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.