FSB FINANCIAL STABILITY BOARD

High-level Recommendations for the Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets

Final report

17 July 2023

The Financial Stability Board (FSB) coordinates at the international level the work of national financial authorities and international standard-setting bodies in order to develop and promote the implementation of effective regulatory, supervisory and other financial sector policies. Its mandate is set out in the FSB Charter, which governs the policymaking and related activities of the FSB. These activities, including any decisions reached in their context, shall not be binding or give rise to any legal rights or obligations.

Contact the Financial Stability Board

Sign up for e-mail alerts: www.fsb.org/emailalert
Follow the FSB on Twitter: @FinStbBoard
E-mail the FSB at: fsb@fsb.org

Table of Contents

1. Introduction

Crypto-assets, as defined by the FSB[1], are a type of private sector digital asset that depend primarily on cryptography and distributed ledger or similar technology. The FSB in its crypto-assets report published in February 2022 concluded that "crypto-assets markets are fast evolving and could reach a point where they represent a threat to global financial stability".

The February 2022 G20 Finance Ministers and Central Bank Governors Communiqué requested:

"*We encourage the FSB, in close coordination with other standard-setting bodies, to accelerate and deepen its work to monitor and share information on regulatory and supervisory approaches to unbacked crypto-assets, stablecoins, decentralized finance, and other forms of crypto-assets and to address any gaps and arbitrage, including by recommending coordinated and timely policy actions to preserve global financial stability, thus creating the necessary conditions for safe innovation*."[2]

On 11 July 2022, the FSB issued a public communication[3] that highlights the potential risks and threats arising from crypto-assets; stresses that crypto-asset activities do not operate in a regulation-free space; expresses concern about lack of conformance with existing standards, applicable rules and regulations; and states that crypto-assets providers must not commence operations in any jurisdiction unless any such service provider meets all applicable regulatory requirements. The communication also reaffirms the FSB's role in facilitating cooperation among jurisdictional financial authorities and international standard-setting bodies (SSBs) to ensure that crypto-asset activities and markets are subject to effective regulation and oversight commensurate with the risks they may pose, while supporting responsible innovation and providing sufficient flexibility for jurisdictions to implement domestic approaches.

In October 2022, the FSB published a consultative report on regulation, supervision and oversight of crypto-asset activities and markets, including a set of high-level recommendations. This final report takes into account feedback from the public consultation report and stakeholder outreach. In light of the events that took place in crypto-asset markets in 2022 and early 2023 and the potential threat to the wider financial system, the report also reflects enhancements of key areas. This final report contains solely the high-level recommendations and the glossary, which are core components of the FSB framework. The analysis presented in Sections 2 and 3 of the consultative report remains valid, and thus is not repeated in this final report.

Whereas the FSB's review of its High-level Recommendations on the Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements that is published alongside this report is focused on stablecoins as a subset of crypto-assets, this report's focus is on the crypto-asset activities and markets more broadly.

---

1 FSB (2020): *Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements: Final Report and High-Level Recommendations*, October.

2 *Communiqué G20 Finance Ministers and Central Bank Governors Meeting*, 17-18 February, 2022. Jakarta, Indonesia.

3 FSB (2022): *FSB Statement on International Regulation and Supervision of Crypto-asset Activities*, July.

In line with the mandate of the FSB, the focus of this report is on regulatory, supervisory and oversight issues relating to crypto-assets to help foster safe innovation. The report therefore does not comprehensively address all specific risk categories related to crypto-asset activities, such as: Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT); data privacy; cyber security; consumer and investor protection; market integrity; competition policy; taxation; monetary policy; monetary sovereignty; and other macroeconomic concerns.

The FSB has been working closely with the International Monetary Fund (IMF), World Bank, the Organization for Economic Cooperation and Development (OECD), the Basel Committee on Banking Supervision (BCBS), the Bank for International Settlements' Committee on Payments and Market Infrastructures (CPMI), the International Organization of Securities Commissions (IOSCO), and the Financial Action Task force (FATF) to ensure that the work underway regarding the monitoring and regulation of crypto-asset activities and markets is coordinated and mutually supportive.

2. Objectives, scope and follow-up

2.1. Objectives and scope

The proposed recommendations seek to promote the comprehensiveness and greater international consistency of regulatory and supervisory approaches to crypto-asset activities and markets, including crypto-asset issuers and service providers[4]. The recommendations are intended to be flexible so that they can be incorporated into the wide variety of regulatory frameworks potentially applicable to crypto-asset activities and markets around the world, and do not displace existing applicable regulatory, supervisory and oversight frameworks. These recommendations apply to any type of crypto-assets in any jurisdiction and should inform the regulation of any type of crypto-asset activities, including those conducted through so-called decentralized finance (DeFi) protocols, that pose, or potentially pose, risks to financial stability, both individually and collectively. Central bank digital currencies (CBDCs) are not subject to these recommendations. These recommendations should be applied to crypto-asset issuers and service providers in a way that is proportionate to their risk, size, complexity and systemic importance.

Crypto-asset activities that meet the definition of a Global Stablecoin ("GSC") arrangement, as defined in the FSB High-level Recommendations for the Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements[5] should also be subject to regulatory and supervisory approaches that implement the FSB's recommendations for GSC arrangements. Authorities may choose to apply relevant High-level Recommendations on GSC arrangements as appropriate to stablecoin arrangements more widely, taking into account the risk, size and complexity of those stablecoins.

Crypto-asset markets are fast evolving and could reach a point where they represent a threat to global financial stability due to their scale, structural vulnerabilities and increasing

4 Crypto-asset issuers and service providers are defined in the Annex of this document.

5 FSB (2020). An updated version of the recommendations is being consulted on in parallel with this report.

interconnectedness with the traditional financial system. The rapid evolution and international nature of these markets also raise the potential for regulatory gaps, fragmentation and arbitrage. Although the extent and nature of use of crypto-assets varies somewhat across jurisdictions, financial stability risks could rapidly escalate, underscoring the need for both timely and pre-emptive evaluation of possible policy responses, as well as regulatory action where existing requirements apply. Authorities need to be ready to regulate, supervise, and oversee these activities and the associated issuers and service providers that have the potential to pose risks to financial stability.

The recommendations are addressed to financial regulatory, supervisory and oversight authorities at a jurisdictional level. They set out the key objectives that an effective regulatory and supervisory framework should achieve but are high-level and flexible so that they can be incorporated into a wide variety of regulatory frameworks. The recommendations establish a global regulatory baseline, and some jurisdictions may also decide to take more restrictive regulatory measures.[6] Their aim is to promote a regulatory, supervisory and oversight framework that is technology-neutral and focuses on underlying activities and risks.

The recommendations focus on addressing risks to financial stability, and they do not comprehensively cover all specific risk categories related to crypto-asset activities, such as: AML/CFT; data privacy; cyber security; consumer and investor protection; market integrity; competition policy; taxation; monetary policy; monetary sovereignty and other macroeconomic concerns. A comprehensive supervisory and regulatory framework for crypto-asset activities that effectively addresses these other important policy objectives will improve the stability of the crypto-asset market and thereby reduce the risks of negative spillovers to the wider financial system. The FSB therefore supports related efforts by SSBs and authorities to ensure such a comprehensive regulatory framework for the crypto-asset ecosystem. For example, regulations that address investor protection and market integrity can also reduce financial stability risk by increasing regulatory and public transparency.

Authorities should seek to apply the recommendations consistent with their respective mandates. An effective application of these recommendations by relevant authorities in jurisdictions in which the crypto-asset activities, issuers and service providers are active will help to ensure a comprehensive regulatory coverage and reduce the scope for regulatory arbitrage or evasion.

2.2. Follow-up and review

The FSB and the SSBs will continue to encourage consistency and a common understanding of the key elements of comprehensive regulatory, supervisory and oversight frameworks for crypto-asset activities and markets, and will support authorities in implementing the recommendations as crypto-asset activities and markets evolve.

The FSB will, in close cooperation with relevant SSBs, take the appropriate actions to (i) continue to coordinate international regulatory, supervisory and oversight approaches for crypto-asset activities to ensure they are comprehensive, consistent and complementary, including by

6 For example, jurisdictions could choose to prohibit certain or all crypto-asset activities.

considering the findings of the vulnerability analysis work on DeFi, crypto-asset service providers that combine multiple functions and whether additional policy work is warranted; and (ii) conduct a review of the implementation of the recommendations by end-2025 that may help determine whether a further review of the recommendations [or further action to promote implementation] may be necessary.

Table 1 shows the indicative timelines for this work following the publication of the high-level recommendations.

Table 1: Follow-up work to the FSB consultative report and recommendations

Continue to coordinate international regulatory and supervisory approaches for crypto-asset activities	
The FSB will continue to coordinate international regulatory and supervisory approaches for crypto-asset activities to ensure that they are comprehensive, consistent and complementary. Depending on the outcome of the FSB's analysis of potential risks to financial stability stemming from DeFi and crypto-asset service providers that combine multiple functions, the FSB will consider the regulatory implications in these areas and assess whether additional policy work is warranted.	• By end-2024
Review the implementation of the recommendations	
FSB will, in consultation with relevant SSBs and international organisations, conduct a review of the implementation of recommendations in FSB jurisdictions and assess the need to update the recommendations.	• By end-2025

3. Final recommendations

Recommendation 1: Regulatory powers and tools

Authorities should have and utilise the appropriate powers and tools, and adequate resources to regulate, supervise, and oversee crypto-asset activities and markets, and enforce relevant laws and regulations effectively, as appropriate.

Authorities within a jurisdiction, either independently or collectively, should have and utilise the appropriate powers and tools and adequate resources to regulate, supervise, and oversee crypto-asset activities and markets as appropriate.

Authorities should require that crypto-asset issuers and service providers meet all applicable regulatory, supervisory and oversight requirements of a particular jurisdiction before commencing any operations in that jurisdiction and adapt to new regulatory requirements as necessary and appropriate.

Authorities should have the powers and capabilities to enforce applicable regulatory, supervisory and oversight requirements, including authorisation and licensing requirements, and the ability to undertake inspections or examinations.

When crypto-asset issuers or service providers are not complying with applicable laws or regulations, authorities should have the powers and capabilities to require corrective actions and

take enforcement actions as appropriate. Authorities should ensure they have the powers and capabilities to address the risks arising from efforts by crypto-asset issuers and service providers to evade regulation and oversight by operating in foreign jurisdictions. This may include consideration of restrictions on the access by domestic users to foreign crypto-asset service providers and markets, or the provision of services by foreign crypto-asset issuers and service providers, when they do not comply with applicable domestic regulations and are not regulated to international standards.

Authorities should require crypto-asset service providers to have a well-founded, clear, transparent and enforceable legal basis for each material aspect of their activities in all relevant jurisdictions.

Recommendation 2: General regulatory framework

Authorities should apply comprehensive and effective regulation, supervision, and oversight to crypto-asset activities and markets – including crypto-asset issuers and service providers – on a functional basis and proportionate to the financial stability risk they pose, or potentially pose, and consistent with authorities' respective mandates in line with the principle "same activity, same risk, same regulation".

Authorities should have in place comprehensive regulatory rules and policies applicable to crypto-asset activities, issuers and service providers proportionate to their risk, size, complexity and systemic importance, and consistent with the economic functions they perform in line with the principle of "same activity, same risk, same regulation" and relevant international standards while also taking into account the specific risks associated with crypto-asset activities. Given the fast-evolving nature of crypto-asset activities and markets and the potential for financial stability risks to rapidly emerge or escalate, authorities should be ready to regulate and supervise crypto-asset activities and markets, that have the potential to pose risks to financial stability.

Consistent with past approaches to technological change, authorities should assess whether existing regulatory, supervisory and oversight requirements adequately address the financial stability risks of crypto-asset activities, including any emerging or new risks that may arise and, if needed, clarify or supplement existing regulatory, supervisory and oversight requirements. In cases when crypto-asset activities outside the scope of financial regulation may pose risks to financial stability, authorities should, as needed, seek to expand or adjust their regulatory perimeter, as appropriate.

The assessment of potential financial stability risks should take into account the interconnectedness between the crypto-asset market and the wider financial system, the overall size and nature of the activities being conducted (including the degree of financial intermediation, leverage, credit, liquidity and maturity transformation), as well as of the risk of spillovers into other jurisdictions.

Authorities should target regulatory outcomes in the crypto-asset market equivalent to those in the traditional financial market so as not to incentivise the circumvention of regulation through

the migration of traditional financial activities to crypto-asset markets. To this end, authorities should consider relevant sectoral standards and policies[7].

Regardless of whether crypto-asset activities are conducted in purportedly decentralised structures or other ways that frustrate the identification of a responsible entity or an issuer of the crypto-assets, authorities should adopt or have in place a regulatory approach that aims at adequate protection for all relevant parties, including consumers and investors, and at achieving the same regulatory outcome.

Recommendation 3: Cross-border cooperation, coordination and information sharing

Authorities should cooperate and coordinate with each other, both domestically and internationally, to foster efficient and effective communication, information sharing and consultation in order to support each other as appropriate in fulfilling their respective mandates and to encourage consistency of regulatory and supervisory outcomes.

Authorities should cooperate in the regulation, supervision and oversight of crypto-asset activities and markets. Authorities should use existing cooperation and information sharing arrangements, such as memoranda of understanding, or ad-hoc arrangements, to the extent practicable, or consider establishing new arrangements that may encompass additional subject areas or jurisdictional authorities and that consider the cross-sectoral nature of some activities.

Cross-border cooperation and information sharing among authorities should aim to facilitate a shared understanding of the risks and activities of crypto-assets, issuers and service providers across jurisdictions in normal times and in times of stress. Authorities should have in place adequate information sharing about crypto-asset service providers and issuers which are part of a group operating in multiple jurisdictions. Authorities should share information and cooperate in a timely and effective way with respect to crypto-asset issuers and service providers that are in financial or operational distress and which may affect a wider range of jurisdictions than where they primarily operate.

Authorities should take additional steps to collaborate with authorities in relevant jurisdictions when they host crypto-asset issuers and service providers with a global reach, taking into account the risk of spillovers into other jurisdictions.

To foster effective cross-border cooperation and coordination, the FSB and the SSBs will continue to promote consistency and a common understanding of key elements of regulatory, supervisory and oversight frameworks for crypto-asset activities and markets. The FSB will continue to monitor issues related to the cross-border nature of crypto-assets and consider mechanisms that facilitate exchange of information about the level of compliance by service providers that are operating across borders and out of jurisdictions that have not implemented a regulatory framework for crypto-asset activities consistent with the FSB high-level recommendations and international standards.

---

[7] For instance, the IOSCO Objectives and Principles of Securities Regulation, CPMI-IOSCO Principles for financial market infrastructures, the Basel Framework, and FATF standards, in particular FATF Recommendations 15 and 16.

Recommendation 4: Governance

Authorities, as appropriate, should require that crypto-asset issuers and service providers have in place and disclose a comprehensive governance framework with clear and direct lines of responsibility and accountability for all functions and activities they are conducting. The governance framework should be proportionate to their risk, size, complexity and systemic importance, and to the financial stability risk that may be posed by activity or market in which the crypto-asset issuers and service providers are participating. It should provide for clear and direct lines of responsibility and accountability for the functions and activities they are conducting.

Authorities should require crypto-asset issuers and service providers to have a robust governance framework. The framework should be proportionate to their risk, size, complexity and systemic importance, and to the financial stability risk that may be posed by the activity or market in which they are participating. It should include clear and direct lines of responsibility and accountability, clear definition of the roles and responsibilities of the management body and the decision-making process, including procedures for identifying, addressing and managing conflicts of interest.

Where crypto-asset activities are conducted in ways that may frustrate the identification of the responsible entity or affiliated entities, such as through so-called DeFi protocols or setting up complex corporate structures, such conduct of activities must not undermine robust governance and accountability arrangements. Authorities should require compliance with rules and regulations for effective governance irrespective of the structures of activities and technology used to conduct the crypto-asset activities.

Recommendation 5: Risk management

Authorities, as appropriate, should require crypto-asset service providers to have an effective risk management framework in place that comprehensively addresses all material risks associated with their activities. The framework should be proportionate to the risk, size, complexity, and systemic importance, and to the financial stability risk that may be posed by the activity or market in which they are participating. Authorities should, to the extent necessary to achieve regulatory outcomes comparable to those in traditional finance, require crypto-asset issuers to address the financial stability risk that may be posed by the activity or market in which they are participating.

Authorities should understand the different risk profiles of crypto-asset issuers and service providers and require them, as appropriate, to establish a risk management framework that is proportionate to their risk, size, complexity, and systemic importance, and to the financial stability risk that may be posed by the activity or market in which they are participating.

Authorities should expect crypto-asset issuers and service providers to be directed by a management which is qualified and of good repute (for example, by applying “fit and proper” standards, where applicable); allocate adequate resources to risk management and other control functions (i.e. compliance and internal audit); and ensure that these control functions are carried out independently of business activities. Authorities should pay particular attention to the compliance functions of each service provider or issuer, which should be expected to monitor all

of the activities of that service provider or issuer, to identify and address any non-compliance issues and deficiencies, and to ensure adherence to applicable laws and regulations.

Authorities should expect crypto-asset issuers and service providers to act honestly and fairly and require them to communicate with users and relevant stakeholders in a clear and not misleading manner, and identify, disclose, manage and, to the extent possible, prevent any conflict of interests.

Authorities, as appropriate, should require crypto-asset issuers and crypto-asset service providers, proportionate to their risk, size, complexity, systemic importance, and to the financial stability risk that may be posed by the activity or market in which they are participating, to identify, measure, evaluate, monitor, report, and control all material risks. Authorities should require crypto-asset service providers to effectively identify and manage risks arising from leverage and credit, liquidity, operational, compliance, and maturity transformation. Authorities should require crypto-asset service providers to have rules and procedures to effectively monitor the transactions they conduct. Authorities should also have in place rules, policies and enforcement tools that comprehensively address these risks both in normal times and in times of stress.

Authorities should, as appropriate, consider applying both prudential and market conduct regulatory tools. Authorities should pay particular attention to technological risks associated with crypto-asset activities. Authorities should require that crypto-asset service providers that are part of an internationally active group properly identify, monitor and manage risks arising from exposures to other parts of the group.

Authorities, as appropriate, should require crypto-asset issuers and crypto-asset service providers, proportionate to their risk, size, complexity, systemic importance, and to the financial stability risk that may be posed by the activity or market in which they are participating, to establish effective contingency arrangements (including robust and credible recovery plans where warranted) and business continuity planning.

Authorities should ensure that crypto-asset issuers and crypto-asset service providers put appropriate AML/CFT measures in place consistent with FATF Standards, including requirements to comply with the FATF ‘”travel rule”.

Taking into account the jurisdictional differences in legal frameworks regarding ownership rights to crypto-assets held by a crypto-asset service provider, authorities should require all crypto-asset service providers involved in holding or safeguarding crypto-assets to have in place adequate controls, to disclose to customers the rights of ownership they have, and to protect customers’ ownership rights, including through segregation and record-keeping requirements. These arrangements should minimise the risk of loss, misuse of or delayed access to assets, including in the event of a service provider’s insolvency. The same requirements should apply when the activities involved in holding or safeguarding crypto-assets are outsourced to a third party.

Authorities should require crypto-asset service providers facilitating trading to ensure that their operations are resilient and transparent and should implement and maintain clear and transparent operating rules for the trading platform.

Recommendation 6: Data collection, recording and reporting

Authorities, as appropriate, should require that crypto-asset issuers and service providers have in place robust frameworks, including systems and processes, for collecting, storing, safeguarding, and the timely and accurate reporting of data, including relevant policies, procedures and infrastructures needed, in each case proportionate to their risk, size, complexity and systemic importance. Authorities should have access to the data as necessary and appropriate to fulfil their regulatory, supervisory and oversight mandates.

Authorities should require that crypto-asset issuers and service providers, proportionate to their risk, size, complexity and systemic importance, have data management systems that record and safeguard relevant data and information collected and produced in the course of their operations, with adequate controls in place to safeguard the integrity and security of relevant data and conform to applicable regulation, including on data retention, data security and data privacy. Appropriate infrastructures should be maintained in order to ensure data quality and reliability and have in place well-defined procedures to monitor data quality and rectify poor data. Authorities should require crypto-asset service providers to have measures in pace to ensure the completeness, accuracy and reliability of data.

Authorities should have full, timely, complete, and ongoing access to relevant data and information, wherever the data is located, to enable them to regulate, supervise and oversee the functions and activities of the crypto-asset activities and markets, considering the level and nature of the risks posed. Authorities should seek to address any impediments to relevant data access or limitations of the data.

Authorities may leverage existing efforts to promote consistent and comparable data collection and reporting based on activity types and economic functions or consider developing new reporting frameworks or policies to support data collection and sharing, as appropriate, across relevant authorities and jurisdictions.

Authorities should seek to promote the public understanding of crypto-asset markets. For service providers that facilitate a wide range of trading services and a large size of trading volume, authorities should assess their ability to access data regarding, but not limited to, the instruments most frequently traded, the principal amounts traded, and the largest counterparties and intermediaries, and the extent to which these data should be made more widely available to the public or publicly disseminated.

Recommendation 7: Disclosures

Authorities should require that crypto-asset issuers and service providers disclose to users and relevant stakeholders comprehensive, clear and transparent information regarding their governance framework, operations, risk profiles and financial conditions, as well as the products they provide and activities they conduct.

Authorities should require that crypto-asset issuers and service providers make available to users and relevant stakeholders, including customers, investors or shareholders, all necessary information regarding how they operate, how they transact, the risk features of their products,

and how they manage and mitigate any potential risks in an understandable manner for the intended audiences. This should include, as appropriate, the governance structure and procedures related to the main activities offered[8] and important conflict of interests emanating from crypto-asset activities.

Authorities should require that crypto-asset issuers and service providers adequately disclose the information related to the product structure and the operation of the activities they conduct. This may include, for example, a prospectus or an equivalent document from a crypto-asset issuer.

Authorities should require the service provider to provide full and accurate disclosure to any client for whom it is providing custody services of the terms and conditions of the custodial relationship and the risks that could be faced by the client if the custodian were to enter bankruptcy. This disclosure should include the ownership rights retained by the client, the safeguards implemented by the service provider for client assets, the existence of any outsourcing arrangements, and any circumstances where a crypto-asset issuer or service provider might not provide timely redemption or withdrawal of assets. Where ownership rights are intended to be transferred to the crypto-asset service provider, authorities should require the service provider to clearly disclose the arrangement to the customer and to obtain the customer's explicit prior consent to the transfer.

Authorities should require crypto-asset issuers and service providers to disclose any material risks associated with the underlying technologies, such as cyber security risk, as well as environmental and climate risks and impacts, as appropriate and in line with jurisdictional legal frameworks.

Recommendation 8: Addressing financial stability risks arising from interconnections and interdependencies

Authorities should identify and monitor the relevant interconnections, both within the crypto-asset ecosystem, as well as between the crypto-asset ecosystem and the wider financial system. Authorities should address financial stability risks that arise from these interconnections and interdependencies.

Authorities should identify and address potential financial stability risks that may originate from or be transmitted or amplified by the crypto-asset ecosystem. Authorities should seek to identify and monitor on an ongoing basis interlinkages and interdependencies among different parts of the crypto-asset ecosystem and assess the aggregated risk arising from interlinkages between the crypto-asset ecosystem, the wider financial system and the real economy.

---

8 For example, key decision-making procedures and voting mechanisms, clear and accurate description of responsibilities and rights of all stakeholders, important change of protocols, available dispute mechanisms or procedures for seeking redress or lodging complaints, composition of balance sheet items, financial conditions, regulatory incidents and penalties Where relevant, this information should also include redemption rights and composition of reserve assets for those crypto-assets that aim to maintain a stable value relative to a specified asset, or a pool or basket of assets.

As a component of monitoring interlinkages between the crypto-asset ecosystem and the wider financial system, authorities should consider the scale of crypto-asset activities and whether this presents systemic risk to the wider financial system.

Where financial stability risks arise from traditional financial institutions' exposures to crypto-assets, authorities should address these risks in line with the recommendations and based on frameworks developed by the SSBs for these institutions.

Recommendation 9: Comprehensive regulation of crypto-asset service providers with multiple functions

Authorities should ensure that crypto-asset service providers and their affiliates that combine multiple functions and activities, where permissible, are subject to appropriate regulation, supervision and oversight that comprehensively address the risks associated with individual functions and the risks arising from the combination of functions, including but not limited to requirements regarding conflicts of interest and separation of certain functions, activities, or incorporation, as appropriate.

Certain crypto-asset service providers, including groups of affiliated service providers, may be undertaking a variety of functions, including facilitating transactions, settlement and clearing, non-custodial and custodial wallet provisioning (including the sale of software and hardware for non-custodial wallets), market-making, offering investment vehicles, lending and borrowing, and proprietary trading and issuance. In some jurisdictions, certain combinations are not permitted. Where combinations are permitted, relevant authorities should work to ensure that these service providers, including groups of affiliated service providers, are subject to robust and comprehensive regulation, supervision and oversight that address the risks arising from the combination of multiple activities and functions, in particular those that fall under different sectoral regimes, with strong protection for investors and consumers. Authorities should consider requirements that address not only risks on a standalone basis, but also additional risks and additional conflicts of interest when those functions and activities are conducted concurrently.

Authorities should require that crypto-asset service providers, including groups of affiliated service providers that, where permissible, combine multiple functions, have transparent organisational and managerial structures, which are consistent with their overall strategy and risk profile and which are well understood by the board and senior management of the service provider, affiliated service providers, regulators and customers.

Authorities should consider whether and, if so, how combinations of multiple functions can be appropriately regulated within a single entity or group of affiliated entities. To the extent that such combinations are a result of non-compliance with existing regulations or will generate acute conflicts of interest which, as determined by authorities, cannot be effectively managed, authorities should apply robust measures as appropriate and in line with jurisdictional legal frameworks, including legal disaggregation and separation of certain functions. Authorities should consider relevant sectoral standards developed by SSBs when they require segregation of functions. Where multiple functions are permitted to exist within a crypto-asset service provider or group of affiliated service providers, authorities should require that such service providers have adequate policies and processes to identify, mitigate and manage actual or

potential conflicts of interests, including prevention of any abuse resulting from concentrated control, management of related-party transactions, in particular those involving affiliated companies, and transparency of related-party transactions. Authorities should consider additional prudential requirements if appropriate to address additional risks or conflicts of interest from this setup.

Authorities should pay particular attention to service providers combining multiple functions that engage in facilitating custody, trading, settlement, lending, and borrowing or proprietary trading, and should apply regulatory measures that are designed for the adequate segregation of risks. For example, this may include legal disaggregation and separation of certain functions.

Cross-border and cross-sectoral information sharing about service providers combining multiple functions and operating across borders and sectors is particularly important. Authorities should share information, as appropriate, to minimize financial distress of these intermediaries from spilling over to other jurisdictions or sectors of the financial system.

Glossary

Blockchain

A form of distributed ledger in which details of transactions are held in the ledger in the form of blocks of information. A block of new information is appended to the chain of pre-existing blocks via a computerised process by which transactions are validated.

Crypto-asset

A digital asset (issued by the private sector) that depends primarily on cryptography and distributed ledger or similar technology.

Crypto-asset ecosystem

The entire ecosystem that encompasses all crypto-asset activities, market and participants.

Crypto-asset issuer

An entity, person, or other structure that creates new crypto-assets.

Crypto-asset market

Any place or system that provides buyers and sellers the means to trade crypto-assets and the associated instruments, including lending, structured investment products, and derivatives. Crypto-asset markets facilitate the interaction between those who wish to offer and sell and those who wish to invest.

Crypto-asset services

Services relating to crypto-assets that may include, but are not limited to, distribution, placement, facilitating exchange between crypto-assets or against fiat currencies, custody, provisioning of non-custodial wallets, facilitating crypto-asset trading, borrowing or lending, and acting as a broker-dealer or investment adviser.

Crypto-asset service providers

Individuals and entities that provide crypto-asset services.

Crypto-asset activities

Activities serviced by a crypto-asset issuer or crypto-asset service provider.

Crypto-asset trading platform:

Any platform where crypto-assets can be bought and sold, regardless of the platform's legal status.

Decentralised Finance (DeFi)

A set of alternative financial markets, products and systems that operate using crypto-assets and ‘smart contracts’ (software) built using distributed ledger or similar technology.

DeFi protocols

A specialised autonomous system of rules that creates a program designed to perform financial functions.

Digital asset

A digital representation of value or contractual rights which can be used for payment or investment purposes.

Global stablecoin (GSC)

A stablecoin with an existing or potential reach and use across multiple jurisdictions and which could become systemically important in and across one or many jurisdictions, including as a means of making payments and/or store of value.

Stablecoin

A crypto-asset that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets.

Wallet

An application or device for storing the cryptographic keys providing access to crypto-assets. A hot wallet is connected to the internet and usually takes the form of software for the user, while a cold wallet is a hardware that is not connected to the internet and stores the cryptographic keys.

Custodial wallet

A service in which crypto-assets are held by a service provider. A user interacts with the service provider to manage the user’s crypto-assets. A custodial wallet is also known as a “hosted wallet”.

Non-custodial wallet

Software or hardware that stores cryptographic keys for a user, making the user’s crypto-assets accessible only to the user, and allowing the user to interact directly with the blockchain and the blockchain-based finance applications. A non-custodial wallet is also known as an “unhosted wallet”.