The Bretton Woods Committee

No. 7 • JULY 2023

This brief is part of a series produced by the Digital Finance Project Team (DFPT) of the Bretton Woods Committee's Future of Finance Working Group (FFWG)

Security Issues with Crypto—The Bank Secrecy Act, Anti–Money Laundering, and Countering the Financing of Terrorism

By Jonathan Everhart, Mahesh Kotecha, and Kunal Thakur

INTRODUCTION

The rise of crypto assets has ushered in significant financial and technological advancements for the global financial system. As with any emerging financial innovation, such advancements can be used for both legal and illegal purposes. One main area that has surfaced is the use of crypto assets in money laundering (ML) and the financing of terrorism (FT). In 2022, approximately $23.8 billion of cryptocurrency was sent through illicit crypto addresses, which represents a 68.0 percent increase over 2021.[1]

In traditional finance (TradFi), financial institutions are required to take action to help identify and mitigate ML/FT activities. This is accomplished through the enactment of global standards on anti–money laundering (AML) and countering the financing of terrorism (CFT) for financial institutions around the world, which include maintaining records of transactions, submitting reports of transactions exceeding certain thresholds, identifying and evaluating customers (which entails following Know Your Customer [KYC] rules), and reporting suspicious activities that may be deemed ML/FT. Because such measures make it increasingly difficult for criminals to conceal illicit activities through conventional TradFi, crypto assets offer a new way for criminals to conceal ML/FT activities.

But AML/CFT practice is being extended to crypto assets. Why is this important? Crypto asset AML/CFT involves the application of standards and regulations to limit and mitigate the use of crypto assets in money laundering and financing of terrorism activities. This is important because crypto assets have become useful mechanisms for such illicit activities. Improving security in crypto assets through effective AML/CFT standards and regulations is vitally important to protect investors and encourage public trust in crypto markets. What we mean by security in this context is having effective AML/CFT compliance measures to protect against the use of crypto assets for money laundering and the financing of terrorism.

The path to trust in crypto leads through security, just as security issues in AML/CFT are a core pillar in TradFi. Security is critical for the crypto sector across products,

services, policies, and practices for the sector to gain global adoption. TradFi provides comprehensive and global AML/CFT standards via the Financial Action Task Force (FATF), which the G7 countries established in 1989 to analyze and develop measures to combat money laundering.[2] There are also similar risks in crypto. However, effective and broad-based adaptation is necessary to address the key new risk elements unique to crypto. The FATF updated its standards in 2018 to cover crypto assets[3] and crypto asset service providers.[4] Through that proactive step, regulators have answered the initial question on whether the crypto industry should be subject to AML/CFT regulation—the recent FATF report shows that more than 70 percent of the 38 FATF member nations have incorporated AML/CFT regulations for crypto into their domestic law and are now seeking to accelerate enforcement of the regulations.[5] Implementation across the wider FATF Global Network of jurisdictions is also slated to increase considerably.[6]

Although there has been progress, the global AML/CFT regime for crypto is inadequate in its overall implementation and enforcement. It is critical to ensure that the current AML/CFT regime for crypto be implemented effectively and enforced globally given the risks unique to crypto. To address this problem, we identify and suggest how to mitigate some of the important gaps in AML/CFT crypto regulations. The key risks and some critical risk mitigation tools/actions to close the gaps and make implementation, enforcement, and evolution of global AML/CFT regulations for crypto more effective are summarized below.

Summary: AML/CFT Crypto Risks

Problem/Gap	Solution
1. Regulatory gaps in the implementation of global AML/CFT standards for crypto	• Collaborate with the FATF and other multilateral forums to (a) support addressing the regulatory gaps in AML/CFT regulation and supervision across international jurisdictions including via grey-listing and (b) mitigate jurisdictional arbitrage. • Accelerate the FATF's work on crypto assets, which is focused on encouraging multilateral implementation and enforcement of the FATF standards for crypto assets and service providers. Organizations like the Egmont Group provide a platform to securely exchange expertise and financial intelligence to support this.
2. Lack of enforcement of implemented AML/CFT standards for crypto	• Improve the enforcement of current AML/CFT regulations within the crypto sector through compliance exams, enforcement investigations, and prosecutions—including public enforcement actions and penalties to deter future illicit acts. • Provide training via professional financial educational bodies for entities to learn more about AML/CFT regulations in the crypto sector. • Utilize decentralized finance (DeFi) monitoring and enforcement technologies that are offered by companies like Chainalysis and Elliptic.
3. Use of anonymity-enhancing technologies	• Utilize KYC processes and encourage digital identity solutions to ensure compliance with privacy laws and AML/CFT requirements.

4. Peer-to-peer (P2P) transactions	• New technologies and regulations should be evaluated for their ability to minimize illicit activity risks from smart contracts, DeFi services, and other P2P mechanisms. • Establish effective regulations for P2P transactions that will require regulators to deploy new technologies and other mechanisms to track and understand the unique ML/FT risks in P2P transactions.
5. Noncompliant crypto asset service providers	• Strengthen engagement with crypto asset service providers and other entities to better inform them of any necessary AML/CFT compliance responsibilities. • Conduct engagement activities on AML/CFT compliance and tools to promote adherence; issue ongoing updated guidelines, alerts, and other publications; and organize public–private information-sharing events, like the Bank for International Settlements' G20 TechSprints. • Consider mechanisms to blacklist, sanction, and selectively block noncompliant service providers.
6. Lack of integration of AML/CFT controls in crypto creation	• Explore how a crypto asset can be designed to enable and incorporate the use of AML/CFT controls to improve code security in mitigating illicit finance risks. • Align crypto asset code in accordance with global standards such as ISO 20022 as a way to combat ML/FT. • Improve cybersecurity corporate governance to mitigate the security code risks in crypto.

THE CURRENT STATE OF AML/CFT CRYPTO REGULATION

The FATF establishes important global AML/CFT recommendations, and countries adopt the recommendations into their own regulatory frameworks. The updated FATF framework for crypto requires that crypto asset service providers be regulated for AML/CFT purposes, licensed or registered, and subject to effective systems for monitoring and supervision.[7] The FATF has made it clear that its AML/CFT standards apply to crypto asset service providers that offer exchanges between a fiat currency and a cryptocurrency or between cryptocurrencies, in addition to transfers, administration and safekeeping, and participation in and provision of financial services related to the offer and/or sale of crypto assets.[8]

The objective of the FATF's 2019 and 2021 updates is to help regulators, supervisors, policymakers, and other country-specific authorities understand and develop regulations for crypto activities and service providers and to aid private sector entities in understanding their AML/CFT obligations and how to comply with them in engaging in crypto activities. Accordingly, the updates enhance the framework using a risk-based approach to crypto activities and service providers. The framework provides for supervision and monitoring of crypto asset service providers for AML/CFT purposes; licensing or registration; customer due diligence, recordkeeping, and suspicious transaction reporting; sanctions and other enforcement measures; and international cooperation.[9]

At the moment, despite clear recommendations from the FATF, differences in regulatory approaches to AML/CFT between countries, including some countries that have not adopted any regulations, have likely caused slower adoption by the traditional banking industry and nonbank financial institutions (among other reasons is a lack of prudential frameworks in countries

and jurisdictions). But there are signs that institutional adoption of blockchain technology itself is growing.[10] While the principle of "same activity, same risks, same regulation" is deceptively simple, its execution is not so clear-cut and is not fully in place. Moreover, the decentralized structure of crypto assets poses a heightened risk that even small gaps or laxity in regulation in one jurisdiction with limited supervisory resources could spawn global crypto activity with risks of contagion, and there is some potential for significant systemic risks given the limited capacity for timely regulatory or legal recourse.[11] Twenty-eight of the 38 FATF member nations have implemented AML/CFT regulations for crypto.[12] However, the rate and extent of regulatory adoption must increase more rapidly to jurisdictions with no or limited rules in place while also broadly incorporating regulations that mitigate the unique risk elements of crypto. Delaying adoption will increase and could entrench the unregulated and potentially illicit use of crypto assets in ML/FT activities and further undermine public trust in crypto markets.[13]

AML/CFT KEY RISKS AND RISK MITIGATION TOOLS AND ACTIVITIES

Many gaps remain in addressing the key AML/CFT risks associated with crypto, notably these:

1. Regulatory gaps in the implementation of global AML/CFT standards across borders
2. The lack of enforcement of AML/CFT standards already adopted
3. The use of anonymity-enhancing technologies designed to escape regulation
4. The use of peer-to-peer (P2P) transactions
5. Crypto asset service providers that are noncompliant with AML/CFT regulatory requirements
6. The lack of integration of AML/CFT controls into the creation of crypto assets

Regulators can and should more effectively promote the adoption of the global FATF AML/CFT standards for crypto assets within their jurisdictions. Certain aspects regarding AML/CFT compliance and enforcement call for clarifications or new requirements that conform to the unique components of crypto assets and crypto asset service providers, such as AML/CFT compliance requirements for P2P transactions and building AML/CFT controls into token creation. Better regulation would help reduce the risks of illicit financing posed by crypto.

1. Regulatory Gaps in the Implementation of Global AML/CFT Standards for Crypto

Regulatory gaps enable crypto asset service providers to engage in regulatory arbitrage, as they may register in one country and provide services across other jurisdictions with different AML/CFT regulation and supervision frameworks unless restricted or barred by national firewalls from doing so. In many instances, varying jurisdictions have in place weak or nonexistent AML/CFT requirements and illicit activity detection methods.

Regulatory gaps lead to inadequate customer and transaction information across multiple jurisdictions, which increases ML/FT risks. Clarity is lacking regarding which crypto asset service providers or entities involved in cross-border transactions are subject to AML/CFT requirements. Furthermore, this lack of clarity extends to countries that are responsible for regulating and monitoring those service providers or entities for compliance with AML/CFT requirements. For instance, the FATF has conducted two annual reviews to analyze the status of the revised FATF standards on crypto assets and service providers. For the second annual review in June 2021, FATF issued a questionnaire to its member jurisdictions regarding their individual implementation of AML/CFT regulations for crypto. Of the 128 jurisdictions that responded,[14]

- 58 jurisdictions reported that they had introduced the necessary regulation to implement AML/CFT regimes for crypto asset service providers, with 52 jurisdictions permitting crypto asset service providers to operate and six jurisdictions prohibiting these service providers;[15]
- 26 jurisdictions reported that they were in the process of enacting the necessary regulations to

regulate crypto asset service providers, with all 26 jurisdictions permitting these service providers;

- 12 jurisdictions reported that they had decided on their approach for AML/CFT regulations for crypto asset service providers but had not yet commenced the necessary regulatory process, with six jurisdictions planning to permit crypto asset service providers and six jurisdictions prohibiting them; and
- 32 jurisdictions reported that they had not yet decided on their approach for AML/CFT regulations for crypto asset service providers, which means these jurisdictions had no AML/CFT regulatory regime and had not commenced the regulatory process to implement one.

As regulatory adoption continues to progress, it is important for regulators and standard setters like the FATF to work with the crypto industry to reduce regulatory gaps across jurisdictions. The regulatory gaps between those jurisdictions that have decided to permit crypto asset service providers to operate and others that have not is a primary area of concern that should be assessed and mitigated. The goal of such collaborative efforts is to avoid creating unintended consequences in the form of regulatory gaps within and between jurisdictions or disparities that open opportunities for regulatory arbitrage within and across jurisdictions, actors, and crypto assets that are certain to be exploited.

Regulators should continue collaborating with the FATF, other multilateral forums, and the crypto asset industry to address the gaps in AML/CFT regulation and supervision across international jurisdictions. To ensure cross-border alignment in adopting and enforcing the global AML/CFT standards for crypto assets and crypto asset service providers, such efforts should be supplemented by bilateral engagements, including information sharing and capacity building. The FATF's work on crypto assets is also focused on encouraging multilateral implementation and enforcement of the FATF standards for crypto assets and crypto asset service providers through organizations like the Egmont Group. The Egmont Group provides financial intelligence units (FIUs) with a global platform to securely exchange expertise and financial intelligence to combat money laundering, terrorist financing, and related illicit crimes.[16] Such efforts to update and enhance global FIU community standards, as well as to ensure their implementation and effective dissemination, to mitigate jurisdictional arbitrage must be accelerated.

FATF member nations should urgently create planning and coordinating mechanisms at leading international forums—including the World Bank and the International Monetary Fund—to aid in the global implementation and enforcement of AML/CFT standards and best practices for crypto assets and service providers. For example, progress has been made in "travel rule" technology development that can serve as a global best practice. The travel rule requires that crypto asset service providers obtain, hold, and exchange information between each other regarding the sender and recipient of a crypto transaction. The information, which includes the identity of both the sender and the recipient, allows for screening against sanctions lists and other financial crime watch lists. Several standards and protocols have been launched and/or are being developed to help enable interoperability and to identify crypto asset service providers in order to exchange data for compliance with the travel rule.[17] However, in countries where no regulations addressing the travel rule are in place, crypto asset service providers are likely not using these solutions. The FATF notes that the private sector has made progress in the development and use of technological solutions to facilitate implementation, particularly for domestic transactions and transactions between crypto asset service providers. But their implementation has been slow and uneven.

2. Lack of Full Enforcement of Implemented AML/CFT Standards for Crypto

From the FATF's recent review of the revised FATF standards on crypto assets and crypto asset service providers, 28 of the 38 FATF member nations reported having now incorporated the revised FATF standards into their domestic laws.[18] However, challenges still

remain. Many jurisdictions' AML/CFT regimes for crypto asset service providers are not yet operational for enforcement, while some jurisdictions have not yet established such regimes—particularly those amongst the FATF's broader Global Network. For comparison, in TradFi, the travel rule is implemented and enforced through multiple payment networks, the most notable being the SWIFT system. The implementation and enforcement of the travel rule for crypto has been slow, despite the FATF's increasing pressure on its member countries to accelerate the rule's adoption and its enforcement within their regulations.

Regulators, supervisors, law enforcement, and other relevant competent authorities can improve the enforcement of current AML/CFT regulations within the crypto sector through such steps as compliance exams, enforcement investigations, and prosecutions. Public enforcement actions and the resulting penalties for failing to comply will promote awareness and the importance of AML/CFT compliance by crypto asset service providers. Public enforcement can also deter future attempts to circumvent regulatory obligations. Professional financial educational bodies (such as the Chartered Financial Analyst Institute [CFA Institute], the Chartered Alternative Investment Analyst Association [CAIA Association], and bankers' training programs) can be encouraged to require those being trained to learn more about AML/CFT regulations in the crypto space at a general level to increase market awareness and sensitivity to such risks.

To aid enforcement in decentralized finance (DeFi), regulators should issue clearer and more frequent guidelines, alerts, and related publications on AML/CFT standards and best practices. Such resources generally highlight troubling patterns and advances in ML/FT activities for regulated entities to monitor within their compliance programs. Additionally, maintaining sanctions lists of individuals, groups, and entities is also a good enforcement tool to facilitate the screening and banning of blocked individuals, groups, and entities and associated transactions. Although these tools offer support, regulators need to develop more capacity and build confidence in using such tools to properly monitor and enforce AML/CFT rules for crypto.

Incorporating technologies that suit the unique elements of crypto can play an important role in assisting regulators. Several monitoring and enforcement technologies are offered by companies like Chainalysis and Elliptic. For example, Chainalysis allows users to trace funds across multiple assets in a single graph, which includes identifying on- and off-ramp addresses and swapping activity to counteract attempts to obfuscate the flow of funds.[19] Elliptic's Investigator is a blockchain investigation tool that enables users to see and explore specific crypto addresses, transactions, and entities, and links them to real-world actors across thousands of assets.[20] Use of solutions like these can enhance the capacity and confidence of regulators in the enforcement efforts that are unique to crypto. Chainalysis, Elliptic, The Blockchain Association, and other industry-leading organizations should continue to provide solutions and best practice guidelines for regulators and others to consider in implementing and enforcing AML/CFT regulations.[21]

Additionally, the DeFi industry will need to take up the issue of AML/CFT more proactively as the decentralized nature of much of the ecosystem presents a unique challenge for regulators to address without industry collaboration. DeFi systems are not subject to the same level of centralized control and supervision as centralized finance or TradFi systems. As such, the DeFi industry will need to develop its own set of best practices and standards, in conjunction with FATF standards, to ensure compliance with AML/CFT regulations. This could involve developing self-regulatory frameworks and working with regulatory authorities to develop new and improve existing rules specifically tailored to the DeFi ecosystem. The regulatory community can do its part by providing clear guidance and support, as FATF has begun to do. Ultimately, it will be up to the DeFi industry to take responsibility for ensuring compliance with AML/CFT regulations. Failure to do so could lead to increased regulatory scrutiny and reputational harm to the DeFi ecosystem, which could stifle global adoption.

3. Use of Anonymity-Enhancing Technologies

Public blockchains, blockchain forensics, and financial analytics have enabled broader investigations into illicit financial flows. As a result, certain crypto assets—called privacy coins or anonymity-enhancing coins (AECs)—have been specifically designed to be fully anonymous, such as Monero. AECs allow for greater transaction anonymity than asset transfers conducted using Bitcoin or the Ethereum network. AECs, which still make up a relatively small industry as compared to the broader crypto industry, use cryptographic methods to obscure transaction details that would normally allow for the tracing of financial flows on the blockchain. Crypto addresses are easy to generate in large numbers. To escape detection, many protocols encourage users not to deploy an address more than once and can rapidly generate thousands of new addresses. Even if a protocol has a complete record of transactions, the identity of the person behind the transactions cannot always be established unless that person uses tokens or wallets to transact with an entity (such as an exchange) that does enforce KYC norms and provides a digital identity, as regulated financial institutions do in TradFi.[22] This hampers the collection and enforcement of taxes, permits money laundering and other forms of financial malfeasance or crime, and undermines confidence in crypto assets.

Criminals are increasingly embracing technologies that increase anonymity and disguise the source of funds, such as better cryptography or use of an opaque blockchain. Crypto asset service providers that offer anonymizing services, such as mixers and tumblers,[23] act as money transmitters by accepting and retransmitting crypto assets to hide the identity of the source up the chain. If they fall under the definition of money transmitters, anonymizing service providers should be subject to AML/CFT regulatory reporting requirements in spotting and reporting suspicious activities and should be subject to cease-and-desist orders and/or subpoena power of the relevant regulators.[24]

Technological innovations offer solutions to the crypto sector to automate KYC and assign digital identities and verifiable credentials while ensuring compliance with privacy laws and AML/CFT requirements.[25] There are growing attempts to create digital IDs for crypto activities, but they may or may not operate with or rely on blockchain technology and are far from universal.[26] Crypto asset service providers should be implementing KYC for all customers, as these service providers are able (if willing) to conduct traditional KYC, customer due diligence, and enhanced due diligence to onboard customers similarly to TradFi. Digital identity could be a more effective and efficient way to do that but is neither required nor unique for the crypto industry. TradFi institutions are also looking to incorporate digital identity solutions. The development of such digital IDs should be encouraged. In the meantime, some jurisdictions may decide to permit only those crypto asset transactions that are carried out within the regulatory ambit of the TradFi system. Such regulatory permissions can be issued not only to currently regulated institutions but also to crypto banks provided that they have adequate and well-managed reserves and the stablecoins they issue (if any) are designed to ensure that the identities of transaction parties can be disclosed when necessary for AML/CFT regulatory and/or legal enforcement purposes.

The Organisation for Economic Co-operation and Development (OECD) recently issued a new Crypto-Asset Reporting Framework (CARF) focusing on global tax transparency around taxpayer information between countries in relation to crypto assets.[27] To prevent duplicative reporting and regulatory overlap, coordinated implementation schedules for both the CARF and the modified Common Reporting Standard will be decided at a later date. A recent PwC report noted that the CARF is intended to achieve transparency in crypto asset transactions through the annual, automatic exchange of crypto asset transactions information between jurisdictions whose residents hold or engage in such transactions.[28] The OECD's CARF generally mirrors FATF rules. Pairing it with audit-based solutions can further aid in mitigating KYC ML/FT risks in crypto. But the efficacy of such new regulatory frameworks is only as good as the robustness of the weakest link in the chain, be it a weak regulator or regulation, or both.

4. P2P Transactions

Crypto allows financial transactions to occur P2P—such transactions are executed without the use of crypto asset service providers or financial institutions. Generally, P2P transactions are not explicitly subject to AML/CFT controls under the FATF standards because the standards place compliance obligations on financial intermediaries rather than on individuals. P2P transactions, such as those involving unhosted wallet users, may pose serious ML/FT risks, as they can potentially be used to avoid AML/CFT controls addressed in the FATF standards. In P2P crypto transactions, there are no obligated entities involved in preventing or mitigating ML/FT risks, such as a service provider's customer due diligence process and its filing of suspicious transaction reports.[29]

Risks from P2P transactions could rise, leveraged by increased technological capacity to engage in automatic P2P transactions through smart contracts without an intermediary institution to enforce KYC or AML/CFT regulations. DeFi platforms have been set up to enable this type of activity to circumvent AML/CFT regulation. Regulating this type of transaction is thus a great challenge currently without clear technological or other solutions.

To effectively combat P2P transaction risks, new regulations should be evaluated for smart contracts, DeFi services, and other P2P mechanisms in order to minimize ML/FT risks. Establishing effective regulations for P2P transactions will require regulators to develop and implement technological and other tools to track and understand the ML/FT risks in P2P transactions, including types of P2P transactions that pose higher risks; the drivers of P2P transactions; and the technology that mitigates or enhances such risks (i.e., privacy, transparency, security, etc.).[30]

5. Noncompliant Crypto Asset Service Providers

Although crypto asset service providers, such as exchanges, can provide safe custody and insurance (which, for example, Coinbase offers), they also pose risks to AML/CFT activities. Not all crypto service providers use KYC, even in instances when they operate as a financial institution—such as a money transmitter of crypto assets—that is subject to AML/CFT responsibilities.[31] Computers and systems for crypto asset service providers can be set up virtually anywhere and are active globally. This is a key difference with TradFi, which generally requires a financial institution to be incorporated, physically domiciled, and regulated. This makes it difficult to ensure compliance by crypto asset service providers with AML/CFT risk management principles that are endorsed by global standards setters such as the FATF, the International Organization of Securities Commissions (IOSCO), the Committee on Payments and Market Infrastructures, and the Basel Committee on Banking Supervision.

Regulators should strengthen engagement with crypto asset service providers and associated entities to better inform them of any necessary AML/CFT compliance responsibilities. Engagement activities include information exchange on AML/CFT compliance and tools to promote adherence; ongoing issuance of updated guidelines, alerts, and other publications; and organizing public–private information-sharing events like the Bank for International Settlements (BIS) Innovation Hub's G20 TechSprints[32] and the Financial Crimes Enforcement Network (FinCEN) Exchanges.[33] For instance, the BIS Innovation Hub Nordic Centre is launching a project—called Project Aurora—to explore the latest data technologies to combat money laundering across financial institutions and international borders.[34] To support Project Aurora, the BIS Innovation Hub could cohost a G20 TechSprint with nongovernmental organizations such as the Bretton Woods Committee in order to boost engagement activities on AML/CFT technologies and regulatory efforts for crypto.

6. Lack of Integration of AML/CFT Controls in Crypto Asset Creation

Currently, AML/CFT controls are not integrated into the creation of crypto assets. This poses ML/FT risks. Market participants, including regulators, should explore how

a crypto asset can be designed to enable and embed use of AML/CFT controls to improve code security in mitigating illicit finance risks. Regulators should also encourage the use of tools to improve the monitoring and operational effectiveness of AML/CFT compliance programs and increase information collection and sharing on cyber vulnerabilities in crypto that are associated with ML/FT activities—for example, operational event risk measurement and management with respect to (a) errors in the development and deployment of crypto assets and (b) the security and privacy of data within AML/CFT compliance programs.[35]

Aligning crypto asset code in accordance with standards such as ISO 20022 is one way to combat ML/FT. ISO 20022 is an international communication standard for sending electronic messages between financial institutions.[36] This standard fundamentally enhances the effectiveness of international money transfers and aids institutions in defending against ML/FT. The ISO 20022 architecture is designed to include blockchain transactions and application program interfaces[37] (APIs). The ISO 20022 reference data standards define universal codes for all of the common data elements in a financial message, such as the securities (using International Securities Identification Numbers, or ISINs) and counterparties (using Bank Identification Codes [BICs] or Legal Entity Identifiers [LEIs]).[38] These data protocols are required to be compliant with the standards. The same reference data standards can be used by blockchain networks within their code to improve AML/CFT controls. Currently, there are several crypto service providers that use ISO 20022–compliant standards, such as Ripple.[39]

Cybersecurity corporate governance is also critical in integrating AML/CFT controls in crypto asset creation, as cybersecurity is a corresponding concern in the protection of investor personal and financial information for AML/CFT compliance purposes in DeFi as in TradFi. Effective cybersecurity controls and governance enhance the required protocols needed to protect against ML/FT activities that result from insufficient security. In 2016, U.S. Securities and Exchange Commission chair Mary Jo White stated that cybersecurity is the biggest risk for the financial system.[40] Fortunately, there are well-established international cybersecurity governance standards for the TradFi sector that entities in the crypto sector can use to create a comprehensive cyber resilience framework. The BIS and the IOSCO provide guidance on cyber resilience for financial market infrastructures,[41] which offers suitable governance standards that can apply to the crypto sector. Additionally, key organizations, such as asset management firms, within the crypto sector can play an important role in incentivizing crypto entities to implement comprehensive cybersecurity governance. Asset management firms, such as the World Bank International Finance Corporation's Asset Management Company, are uniquely positioned to use their funding as an effective mechanism to incentivize the new or existing crypto entities that they finance to incorporate and prioritize cybersecurity to protect against ML/FT activities that could potentially arise from inadequate security.[42] This is of high importance as global crypto adoption is dominated by emerging markets,[43] which are also more significant in the formation of new ventures.

UNIQUE CRYPTO-RELATED FACTORS TO MEASURE IN ASSESSING ML/FT RISKS

Many of the aforementioned risks arise from the unique factors of crypto assets and crypto asset service providers that are distinct from TradFi. In Figures 1 and 2, we outline the key factors that need to be measured when assessing ML/FT risks for crypto assets and service providers. Regulators and the industry must work together to determine how to best measure these factors in creating effective AML/CFT implementation and enforcement rules that address the risks posed. This will support a more effective and balanced risk-based regulatory regime that is uniquely tailored to the crypto sector.

Figure 1. Key Crypto Asset–Specific Factors to Measure in Assessing ML/FT Risks[44]

- *Specific crypto asset market*—the number and value of crypto asset transfers; the value and price volatility of the crypto issued; the market capitalization of the crypto; the nominal and market value in circulation; the number of jurisdictions of users and the number of users in each jurisdiction; the market share in payments for a crypto in each jurisdiction; and the extent to which the crypto is used for cross-border payments and remittances.
- *Fiat-linked crypto assets*—the potential ML/FT risks associated with crypto assets that are exchanged with/for fiat currency or for other cryptocurrencies and the extent to which crypto-based transaction channels/platforms interact with or are connected to fiat-based transaction channels/platforms and digital services/platforms.
- *Payment channel*—the nature and scope of the crypto payment channel or system.
- *Transfers*—the number and value of crypto transfers and those likely to be or relating to illicit activities (e.g., darknet marketplaces, ransomware, and hacking).
- *Anonymizing and de-anonymizing techniques*—the use of anonymizing and de-anonymizing techniques for crypto funds transfers and techniques, and exposure to Internet Protocol anonymizers that may further obfuscate transactions or activities and inhibit a crypto asset service provider's ability to know its users and implement effective AML/CFT measures.
- *Entity*—the size of the business, its capitalization and reserves, the existing customer base, the stakeholders, and the significance of the cross-border activities of the issuer and/or the central entity, if any, governing the arrangement

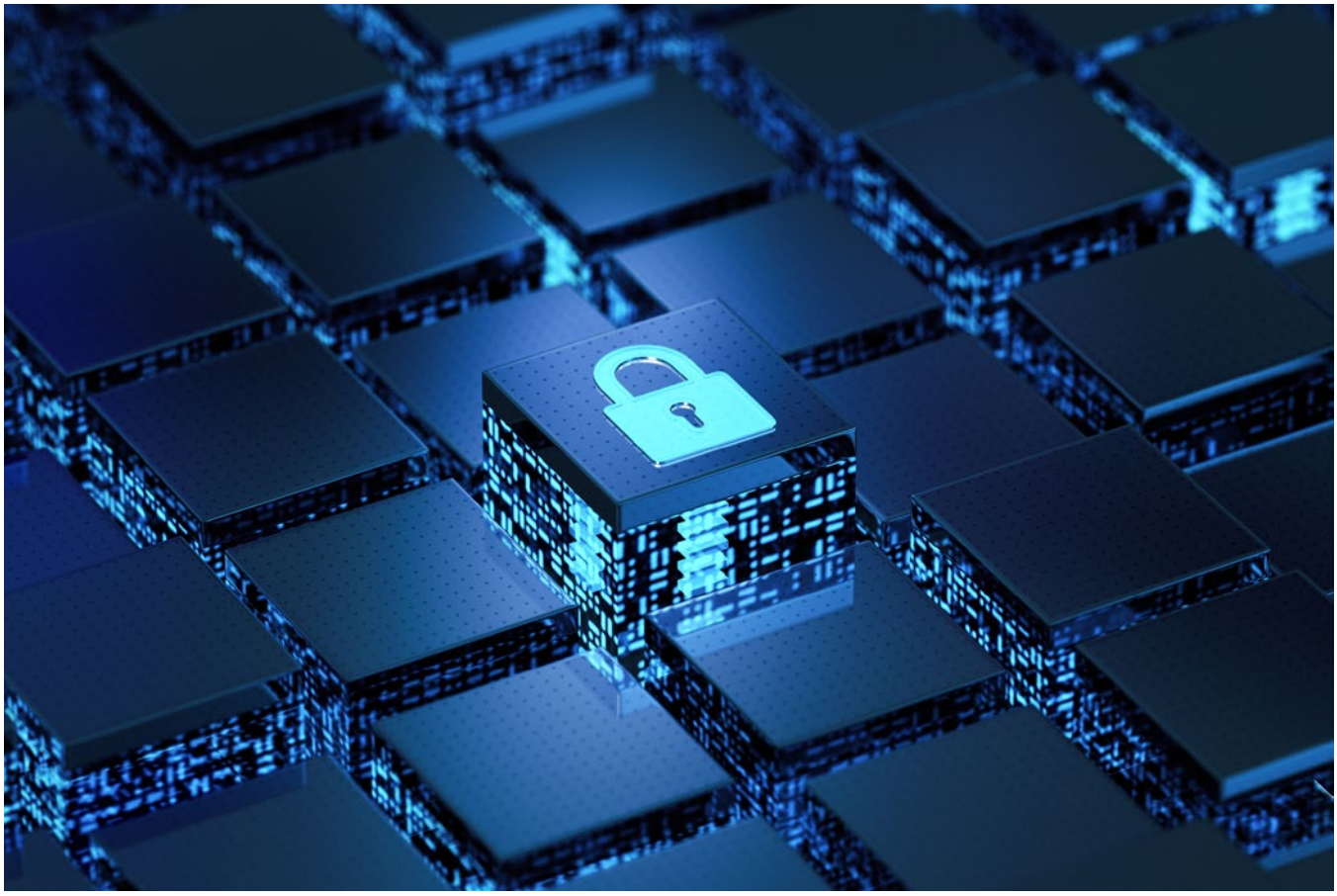

Figure 2. Key Crypto Asset Service Provider Factors to Measure in Assessing ML/FT Risks[45]

- *AML/CFT program*—the sophistication of the crypto asset service provider's AML/CFT program, including (1) the existence or absence of appropriate oversight tools to monitor cryptocurrencies and the crypto asset service provider's activities, and (2) the knowledge and expertise of the individuals responsible for compliance with the AML/CFT program.
- *User base*—the size and type of the user base of the crypto asset service provider, including the provider's access to data on its users and their activity, both within the entity and if there is potential aggregation across platforms.
- *Offerings*—the nature, scope, and adequacy of disclosure of the crypto asset service provider accounts, products, and/or service offerings.
- *Risk profile*—any risk parameters or measures and mitigants in place that may potentially lower the crypto asset service provider's exposure to credit, market, or operational risk (including concentration risks).
- *ML/FT sanctions*—the potential ML/FT sanctions risks associated with the crypto asset service provider's jurisdictional connections.
- *Travel rule*—whether the crypto asset service provider implements the "travel rule" or not.
- *Non-obliged entity and P2P transactions*—size of, nature of, and parties associated with transactions involving non-obliged entities (e.g., unhosted wallets with no obliged entity, crypto asset service providers not subject to regulation and supervision, etc.) and P2P transactions.
- *Crypto assets offered*—the specific types of crypto assets that the crypto asset service provider offers or plans to offer and the unique features of each crypto asset that may present higher risks to the service provider's ability to know its customers and implement effective customer due diligence and other AML/CFT measures.
- *Smart contracts*—a crypto asset service provider's interaction with, or management of, any smart contracts that may be used to conduct transactions.

CONCLUSION

Crypto AML/CFT regulation must become globally adopted and enforced and match the rapid pace of DeFi innovation. The FATF—as a key current global standard–setting organization for AML/CFT standards—has led the way in establishing the foundations for regulating crypto assets and crypto asset service providers. But even the FATF's reach is not universal and needs to grow to match that of DeFi. This limited reach should be addressed by the FATF and its regulatory member network, in collaboration with the crypto industry. The goal should be to continue to collectively raise awareness globally and to develop AML/CFT regulations for crypto that foster a more comprehensive and balanced risk-based regulatory regime. The key risks and risk mitigation tools and actions that we have discussed are the core areas for regulators and the industry to address first, with the goal of making the implementation, enforcement, and evolution of global AML/CFT regulations more effective in detecting and limiting illicit financing linked to crypto assets.

GLOSSARY OF KEY TERMS

Anonymity-Enhancing Coins (AECs)
Anonymity-enhancing coins are specifically designed to be fully anonymous, which allows for greater transaction anonymity than asset transfers conducted using Bitcoin or the Ethereum network.

Anti–Money Laundering (AML) and Countering the Financing of Terrorism (CFT)
Global standards established by the Financial Action Task Force for financial institutions to address money laundering (ML) and the financing of terrorism (FT). The standards include maintaining records of transactions; submitting reports of transactions exceeding certain thresholds; identifying and evaluating customers, which entails following Know Your Customer (KYC) rules; and reporting suspicious activities that may be deemed ML/FT.

Application Programming Interface (API)
Provides routines, protocols, and tools for building software applications and specifies how software components should interact.

Crypto Asset Service Provider
Any natural or legal person who is not covered elsewhere under the Financial Action Task Force Recommendations, and as a business that conducts one or more of the following activities or operations for or on behalf of another natural or legal person: (1) exchange between crypto assets and fiat currencies; (2) exchange between one or more forms of crypto assets; (3) transfer of crypto assets; (4) safekeeping and/or administration of crypto assets or instruments enabling control over crypto assets; and (5) participation in and provision of financial services related to an issuer's offer and/or sale of a crypto asset.

Crypto Asset
A digital representation of value that can be digitally traded or transferred, and that can be used for payment or investment purposes. Crypto assets do not include digital representations of fiat currencies, securities, and other financial assets that are already covered elsewhere in the Financial Action Task Force Recommendations.

Cryptocurrency Mixing or Tumbler Service
A service offered to mix potentially identifiable or tainted cryptocurrency funds with others in order to obscure the trail back to the asset's original source. Mixing aids in protecting privacy but is also used for money laundering.

Financial Action Task Force (FATF)
The organization established by the G7 countries to provide comprehensive and global anti–money laundering and countering the financing of terrorism standards that are adopted by countries into their own regulatory frameworks.

Financial Intelligence Units (FIUs)
Agencies that receive and analyze reports of suspicious transactions from financial institutions and other persons and entities, and that disseminate the resulting intelligence to law enforcement agencies and other FIUs to combat money laundering, associated illicit offenses, and terrorist financing.

Know Your Customer (KYC)
Standards designed to protect financial institutions against fraud, corruption, money laundering, and terrorist financing. These standards include establishing customer identity; understanding the nature of customers' activities and determining that the source of funds is legitimate; and assessing money laundering risks associated with customers.

KEY ABBREVIATIONS

AML — Anti-Money Laundering

CFT — Countering the Financing of Terrorism

CARF — Crypto-Asset Reporting Framework

CRS — Common Reporting Standard

DeFi — Decentralized Finance

FATF — Financial Action Task Force

FinCEN — Financial Crimes Enforcement Network

FT — Financing of Terrorism

KYC — Know Your Customer

ML — Money Laundering

P2P — Person-to-Person

TradFi — Traditional Finance

PHOTO BY FABIO ON UNSPLASH

ENDNOTES

1 Chainalysis, "Crypto Money Laundering: Four Exchange Deposit Addresses Received over $1 Billion in Illicit Funds in 2022," January 26, 2023, https://blog.chainalysis.com/reports/crypto-money-laundering-2022/.

2 FATF (Financial Action Task Force), "History of the FATF," https://www.fatf-gafi.org/en/the-fatf/history-of-the-fatf.html.

3 The FATF standards define a crypto asset—called a "virtual asset" under the standards—as a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Crypto assets do not include digital representations of fiat currencies, securities, and other financial assets that are already covered elsewhere in the FATF Recommendations.

4 The FATF standards define a crypto asset service provider—called a "virtual asset service provider" under the standards—as any natural or legal person who is not covered elsewhere under the FATF Recommendations, and as a business that conducts one or more of the following activities or operations for or on behalf of another natural or legal person: (1) exchange between crypto assets and fiat currencies; (2) exchange between one or more forms of crypto assets; (3) transfer of crypto assets; (4) safekeeping and/or administration of crypto assets or instruments enabling control over crypto assets; and (5) participation in and provision of financial services related to an issuer's offer and/or sale of a crypto asset.

5 FATF, "Second 12-Month Review of Revised FATF Standards—Virtual Assets and VASPs," July 5, 2021, https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Second-12-month-review-virtual-assets-vasps.html. In fact, an argument can be made that implementation and enforcement of AML/CFT regulations for crypto are currently two of the more prevalent global regulatory actions within the crypto space to date, compared with pending regulatory action in other areas.

6 The FATF comprises 39 member nations and more than 200 Global Network jurisdictions around the world.

7 FATF, "Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers," October 28, 2021, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html.

8 FATF, "Updated Guidance for a Risk-Based Approach."

9 FATF, "Updated Guidance for a Risk-Based Approach."

10 See Moody's, "DeFi & Digital Assets—Global Adoption of Blockchain-Based Technologies and Digital Assets Steadily Gains Momentum," October 7, 2022, https://www.moodys.com/research/DeFi-Digital-Assets-Global-Adoption-of-blockchain-based-technologies-and--PBC_1343168.

11 See Jonah Crane, Jonathan Everhart, and Antonio Weiss, "Deep Dive: Enhancing Market Integrity and Investor Protection in Crypto Asset Markets," BWC Digital Finance Project Team Brief No. 6, April 2023, https://www.brettonwoods.org/sites/default/files/documents/BWC-Brief6-Crypto-Integrity_FNL2lo.pdf.

12 FATF, "Second 12-Month Review of Revised FATF Standards."

13 Moreover, according to KPMG, as of February 24, 2023, the FATF has grey-listed South Africa and Nigeria, along with 21 other jurisdictions. These countries have been identified as having deficiencies in their AML/CFT regimes but have formally committed to addressing them. See KPMG, "What Actions Should Be Considered Following the Latest Grey-Listing of South Africa and Nigeria?," 2023, https://kpmg.com/dp/en/home/insights/2022/03/fatf-grey-listing-march-2023.html.

14 FATF, "Second 12-Month Review of Revised FATF Standards."

15 Thirty-five of the jurisdictions reported that their regulatory regimes were operational.

16 The Egmont Group recognizes that financial intelligence sharing is of paramount importance and has become the cornerstone of international efforts to counter money laundering, terrorist financing, and associated predicate offences. As a global organization, the Egmont Group facilitates and prompts the exchange of information, knowledge, and cooperation amongst member FIUs. See Egmont Group, https://egmontgroup.org/.

17 FATF, "Targeted Update on Implementation of FATF's Standards on VAs and VASPs," 2022, www.fatf-gafi.org/publications/fatfrecommendations/documents/targeted-update-virtual-assets-vasps.html.

18 FATF, "Second 12-Month Review of Revised FATF Standards."

19 Chainalysis Reactor, https://www.chainalysis.com/solutions/investigations/.

20 Elliptic Investigator, https://www.elliptic.co/solutions/crypto-investigations.

21 See the responses to the FATF consultation on virtual assets by Elliptic, Blockchain Association, Blockchain for Europe, Chamber of Digital Commerce, CoinCenter, and Global Digital Finance.

22 See Igor Makarov and Antoinette Schoar, "Cryptocurrencies and Decentralized Finance (DeFi)," March 23, 2022, Brookings Papers on Economic Activity, Spring (2022): 141–96, https://www.brookings.edu/wp-content/uploads/2022/03/16265-BPEA-Sp22_MakarovSchoar_WEB-Appendix.pdf.

23 A cryptocurrency mixing or tumbler service is a service offered to mix potentially identifiable or tainted cryptocurrency funds with others, so as to obscure the trail back to the asset's original source. Mixing aids in protecting privacy but is also used for money laundering. See CipherTrace, "Mixers, Tumblers, Foggers," Mastercard, https://ciphertrace.com/glossary/mixer-tumbler-fogger/.

24 In comparison, cryptocurrency exchanges are legal in the United States and fall under the regulatory scope of the Bank Secrecy Act. Exchanges must register with the Financial Crimes Enforcement Network, implement an AML/CFT program, maintain appropriate records, and submit reports to the authorities.

25 See "Use Case 1: Easier Digital Identity Verification and Data Privacy" in Deepika Sharma, Natalya Thakur, Dawn Fitzpatrick, Michael Kruse, and Adam Schneider, "Emerging Digital Finance Ecosystem and Positive Use Cases," BWC Digital Finance Project Team Brief No. 2, June 2022, https://www.brettonwoods.org/sites/default/files/documents/2022-06-19_DFPT_Brief_II_Final.pdf.

26 As noted in BWC Digital Finance Project Team Brief No. 2 at footnote 4, the government of Sierra Leone launched Africa's first digital identity platform with the United Nations Development Programme, the United Nations Capital Development Fund, and Kiva. The World Bank is pursuing this subject more widely in 49 countries (see the World Bank Identification for Development website: https://id4d.worldbank.org/). However, the success of such efforts depends on the local capacity and institutional infrastructure within host countries, limitations of which can hamper successful use of digital IDs for financial inclusion.

27 Organization for Economic Cooperation and Development, Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard (Paris: OECD, 2022), https://www.oecd.org/tax/exchange-of-tax-information/crypto-asset-reporting-framework-and-amendments-to-the-common-reporting-standard.htm.

28 PwC, "OECD Issues New Crypto-Asset Reporting Framework," October 2022, https://www.pwc.com/us/en/services/tax/library/oecd-issues-new-cryptoasset-reporting-framework.html.

29 FATF, "Updated Guidance for a Risk-Based Approach."

30 FATF, "Updated Guidance for a Risk-Based Approach."

31 Large volumes of transactions are reported between KYC (e.g., Coinbase and Gemini) and non-KYC (e.g., Binance) exchanges. It is alleged that non-KYC entities serve as a gateway for money laundering and other illicit activities (e.g., Hydra Market).

32 BIS Innovation Hub, G20 TechSprint, https://www.bis.org/about/bisih/topics/suptech_regtech/techsprint.htm.

33 U.S. Treasury, Financial Crimes Enforcement Network (FinCEN), FinCEN Exchange, https://www.fincen.gov/resources/financial-crime-enforcement-network-exchange.

34 BIS Innovation Hub, "Project Aurora: Using Data to Combat Money Laundering across Firms and Borders," https://www.bis.org/about/bisih/topics/fmis/aurora.htm.

35 See ORX, "What Is the Operational Risk Exposure from Cryptoassets?," November 9, 2021, https://managingrisktogether.orx.org/news-blogs-updates/what-operational-risk-exposure-cryptoassets.

36 Swift, "Swift Issues Guiding Principles for Screening ISO 20022," October 5, 2021, https://www.swift.com/news-events/news/swift-issues-guiding-principles-screening-iso-20022.

37 FATF, "Updated Guidance for a Risk-Based Approach."

38 International Securities Services Association, "Crypto Assets: Moving from Theory to Practice," April 2022, https://issanet.org/content/uploads/2022/04/Crypto-Assets-From-Theory-into-Pratice-Revision-2022.pdf.

39 See Ripple, "ISO 20022 Overview," https://ripple.com/lp/iso-overview/.

40 Lisa Lambert and Suzanne Barlyn, "SEC Says Cyber Security Biggest Risk to Financial System," Reuters, May 17, 2016, www.reuters.com/article/us-finance-summit-sec-idUSKCN0Y82K4.

41 BIS, "Guidance on Cyber Resilience for Financial Market Infrastructures," June 2016, https://www.bis.org/cpmi/publ/d146.pdf.

42 Jonathan R. Everhart and Helen Turner, "Incentivizing Cybersecurity Governance in Emerging Markets Private Equity Investments via the World Bank–IFC Asset Management Company," 2023, Brown University Digital Repository, https://doi.org/10.26300/nbh5-bg97.

43 See Leo Schwartz, "Global Crypto Adoption Dominated by Emerging Markets, Chainalysis Finds," Fortune, September 14, 2022, https://fortune.com/crypto/2022/09/14/global-crypto-adoption-dominated-emerging-markets/.

44 FATF, "Updated Guidance for a Risk-Based Approach."

45 FATF, "Updated Guidance for a Risk-Based Approach."

Future of Finance Working Group

CO-CHAIRS: William C. Dudley and Afsaneh Beschloss

Digital Finance Project Team

CO-LEADS: William C. Dudley and Carolyn Wilkins

Kofi Appenteng, Daniela Bassan, Richard Berner, Joe Brocato, Marcus Burnett, Keith Carter, Bill Coen, Carole Crawford, Thierry Déau, Larissa Delima, Dante Disparte, Douglas Elliott, Anthony Elson, Amara Enyia, Samson Enzer, Jonathan Everhart, Diana Farrell, Dawn Fitzpatrick, Samim Ghamami, Daniel Gleizer, Michael Goldfarb, Michael Greenwald, Josh Hawkins, Sarah Hirsch, Greg Johnson, Zennon Kapron, Elaine Khoo, Chan Kok Seong, Teresa Kong, Mahesh Kotecha, Michael Kruse, Caitlin Long, Rory MacFarquhar, Mina Mashayekhi, Barbara Matthews, Jesse McWaters, Sultan Meghji, Helena Ooi, Jonathan Padilla, William Papp, Franco Passacantando, Rebecca Patterson, Meghan Pearce, Frankie Phua, Ian Qiu, Jessica Renier, Daniel Runde, Jason Schenker, Adam Schneider, Deepika Sharma, Raisa Sheynberg, Andrew Slack, Heather Smith, Rajesh Swaminathan, Suan Teck Kin, Natalya Thakur, Kunal Thakur, Lynn Thoman, Tomicah Tillemann, Peter Tomozawa, Marsha Vande Berg, Courtney Vaughan, Antonio Weiss, Benjamin Weiss

THE BRETTON WOODS COMMITTEE
1701 K St NW #950, Washington, DC 20006
www.brettonwoods.org