hands with the Australian Central Bank to work on the Australian CBDC. Further, the payments systems regulation also seeks to regulate “buy now, pay later” services such as Amazon Pay.

Conclusion

As digital currencies and crypto-assets boomed in 2021, regulators stepped up their game to safeguard investors and ordinary customers from financial crimes, hacks, and frauds that rose simultaneously. The stakes grew higher as more and more money flowed into the burgeoning industry. And so did the responsibility of various regulatory authorities around the globe.

Rising up to the challenge, the FATF issued updated and revised guidelines to curb money laundering and terrorist financing at the international level. While doing so it also rallied for greater regulatory clarity. Individual nations followed the cue, legislating timely and progressive regimes to mitigate actual and potential risks.

As always, the U.S. saw most activity on the regulatory front, with laws and amendments at the federal and state levels. Crypto ETFs started trading as well, which was a high point for the industry's growth and maturity. The much-needed comprehensive crypto bill was also introduced in the U.S., as it was in the EU. The UK, as well, adopted a holistic approach towards regulating crypto-assets.

Switzerland prevailed as the hub for business-friendly but robust regulatory regimes, while Canada legislated for greater clarity in its framework. Singapore, at the same time, witnessed a mix of positive and negative actions, while remaining a preferred destination for global crypto-based businesses. And with that, we begin another year where several regulatory enhancements are charted and upcoming in key jurisdictions around the world. How things pan out and what comes of them, is something that remains to be seen.

Contact Us

contact@merklescience.com

Follow Us

merklescience @MerkleScience merklescience Merkle Science