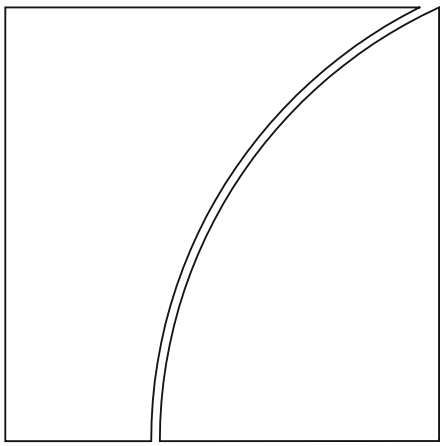
Financial Stability Institute

FSI Insights

on policy implementation

No 31



Supervising cryptoassets for anti-money laundering

By Rodrigo Coelho, Jonathan Fishman and Denise Garcia Ocampo

April 2021

JEL classification: F30, F31, G18, G23, G28, O32, O38
Keywords: anti-money laundering, supervision, cryptoassets, cryptoasset service provider, virtual asset service provider, travel rule, peer-to-peer

BANK FOR INTERNATIONAL SETTLEMENTS

FSI Insights are written by members of the Financial Stability Institute (FSI) of the Bank for International Settlements (BIS), often in collaboration with staff from supervisory agencies and central banks. The papers aim to contribute to international discussions on a range of contemporary regulatory and supervisory policy issues and implementation challenges faced by financial sector authorities. The views expressed in them are solely those of the authors and do not necessarily reflect those of the BIS or the Basel-based committees.

Authorised by the Chairman of the FSI, Fernando Restoy.

This publication is available on the BIS website (www.bis.org). To contact the BIS Media and Public Relations team, please email press@bis.org. You can sign up for email alerts at www.bis.org/emailalerts.htm.

ISSN 2522-2481 (print)
ISBN 978-92-9259-460-2 (print)

ISSN 2522-249X (online)
ISBN 978-92-9259-459-6 (online)

Contents

Supervising cryptoassets for anti-money laundering[1]

Executive summary

Supervision of cryptoasset service providers (CSPs) remains nascent globally. While AML/CFT international standards are in place, most jurisdictions have just begun to implement and enforce them. Across the countries surveyed for this study, there is a range of stages of development, with some countries still finalising their regulations and a small number performing more active supervision, such as conducting examinations and taking enforcement actions. In most cases, however, effective implementation remains a work in progress. As a result, the state of supervision could be best described as in flux, and this study constitutes a snapshot in time.

As jurisdictions finalise regulation, the key question remains as to who and which activities fall within the regulatory perimeter. Regulatory treatment for CSPs is contingent on the risks posed by both the type of cryptoasset(s) offered by the CSP and the activity in which firms engage. Authorities have chosen different criteria for categorising cryptoassets across various jurisdictions and differed in definitions of related activities that would fall into the regulatory scope. Notwithstanding this heterogeneity, authorities largely agree on the application of the basic principle of "same business, same risks, same rules".

The question in turn depends on the authorities' assessment of which risks posed by cryptoassets and related activities should be captured by regulation and, in such case, whether those risks are captured by existing regulation or whether there is a gap that needs to be addressed. For gaps in AML/CFT regulation, implementing international standards, particularly those issued by the Financial Action Task Force (FATF), should provide a solid basis for effective AML/CFT compliance and guidance. An additional challenge relates to the identification of the underlying economic function of the financial services that providers offer, particularly when novel instruments and operating models do not conform to existing definitions.

Overall, most supervisors have an open dialogue with the private sector and provide an "on-ramp" period for service providers. The continuing difficulty for supervisors and the private sector in defining which natural or legal persons are covered by cryptoasset regulation and the generally limited level of knowledge of AML/CFT regulatory requirements in the private sector compared with what exists in more traditional financial services requires partnership between the public and private sectors. While providers are ultimately responsible for understanding and implementing their obligations, extensive outreach and a gradual "on-ramp" of supervision are consistent with the launch of new regulations and a rapid evolution in this industry. Such an approach helps to prevent widespread lack of effective compliance.

While much work remains on implementation, most jurisdictions have performed or are in the process of performing an AML/CFT national risk assessment. These assessments largely conclude that the risks associated with cryptoassets are relatively high or have grown over the last few years, and

[1] Rodrigo Coelho (Rodrigo.Coelho@bis.org) and Denise Garcia Ocampo (Denise.GarciaOcampo@bis.org), Bank for International Settlements, and Jonathan Fishman (jonathan.fishman@treasury.gov), United States Department of the Treasury. The views expressed in this paper are those of the authors and not necessarily those of the BIS, the Basel-based committees or the United States Department of the Treasury.

The authors are grateful to the representatives from the authorities interviewed and to Raphael Auer, Ke Chen, Carolina Claver, Johannes Ehrentraud, Grace Jackson, Ken Menz and Nadine Schwarz for helpful comments. We are also grateful to Esther Künzi for valuable support with this paper.

such assessments should provide a strong basis for calibrating regulation and supervision. However, some assessments could use greater depth and others have not been made public. Where jurisdictions do not publicise at least the key conclusions of their assessments, they miss an opportunity to educate the public, especially in such a new and evolving sector. In addition, the lack of published risk assessments may make AML/CFT risk decisions, such as customer risk scoring in onboarding processes, more difficult for supervisors and the private sector.

Enforcement actions remain limited in number and have been undertaken by very few jurisdictions, leaving room for improvement. This is partly because of the recency of regulation in most jurisdictions. In jurisdictions where such actions have been taken, the sanctioned conduct often has an element of unregistered activity or fraud. Given the importance of public and transparent enforcement actions to demonstrate authorities' commitment to implementing regulations and the role of these actions in helping the overall AML/CFT system to mature, further attention is needed in this area. Having said that, more enforcement actions are expected in the future as the supervisory frameworks in many jurisdictions mature.

The travel rule is a binding FATF obligation, but most jurisdictions have not effectively implemented it. A number of jurisdictions question whether they can reasonably impose the travel rule on CSPs until there are technological solutions available that would make compliance less onerous, as SWIFT does for correspondent banking. Surveyed authorities also raised concerns that if these technological solutions were not commonly accepted or interoperable, compliance with the travel rule would remain burdensome. Other jurisdictions, however, are implementing the rule now since it is currently feasible, albeit difficult. Those that have implemented this requirement could offer an example for those that have yet to do so.

P2P transactions pose challenges, but views differ as to their magnitude. Some jurisdictions consider these transactions as the equivalent of cash exchange and believe the risk they pose falls within the risk tolerance of the FATF standards and national regulation. This is particularly the case where authorities expect P2P transactions to remain limited in number, with most of these assets passing through CSPs before they can be used. The availability of ledger analytic tools to track these assets also partially tempers the concern among some authorities regarding P2P transactions as it suggests transparency is achievable. However, others believe the comparison to cash is not exactly apt and have concerns related to the disintermediation P2P transactions may represent. Moreover, there is a distinct risk that P2P transactions will grow rapidly in scale, especially as cryptoassets become more widely accepted. The potential risks posed by P2P transactions seem to suggest that additional mitigation measures may be needed. In any case, many jurisdictions need a clearer assessment of the risks to guide their decisions going forward.

There is an opportunity to adopt new approaches that take advantage of the inherently data-rich nature of the cryptoasset sector. Authorities are committed to supporting responsible financial innovation while also ensuring adequate supervision. New supervisory methods and suptech applications could help pursue this balance and maximise their resources. That should allow them to make more intensive use of data and technological tools like blockchain analytics to improve the effectiveness of their supervisory frameworks.

International cooperation to oversee this sector effectively is key. The inherently cross-border nature of cryptoassets, as well as the uneven global implementation of international standards in this area, make international cooperation a critical component for effective supervision. This is especially true in view of how new the sector is. Supervisors appear to have the necessary legal authorities and channels for international cooperation in place, but actual use of them is another area requiring improvement.

Section 1 – Introduction

1. **Cryptoassets can be broadly defined as a type of digital asset that depends primarily on cryptography and distributed ledger or similar technology.**[2] This definition includes digital means of exchange and other digital tokens, such as security tokens, asset-linked tokens and utility tokens. This definition, which is used by the Financial Stability Board (FSB) and employed for this study, is slightly different from the term "virtual assets" (VAs) used by the Financial Action Task Force (FATF). The FATF defines a VA[3] as "a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes" and is not limited to digital assets that rely on cryptography and distributed ledger technology (DLT).[4] Both definitions encompass, among others, Bitcoin and so-called stablecoins.[5]

2. **While certain cryptoassets have the potential to make payments and transfers more efficient, some of their features may heighten money laundering/terrorist financing (ML/TF) risks.** In particular, the speed of transactions, global reach and potential for increased anonymity and obfuscation of transaction flows and counterparties make cryptoassets particularly suitable for criminal uses. In addition, some transactions may take place without the involvement of financial intermediaries, in which case no regulated financial institution can necessarily apply AML/CFT preventive measures, such as customer due diligence, record-keeping and suspicious transaction reporting. Moreover, many cryptoassets or service providers specifically incorporate technology designed to prevent transparency, such as tumbling or mixing services or anonymity-enhanced coins (AECs).

3. **The scale of illicit use of cryptoassets is significant, highlighting the importance of AML/CFT regulation and supervision, as well as law enforcement, in this area.** One private sector firm estimates that in 2019 about 1.1% of all cryptocurrency transactions (worth around USD 11 billion) were illicit, an increase from the previous two years.[6] Another firm found in looking at Bitcoin alone that in 2020 criminally associated bitcoin addresses sent USD 3.5 billion.[7] The same source also estimates that a third of the bitcoin sent across borders goes to exchanges with obviously weak customer due diligence controls. The above figures underscore the scale and urgency of the ML/TF threat from cryptoassets and the importance of effective regulation and supervision.

4. **The FATF has acted swiftly with a view to preventing the misuse of VAs for ML/TF.** By 2014, the FATF had already published a report presenting a conceptual framework for understanding and addressing the ML/FT risks associated with virtual assets.[8] Then in 2018, it formally amended the FATF Recommendations to confirm their application to VAs and virtual assets service providers (VASPs).[9] This

2 FSB (2019).

3 FATF (2019a).

4 Another distinction is that FATF's definition of VAs only covers non-legal tender forms of the assets and legal tender forms are covered elsewhere in the FATF standards.

5 Stablecoin is a cryptoasset that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets.

6 Chainalysis (2020).

7 Ciphertrace (2021).

8 FATF (2014).

9 The FATF defines a VASP as any natural or legal person – which is not already covered by financial institutions or intermediaries standards – which as a business conducts one or more of the following activities for or on behalf of another natural or legal person: exchange between virtual assets and fiat currencies; exchange between one or more forms of virtual assets; transfer of virtual assets; safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

amendment required that VASPs be regulated for AML/CFT purposes, licensed or registered, and subject to effective systems for monitoring or supervision in a similar manner to the obligations that exist for other kinds of financial institutions. Detailed guidance on the application of these standards followed in 2019 in the form of an interpretative note, which further clarified the expectations on the application of the risk-based approach (RBA) to VA activities and VASPs; supervision or monitoring of VASPs; licensing or registration; preventive measures; sanctions and other enforcement measures; and international cooperation.[10] More recently, the FATF published a report identifying red flag indicators that will help authorities, financial institutions and VASPs detect whether VAs are being used for criminal activity.[11] While the FATF has thus established international standards in this area, national authorities are free to go above and beyond them.

5. **While significant progress has been made in the adoption of the FATF standards at the national level among some FATF members, the implementation of effective supervisory practices is lagging behind.** A recent report by the FATF[12] indicates that 35 out of 54 reporting jurisdictions had reported that they had implemented the revised FATF standards, with 32 of these jurisdictions regulating VASPs and the other three opting for prohibiting the operation of VASPs in their jurisdiction. The level of implementation in non-FATF members is likely to be much lower. The report also suggests that while there has also been progress in the implementation of VASP supervision, most jurisdictions are in the very early stages in this process and more work is needed to ensure that VASPs meet their AML/CFT obligations.

6. **The effectiveness of international standards depends on effective implementation by national authorities.** This paper assesses AML/CFT supervisory practices relating to CSPs.[13] In light of the recency of supervisory frameworks for cryptoassets and related activities in most jurisdictions, the paper pays particular attention to emerging practices and common challenges faced by financial authorities. Authorities from eight jurisdictions were surveyed and interviewed for this paper.[14] These were selected taking into account both geographical diversity and the maturity of each supervisory framework in this area. Publicly available information such as FATF reports, national risk assessments and published details of enforcement actions were also used as input.

7. **The remainder of this paper is structured as follows.** Section 2 outlines the national regulatory frameworks for cryptoassets and CSPs with a particular focus on AML/CFT obligations. Section 3 presents the supervisory approaches used to address the ML/TF risks in CSPs. Section 4 discusses the key features of remedial measures and enforcement actions applied to address regulatory concerns and breaches, while Section 5 explores approaches to ensuring effective cooperation and information-sharing. Section 6 concludes the paper and identifies policy priorities.

10 FATF (2019a).

11 FATF (2020b).

12 FATF (2020a).

13 For the purposes of this paper, the term "cryptoasset service provider" (CSP) is used to refer in general to any natural or legal person which as a way of business engages in activities related to cryptoassets. These activities may include creating, distributing, storing, exchanging or providing supporting services related to cryptoassets. The term "VASP" is used whenever we are referring to the FATF's work.

14 Canada (CA), Germany (DE), Japan (JP), the Netherlands (NL), Singapore (SG), Switzerland (CH), the United Kingdom (UK) and the United States (US).

Section 2 – Regulatory frameworks

8. **Novel cryptoasset business models may pose financial crime, consumer/investor, market integrity and financial stability risks[15] not yet captured by the existing regulatory frameworks, presenting challenges on adapting regulations to meet new needs.** This is the case, for example, of financial crime risks posed by new market actors such as cryptoasset issuers, exchanges and wallet providers, or of financial stability risks posed by global stablecoin arrangements. On a global basis, international standard-setting bodies (SSBs)[16] have broadened the scope of their standards and recommendations (eg FATF), have revised them (eg FSB) or are in the process of assessing the adequacy of their standards (eg the Basel Committee on Banking Supervision, the Committee on Payments and Market Infrastructures and the International Organization of Securities Commissions) to capture the different risks for the global financial system posed by cryptoassets and related activities not previously covered in their frameworks.

9. **Regulatory treatment for cryptoassets and CSPs is contingent on the risks posed by both the type of cryptoasset and the activity in which firms engage.** If the risks posed by a cryptoasset are the same as those of an existing regulated product, service or intermediary, then the relevant rules apply to the cryptoasset or CSP. In such cases, authorities are clarifying the application of existing requirements by providing guidance, amending their regulation or referencing them in crypto-specific frameworks. For risks which are not yet captured by existing frameworks, jurisdictions are assessing whether such risks should be covered by regulation and, in such cases, whether there is a gap[17] that needs to be addressed through new requirements. However, there are at least two relevant challenges when analysing regulatory treatment of CSPs: absence of a common classification of cryptoassets, and the lack of a harmonised scope of activities that define whether an entity is considered a CSP among SSBs and across jurisdictions.[18]

Regulatory classification of cryptoassets

10. **Authorities consider a number of factors to understand the nature of and assess the risks posed by cryptoassets.** These include, but are not limited, to:

- nature of the issuer (eg identifiable, non-identifiable; public, private; regulated, unregulated);
- intended use of the cryptoasset (eg used as a means of raising funds, of investment, of payment, granting rights to services/products in a company's network or ecosystem);
- holders' rights (eg claim to the delivery of an underlying asset, to a granted interest, to access or use a service in a network or platform);
- claim redemption (eg contractual claim, fixed redemption claim, dependent on price development);
- control over the ledger (eg open to the public, open to specific parties, closed to a limited number of authorised parties);

15 See Cuervo et al (2019) for illustrative examples of cryptoasset-related risks.

16 See FSB (2019a).

17 See FSB (2019a) for an overview of the work done by SSBs to address potential gaps in the regulation of cryptoassets and FSB (2020) for an analysis of potential gaps in existing regulatory frameworks in relation to stablecoins and "global stablecoin" arrangements. At a European level, see Saulnier and Giustacchini (2020) for examples of gaps in existing EU regulatory and legal frameworks.

18 While these are challenges in the analysis of cryptoasset regulatory frameworks, such challenges of non-identical definitions and regulatory treatments apply across a broad scope of financial activities as well.

- validation of the ledger (eg permissioned, permisionless); and
- mechanism to transfer the cryptoasset's ownership (eg centralised, peer-to-peer, decentralised).

11. **To define the appropriate regulatory treatment, authorities find it helpful to differentiate cryptoassets by certain criteria.** There are a number of different criteria for classifying cryptoassets. Examples of criteria used by some jurisdictions or SSBs to categorise cryptoassets are functionality, stabilisation mechanism and systemic importance (Table 1). Classification criteria are likely to continue to evolve as new business models emerge in the markets.

Selected examples of cryptoasset classification criteria — Table 1

Functionality criteria

Categories	Payment/exchange	Investment	Utility
Description	Intended to be used as means of payment or exchange	Provides rights and obligations similar to traditional financial instruments like shares, debt instruments or units in a collective investment scheme.	Grants holders access to a current or prospective service/product in one or multiple company's network or ecosystem
Subcategories or labels*	payment token, e-money token, exchange token	security token	utility token
	hybrid token		

* Examples of subcategories or labels used by some surveyed authorities

Stabilisation mechanism criteria[19]

Categories	Asset-linked	Algorithm-based
Description	Stablecoin that purports to maintain a stable value by referencing physical or financial assets or cryptoassets (FSB (2020)). Can be further differentiated into currency-based, financial instrument-based, commodity-based and crypto asset-based stablecoins.	Stablecoin that purports to maintain a stable value via protocols that provide for the increase or decrease of the supply of the stablecoins in response to changes in demand (FSB (2020)).
Subcategories or labels**	asset-referenced token, stable token	algorithmic stablecoins

Systemic importance criteria

Categories	Global	Non-global
Description	Stablecoins with a potential reach and adoption across multiple jurisdictions and the potential to achieve substantial volume (FSB (2020)).	Stablecoins without a potential reach and adoption across multiple jurisdictions and the potential to achieve substantial volume.
Subcategories or labels**	significant asset-referenced token, significant e-money token, systemic stable token	asset-referenced token, e-money token, stable token

** Examples of subcategories or labels proposed in regulations currently in consultation processes in some surveyed jurisdictions.[20]

[19] Applicable to cryptoassets designed to maintain a stable value (so-called stablecoins) relative to another asset (typically a unit of currency or commodity) or a basket of assets. These may be collateralised by fiat currency or commodities, or supported by algorithms. See FSB (2020) for further information.

[20] See EC (2020) and HM Treasury (2021).

12. **There is no internationally agreed taxonomy for classifying cryptoassets across different types of regulations (eg prudential, market integrity, consumer protection, AML/CFT or data privacy regimes).**[21] Rapidly changing technologies and new business models in this area also pose a challenge in defining a taxonomy for these assets. Furthermore, complexity is added when cryptoassets fall into two or more categories depending on their design features and intended use over their life cycle.[22]

13. **As with any other financial product or service, the classification of the cryptoasset determines which regulation applies.** In general, underlying financial service functionality is the criterion used by authorities to determine whether an entity dealing with a particular cryptoasset falls within the regulatory perimeter[23] and, if so, which legal body and respective obligations apply. If the features of a cryptoasset are such that it performs the same function as a regulated product or service, then the same rules apply to the entity on banking, payment services, fund management, securities trading, financial market infrastructure, consumer/investor protection or AML/CFT regulation. Some jurisdictions are adding the stabilisation mechanism and systemic importance criteria in regulatory proposals currently in process of consultation to address the potential risks[24] that stablecoins could pose when widely used as means of payment.

Definition of cryptoasset service providers

14. **A number of activities can be performed with cryptoassets.** These include activities which by nature may be mapped to the ones performed in traditional financial markets (eg providing money transfer) and others which are completely new to the financial system (eg mining). Aiming for a comprehensive view of all services and actors involved, cryptoasset-related activities may be mapped to the life cycle of the cryptoasset itself. Based upon the conceptual framework proposed by the Cambridge Centre for Alternative Finance (CCAF) (2020a) on the phases of a digital asset[25] life cycle, there are three categories by which cryptoasset-related activities may be classified:

- Primary market activities: relate to the issuance and distribution of assets (eg issuer and investor onboarding, deal structuring, risk assessment, asset registration, distribution of the asset to market participants).
- Secondary market activities: comprise trading (eg admission of the asset to trading, price discovery, order matching, asset transmission), clearing and settlement and servicing (eg asset management, custody).
- Tangential activities: aimed at supporting and ensuring that primary and secondary market activities are conducted in an efficient manner (eg infrastructure services, ancillary services).

[21] The MiCA proposal is the first regulatory approach that intends to harmonise cryptoasset classification for regulatory purposes among EU members states. See EC (2020).

[22] For instance, this may be the case of stablecoins, which could be classified under more than one category and such classification could change as the nature and use of a stablecoin evolves (FSB (2020)).

[23] The regulatory perimeter describes the boundary that separates regulated and unregulated financial services and determines the type and scope of rules (eg on safety and soundness, consumer/investor protection, AML/CFT) applicable to firms conducting regulated activities.

[24] See Arner, Auer and Frost (2020) for an analysis of risks and potential regulatory treatment for stablecoins and FSB (2020) for an analysis of potential risks to financial stability from "global stablecoin" arrangements and high-level recommendations for their regulation, supervision and oversight.

[25] For the CCAF, cryptoassets are a subset of digital assets: "this distinction is based on the novel characteristics that set them apart from other digital assets: (i) the lack of a formal issuer, and (ii) the unique incentive role performed in the underlying distributed ledger or application". See CCAF (2020a).

15. **For regulatory purposes, the definition of a CSP is contingent on the activities in which it intends to engage and whether the activity is carried out by way of business.** As in the case of cryptoassets, there is no common international taxonomy agreed by regulators to categorise the activities involving cryptoassets at this juncture. Consequently, the scope of activities and actors which are considered to define whether an actor is a CSP for regulatory purposes varies among jurisdictions.

16. **To address this challenge in the financial crime area, the FATF has introduced a definition of a "virtual asset service provider" (VASP).** For ML/FT risks, the FATF defines[26] a VASP as any natural or legal person – which is not already covered by financial institutions or intermediaries standards – which as a business conducts one or more of the following activities for or on behalf of another natural or legal person:

(i) exchange between virtual assets and fiat currencies;

(ii) exchange between one or more forms of virtual assets;

(iii) transfer of virtual assets;

(iv) safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and

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

17. **Notwithstanding the VASP definition, surveyed jurisdictions differ from each other and from FATF standards in the scope of the activities considered to define an actor as a CSP.** For example, in some jurisdictions, the exchange between one or more forms of cryptoassets is not within the regulatory perimeter. In others, token issuance providers are not considered CSPs. In yet other cases, authorities go beyond the scope defined by the FATF. In Japan, for example, network operators, gatekeepers, platform and application developers and technical maintenance providers, according to their business scheme, can be considered to fall under regulated CSPs (eg application developers in a decentralised finance[27] (DeFi) ecosystem). In the United Kingdom, P2P exchange platforms are considered CSPs.[28] Table 2 below shows the differences in the activities considered to define an actor as a CSP across surveyed jurisdictions.

18. **CSPs have to comply with different regulatory requirements within and across jurisdictions.** These may include requirements related to authorisation, capital requirements, risk management, governance, security, operational resilience, reporting, market conduct and financial integrity. These regulatory requirements may vary depending on the nature of the service provided or the risks posed by the features of the cryptoasset for which the service is provided.[29]

[26] See FATF (2019b).

[27] Decentralised finance (DeFi) refers to the decentralisation in the provision of financial services through a combination of infrastructure, markets, technology, methods and applications (Arner, Buckley and Zetzsche (2020)). There are a number of different types of decentralisation in financial services. These vary in the degree to which they affect different segments of financial services, but generally take three broad forms: decentralisation of decision-making, decentralisation of risk-taking and decentralisation of record-keeping (FSB (2019b)).

[28] This is the case where the provider is a centralised entity that is completing, matching or authorising a transaction between two people.

[29] For example, the EU proposal of regulation on cryptoassets considers a different amount of permanent minimum capital requirement depending on the nature of the service provided as well as additional obligations for specific cryptoasset services. In addition, the EU proposal considers that some requirements may be enhanced for service providers of stablecoins which could pose systemic risks for the financial sector. See EU (2020) for further information.

Who is considered a CSP?*

Table 2

Activity/service**	CA	CH	DE	JP	NL	SG	US	UK
1. Issuance and distribution								
Issuance (eg Tokeny)	✓	✓	✓	✓		✓	✓	✓
Distribution (eg Binance Launchpad)	✓	✓	✓	✓		✓	✓	✓
2. Trading								
Exchange (virtual to fiat) (eg Quoinex, Coinbase, Binance)	✓	✓	✓	✓	✓	✓	✓	✓
Exchange (virtual to virtual) (eg Qryptos, Coinbase, Binance)	✓	✓	✓	✓		✓	✓	✓
Brokerage (eg Liquid, Binance)	✓	✓	✓	✓	✓	✓	✓	✓
OTC services (eg Cumberland)	✓	✓		✓	☑	✓	✓	✓
Market-making (eg Algoz)		☑		✓		✓	✓	
3. Servicing								
Asset management (eg Bitwise)	✓	✓		✓		✓		✓
Custody (eg Bitwise)	✓	✓	✓	✓	✓	✓	✓	✓
Providing operational and administrative services (eg Fidelity Digital Assets)	✓	☑	✓	✓		✓	✓	✓
4. Other supporting activities								
Infrastructure (network operation, transaction validation and processing, platform and application development, technical support)		☑		☑				
Ancillary services (data and analytics, advisory, rating, accounting, insurance)						***		

(*) This table shows a high-level summary of some jurisdictions' regulatory treatment of certain activities, and the legal and regulatory frameworks and treatment of particular businesses schemes or activities depend on their specific facts and circumstances.

(**) Clearing and settlement activities are not covered in our analysis given that up-to-date financial market infrastructure operators do not use cryptoassets for clearing and settlement activities.

(***) Accountants and insurance intermediaries are subject to AML/CTF regulation but are not considered as CSPs.

☑ Dependent on the business scheme if entities practically provide the intermediary functions of cryptoasset exchange/transfer/administration, such entities can be subject to regulation.

CCAF (2020a) definitions:
Issuance: definition of cryptoasset nature and form, assessment of the suitability of the cryptoasset to be issued and issuance to market.
Distribution: initial offering of the cryptoasset, including investor onboarding.
Exchange: venue for buyers and sellers to exchange cryptoassets.
Brokerage: arranging trade by bringing buyers and sellers together on a commission basis.
Over-the-counter (OTC) services: facilitating trade taking place outside a formal trading venue.
Market-making: providing liquidity to the markets by buying and selling cryptoassets.
Asset management: managing cryptoasset portfolios on behalf of clients on a commission basis.
Custody: safekeeping of assets.
Operational and administrative services: asset servicing such as interest and dividend payment, corporate actions.

Source: FSI staff.

AML/CFT regulation of cryptoasset service providers

19. **Some authorities have adjusted their regulatory perimeter to include cryptoassets, related activities and providers under the scope of the AML/CFT framework.** By doing so, they have aligned their regulatory frameworks with most of the recommendations issued by the FATF in 2018[30] and in 2019 (Box 1), although some of these recommendations have yet to be implemented by some countries. In other jurisdictions, the AML/CFT legal framework was considered sufficiently flexible to accommodate CSPs without requiring any specific changes. In those cases, de facto implementation took place via issuance of guidance and interpretation notes by financial sector authorities. In other cases, the requirements were introduced in a crypto-specific regime. As the FATF pointed out in its 12-month review of the revisions to its standards, however, the vast majority of jurisdictions in the world have not implemented these standards or done so fully. The surveyed jurisdictions are therefore not representative in this regard.

Box 1

FATF standards and guidance on virtual assets and virtual asset service providers

The FATF standards ensure that VAs are subjected to fundamentally similar objections as those which apply to other kinds of assets. The FATF's rules apply when VAs are exchanged for fiat currency, but also when they are transferred from one VA to another, among other circumstances, such as administration of assets and financial services related to initial coin offerings. To date, the FATF has issued the following standards and guidance:

- Amendment to FATF Standards (October 2018): The FATF adopted changes to its Recommendations to explicitly clarify that they apply to financial activities involving virtual assets, and also added two new definitions to the Glossary, "virtual asset" (VA) and "virtual asset service provider" (VASP).
- Amendment to FATF Standards (June 2019): The FATF adopted an Interpretive Note to Recommendation 15 to further clarify how the FATF requirements should apply in relation to VAs and VASPs, in particular with regard to the application of the risk-beased apporach to VA activities and VASPs; supervision or monitoring of VASPs; licensing or registration; preventive measures, such as customer due diligence, record-keeping, and suspicious transaction reporting; sanctions and other enforcement measures; and international cooperation.
- FATF Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (June 2019): The FATF adopted this guidance to provide details of the full range of obligations applicable to VASPs as well as to VAs under the FATF Recommendations, following a Recommendation by Recommendation approach.
- Twelve-Month Review of Revised FATF Standards on Virtual Assets and VASPs (July 2020): FATF report that sets out the findings of a review of the implementation of its revised standards 12 months after finalisation of these amendments. The report found that while progress has been made, there are gaps in global implementation of the FATF standards, especially among countries in the FATF's global network.①

① As of publication of this study, a revision to the June 2019 guidance and a second iteration of the 12-month review were under way.

Source: FATF.

20. **There is significant variability in the definition of the regulatory perimeter across jurisdictions.** All surveyed jurisdictions already regulate certain categories of service providers such as the ones facilitating the exchange between cryptoassets and fiat currencies. Others, however, are left outside the supervisory perimeter. There is therefore no common understanding on the entities and activities that

[30] This was the case, for example, in the European Union, where national authorities have transposed the amendments of the Fifth Anti-Money Laundering Directive (AMLD5) into their respective legislation.

lie within the scope of regulation and supervision. Ongoing work at the FATF to address these questions in guidance currently under way may be helpful in this regard.[31] To overcome challenges posed to defining whether a business models falls into the regulatory perimeter, some jurisdictions, eg the United Kingdom, are applying a case by case approach (Box 2).

Box 2

Regulatory perimeter: the Financial Conduct Authority's case by case approach

In 2019, the Financial Conduct Authority (FCA) published guidance on the regulatory perimeter in relation to cryptoassets to give market participants and interested stakeholders clarity on the types of cryptoassets that fall within the FCA's regulatory remit. This guidance recognised the diversity of business models in the cryptoasset space in the United Kingdom. From January 2020, the FCA became the AML/CFT supervisor for certain cryptoasset activities. As part of the regime created by the Money Laundering, Terrorist Financing and Transfer of Funds Regulations (MLRs), any firm that is in scope had to apply for registration with the FCA. The FCA received a significant number of applications from firms with different business models, some of which were already regulated by the FCA for other activities whilst others were new to regulation.

A key challenge faced by the FCA was to analyse the business models of each firm to establish if the firm was within the scope of the regime and could be effectively supervised. The FCA created a "cryptoasset perimeter" group with experts from across the FCA including legal, supervisory, authorisation and policy teams. This group considered the registration cases involving complex business. This has enabled the FCA to understand the types of business within the regime's scope, identifying group structures and the interplay between them and identifying money laundering or terrorist financing risks posed by these diverse business models.

In the course of the perimeter group's work, the FCA identified firms that needed to be registered under the MLRs as well as to hold FCA authorisation for activities within the Regulated Activities Order in relation to the Financial Services and Markets Act (examples were wholesale firms, such as multilateral trading facilities and payments firms, eg e-money and payments institutions). It was necessary to look closely at the roles and responsibilities of the permissions that the firm was seeking in order to ensure that there was no gap in responsibilities and that appropriate supervisory strategies could be developed when registered and authorised.

Similarly, the FCA saw businesses that acted as cryptoasset traders which allow consumers to access the cryptoasset ecosystem using the facility of cryptoasset P2P exchanges. The group looked carefully at how these models worked, seeking extensive information including contracts and agreements between the entity and the various P2P exchanges and how commissions/fees were paid out to make a determination. Those traders that seemed to be acting by way of business in the United Kingdom were typically considered to be within the scope of the regulations; however, the determination relies on a case by case assessment for which the FCA provided more detailed guidance to include factors to consider when deciding if the firm is acting by way of business in the UK.①

① FCA (2021).

Source: Financial Conduct Authority.

21. **Several authorities have enlarged the scope established by the FATF standards[32] and also regulate providers offering services in their jurisdictions, even if those service providers are located and legally domiciled elsewhere.** This goes beyond the minimum requirement of regulating VASPs incorporated or created in the jurisdiction, or where their place of business is located if a natural person. In such cases,[33] AML/CFT requirements apply equally to domestic and foreign-located CSPs, even if they do not have a physical presence in their jurisdiction and regardless of where the CSP is incorporated or

[31] The FATF Supervisors' Forum is another initiative which provides authorities with the opportunity to discuss how to implement the new global standards on VAs and VASPs.

[32] The FATF standards require authorities to regulate at least CSPs incorporated in their jurisdiction.

[33] Canada, Japan, Netherlands, Singapore and the United States.

headquartered, as long as it does business in the jurisdiction in question. This practice gives rise to the question of how to define "offering services." Canada, the Netherlands and Singapore have released public guidance to offer regulatory clarity on this. Some authorities are currently assessing whether to include into the regulatory perimeter financial accounts with cryptoassets held in foreign-located CSPs.[34]

Box 3

CSPs subject to regulation in the Netherlands

In November 2019, the Netherlands Bank (DNB) published guidance to clarify which entities providing services for the exchange of cryptoassets or custodian wallets, in a professional capacity or on a commercial basis, are subject to the DNB's regulatory framework and required to register as a CSP.

Under this guidance, entities providing services from the Netherlands, either domestically or abroad, are required to register as CSPs. In addition, entities providing services in the Netherlands from another EU member state (including non-EU member states that are party to the Agreement on the European Economic Area), irrespective of whether they are also registered there, are also required to register with DNB. In the case of the latter, a variety of factors are considered to determine whether foreign entities are providing services in the Netherlands, including whether there are payments made by the entity to a search engine service for displaying advertisements in one or several member states or whether the entity shows reviews from customers from specific countries on its website.①

① Entities operating from another country that is not an EU member state are prohibited from providing cryptoasset-related services. Entities established in a non-EU member state that wish to provide these services in the Netherlands must establish a presence in the Netherlands or another member state and apply for registration with DNB. If they fail to do so, they are in non-compliance with the Dutch AML/CFT legal framework, and DNB can take appropriate enforcement action.

Source: Netherlands Bank (2019).

22. **Some authorities have imposed a ban on all or certain activities with cryptoassets.** In some jurisdictions, for example, the marketing of financial products to retail clients for which the return depends, directly or indirectly, on virtual currencies is prohibited (eg Belgium). In others, all cryptoasset-related activities are considered illegal (eg China).[35] Notwithstanding this prohibition, national authorities in these jurisdictions are expected by the FATF standards to assess their risks and to take actions to identify illicit CSP activity.

23. **Licensing and registration regimes of CSPs vary among jurisdictions.** CSPs in Canada, Germany, Switzerland and the United States are authorised under existing licensing or registration processes depending on the type of service provided and the economic function of the cryptoasset supported (eg payment institution, e-money institution, payment service provider, money services business, trading facility or broker-dealer). Other jurisdictions such as Japan,[36] the Netherlands, Singapore and the United Kingdom have introduced FATF recommendations into a bespoke licensing or registration regime where CSPs need to apply for crypto-specific types of licence or registration (eg cryptoasset exchange provider, custodian wallet provider or digital payment token service provider).[37]

[34] For example, in December 2020 the Financial Crimes Enforcement Network (FinCEN) announced in Notice 2020-2 that it plans to revise the regulations implementing the Bank Secrecy Act to expand reportable accounts of foreign financial accounts to include virtual currency as a type of reportable account.

[35] See Ehrentraud et al (2020).

[36] Under Japanese regulation, CSPs are to be regulated under the name of "crypto-asset exchange service provider", whether CSPs provide cryptoasset exchange or custodial etc services, as long as they pass the bespoke regulatory scrutiny aligned with each business model.

[37] See CCAF (2020b) for an analysis of a geographical distribution of licensed firms and types of licences held.

Licensing/registration regimes for CSPs

Table 3

	Licensing/registration regime	Number of registered/licensed CSPs
CA	Registration with the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) as a money service business (MSB); more specifically, an MSB dealing in virtual currency (VC).	158 MSBs have registered for VC activities; 379 registered MSBs are updating their registration information to add VC services to their list of activities (as of Jan 2021).
CH	Licensed by the Swiss Financial Market Supervisory Authority (FINMA) under existing prudential rules (eg a banking licence; securities dealer)[38] or required to become a member of a self-regulatory organisation supervised by FINMA.	130 firms providing custody wallet services and operating trading platforms with virtual currencies (as of Sep 2020).
DE	Licensed by the Federal Financial Supervisory Authority (BaFin) as "crypto custody business" for activities related to the custody of cryptoassets. For other activities, licensed by BaFin either as "banking services" conducted by credit institutions or as "financial services" that may be conducted by banks and by "financial services institutions".	Not available.
JP	Registration with the Financial Services Agency of Japan (JFSA) as "crypto asset service provider".	25 firms registered as CSP (as of Dec 2020).
NL	Registration with DNB as "crypto service provider".	16 firms registered as CSP (as of Feb 2021).
SG	Licensed by the Monetary Authority of Singapore (MAS) under the Securities and Futures Act as a recognised market operator or capital market services licence holder; or under the Payment Services Act as a Standard Payment Institution or Major Payment Institution under the activity of "digital payment token service providers".	10 firms licensed under the Securities and Futures Act and 103 firms providing digital payment token services under the Payment Services (Exemption for Specified Period) Regulations 2019, whose licence applications are being processed by MAS (as of Jan 2021).
UK	Registration with the Financial Conduct Authority (FCA) as "cryptoasset exchange provider" and "custodian wallet provider".	104 firms operating with temporary registration and four with full registration (as of Jan 2021).
US	Acting as MSB, subject to licensing and registration obligations for each state in which they operate in addition to federal registration requirement. Acting as commodity futures merchants, subject to licensing and registration obligations under the Commodity Futures Trading Commission (CFTC) specific to their type of financial intermediary. Acting as a participant in the securities markets, subject to registration obligations under the Securities and Exchange Commission (SEC) specific to their type of business, as well as licensing with a self-regulatory organisation, such as FINRA, and often in the states in which they operate. Acting as a depository institution or trust, subject to charters (such as bank charters) at the state and/or federal level. Entities such as futures commission merchants and introducing brokers are required to register with the CFTC; MSBs are required to register with the Financial Crimes Enforcement Network (FinCEN); and participants in securities markets such as national securities exchanges, securities brokers and dealers, clearing agencies, investment advisers, and investment companies are required to register with the SEC.	Over 420 firms are registered with FinCEN as MSBs, which are also listed in the FinCEN-managed public MSB registrant database. A number of firms (currently fewer than 20) are registered with FINRA as broker-dealers permitted to transact in cryptoassets that are securities. These brokers along with broker-dealers who deal in traditional (eg non-cryptoasset) securities are listed on the Brokercheck website maintained by FINRA (as of Jan 2021).

[38] Where a firm lodges virtual currency holdings on a commercial basis from customers in "wallets" and manages accounts for them, a banking licence is required. For firms operating blockchain-based applications like crypto trading platforms, a security dealer licence is required. Other types of blockchain-based applications may require a financial market infrastructure licence.

24. **CSPs in all surveyed jurisdictions have to comply with most AML/CFT preventive measures established in the FATF recommendations in a manner similar to other kinds of financial institutions.**[39] These obligations include:

- performing customer due diligence (CDD) on new and existing customers;
- record-keeping of transactions where required ;
- assessing risks and applying a risk-based approach;
- having internal controls to assess compliance with AML/CFT policies;
- performing enhanced due diligence (EDD) in specific circumstances; and
- reporting their suspicions promptly to the relevant Financial Intelligence Unit.

25. **There is, however, one exception – the so-called "travel rule" (TR)**. The travel rule in this context refers to how the FATF applies its wire transfer rules to cryptoassets. This requirement establishes that, for any cryptoasset transfer, CSPs must obtain and hold accurate information on the originator and beneficiary and submit this information to the next financial intermediary in the transaction. While this is a part of the FATF recommendations, several surveyed jurisdictions have not implemented this requirement.

Box 4

Implementing the travel rule

The application of the FATF's standards related to wire transfers, known colloquially as the travel rule (TR), stands out as an area in which there is significant diversity across jurisdictions and a need for more consistent supervision. The FATF has provided clear guidance that its Recommendation 16, which imposes the TR, is a current, binding obligation.

For instance, the TR has been an obligation in the United States for bank and non-bank financial institutions since 1996. Entities subject to the TR must share certain information such as names, addresses and account numbers of both the originators and beneficiaries for payments of USD 3,000 or more with the receiving financial institution or money services businesses.

However, other jurisdictions remain uncertain how to apply the TR, in light of the fact that the robust infrastructure available to support compliance for banks is lacking for cryptoasset providers, making compliance for them technically feasible but much less efficient than for banks. Accordingly, regulatory implementation and supervision of this recommendation exists in a limbo for many jurisdictions. Some authorities noted that waiting for the further development of efficient tools before implementation may create a disincentive for the private sector to develop better tools, as the private sector may be faced with more stringent supervision once they are in place. Some jurisdictions are, moreover, uncertain as to what technological threshold they would need to see the industry reach in order to consider implementation feasible. Another challenge is the interoperability of these solutions. Even if a feasible solution is developed, it is likely that the integration of two or more different solutions will not be straightforward. As a result, international cooperation in this area seems key to achieving a global solution.

Efforts by private industry are ongoing to develop a solution or protocol that would enable TR compliance. For example, the InterVASP Messaging Standard Overview – IVMS101 is a technical data standard developed by the private sector to enable interoperability between protocols. In addition, by August 2020 the first transmission between two Swiss CSPs took place using the Travel Rule Protocol (TRP) implemented as a software solution by the Swiss software developer 21 Analytics. Similarly, by November 2020 Sygna Bridge was the first solution to go through an independent assessment by the Association of Cryptocurrency Enterprises and Startups in Singapore. However, neither of these solutions has been widely adopted.

[39] Similarly, although financial institutions engaging in supporting activities with cryptoassets are not considered CSPs, they are subject to the same AML/CFT preventive measures.

Section 3 – Supervisory practices

26. **Supervision of CSPs is at the early stages of implementation in most jurisdictions.** Supervisory implementation of regulations remains in a nascent stage, with many of the world's leading economies still in the process of developing an approach to cryptoassets. Many of the jurisdictions consulted for this study were in the process of bringing regulation and supervision online as the study progressed, with efforts delayed by the Covid-19 pandemic and other unexpected complications in practical implementation. As a result, their recent supervisory work has focused on ensuring robust registration and licensing of new entities, providing guidance on supervisory expectations and in some cases detecting unlicensed service providers. Some desk-based supervision has also taken place.[40]

27. **Almost all the surveyed jurisdictions have undertaken some process of risk assessment relative to cryptoassets and made results available to the public.** However, globally, jurisdictions vary greatly in the recency and comprehensiveness of these efforts, and there may be scope to deepen risk assessments and fortify efforts to share conclusions with the public. Competent authorities in Japan and Switzerland, for instance, have included cryptoassets in their national money laundering and terrorist financing risk assessment process, and other jurisdictions have specifically studied the risk of cryptoassets in a standalone process. Among surveyed jurisdictions, the general consensus suggests a rising level of ML/TF risks related to cryptoasset activities, as multiple jurisdictions report that their risk assessments currently in process are likely to show an increased risk when compared with previous assessment exercises. While part of this rise may result from increased awareness of risks that already existed, most jurisdictions appear to believe that the inherent risks themselves are growing to one degree or another.

Box 5

Switzerland's 2018 National Risk Assessment

In October, 2018, Swiss authorities published the results of a dedicated risk assessment on cryptoassets. The thorough, 45-page report concluded that although the observed number of Swiss money laundering cases at the time was low and no cases could be found of terrorist financing, the risk was nonetheless high, both to Switzerland and internationally. Swiss authorities highlighted anonymity and the tendency towards the disintermediation of financial institutions in the sector as the primary drivers of the risk. Switzerland's assessment also discusses the importance of law enforcement efforts alongside those of supervisors and gives an explanation of how some common business models fit into the Swiss regulatory framework.

The report emphasises that international cooperation and coordination is among the most important tools needed to combat the risks posed by cryptoassets and notes the importance of consistent global implementation of the FATF's standards in this regard: "Due to the transnational nature of the dangers of money laundering and terrorist financing using cryptocurrencies, the most important measures to reduce the associated risk must be coordinated at the international level." The risk of poor results from international cooperation requests and regulatory arbitrage by companies receives specific mention and Switzerland expresses a specific commitment to encourage "harmonised" international implementation of FATF standards as one of its key policy responses to the identified risks.

Source: Swiss Confederation (2018).

28. **As with AML/CFT regulation, supervisory practices across the surveyed jurisdictions differ most significantly in their fundamental approach to the incorporation of cryptoassets.** While some jurisdictions apply their existing AML/CFT supervision frameworks to cryptoassets, others consider CSPs an entirely new category of financial institution and apply a framework specifically designed to address

[40] Canada and the United States, for instance, have experimented with virtual or partially virtual exams due to Covid-19, with largely positive results. German supervisors have also undertaken remote processes during the pandemic, despite having been forced to adapt some activity.

them. Jurisdictions appear to agree on the need for agile frameworks that can evolve with technological innovation, although they have taken different avenues to achieve this. The fundamental question is whether cryptoassets are a new way to provide the same financial services as more traditional institutions such as banks which are addressed in existing regulation, or are instead providing a new financial service which existing regulation does not cover. Each approach has strengths and weaknesses, but overall more jurisdictions are moving to a functional approach based on the underlying financial service provided. Many jurisdictions see this foundation as offering more flexibility, more technology neutrality, and less need to evolve the regulations as quickly as the technology evolves. This approach is not, however, universal.

29. **Some jurisdictions have created a dedicated supervisory team specifically focused on cryptoassets, and others intend to do so.**[41] Those that have not taken this approach have instead attempted to develop and integrate new expertise into their existing personnel and practices. Some jurisdictions also indicated an intent to create a unit focused on cryptoassets. Overall, jurisdictions agree that simply continuing their current practices without evolution or modernisation does not give them sufficient capacity. Successfully developing cryptoasset expertise and integrating it into existing supervisory practices poses a challenge for all supervisors.

Box 6

The Financial Services Agency of Japan's dedicated supervisory team

In 2017, in response to the unique challenges posed by cryptoassets, the Financial Services Agency of Japan (JFSA) established the Fintech Monitoring Office composed of specialists in information technology including blockchain and experts on AML/CFT regulation. As early as 2018, after assessing AML/CFT internal controls and risk management systems of provisionally registered CSPs as inadequate, the JFSA took a range of supervisory actions, including business improvement and suspension orders. In addition, the JFSA declined the definitive registration of various CSPs whose governance and/or AML/CFT regime were considered weak.

Since then, the team has been closely monitoring registered CSPs as well as following up on their actions to address the shortcomings that had been previously identified. In order to do that, supervisors have at their disposal an extensive amount of qualitative and quantitative information that the JFSA collects regularly from CSPs. This includes information on the risk profile of their clients, services provided, types of cryptoassets transacted and the risk analysis and transaction monitoring tools used by the CSP. The JFSA uses these data to assess the CSP's risk exposures and assign a risk rating to individual entities. The team then further utilises the results to develop annual on- and off-site monitoring plans, and identifies prioritised target accordingly. The JFSA's specialists also conduct extensive private sector outreach to maximise the benefit from their expertise.

30. **Most jurisdictions have thus far taken limited measures to implement active supervision, especially on-site examinations.** Most surveyed authorities intend to ramp up these efforts as their regulation matures, and the lack of active supervisory measures appears to be a product of the simple fact that the regulations themselves are so new and authorities are focused primarily on working through initial licensing as well as outreach and education. Covid-19 has also played a role in creating delays. However, there are exceptions to this rule. Japan, Switzerland and the United States, for example, have conducted a number of on-site and remote examinations.

31. **The means used to prevent unregistered or unlicensed providers of cryptoasset services are notably consistent across surveyed jurisdictions.** Using a combination of open source internet research, blockchain and financial intelligence analysis, tip-offs and investigative authorities, authorities work to identify unregistered providers. The key challenge lies in the limits of supervisory resources as compared with the potential scale of the problem, especially in view of the need to supervise providers which may be located abroad. This phenomenon can force regulators to confront arbitrage and complications caused by uneven implementation of international standards and difficulties with

[41] Japan and the Netherlands, for instance, have both created specialised units.

information-sharing and supervisory cooperation across borders. To some extent, regulators can use domestic requirements to mitigate the risk of regulatory arbitrage. For example, in Canada, financial entities are prohibited from opening or maintaining an account, or have a correspondent banking relationship, with a foreign money services business unless they are registered with FINTRAC.

Box 7

MAS technology-enabled supervision

In Singapore, the Monetary Authority of Singapore (MAS) has been using its surveillance capabilities in its supervision for ML/TF risks. For example, MAS conducts network analysis of Suspicious Transaction Reports (STRs) filed by Financial Institutions (FIs) to identify clusters of higher-risk activities for more intensive supervisory scrutiny and also performs analytics on FIs' transactions to identify concerning flows warranting closer examination.

MAS also conducts close surveillance of the digital payment token (DPT) sector.① given the inherently higher ML/TF risks and the cross-border nature of these activities. MAS uses data analytics techniques to detect unlicensed DPT activities for enforcement action, using both public and other data sources (such as corporate registry information, intelligence and STRs).

It also uses real-time blockchain information to augment statutory information collected from licensed entities. This allows for more timely prioritisation of supervisory measures to target emerging risks and typologies. Key insights from these analyses are also shared with industry to raise risk awareness and vigilance.

① In Singapore, the Payment Services Act 2019 ("PS Act") came into force on 28 January 2020. Under the PS Act, a DPT is defined to be any digital representation of value, without necessarily any reference to fiat currency, and is, or is intended to be, a medium of exchange accepted by the public, or a section of the public, as a payment for goods or services or for the discharge of a debt. The PS Act covers persons who deal in DPTs or facilitate the exchange of DPT to fiat/other DPTs. MAS plans to further expand the regulatory scope of the PS Act in 2021 to include additional DPT activities.

32. **Addressing the lack of general AML/CFT experience in the private sector is a key priority for most authorities**. Most authorities have taken specific outreach steps in order to help the private sector understand and comply with new law and regulation related to cryptoassets. For example, the Netherlands held a seminar on AML/CFT requirements aimed at CSPs in 2019 and conducted a webinar on sanctions legislation for the cryptoasset community in 2020. Singapore partnered with local crypto industry associations to organise a series of virtual webinars in 2020 to clarify licensing admission criteria, and reiterate AML/CFT supervisory expectations using illustrative case studies. Canada specifically incorporated a transition period into the implementation of regulations, a practice many other jurisdictions also employed. Similarly, many jurisdictions described the licensing/registration process as an opportunity for educating service providers as much as a regulatory decision, given the relatively lower level of AML/CFT sophistication in some corners of the cryptoasset industry. A possible mechanism to deepen this process could lie in encouraging the formation of industry associations and trade groups to facilitate this engagement. This is particularly helpful given the diversity of the businesses making up the sector.

33. **There is a clear need for supervisory innovation to match the innovative nature of the cryptoasset sector.** National authorities believe that suptech[42] technologies such as machine learning and artificial intelligence can greatly help in the effective supervision of cryptoasset activities. The existence of a public blockchain for many cryptoassets creates an additional data set that authorities may be able to use. Dutch authorities, for example, are working on new, data-driven approaches to supervision to take advantage of the digitalisation and data-rich nature of the cryptoasset landscape. They are also requiring

[42] Broeders and Prenio (2018) define suptech as the use of innovative technology by supervisory agencies to support supervision. It includes advanced data collection and analytics tools used by the authorities to digitise reporting and supervisory processes, resulting in more efficient and proactive monitoring of risk and compliance at financial institutions.

a periodic form to be completed on risk from providers to enable these supervisor approaches. Japanese authorities have been using a multi-stakeholder approach,[43] which was advocated under its G20 Presidency in 2019, aiming at striking the right balance between adopting stringent regulatory requirements and promoting financial innovation.[44] Some authorities are also examining whether they need to change data reporting requirements for providers. While new approaches can be innovative, it can also be a simple process of evolution of existing systems. Canada, for instance, has introduced a new requirement for CSPs and all other reporting entities (eg real estate brokers or sales representatives, securities dealers) to report large virtual currency transactions, similar to what currently exists for cash transactions, called the Large Virtual Currency Transaction Report (LVCTR).[45]

Box 8

Large virtual currency transaction requirements in Canada

On 1 June 2021, the remainder of the amendments to the Proceeds of Crime (Money Laundering) and Terrorist Financing Act will come into force in Canada. These include the requirements related to reporting, record-keeping and client identification relating to large cash transactions and values of CAD 10,000 or more in virtual currencies.

These amendments include a requirement that all regulated entities, including CSPs, keep a large virtual currency transaction record in respect to every amount of CAD 10,000 or more in virtual currency that they receive from a person or entity in a single transaction or in multiple transactions within a 24-hour period to the extent that they are conducted by or on behalf of the same client or are for the same beneficiary. These records should contain information on the name of every other person or entity that is involved in the transaction, the nature of their principal business or their occupation, and the number of every other account that is affected by the transaction, among other things.

In addition, regulated entities are required to verify the identity of a person or entity from which they receive a large virtual currency transaction and take reasonable measures to determine whether the person from whom the virtual currency is received is acting on behalf of a third party. Furthermore, regulated entities have the obligation to report these transactions to FINTRAC to the extent that some criteria are met. Failure to report a large virtual currency transaction may lead to a fine of up to CAD 500,000 for the first offence and CAD 1 million for subsequent offences.

Source: FINTRAC (2021).

34. **There is a general perception that P2P activity is a potential source of risks and a major challenge.** This is because P2P transactions typically do not involve any entity within the regulatory perimeter and therefore would not be subject to AML/CFT measures and controls applied by financial institutions.[46] Risks arising from such transactions may become particularly relevant if cryptoassets are mass-adopted. In this scenario, the volume of cryptoasset activities without the involvement of a regulated entity is likely to increase substantially, particularly if acceptability and penetration of specific cryptoassets are high.[47] However, some jurisdictions consider that risks posed by this type of transaction are similar to the ones originated from cash transactions, thereby falling within the risk tolerance of the FATF standards

[43] This includes government, the private sector, academia and civil society, which all participate in discussions and decision-making. For further information, see the introductory remarks by Commissioner Toshihide Endo at Session 2 of the G20 Seminar on Technological Innovation, "Our Future in the Digital Age", June 2019.

[44] This is achieved via the Blockchain Governance Initiative Network, which "aims at providing an open and neutral sphere for all blockchain stakeholders to deepen common understanding, address issues they face in order to attain sustainable development of the blockchain community".

[45] On the topic of suptech applications for anti-money laundering, see Coelho et al (2019).

[46] Peer-to-peer transfers of cryptoassets, without the use or involvement of a cryptoasset service provider or a financial institution, are not explicitly subject to AML/CFT obligations under the revised FATF standards.

[47] According to Ciphertrace (2021), 40% of Bitcoin payment volume went to private wallets in 2020, indicating that a very substantial proportion of payment activity takes place outside regulated service providers.

and national regulation. The availability of ledger analytic tools to track these assets may also be a relevant mitigating factor to the risks posed by P2P transactions.

35. **Global coordination and cooperation are key to addressing risks arising from P2P transactions.** There is a need for further cooperation in this area with a view to identifying and developing a consistent strategy to understand the scope of P2P transactions and mitigate their potential risks. In addition, although internationally standards do not cover P2P transactions, a timely implementation of such standards is critical in order to reduce the scope of activity outside the supervisory perimeter and to mitigate the risks of regulatory arbitrage. Although true P2P transactions take place without the involvement of a CSP or financial institution, the timely implementation of internationally agreed standards is still critical to reducing the overall scope of activity outside the supervisory perimeter and ensuring that when assets pass through a service provider before or after P2P transactions, international standards apply. Many authorities also note that self-description of P2P status is not determinative, and many businesses that call themselves "P2P" platforms are in fact regulated service providers under the FATF standards and applicable national regulations, especially as authorities anticipate the coming FATF guidance update will clarify the FATF's definitions in an expansive way. Additionally, some obligations, such as targeted financial sanctions, apply to individuals and thus would come in to play in P2P transactions. Lastly, in the context of potentially mass-adopted cryptoassets, a coordinated approach is needed to ensure that the features of such cryptoassets as well as the rules governing their operation embed sufficient controls as to mitigate ML/TF risks as much as possible.

Section 4 – Enforcement actions

36. **Authorities in the surveyed jurisdictions generally have powers to impose the same remedial actions and sanctions to CSPs that are applicable to other financial intermediaries in response to AML/CFT violations.** Remedial actions and sanctions available to authorities usually include a range of instruments that may be applied according to the severity of the misconduct. This includes warning letters, orders to comply with specific instructions, public naming, fines, suspension or revocation of licence or registration, prohibiting individuals from operating in financial services, and removing, replacing or restricting the powers of managers, directors and controlling owners. This wide range of remedial actions and sanctions, in principle, gives authorities sufficient flexibility to exercise their enforcement powers in a dissuasive and proportionate manner as prescribed by FATF standards.

37. **However, the application of remedial actions and sanctions in the case of CSP non-compliance with AML/CFT legislation is still very limited.**[48] This is, in part, because in most surveyed jurisdictions CSPs did not have obligations under the AML/CFT legislation until recently. In contrast, in a few jurisdictions with more mature AML/CFT supervisory regimes for cryptoasset activity, enforcement actions have been used extensively in response to different types of violations, including the application of robust and dissuasive sanctions for egregious cases. Common violations which have been the object of enforcement actions in these jurisdictions include fraud, the provision of services without a licence or registration, and deficiencies in AML/CFT programmes such as inadequate internal controls and record-keeping.[49]

38. **Thus far, criminal enforcement agencies have done the bulk of enforcement, and civil enforcement actions are more rare.** The relative lack of enforcement actions in this area is the result primarily of how new the regulations are. That is, many jurisdictions have simply not had time to take enforcement actions based on their cryptoasset regulations because they have come into force so recently

[48] According to FATF (2020a), only eight jurisdictions had reported that they had imposed criminal, civil or administrative sanctions on cryptoasset service providers for non-compliance with AML/CFT obligations.

[49] See FATF (2020a) for further information.

and authorities have been focused on education as their top priority. Nevertheless, jurisdictions should look to the example of those authorities that have taken such actions as the novelty of the regulations recedes. Enforcement actions in cases where such measures are warranted are one of the milestones that help regulation and supervision mature.

39. **Most surveyed authorities make their sanctions public, but the granularity of the information provided varies significantly.** In general, authorities acknowledge the importance of disclosure and transparency of enforcement actions taken in response to AML/CFT violations by firms and individuals irrespective of the nature of the activity. Authorities have cited deterring firms from engaging in similar behaviour in the future and promoting a better understanding of authorities' expectations in relation to AML/CFT obligations among the benefits of making these actions public. Accordingly, some jurisdictions provide extensive granularity on the underlying offense and the corresponding sanction.[50] In addition, some jurisdictions publish guides to the enforcement process, thus contributing to enhanced consistency and transparency in the application of sanctions and remedial actions.[51]

Box 9

Enforcement actions by BaFin and FinCEN

In April 2017, the German Federal Financial Supervisory Authority, BaFin, issued cease and desist orders against Onecoin Ltd, Dubai, OneLife Network Ltd, Belize. and One Network Services Ltd, Bulgaria, with a view to stopping own funds trading in "OneCoins" in Germany. These administrative actions followed two other cease and desist orders: one against IMS International Marketing Services GmbH, for "passing on money from 'OneCoins' investors", and another against Onecoin Ltd, Dubai, for "involvement of it in IMS' unauthorized money remittance business".

Onecoin Ltd, Dubai, OneLife Network Ltd, Belize, and One Network Services Ltd, Bulgaria, were part of a network of companies that marketed units of a virtual currency, which they declared to be a cryptocurrency, under the "OneCoin" brand using a multi-level marketing structure both in Germany and around the world. According to BaFin, between December 2015 and December 2016 IMS had accepted in total approximately EUR 360 million on the basis of the agreement concluded with Onecoin Ltd, Dubai.

In October 2020, the Financial Crimes Enforcement Network (FinCEN) imposed a USD 60 million civil money penalty against Larry Dean Harmon, the founder, administrator and primary operator of Helix and Coin Ninja for violations of the Bank Secrecy Act (BSA) and its implementing rules.

Mr Harmon operated Helix as an unregistered money service business (MSB) from 2014 to 2017 and Coin Ninja from 2017 to 2020. Helix and Coin Ninja operated as an exchanger of cryptoassets by accepting and transmitting bitcoin through a variety of means.

FinCEN's investigation revealed that Mr Harmon wilfully violated the BSA's requirements by failing to register as an MSB, failing to implement and maintain an effective AML/CFT programme, and failing to report suspicious activities. In particular, Mr Harmon failed to collect and verify customer names, addresses and other identifiers on over 1.2 million transactions. The investigation also revealed that Mr Harmon engaged in transactions with narcotics traffickers, counterfeiters and fraudsters, as well as other criminals.

Sources: BaFin (2017); FinCEN (2020).

[50] In the United States, for example, public information on enforcement actions usually provides extensive detail and includes legal documents such as deferred prosecution agreements and consent orders.

[51] The Enforcement Guide (FCA (2020b)) sets out the FCA's approach to imposing financial penalties and other disciplinary sanctions, explaining the powers behind the money laundering regulations applied.

Section 5 – Cooperation and information-sharing

40. **The inherently cross-border nature of cryptoassets lends particular importance to the quality of international cooperation and consistent implementation of international standards worldwide.** Cooperation and international implementation is important to not only avoid regulatory arbitrage and bring consistency to the decision of whom to regulate, but also to the supervision of cryptoassets overall. At the same time, cross-border cooperation is an area in need of improvement. In particular, many of the risks and challenges posed by activities involving cryptoassets are global and supervisors worldwide could benefit from more effective cross-border cooperation and enhanced information-sharing on emerging practices in the area of AML/CFT supervision of cryptoasset activities. In addition, given the global nature of cryptoasset activities, more proactive information-sharing on trends, typologies and suspicious activity can go a long way towards deterring illicit activity using these instruments. Discussions are ongoing at various multilateral forums and informally among jurisdictions on a bilateral basis, but there is a need for more progress and greater efforts by authorities to develop an international network of supervisors.

41. **Surveyed authorities have legal powers and institutional arrangements in place to exchange information on cryptoasset activities with foreign supervisory authorities.** The arrangements are primarily based on pre-existing bilateral or multilateral memoranda of understanding (MoUs) intended to address financial crime-related topics or a broader set of issues. These arrangements allow authorities to exchange certain supervisory information and therefore to better supervise cryptoasset firms operating across borders.[52] Information may also be exchanged amongst Financial Intelligence Units via the Egmont Group or via the Mutual Legal Assistance Treaty process. Relevant exchanges of information on trends, typologies, challenges in the implementation of international standards (eg travel rule) and emerging supervisory practices also take place via international working groups and other types of cooperation mechanisms dedicated to understanding and mitigating potential risks arising from cryptoasset activities.[53] Furthermore, authorities regularly share information with their foreign counterparts by participating in firm-specific supervisory colleges, particularly for large international institutions.

42. **A collaborative approach between financial authorities and the industry is key to raising awareness about and mitigating ML/TF risks in cryptoasset activities.** Surveyed authorities recognise several benefits of proximity with market participants. First, many of these firms have not been previously subject to any form of regulation and may therefore be unfamiliar with the fundamentals of the AML/CFT regime. Accordingly, authorities use different channels to communicate with the industry with a view to raising market participants' awareness about AML/CFT regulatory requirements, good practices and supervisory expectations.[54] Second, the cryptoasset environment is fast-changing and authorities use a two-way interaction with market participants and self-regulatory organisations (SROs) to provide information about new typologies[55] but also to learn from the industry about recent trends in this area.

[52] The Egmont Group, which comprises 166 Financial Intelligence Units, provides a platform for secure exchange of expertise and financial intelligence to combat ML/TF.

[53] Since 2018, the JFSA has been organising and hosting the "Roundtable on Supervisory Oversight of Cryptoassets". This forum, which brings together several supervisory and international organisations, seeks to provide a venue for authorities to discuss relevant issues related to cryptoasset activities and promote international cooperation in this area.

[54] The Netherlands Bank, for example, has created a website on AML compliance for cryptoasset service providers and a specific email address to address questions from these firms.

[55] See, for example, the FinCEN Advisory on Illicit Activity Involving Convertible Virtual Currency, which highlights prominent trends in illicit cryptoasset use, including several common operating models of unregistered cryptoasset money service businesses operating in the United States.

Lastly, close collaboration between supervisors and the industry fosters the discussion on topical issues and common challenges faced by both parties, such as the identification of suitable technological solutions for implementing the TR.[56]

Section 6 – Conclusion

43. **While significant progress has been made by SSBs and financial authorities, more remains to be done.** In particular, the first priority should be implementing the FATF standards wherever that has not taken place yet. This is the absolute minimum needed to mitigate the risks posed by cryptoassets at a global level. In addition, international guidance and targeted policy actions may be necessary to address relevant vulnerabilities and mitigate potential ML/TF risks. Three policy priorities stand out:

- **Defining the regulatory perimeter and detecting unlicensed activities:** In particular, there remains some confusion on the part of jurisdictions about which firms, activities and services should be captured by the regulatory perimeter under their existing regulations and international minimum standards, particularly when novel instruments and operating models that do not conform to existing definitions are concerned. The inherent cross-border nature of cryptoasset services further exacerbates this issue, as firms offering services in one jurisdiction may be located and legally domiciled elsewhere. Work under way at the FATF to address these questions may be helpful to mitigate uncertainties and close potential gaps in risk coverage. Consistent implementation of the FATF standards would also contribute to deterring unlicensed activity.
- **Implementing the travel rule:** Despite its being part of the FATF Recommendations, most jurisdictions have not effectively implemented the travel rule. This is in part because many authorities consider that there are no technological solutions that would allow a convenient and sustainable implementation of the TR. However, a few jurisdictions have implemented and enforced compliance with the travel rule for CSPs, demonstrating that it is possible. Those that have implemented this requirement could serve as an example to those that have yet to do so.
- **Understanding and mitigating risks posed by P2P transactions:** P2P transfers are a primary concern for numerous jurisdictions. This is because these transactions would typically not involve any entity subject to AML/CFT requirements. Therefore, understanding the risks posed and adopting mitigation measures for P2P transactions based on thoughtful risk assessment, or innovative applications of technology,[57] may be needed. In addition, timely implementation of internationally agreed standards is essential to reduce the scope of activity outside the supervisory perimeter and to mitigate the risks of regulatory arbitrage.

44. **In addition, supervision of CSPs is in its early stages in most jurisdictions and further efforts are needed to bring it up to speed.** The implementation of effective supervisory practices is in a nascent phase in most jurisdictions, and more work is needed to ensure CSPs' compliance with AML/CFT obligations. Similarly, the number of enforcement actions taken in this space remains limited at this stage. While this is natural considering the recency of regulation in most surveyed jurisdictions, further attention in this area is needed as on-site inspections and enforcement actions are fundamental elements of deterrence and education.

45. **As cryptoasset markets mature, cooperation and coordination at national and international level will be crucial.** Innovations in cryptoassets and business models will continue to emerge and evolve,

[56] The JFSA, for example, has been working closely with the market participants and with the Japan Virtual and Cryptoasset Exchange Association (Japan's self-regulatory organisation for cryptoasset activities) with a view to discussing potential solutions to overcome the challenges regarding the implementation of the travel rule.

[57] Such would be the case of embedding supervision into decentralised trading of cryptoassets. See Auer (2019).

posing new challenges at a national and international level. This may require cross-sectoral, cross-authority and cross-border cooperation to monitor new and emerging risks, ensure adequate coordination and avoid regulatory arbitrage in the cryptoasset space. Information-sharing on innovative technologies may also go a long way towards enhancing the effectiveness of AML/CFT supervision.

46. **Finally, there is a critical need for swift and global implementation of international standards.** The inherently global nature of cryptoassets lends itself to regulatory and supervisory arbitrage. Jurisdictions cannot fully mitigate their risks as long as they are exposed to weaknesses and inconsistencies across borders. Consistent implementation of the international standards, especially those defined by the FATF, is essential.

References

Arner, D, R Auer and J Frost (2020): "Stablecoins: risks, potential and regulation", *BIS Working Papers*, no 905, November.

Arner, D, R Buckley and D Zetzsche (2020): "Decentralised finance", March.

Auer, R (2019): "Embedding supervision: how to build regulation into blockchain finance", *BIS Working Papers*, no 811, September.

Broeders, D and J Prenio (2018): "Innovative technology in financial supervision (suptech) – the experience of early users", *FSI Insights on policy implementation*, no 9, July.

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) (2017): "BaFin issues cease and desist orders holding the companies to stop own funds trading in 'OneCoins' in Germany", April.

Cambridge Center for Alternative Finance (CCAF) (2020a): "Legal and regulatory considerations for digital assets", September.

——— (2020b): "3rd global cryptoasset benchmarking study", September.

Chainalysis (2020). "The 2020 state of crypto crime", January.

Ciphertrace (2021). "Cryptocurrency crime and anti-money laundering report", February, 2021.

Coelho, R, M De Simoni and J Prenio (2019): "Suptech applications for anti-money laundering", *FSI Insights on policy implementation*, no 18, August.

Cuervo, C, A Morozova and N Sugimoto (2019): "Regulation of cryptoassets", *IMF Fintech Notes*, December.

Ehrentraud, J, D Garcia Ocampo, L Garzoni and M Piccolo (2020): "Policy responses to fintech: a cross-country overview", *FSI Insights on policy implementation*, no 23, January.

European Commission (EC) (2020): "Proposal for a regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending directive (EU) 2019/1937", September.

Financial Action Task Force (FATF) (2014): "Virtual currencies: key definitions and potential aml/cft risks", June.

——— (2015): "Guidance for risk-based approach: effective supervision and enforcement by AML/CFT supervisors of the financial sector and law enforcement", October.

——— (2019a): "International standards on combating money laundering and the financing of terrorism & proliferation: the FATF recommendations", June.

——— (2019b): "Guidance for a risk-based approach to virtual assets and virtual asset service providers", June.

——— (2020a): "12 month review of revised FATF Standards – Virtual Assets and VASPs", July.

——— (2020b): "Virtual assets red flag indicators of money laundering and terrorist financing", September.

Financial Conduct Authority (FCA) (2020a): "Cryptoassets: AML/CTF regime: register with the FCA", January.

——— (2020b): "Enforcement Guide", October.

Financial Crimes Enforcement Network (FinCEN) (2019): "Advisory on illicit activity involving convertible virtual currency", May.

Financial Stability Board (FSB) (2019a): "Crypto-assets: work underway, regulatory approaches and potential gaps", May.

——— (2019b): "Decentralised financial technologies: report on financial stability, regulatory and governance implications", June.

——— (2020): "Regulation, supervision and oversight of 'global stablecoin' arrangements", October.

Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) (2020): "First Bitcoin 'mixer' penalised by FinCEN for violating anti-money laundering laws", October.

——— (2021): "FINTRAC interpretation notices and policy interpretations", January.

HM Treasury (2021): "UK regulatory approach to cryptoassets and stablecoins: consultation and call for evidence", January.

Netherlands Bank (2019): "'In or from the Netherlands' within the meaning of the Wwft", November.

Saulnier, J and I Giustacchini (2020): "Digital finance: emerging risks in crypto-assets – regulatory and supervisory challenges in the area of financial services, institutions and markets", European Parliamentary Research Service, September.

Swiss Confederation – interdepartmental coordinating group on combating money laundering and the financing of terrorism (2018): "National Risk Assessment (NRA): risk of money laundering and terrorist financing posed by crypto assets and crowdfunding", October.