VIRTUAL ASSETS AND ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM (1)—SOME LEGAL AND PRACTICAL CONSIDERATIONS

Introduction

The last decade has seen a phenomenal rise in the number of new digital instruments promising easier, faster, and cheaper global payments and transfers.[1] These digital representations of value and contractual rights comprise a broad (and expanding) category of assets. Common marketplace terms referencing such new products include *cryptocurrencies*, *digital currencies*, *crypto assets*, *virtual assets*, all describing systems of storing/capturing value and rights in digital form. Some of the most well-known digital assets rely on cryptographic technology to secure transactions and control the creation of additional units, underpinned by distributed ledger technology (DLT), such as blockchain, to construct a ledger (or a database) that is maintained across a network. The first of these instruments—Bitcoin—was launched in 2009. Since then, thousands of *cryptocurrencies* have been issued, with varying degrees of success. As of September 19, 2021, with a capitalization of at least US$1.97 trillion (for the top 101 cryptocurrencies) and, for a dozen of them, a daily turnover of more than US$1 billion,[2] cryptocurrencies now represent a small but not negligible portion of financial markets. This space is characterized by the speed at which different types of assets and business models are created, as well as their complexity. This includes stablecoins with the potential for mass adoption (see below. A new "ecosystem" has been created, along with new actors (new financial service providers and intermediaries). In line with the terminology set by the Financial Action Task Force (FATF),[3] the internationally recognized standard[4] setter for anti-money laundering and combating the financing of terrorism (AML/CFT), this note refers to these new instruments as *virtual assets* (VA) and to the new actors as *virtual asset service providers* (VASPs). The FATF definition of VA explicitly excludes digital representation of fiat currencies, securities and other assets that are covered elsewhere in the FATF standards. For this reason, national digital currencies, including central bank digital currencies (CBDCs), while they may, in practice, share some similarities with VAs, are not discussed in this note.[5]

VAs offer many potential benefits. As noted in the IMF's earlier publications,[6] these include greater speed, lower cost and increased efficiency in making payments and transfers, including across borders, with the potential to improve financial inclusion. DLT offers potential benefits that go far beyond VAs. Many countries across the world are currently looking into leveraging this new technology to issue domestic "currency" in virtual form—CBDCs.

At the same time, however, VAs are susceptible to criminal abuse. Some of their features—in particular their varying degrees of anonymity or pseudonymity—raise new challenges for country authorities. Criminals have misused these features to facilitate fraud, theft, money laundering (ML) and terrorist financing (TF), amongst other crimes.

Without strong mitigation, VAs can pose a significant threat to the integrity of the global financial system. ML, related predicate crimes,[7] TF, and the

The views expressed in this Note are those of the authors and do not necessarily represent the views of the IMF, its Executive Board, or its management. The authors are grateful to Yan Liu for her support and guidance, and to Nadim Kyriakos-Saad, Trevor Rajah, Wouter Bossu, Steve Dawe, Christophe Waerzeggers, Arthur Rossi, Kohei Noda, Jane Duasing for their review and comments. This note also greatly benefited from comments from colleagues in other Departments of the IMF and staff of the FATF Secretariat.

[1]See IMF Staff Discussion Note "Virtual Currencies and Beyond: Initial Considerations" (2016).

[2]See https://coin.dance/stats and https://coinmarketcap.com/.

[3]The FATF is an inter-governmental body established in 1989 to set standards and promote effective implementation of legal, regulatory, and operational measures for combating ML as well as, subsequently, TF and PF. It comprises 39 members representing most major financial centers in the world.

[4]The FATF standards comprise the 40 Recommendations, their Interpretive Notes, and the accompanying Glossary.

[5]On legal issues pertaining to CBDC: see Bossu, W., Itatani, M., Margulis, C., Rossi, R., Weenink. H., and Yoshinaga, A., *Legal Issues of Central Bank* Digital *Currencies: Central Bank and Monetary Law Considerations,* IMF, WP/xx/20.

[6]See for example Bali Fintech Agenda, IMF Policy October 2018 and January 2016 Staff Discussion Note "virtual Currencies and Beyond: Some Initial Considerations" (SDN/16/03).

[7]These are the underlying offenses that generate illegal proceeds to be laundered. Pursuant to the FATF standards, the ML offense should apply to all serious offenses, with a view to including the

Box 1. Key Terminology I

While FATF has clearly defined Virtual Assets as "a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes.," several other terminologies are frequently used in different contexts to cover similar assets. They do not, however, have an internationally-agreed upon definition. Here are some examples:

Crypto assets: The IMF, in some of its most recent publications, refers to crypto assets, which it defines as digital representations of value, made possible by advances in cryptography and distributed ledger technology.[1]

Cryptocurrency: Several others refer to cryptocurrency (or crypto currency) which is generally understood as a digital asset designed to work as a medium of exchange wherein individual coin ownership records are stored in a ledger existing in the form of a computerized database using strong cryptography to secure transaction records, to control the creation of additional coins, and to verify the transfer of coin ownership. It typically does not exist in physical form (like paper money) and is typically not issued by a central authority.

Stablecoins and Global Stablecoins (GSCs): The FSB considers stablecoins to be "a type of crypto asset that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets"[2] They may be pegged to a fiat currency or to a commodity. The so-called GSCs include initiatives, such as Diem (previously Libra), built on an existing large and/or cross-border customer base, which have the potential to scale rapidly to achieve a global or other substantial footprint.[3] The FATF considers that the term "stablecoin" is not a clear legal or technical category, but is primarily a marketing term used by promoters of such coins. In order to avoid unintentionally endorsing their claims, it refers to them as "so-called stablecoins." Coins referred to as "global stablecoins" in G20 and other reports are named "so-called stablecoins with the potential for mass adoption" for FATF purposes for the same reason.[4]

These assets rely on Distributed Ledger Technology (DLT): DLT is a database that is stored, shared, and synchronized on a computer network. Data is updated by following rules for achieving consensus among the network participants. While blockchain is a type of distributed ledger technology, the latter does not necessarily maintain its record using the same chain of blocks architecture.[5]

[1]IMF, Digital Money Across Borders: Macro-Financial Implications.

[2]FSB, Addressing the regulatory, supervisory and oversight challenges raised by "global stablecoin" arrangements: Consultative document, April 2020.

[3]See http://www.fatf-gafi.org/publications/fatfgeneral/documents/statement-virtual-assets-global-stablecoins.html.

[4]FATF report to G20 June 2020.

[5]IMF, Digital Money Across Borders: Macro-Financial Implications.

financing of the proliferation of weapons of mass destruction (PF) can all be facilitated with VAs and can all have serious economic consequences.[8] Preserving the integrity of the global financial system is a necessary aspect of ensuring financial stability, sustainable growth and inclusive economic development. Effective anti-money laundering and combating the financing of terrorism (AML/CFT) frameworks are crucial in that respect.

So far, countries have taken a variety of measures to mitigate the financial integrity risks raised by VAs. These measures range from full or partial regulatory coverage of all or some VA-related activities, to a ban of some or all transactions in VAs. This disparate and fragmented approach has not proven effective and leaves room for regulatory arbitrage.

Growing concerns about the illicit use of VAs have spurred the international community into action. Specifically, the IMF, World Bank, G20, and G7, amongst others, have called for a responsible, balanced approach to VAs—one that enables the legitimate use of VAs and fosters innovation while mitigating the risks. In June 2019, the FATF finalized amendments to its

widest range of predicate offenses. At a minimum, it should apply to the 21 categories of offenses in the FATF glossary (e.g., fraud, drug trafficking, corruption and bribery, and tax crimes).

[8]See https://www.imf.org/-/media/Files/Publications/PP/2019/pp101718-2018-review-of-the-funds-aml-cft-strategy.ashx.

global standards to clearly impose AML/CFT requirements on VAs and VASPs (see Annex 1). In June 2020, it noted that while progress was being made in the implementation of its new standards by the public and private sector, considerably more effort was needed. The FATF will conduct a second 12-month review of the implementation of its new standards by June 2021 and consider whether further updates are necessary.

The purpose of this Note is to assist countries in their understanding and mitigation of the ML, TF, and PF[9] risks related to VAs. This is the first of two Fintech Notes dedicated to VAs and AML/CFT.[10] This first note is broad in scope. It explains why VAs are vulnerable for misuse for ML/TF/PF purposes and clarifies which assets and service providers should be subject to AML/CFT measures. It discusses the measures that all countries should take, and the type of action necessary in instances of criminal misuse of VA. A second Fintech note[11] focuses on the AML/CFT regulatory and supervisory framework for VASPs. Both notes are based on the FATF standards and draw heavily on the FATF's 2019 "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers."[12] They aim at providing policy makers and authorities with AML/CFT responsibilities with an overview of the legal and operational considerations that the implementation of a sound AML/CFT framework for VAs and VASPs raises. In some instances, the Notes make reference to specific types of VAs, VASPs and related products. These references are made for illustrative purposes only, and do not constitute an endorsement of the specific VAs, VASPs and related products. Finally, at the time of drafting, no country had been assessed against the new standards and many country authorities were in the process of establishing how best to incorporate the new standards in their AML/CFT framework. For these reasons, this note does not refer to country specific examples.

The Financial Integrity Risks Related to VAs

While generally used for legitimate purposes, VAs have also been misused to serve nefarious goals. Some cases of large-scale fraud, theft, ML, and other crimes using VAs have involved millions of U.S. dollars' worth of illegal proceeds.[13] The exact extent of misuse of VAs around the globe is unclear, but so far appears to be smaller in volume and frequency than misuse of traditional financial services.[14] Some firm-specific estimates as well as estimates issued by some regional agencies indicate that criminals still favor traditional assets. But they also reveal that the misuse of VAs is not negligible and is rapidly increasing.[15]

Several factors make VAs potentially attractive to criminals. They notably include the following:

- **Potential for greater anonymity and availability of anonymity enhancing features**. In many cases (e.g., Bitcoin), transactions are visible online and traceable from one wallet to another. But linking a particular address or wallet to a specific individual is challenging. This challenge is compounded by the availability of mechanisms designed specifically to hinder the traceability of flows. They include anonymity enhancing features (such as mixers and multiple layers of encryption, stealth addresses and ring signatures) that limit the information available, including regarding the value and counterparties of a transaction. Some also obfuscate identification through secondary information (e.g., by preventing

[9]The proliferation financing risks include the risks of potential breaches, non-implementation or evasion of the targeted financial sanctions related to PF.

[10]Both Fintech notes are part of the IMF's broader efforts to assist its members strengthen their AML/CFT framework. For further information on the IMF's AML/CFT program, see Footnote 2.

[11]Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT)—(2) Effective AML/CFT Regulatory and Supervisory Framework: Some Legal and Practical Considerations.

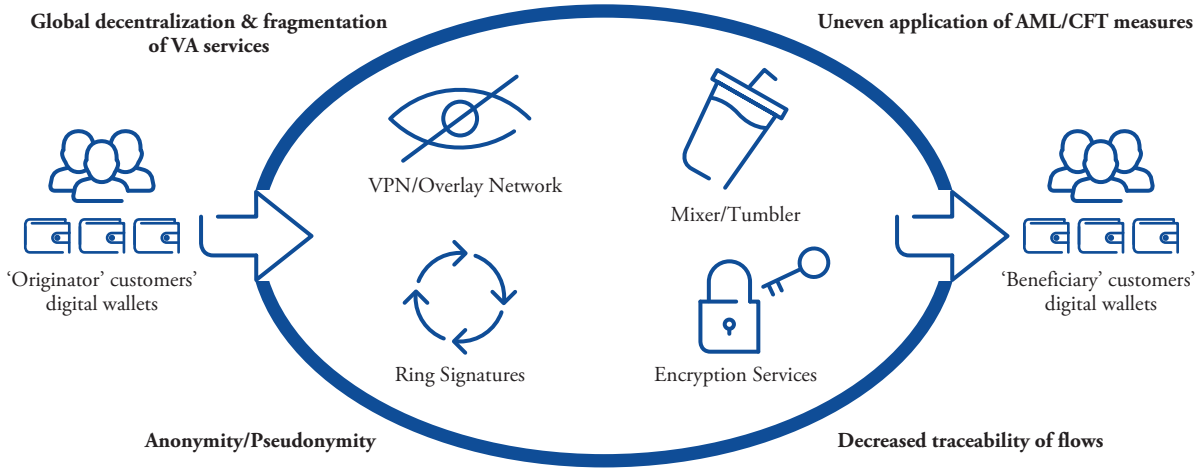
[12]See https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf.

[13]For example, the Silk Road Case, AlphaBay, and the Wannacry ransomeware attack. While these cases ultimately resulted in successful law enforcement action, success remains rare.

[14]12-month Review of The Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers, FATF, 2020.

[15]See https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019; the European Union Agency for Law Enforcement Cooperation estimates that three to four percent of illicit proceeds in Europe are laundered through VAs and mentions collection of donations in Vas. for TF purposes. European Union Terrorism Situation and Trend Report 2019; other examples include: Ciphertrace in its Q3 2018 report states that "transactions on the 20 top cryptocurrency exchanges globally revealed that 97% of direct bitcoin payments from identifiable criminal sources were received by unregulated cryptocurrency exchanges" and "the top exchanges have laundered a significant amount of bitcoin, representing approximately $2.5 billion at today's prices." Criminal sources referred here are mostly fraud and theft of VAs. https://ciphertrace.com/wp-content/uploads/2018/10/crypto_aml_report_2018q3.pdf; Chainalysis noted that over the course 2019 it traced $2.8 billion in Bitcoin that moved from criminal entities to exchanges. https://blog.chainalysis.com/reports/money-laundering-cryptocurrency-2019.

Figure 1. Financial Integrity Risks in Transfers of VAs



Source: IMF staff.

the identification of the IP addresses, geolocation data, device identifiers, and transaction hashes).[16]

- **Non-face-to-face activities.** VAs-related activities are conducted online and are generally not in the same physical location. This complicates the identification of the customer during the onboarding process or at the time of transactions and increases the risk of forged or inaccurate identification information being provided. Although some conventional financial services also allow non-face-to-face onboarding and transactions, the anonymity feature of VA activities could exacerbate these challenges.
- **Potential for decentralization and fragmentation of near instant global services.** The fast-moving nature of VAs provides an opportunity to quickly exchange between different VAs for a more sophisticated disguise of the origins of funds in a cross-border context.[17] VASPs can have a physical presence in one jurisdiction, be registered in another, place their server in yet another (or multiple others), and provide services globally without the need for a central center of command. This complicates the prevention of illegal transactions and the analysis of financial intelligence derived from suspicious transaction reports as case information can be fragmented across different countries. It also complicates law enforcement action as there is generally no single entity to investigate and target.
- **Uneven application of domestic AML/CFT measures.** Most countries are still in the early stages of implementation of the relevant FATF standards, which creates significant potential for regulatory arbitrage, thus providing opportunities for criminals to exploit VASPs domiciled or operated in countries with nonexistent or minimal VA and VASPs AML/CFT regulations.

Ultimately, these factors pose significant challenges to domestic authorities as well as to VASPs. They hinder the effective implementation of the AML/CFT preventive framework and of law enforcement action. The following figure illustrates how, in the absence of AML/CFT controls, the use of VAs with anonymity enhancing features and the other factors listed above create a perfect storm with potentially significant ML/TF/PF risks. Figure 1 illustrates how certain tools or features of VA activities can make transfers of VA more susceptible to misuse.

The most prevalent offenses that involve VAs appear to be narcotics-related crimes and fraud. After amending its standards to address VAs and VASPs more explicitly, the FATF also agreed to undertake a 12-month review to measure the implementation of the revised standards by jurisdictions and the private

[16]For example, a VPN or an anonymized overlay network (e.g., Tor), which encrypts and routes communications through multiple computers can be used to mask Internet activity. Software to emulate an operating system within a user's operating system, with operations of the virtual machine encrypted, is also available.

[17]Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins, FATF, 2020.

Box 2. Key Terminology II

With the development of VAs, several technologies and mechanisms appeared. The following are some examples, as they are generally understood:

Digital Wallet: Digital wallets are a virtual account that can hold VAs. They can be in different forms including hardware wallets, desktop wallets (on a computer/laptop desktop), online wallets (internet-based cloud storage wallets), mobile wallets (held on smartphones) or printed wallets (held on paper).

Mixer/Tumbler: Mixers (or tumblers) combine and intermingle multiple transactions, distributing them among multiple wallets.

Ring Signature: A tool to hide the originator of a transfer by requiring signatures from several VA users (e.g., randomly chosen) to conduct a transaction.

Transaction Hash: Alphanumeric unique identifier of a transaction.

Box 3. FATF Definition of Virtual Asset

The FATF Glossary defines a *virtual asset* as "a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes."

It also clarifies that "VAs do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations."

sector, as well as monitoring for any changes in the typologies, risks and the market structure of the virtual assets sector. In this context, it notably found that the types of offenses involving VAs include ML, the sale of controlled substances and other illegal items (including firearms), fraud, tax evasion, sanctions evasion, computer crimes (e.g., cyberattacks resulting in thefts), child exploitation, human trafficking and TF.[18] Among them, narcotics-related and fraud offenses (e.g., investment scams and swindling, blackmail, and extortion) are the most prevalent. The value of VA involved in most cases detected has been relatively small compared to those using traditional financial products and services, but professional ML networks have also appeared to start exploiting this vulnerability and use virtual assets as one of their means to launder illicit proceeds. Trends have been noted of the use of VASPs registered or operating in jurisdictions without effective AML/CFT controls, the use of multiple VASPs and the use of anonymity-enhancing tools and methods.

[18]See: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/12-month-review-virtual-assets-vasps.html. A second FATF review is ongoing at the time of publication.

Key Concepts

Virtual Assets

The FATF uses a broad concept of VA to capture the widest range of virtual instruments that can be misused for ML/TF/PF purposes (see definition in Box 3). The domestic legal classification of a digital asset (e.g., as a security or a commodity) and commonly used market terminology (e.g., cryptocurrency) do not have bearing on the VA categorization under the FATF standards.

Whether an asset falls within this definition depends on its nature and use. This determination may not always be entirely straightforward, not in the least since many basic concepts in the virtual space are still lacking a universally agreed-upon definition. Different virtual instruments serve different purposes. For instance, tokens[19] can have many uses (so-called

[19]"Token" is a very general term and relates to a representation of anything (tangible or intangible, of economic value or not, a stake, a voting or access right, etc.) in a particular ecosystem. Tokens can be explained as lines of code embedded in DLT networks that may serve different purposes. For instance, a token can be used as a digital means of exchange, digital investment, or a resource. Regardless of the classification, the main functionality of tokens on a DLT is to enable parties to conduct operations, whether these refer to services, goods, or financial instruments, with the token acting as an independent representation of those services, goods, or financial instruments (See notably IMF Fintech Note: Keeping Pace with Change: Fintech and the Evolution of Commercial Law [TO BE PUBLISHED]). Tokens are also not necessarily limited to one particular role; they can fulfill multiple roles in their native ecosystem.

security tokens[20] provide an economic stake in a legal entity or other financial asset; so-called *utility tokens*[21] generally confer no ownership rights but grant certain rights of use or access; hybrids can confer both ownership and access rights). As per the FATF's definition, the focus should be on digital assets that represent value and can be used as a method of payment or investment.

As a result, VAs as defined by the FATF notably include:

- Both centralized and decentralized assets that are convertible to money or another type of VA.[22]
- Mainstream digital assets often referred to as *digital currencies* or *cryptocurrencies* (e.g., Bitcoin, Ethereum, Monero), including those that are pegged (e.g., so-called GSCs, regardless of whether they are commodity-backed (e.g., Digix Gold Tokens), money-backed (e.g., Tether), or cryptocurrency-backed (e.g., Synthetix).
- Asset that have been tokenized.[23]

Conversely, certain other types of assets are clearly not VAs under the FATF standards. They notably include (i) tokens that cannot be used for payment or transfer of value, such as certain utility tokens that only grant a certain right (e.g., of access or to vote); (ii) tokens that do not intersect with the real economy: nonconvertible digital assets that are specific to a particular virtual domain and cannot be exchanged for fiat (e.g., airline frequent flyer airmiles, credit card awards, or similar loyalty program rewards or points); and (iii) national digital currencies (including CBDCs). Although exhibiting many of the same characteristics of those conducted using VAs, transactions or activities involving CBDCs will be subject to the preexisting FATF standards applicable to "traditional" financial assets.

In some instances, however, the determination as to whether an asset qualifies as a VA may be challenging. As the virtual landscape evolves, the nature and use of digital assets will continue to change. Some types of digital assets that are at present excluded from the FATF definition may eventually be revealed to possess attributes of VAs or have financial integrity implications.[24] Careful, ongoing monitoring of the developments in the virtual space is therefore needed in order to ensure that all relevant virtual assets are captured by the AML/CFT framework.

Virtual Assets Service Providers

VAs have given rise to a new "ecosystem" of professionals - VASPs. Although some users prefer to handle their VAs themselves (and indeed, one of the espoused benefits of VAs is the ease with which users can transact without the need for a financial intermediary), others prefer to rely on professional service providers, or may need a facilitator to connect them with other users or to provide a platform for their transactions. These new activities raised the question as to which business models and professionals should be subject to AML/CFT regulation.

The FATF identified the type of VASPs relevant for AML/CFT on the basis of their activities. Whether specific persons or entities are considered VASPs (see definition of VASP in Box 4) depends on how they use VAs and for whose benefit. The scope of the FATF definition includes both virtual to virtual and virtual to fiat transactions or operations.

All five categories are comprised of those acting "as a business." This notably entails some form of remuner-

[20]Security tokens are widely recognized as tokens that entitle holders to the underlying assets, dividends or interest payments—these tokens are "analogous to equities, bonds or derivatives" (from Techarati.com). However, there is no universally accepted definition of security token and such designation will depend on whether a token meets the definition of a "security" under applicable national legislation.

[21]Utility tokens are widely recognized as tokens that exist with the sole purpose of conferring access rights to an application or service—such as Binance coin, Lisk, or the ZIL (from Techarati.com).

[22]Convertible VAs have a determinable value in money and can be exchanged for money. Centralized VAs have a single administrating authority—a third party that controls the system by issuing the VA, establishing the rules for its use, and maintaining a central payment ledger. The administrator also has the power to withdraw the VA. By contrast, decentralized VAs are distributed, open-source, peer-to-peer VAs that have no central administrating authority and no central monitoring or oversight. All computers in a particular network comprise a "node" that contains information on a transaction. The network of nodes must validate/authenticate all transactions using complex algorithms before they can be added to ledger. Additions to the blockchain are permanent and immutable.

[23]Tokenization is the process of converting rights—or a unit of asset ownership—into a digital token on a blockchain. Any asset, whether tangible (e.g., real estate or precious metals and stones) or intangible (including financial instruments and rights to intellectual property), can be tokenized. An asset-backed token represents an ownership right and derives its value from the underlying asset.

[24]Discussions are underway including in the context of the public consultation held by the FATF on which entities are captured by the standards as VASPs. The revised Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (expected to be published in late 2021) will provide further clarification.

Box 4. FATF Definition of Virtual Asset Service Provider

A **VASP** is any natural or legal person who is not covered elsewhere under the Recommendations and conducts, as a business, one or more of the following activities or operations for or on behalf of another natural or legal person:

(i) Exchange between VAs and fiat currencies, and/or (ii) between one or more forms of VAs;

(iii) Transfer of VAs;

(iv) Safekeeping and/or administration of virtual assets or instruments enabling control over VAs; and,

(v) Participation in and provision of financial services related to an issuer's offer and/or sale of a VA.

ation (e.g., commission, spread, or other benefit). In this context, it includes those providing the following services:

- **VA exchanges:** if they provide an intersection between the virtual and real economy or between different virtual environments. They may directly transact with customers or actively facilitate such transactions between users (peer-to-peer). Exchanges exist in many forms including: VA kiosks (e.g., ATMs, bitcoin teller machines, bitcoin ATMs, or vending machines), cryptocurrency exchangers, converters, VA brokerage services, VA trading services, VA escrow services.
- **VA transfer services:** including the conduct of transactions on behalf of other persons by moving VAs from one address or account to another.
- **Custodial services:** such as virtual wallet providers that host wallets or maintain custody or control over another person's VAs.
- **Administration of another person's VAs:** where someone conducts as a business the management or administration (including transmission) of VAs independently of the owner (with the assumption that such decisions are taken with the permission or pursuant to the instruction of the owner).
- **Financial services related to an issuer's offer and/or sale of a VA (such as in an initial coin offering, ICO):** Similar to an initial public offering (IPO), an ICO is one way of funding a start-up. A quantity of virtual tokens (or "coins") will be sold to investors in exchange for money or more mainstream cryptocurrencies. Such tokens represent functional units of value if the ICO's funding goal is ultimately met and the project is launched. Virtual brokers can also provide advisory and other financial services related to the launch of ICOs (similar to the role of an underwriter in traditional IPOs).

In practice, VASPs often conduct a combination of these activities. Common examples include VASPs that offer exchange and transfer services, or financial intermediaries who administer and transfer VAs as part of financial services related to an issuer's offer and/or sale of a VA. Oftentimes, financial intermediaries offering custodial services are also involved in transfers of VAs; for instance, wallet providers often send and receive VAs through the use of private and public keys to sign transactions digitally.

Other actors in the VA space are not considered VASPs under the FATF standards. Individuals acting on a private basis (i.e., not conducting a business) are not VASPs. As with traditional assets, individuals using, transferring, or otherwise managing funds for personal use are not subject to AML/CFT obligations. This includes peer-to-peer transactions where neither party is a VASP or other AML/CFT-regulated entity. Likewise, individuals or businesses merely providing a forum connecting other users do not trigger AML/CFT obligations. Operators of platforms that merely allow for peer-to-peer activity to take place without any intermediation (i.e., any one of the activities listed in the FATF definition) generally do not fall within the FATF definition of VASP. Such platforms include those that provide a forum for the trading, sale/purchase, exchange, or conversion of cryptocurrencies among users.

The delineation between a VASP and non-VASP is not always clearly laid out in the prevailing standards. The FATF standards require that AML/CFT requirements for VASPs (as for "traditional financial service providers") be activities-based. However, sharp distinctions between various types of activities have yet to be drawn in all cases. For example, the distinction between merely hosting activity and providing intermediation is tenuous. While it is clear that sites

connecting users who then conduct financial activities off-site are clearly not VASPs, the degree to which various sites support such activities vary. The current FATF guidance focuses on "active" facilitation of financial activity, although what constitutes "active" facilitation is not defined and different countries may have varying interpretations of active and passive facilitation (which could justify amendments in the next iteration of the guidance). Further, the use of smart contracts[25] and decentralized (distributed) applications (DApps)[26] can present challenges to establishing who really controls a specific VA. Under the FATF standards, an "owner or operator" of a dApp may come within the definition of a VASP. This raises the question of how one demonstrates control on or benefits from a decentralized platform that operates on a consensus. It is questionable whether the traditional notion of ownership can apply once a self-executing application has been released. Regardless of these challenges, the focus should remain on the nature of the financial activity or conduct surrounding the VA and the ML and TF risks it poses rather than the underlying technology.

Countries must ensure that VAs and, unless they ban VA activities, VASPs are properly regulated in their domestic legal frameworks. Towards this end, they should ensure that their AML/CFT frameworks apply to all relevant entities and professionals. A second Fintech Note provides a discussion of the development of such regulatory frameworks.[27]

Countries may consider that their pre-existing AML/CFT laws adequately incorporate VASPs. For example, they may be defined as a type of money service business, payment service provider or dealer in securities. If applying pre-existing laws, countries must ensure that their AML/CFT laws cover all VASPs and virtual assets and are sufficiently tailored to the specific requirements of VASPs. Alternatively, countries may include VASPs as a new category of AML/CFT-obliged entity under their laws.

Countries should also ensure their AML/CFT framework applies to financial institutions and DNFBPs (as defined by the FATF) where they provide covered VA-related services or financial activities or operations. This could include financial institutions such as banks and securities broker-dealers and can also include DNFBPs such as casinos. Financial institutions and VASPs have largely equivalent requirements under the FATF standards. Where DNFBPs engage in VA activities, countries and competent authorities should subject such DNFBPs to a legal and regulatory framework on par with the one called for under the FATF standards for financial institutions.

Operational Aspects of an Effective AML/CFT System—Legal and Practical Considerations

To address the financial integrity risks related to VAs, a solid, multipronged approach is necessary. In 2018 and 2019, the FATF adopted changes to its standards to explicitly apply them to the virtual context and provided additional tailoring where necessary (see Annex 1). As is the case with traditional assets, the mitigation of the ML/TF/PF risks related to VAs therefore requires several steps, starting with a risk assessment as well as a review and commensurate tailoring of the existing legal and institutional framework. Mitigation also requires the active, ongoing participation of the private sector (VASPs, in particular and unless VA activities are prohibited, but also financial institutions and DNFBPs as defined by the FATF) and of a range of governmental agencies (e.g., policy makers, AML/CFT supervisors, financial intelligence units, FIUs, and law enforcement agencies, LEAs). Finally, in light of the often cross-border nature of VA-related activities, including criminal activities, it also requires extensive dialogue and cooperation with foreign counterparts.

Some action is required from all countries. Ultimately, countries are free to regulate or prohibit activities in VAs (see the second Fintech Note). But all must take some action. Even if a jurisdiction prohibits the activities of VASPs, it must still assess the ML/TF/PF risks associated with VAs, and undertake corre-

[25]E.g., in instances where a person or entity exercises, as a business, exclusive and independent control over smart contracts to which they are not a party involving another person's VAs. How the element of independent control relates to smart contracts (which are self-executing by nature as the terms of the agreement are directly written into lines of code) remains to be seen.

[26]Facilitation of peer-to-peer activity can also take place in the form of decentralized (distributed) applications (DApps), a broad term referring to generally open-source software programs that operate on a peer-to-peer network. DApps use smart contract technology to connect a frontend user interface with the underlying blockchain (backend code). DApps have a number of uses: most, if not all, cryptocurrencies are dapps; they can be used as decentralized payment systems or to enable lending (e.g., with stablecoin), by connecting users directly in their transactions, cutting out the traditional middleman/woman (banks and other financial institutions). True to their name, dApps are not controlled by a centralized authority and run on consensus mechanisms.

[27]Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT)—(2) Effective AML/CFT Regulatory and Supervisory Framework: Some Legal and Practical Considerations

sponding outreach, as well as take action to enforce that prohibition. It must also adopt risk mitigation strategies that account for the cross-border element of VA activities, and cooperate with other countries as needed. The following focuses on those actions that all countries should take.

Risk Assessment

As is the case with respect to traditional assets, effective mitigation requires a prior determination of the level of ML/TF/PF risks of VAs. Blanket assumptions about the level of risks of VAs and related activities may lead to inappropriate allocation of resources and mitigating action. Countries should establish the actual and inherent ML/TF/PF risks impacting their jurisdiction, so as to be in a position to tailor mitigation and focus their AML/CFT efforts on the higher risks. This notably entails an assessment of the VA and VASPs' threat and vulnerability to ML and TF. This, in turn, requires an analysis of the risk factors specific to the sector (e.g., related to the properties of VA activities, products or services offered, delivery channels, customer base, and geographical areas of VASPs operations). Of particular importance are the availability and significance of decentralized VAs, as well as VAs or services that hinder the traceability of transactions and the ability of VASPs to implement AML/CFT measures. The risk assessment should also establish the quality of AML/CFT measures applied by VASPs, and other reporting entities that engage in VA financial activities, including their risk management policy and internal oversight mechanisms (see Fintech Note on Virtual Assets and AML/CFT (2)).

Such an assessment requires solid technical knowledge of the virtual world, close engagement with the private sector, and international cooperation. Efforts towards in-depth understanding of VAs, related products and services and of the VASPs' role in the domestic financial system is essential. But it is also challenging, in light of the complexity of the VA sector and of the speed at which it evolves. In this context, close dialogue with IT professionals and existing VASPs is key, as the latter may provide expert advice and share their own perceptions of the ML/TF/PF risks posed by certain types of VAs, as well as common and recent typologies of misuse of VAs for criminal purposes. They may also share useful information such as data on the market share of different VAs, their turnover, customer base, and geography of operations. As most VAs are global in nature, increased dialogue with foreign counterparts is also critical. It also requires understanding of the country's broader context. A number of non-VA-related policies and regulations may also have an impact on the level of ML/TF/PF risks, such as those related to consumer protection, company formation, economic citizenship, prudential supervision, monetary policy and the tax regime.

So-called global stablecoins (GSCs) are potential game changers.[28] Unless strong AML/CFT measures are implemented, they can pose significant financial integrity risks. When reviewing GSCs projects, countries are well-advised to assess all features of these arrangements and of the domestic framework. They should ensure that the risks are understood by all private and public stakeholders, and that effective mitigating measures are in place, both in the GSCs network (e.g., with multiple control points) and domestically (e.g., appropriate legal and institutional framework).

Legal Foundation

Adapting to a world in which VAs exist may require updating a country's legal framework. The need for updates will vary on a case-by-case basis and will require a number of steps:

(i) An *ex ante* policy discussion of the type of approach that a country wishes to implement to mitigate the risks. Some countries have taken a decision to ban VA-related activities (e.g., due to a lack of appropriate resources to regulate the sector); others have opted to regulate AML/CFT activities.[29]

(ii) Regardless of the option chosen, a review of the legal framework is necessary to establish the breadth of the legal and regulatory changes needed (e.g., a ban would need to be in law or other enforceable means to ensure that unauthorized activities can be detected and sanctioned).

(iii) Further, a review of the criminal law framework is necessary to ensure that it allows for effective enforcement action (both of a ban and of criminal misuse of VAs).

Regardless of their extent, effectively implementing the amendments to the legal framework, requires coun-

[28]See FSB: Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements

[29]This is addressed in more details in the second Fintech Note on VAs and AML/CFT.

tries to adopt practical measures and take necessary policy considerations (e.g., to identify and address misuse of VAs and illegal activities of VASPS, the ability to freeze and seize VAs as discussed further below).

Legal Framework for Preventing and Sanctioning ML and TF

A country's legal framework should adequately criminalize ML and TF activities that involve VAs. Given that VAs are just another representation of value, they should be captured to the same extent as traditional assets. As a result, both the ML offense and the TF offense should apply, regardless of whether traditional assets or VAs are involved. This applies in all cases, including when a country has chosen to ban or restrict VA activities within its territory. In many countries, it is likely that the ML and TF offenses already apply,[30] but in others, this may require amendments to the relevant criminal laws.[31]

Further legal or regulatory changes may be needed to facilitate enforcement actions. Examples of such changes include a broadening of provisions related to customs declarations,[32] international cooperation, or LEA's ability to conduct investigations (e.g., to provide for additional investigative powers specific to VAs), as well as provisions related to freezing/seizing, including in the context of implementation of targeted financial sanctions, confiscating, and management of proceeds of crime, among others.

Financial Intelligence

Some adjustments to existing practices may be needed to ensure appropriate receipt and analysis of financial intelligence. FIUs may wish to revise their templates for reporting to capture additional transaction and customer information specific to virtual transactions (e.g., wallet account information), transaction details (including transaction hash and information on the originator and the recipient), login information (including IP addresses), and mobile device information. FIUs will also need to have a solid understanding of how transactions operate in the virtual space, including in instances where enhanced anonymity features are involved, and the diversity of different types of VAs used for criminal purposes. In addition, FIUs will need to be able to conduct operational analysis based on the information received from VASPs and other reporting entities, thereby building networks of potential subjects and identifying financial transactions that may be indicative of ML/TF/PF activity for sharing with appropriate law enforcement authorities to facilitate investigation.

Investigations and Prosecutions of Activities in the Virtual Space

LEAs need to be able to pursue investigations related to VAs and VASPs. Responsibilities and powers of investigation should notably include compulsory measures for the production of records held by VASPs and for the freezing or seizing of VAs. While many traditional investigative skills remain useful, they may not be entirely sufficient to deal with VAs, and LEAs may need to develop new skill sets related to conducting investigations online (e.g., ability to use monitoring/screening tools to trace VA transactions, searches of cell phones and computers, where permitted). As a starting point, countries should consider whether they have adequate expertise (e.g., investigators specialized in cybercrimes). In many instances, specific training will be useful (e.g., on conducting investigations online, with a focus on identifying VAs and related transactions on the blockchain, and simulation trainings to understand the use of the darknet). In many cases, this might require strengthening interagency cooperation, developing special units with the relevant tech expertise, and ensuring adequate dialogue with foreign counterparts (see Annex 2 for examples).

Some technological solutions can assist with investigations. In addition to having a solid understanding of VAs, the DLT and the measures used to obfuscate the traceability of VA transactions (e.g., mixers), LEAs should also be aware of the new analysis tools available. For example, blockchain explorers are proving useful to investigators as they facilitate blockchain analysis by enabling searches related to addresses, transactions and

[30]This is notably due to the fact that the FATF standards have long required that the ML and TF offenses also apply to "incorporeal assets" and to "funds and other assets" which should include VAs.

[31]This is because *nullum crimen sine lege* and the need to interpret criminal laws restrictively.

[32]Appropriate mechanisms should be in place to detect or declare cross-border movements of VAs, if countries chose to consider VAs and the activities of VASPs to fall under the parameters of physical transportation of physical monetary instruments. If countries consider that this applies to VAs, appropriate changes may need to be made to relevant laws pertaining to cross-border movement of currency and bearer negotiable instruments, to include declaration/disclosure requirements for VAs (e.g., if they are being carried across borders on desktop wallets).

other details on the basis of records maintained by the DLT. Certain firms now specialize in collecting and analyzing transaction data across VA networks.[33] LEAs may therefore consider deploying additional technological solutions to help with their analysis.

Prosecutors and judges will also need to develop their understanding of VAs and VA-related activities. In most instances, given the specific nature of VAs and manner in which VASPs operate, this will most likely require enhanced training of prosecutors and the judiciary to ensure that they are able to understand the technological evidence and legal framework for VAs and VASPs in order to handle cases appropriately.

Seizing, Freezing, Confiscation, and Management of VAs

Where warranted, tainted VAs should be subject to freezing or seizing and confiscation. The circumstances that lead to such measures are likely to be the same as for traditional assets, but the modalities may need to be tailored to the virtual space.

- **Seizing/Freezing**: In order to seize VAs, LEAs typically need to identify both the public and private keys related to VAs and have applications that manage the keys, recovery seeds, and/or VA wallet files. This may require specialist investigative skills and the use of different types of technologies. Given the highly mobile nature of VAs (e.g., any individual with knowledge of a subject's private keys or recovery seed can access the VA wallet despite law enforcement's seizure of wallet), seizure should ideally apply almost instantaneously (e.g., by moving VAs immediately into a LEA-controlled wallet). This may require adjusting some legal requirements and practices (e.g., freezing/seizing orders to be issued by a court) to allow for sufficient speed. Countries may therefore need to establish the relevant framework to allow such possible seizure, as well as to enable LEAs to locate the associated instruments of the wallet or access private keys and/or recovery seeds.
- **Management of seized VAs.** Competent authorities could choose to either (i) convert VAs into fiat currency and manage the seized monies in a traditional fashion or (ii) manage the VAs in their existing form (i.e., creating a wallet—held and managed by LEA or a wallet service provider—into which seized VAs can be moved), which may require new policies and procedures (e.g., maintain records of private keys, recovery seeds).[34] Additional considerations arise from the high-price volatility of VAs, especially in light of potentially lengthy criminal procedures, and cybersecurity related risks. Decisions will need to be taken as to the value at which the VAs should be held (e.g., the price at the time the enforcement measure was taken or the price at the end of the criminal law process), as this can have implications following the adjudication and final outcome of the case. Efforts must also be made to secure the official wallets, commensurate with the cyber risks of the different types of wallet (e.g., cold storage[35] is likely to be less prone to cyberattacks).
- **Confiscation.** Courts should establish how to handle the confiscated VAs. They can choose to hold VAs or convert them to fiat. This may include similar considerations as seizing assets as noted earlier and may require adjusting the legal framework.

International Cooperation

In light of the highly mobile nature of VAs, close and swift cooperation between countries is key. There needs to be a clear legal basis for exchanging information and cooperating, even for countries that have restricted or banned VA-related activities. In some instances, traditional processes such as mutual legal assistance (MLA) requests may be too slow and thus ineffective in a virtual context. Therefore, there may be a greater need to build up informal cooperation channels with different authorities (for instance, police and tax authorities) who would have the ability to take swift, conservatory action, including for freezing/seizing of wallets, until more formal international cooperation processes have been initiated. Where MLA depends on dual criminality, additional issues may arise when other countries' criminal justice frameworks do not properly capture VAs. Finally, good domestic coordination is also useful since different authorities may have different channels for communication with their

[33]Examples of such firms include Chainalysis, CipherTrace, Coinfirm, Scorechain, Merkle Science and TRM Labs.

[34]This is similar to a wallet backup.

[35]Cold storage refers to offline wallets that are not connected to the internet, and can include information stored in paper wallets (which are pieces of paper with information related to keys) and hardware wallets (which can be a remote device with relevant information on keys, which can be connected to a computer as required (e.g., USB sticks)).

foreign counterparts (see examples of LEA cross-border cooperation and initiatives in Annex 2).

Conclusion

The new FATF standards provide much needed clarity on ML/TF/PF risk mitigation in the virtual space. By explicitly addressing VAs in its standards, the FATF has facilitated the transposition of those standards into the domestic legal and regulatory frameworks. This is key in guiding country authorities in the necessary legal and regulatory adjustments that might be needed, and in ensuring greater consistency in countries' approaches to mitigating the financial integrity risks of VAs. By addressing VAs in broadly the same way as other types of assets, the FATF ensured that VAs are treated adequately while taking their intrinsic characteristics into account.

The main challenges to mitigation include keeping up with the technology and increasing dialogue amongst stakeholders. For the foreseeable future, VAs are here to stay and they are likely to be used increasingly in cross-border transactions. In particular, broad use of the so-called GSCs would require rapid and coordinated actions across the globe to manage the associated financial integrity risks. A solid understanding of VAs' underpinnings and operating models is therefore a necessity for all AML/CFT stakeholders. In most instances, this will require building up the expertise and capacity of the relevant domestic authorities: policy makers, AML/CFT supervisors, FIU, LEAs, and the judiciary. Close dialogue with the VASP industry can be particularly helpful in that respect. Given the cross-border nature of the virtual space, close and prompt cooperation among jurisdictions is key to any effective mitigation strategy. Finally, a good understanding of the potential that technology offers to support the implementation of the AML/CFT framework would also be beneficial.

More broadly, the AML/CFT community, including the FATF and international organizations such as the IMF, will need to continue their engagement. Countries are likely to face ongoing challenges in their mitigation of the risks in light of the rapidly evolving nature of VAs. The international community will need to support countries in their efforts to address the challenge. This support should include continued monitoring of developments in the virtual space and continued efforts to facilitate the effective implementation of the FATF standards. For the IMF, this should include the provision of advice and capacity development activities.