FSB FINANCIAL STABILITY BOARD

Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets

Consultative document

11 October 2022

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

Proposed recommendations for the regulation, supervision and oversight of crypto-asset activities and markets

1. Authorities should have the appropriate powers and tools, and adequate resources, to regulate, supervise, and oversee crypto-asset activities and markets, including crypto-asset issuers and service providers, as appropriate.
2. Authorities should apply effective regulation, supervision, and oversight to crypto-asset activities and markets – including crypto-asset issuers and service providers – proportionate to the financial stability risk they pose, or potentially pose, in line with the principle "same activity, same risk, same regulation."
3. 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.
4. Authorities, as appropriate, should require that crypto-asset issuers and service providers have in place and disclose a comprehensive governance framework. 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 the 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.
5. Authorities, as appropriate, should require crypto-asset service providers to have an effective risk management framework that comprehensively addresses all material risks associated with their activities. 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. 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.
6. Authorities, as appropriate, should require that crypto-asset issuers and service providers have in place robust frameworks 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.
7. Authorities should require that crypto-asset issuers and service providers disclose to users and relevant stakeholders comprehensive, clear and transparent information regarding their operations, risk profiles and financial conditions, as well as the products they provide and activities they conduct.
8. 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.
9. Authorities should ensure that crypto-asset service providers that combine multiple functions and activities, for example crypto-asset trading platforms, are subject to regulation, supervision and oversight that comprehensively address the risks associated with individual functions as well as the risks arising from the combination of functions, including requirements to separate certain functions and activities, as appropriate.

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*."

On 11 July, the FSB issued a public communication 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 to ensure that crypto-asset activities and markets are subject to effective regulation and oversight commensurate to the risks they may pose, while supporting responsible innovation and providing sufficient flexibility for jurisdictions to implement domestic approaches.

Whereas the FSB's review of its High-level Recommendations on the Regulation, Supervision and Oversight of 'Global Stablecoin' Arrangements that is issued 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:

- Section 1 of this report describes essential activities and analyses the interconnectedness of crypto-asset markets;
- Section 2 provides an overview of applicable international standards and describes regulatory and supervisory approaches to crypto-asset activities in FSB member and non-FSB member jurisdictions represented on FSB Regional Consultative Groups (RCGs);
- Section 3 identifies issues and challenges as well as potential gaps in regulatory, supervisory and oversight approaches to crypto-asset activities; and

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

- Section 4 proposes a set of high-level recommendations for the regulation, supervision and oversight of crypto-asset activities and markets.

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 ensure 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 Basel Committee on Banking Supervision (BCBS), the 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.

1. Crypto-assets and markets: activities and interconnectedness

1.1. Crypto-asset markets: essential functions and activities

The crypto-asset ecosystem features a wide range of functions and activities, many of which resemble those in the traditional financial system. Currently, there is no universally agreed taxonomy of crypto-asset functions or activities. Table 1 identifies essential functions around crypto-assets, as well as prevalent activities associated with these functions. Annex 1 provides a list of activities, their service providers, associated vulnerabilities and risks, as well as potentially relevant international standards.

Table 1: Essential functions and activities in the crypto-asset ecosystem

Functions	Activities
Creation, issuance, distribution, redemption and underlying infrastructure	1. Creating, issuing, and redeeming crypto-assets, distribution, underwriting, placement, market-making, marketing and sales
	2. Operating infrastructure and validating transactions
Wallets and custody	3. Provision of custodial (hosted) wallet and custody services
	4. Provision of non-custodial (unhosted) wallets
Transfer and transactions	5. Payment for/of goods, services, gifts and remittances.
	6. Exchange between crypto-assets or against fiat currencies, clearing and settlement
Investment, leverage and risk management	7. Use as collateral to borrow/purchase other crypto-assets
	8. Trading/borrowing/lending of crypto-assets
	9. Insurance
	10. Direct/outright exposures to crypto-assets
	11. Synthetic/derivative exposures to crypto-assets

1.2. Interconnectedness within the crypto-asset market

The FSB's crypto-asset report stated that:[2]

"Direct connections between crypto-assets and systemically important financial institutions and core financial markets, though expanding, remain limited at the present time. Episodes of price volatility have, so far, been contained within crypto-asset markets and have not 'spilled over' or presented a threat to the resilience of broader financial markets and infrastructures."

However, the crypto-asset market is highly interconnected, which may lead to rapid contagion and the spread of stress among crypto-asset market participants.

---

2 FSB (2022a): *Assessment of Risks to Financial Stability from Crypto-assets*, February.

The crypto-asset market structure fosters vulnerabilities. Investment and activity in the crypto-asset market is largely self-contained and is mostly for speculative purposes with limited connections to the real economy. Many intermediaries, particularly trading and lending platforms, have sought to grow rapidly by advertising high returns and investing in risky products provided by other intermediaries. Such a business strategy relies upon an ongoing increase in the price and value of crypto-assets or an inflow of new investment to meet its obligations. Some lending platforms have also sought to generate yield by extending concentrated loans to large crypto-asset market participants. These business models have generated extensive and complex financial relationships. Similar to in traditional finance, high yield is most often achieved by taking greater credit risks, greater liquidity/maturity mismatches or more leverage.

Due to the pseudonymity or anonymity of crypto-asset market participants, many intermediaries require "over collateralisation"[3] in crypto-asset margin trading and lending as a substitute for creditworthiness screening. However, given the high volatility of crypto-assets, sharp declines in asset values may occur, reducing the value of collateral and potentially triggering margin calls or collateral liquidation. In such cases, the high degree of interconnectedness in the crypto-asset market may lead to cascades of liquidations, contributing to the propagation and amplification of risk contagion and market strains.

Stablecoins contribute to the growing interconnectedness of participants within the crypto-asset market. Due to their claim to maintain price stability, stablecoins currently facilitate the trading, lending and borrowing of other crypto-assets that may be more volatile. Stablecoins are also used extensively as collateral to borrow other crypto-assets. Some stablecoins used as collateral are borrowed by investors and collateralised by other crypto-assets, similar to rehypothecation. Stablecoins therefore play a pivotal role in crypto-asset markets. As most stablecoin transactions occur on trading platforms and through other intermediaries that are already critical connections points within crypto-asset markets, stablecoins may exacerbate interconnectedness and complexity.

Interconnectedness also comes from the co-ownership or affiliation of trading platforms and other crypto-asset service providers as well as implicit or explicit bailout arrangements, any of which may create incentives for inappropriate related-party transactions or other self-dealing. Some large crypto-assets trading platforms are invested in crypto-asset issuers or have overlapping or affiliated ownership with crypto-asset issuers.[4] They may use the platform to promote their related issuers and products or conduct activities in a way that could undermine investor protection and market integrity.

Similar interconnectedness also exists in traditional finance but is mitigated by regulatory constraints and prudential and other requirements (e.g., capital, liquidity and margin requirements, a limitation or prohibition of re-hypothecation, restrictions on co-ownership) that help prevent excessive risk-taking and reduce risk transmission. However, many crypto-asset

---

3 "Over collateralization"- describes the situation in which the value of an asset or assets used as collateral on a loan exceeds the loan value. It is widely used in crypto-asset lending to mitigate counterparty risk.

4 During the recent Tether depegging, crypto-asset exchange Bitfinex, which belongs to the same parent company as Tether, reportedly made efforts to defend the USDT peg by shoring up bid depth.

activities are currently operating in non-compliance with such constraints or seeking to structure their activities to operate in jurisdictions where such constraints are not applicable.

The recent failure of several crypto-asset intermediaries, such as Celsius Network and Voyager Digital, exemplified risk transmission within the crypto-asset market due to significant liquidity and maturity mismatch (in the case of Celsius) and interconnectedness (in the case of Voyager). Trading and lending platforms such as these were able to offer high yields to investors by taking on significant liquidity/maturity risk, promising investors immediate redemption while investing proceeds in less liquid assets, and using the borrowers' collateral to increase leverage. As long as inflows to the platforms exceeded outflows, the intermediaries benefitted from a liquidity/maturity premium. However, when market sentiment turned, these entities proved to have insufficient resources or inadequate risk-management to be resilient to rapid customer redemptions, forced liquidations or the default of large counterparties. Due to extensive interconnectedness, contagion spread rapidly within the crypto-asset market.

1.3. Interconnectedness with the wider financial system

The outcome of the recent market volatility has so far been consistent with the FSB's judgment that interconnections between crypto-asset market and the wider financial system are still limited. Though the recent turmoil in crypto-asset markets resulted in a sharp and wide depreciation in crypto-asset market values and the failure of some service providers, this turmoil has not yet transmitted significant financial stability concerns to the wider financial system.

However, recent market trends have also highlighted the increasing correlation between crypto-asset markets and traditional financial markets. Correlations between crypto-asset prices and mainstream equity indices have been steadily increasing since year-end 2021 and peaked in May 2022[5], when the market stress began. One possible contributor to the recent strains in crypto-markets is the tightening of financial conditions across most advanced and emerging economies, which caused a broad re-assessment of risk appetite across markets, and particularly in more speculative markets.

Additionally, most traditional financial institutions have limited direct exposure to crypto-assets, but some are starting to engage in crypto-asset related products to serve client demands and hedge underlying exposures, which will increase the interconnectedness between crypto-asset market and the traditional financial sector. Some traditional financial firms are also offering crypto-asset collateralised lending and providing payment and deposit-like services to crypto-asset service providers. Traditional financial firms are also engaging in the capital formation of new crypto-asset projects, e.g., underwriting, placement, and market-making of traditional capital instruments on behalf of crypto-asset clients. In addition, the growing exposure of retail investors across the globe to crypto-assets and their losses amid alleged fraud and illegal activity by crypto-asset issuers and service providers demonstrates the potential for vulnerabilities and volatility in the crypto-asset markets to have negative consequences for broader confidence in the financial system.

---

[5] The correlation between some crypto-assets (such as Bitcoin) and certain index (such as Nasdaq) has since then declined. It is still early to decide whether the crypto-asset market correlation is diverging again from traditional financial markets.

2. Development of regulatory and supervisory approaches and standards

Given the similarity between economic functions and activities in the crypto-asset market and the traditional financial system, many existing international policies, standards, and jurisdictional regulatory frameworks are relevant for crypto-asset activities. However, the extent to which authorities can effectively apply these international standards across jurisdictions depends on the extent to which these standards and policies are reflected in their domestic legal and regulatory frameworks. Further, crypto-asset market participants may be acting in non-compliance with legal and regulatory requirements in some jurisdictions.

2.1. International standards and policies

A high-level assessment of the relevance of existing international standards suggests that:

- The Basel Framework, including prudential requirements on capital and liquidity, as well as risk management guidelines such as guidance on operational resilience and the sound management of operational risk, applies to crypto-asset activities conducted by banks. The second public consultation of the Basel Committee for Banking Supervision (BCBS) on the prudential treatment of banks' crypto-asset exposures[6] proposes a tailored application of prudential requirements to banks' exposures to crypto-assets to address credit, market, liquidity and operational risks.

- The Bank for International Settlements' Committee on Payments and Market Infrastructure's (CPMI) and the International Organization of Securities Commissions (IOSCO)'s Principles for financial market infrastructures (PFMI) apply to systemically important financial market infrastructures (FMIs). In July 2022, CPMI-IOSCO published guidance on the application of the PFMI to stablecoin arrangements (SAs).[7] This guidance, which follows the consultative report of October 2021, reconfirms that if an SA performs a transfer function and is determined by authorities to be systemically important, the SA as a whole is expected to observe all relevant principles of the PFMI. The guidance provides further clarifications on how systemically important SAs should observe certain aspects of the PFMI.

- The IOSCO Objectives and Principles for Securities Regulation and other standards or guidance issued by IOSCO apply to all activities involving crypto-assets deemed regulated financial instruments/securities and all derivatives instruments, irrespective of the classification of the underlying asset. On that basis, IOSCO standards may be applied to a broad range of activities and entities, including issuers and market intermediaries such as trading, lending and borrowing platforms and protocols (decentralised or centralised), custodians, broker dealers, investment advisers, market makers etc.

---

6 BCBS (2022): *Prudential treatment of cryptoasset exposures - second consultation*, June.

7 CPMI and IOSCO (2022). Press release: *CPMI and IOSCO publish final guidance on stablecoin arrangements confirming application of Principles for Financial Market Infrastructures*, July.

- Financial Action Task Force (FATF) standards apply extensively to all virtual assets (VAs) and virtual assets service providers (VASPs) as defined in the FATF recommendations and guidance.

The ongoing and planned work by the international standard-setting bodies (SSBs) is summarised in Annex 4.

2.2. Regulatory and supervisory approaches at the jurisdictional level

In early 2022, the FSB conducted a stock-take survey on the regulatory and supervisory approaches across FSB jurisdictions as well as certain non-FSB RCG jurisdictions.[8] Annex 3 provides an illustrated summary of aggregated responses.

Many authorities highlighted the importance of monitoring the scale of crypto-asset activities operating without adequate regulatory oversight and/or in non-compliance with regulation. Some focus areas of ongoing and planned regulatory initiatives are: investor protection and market integrity, the interaction of already regulated entities with crypto-asset providers, the extension of the regulatory perimeter to capture crypto-asset activities, the enhancement of data standards, and the application or retrofitting of existing standards or requirements to crypto-assets.

2.2.1. Application of existing regulation vs. adoption of specific regulation

The survey suggests that in most jurisdictions, crypto-asset activities are subject to some form of regulation.[9] There is variance across jurisdictions in the extent to which authorities apply existing regulations to crypto-asset activities. A few jurisdictions have in place, or are in the process of formulating, a specific regulatory framework for crypto-assets. Most authorities are so far applying existing regulation to crypto-asset activities based on the crypto-asset's economic function(s), i.e., whether it serves as a means of payment, security, commodity, and/or derivative, or the nature of the activities in which the crypto-asset is used, such as its offer and sale to investors. The applicability of existing financial regulation relies on whether the activities and underlying functions are regulated activities or assets under a jurisdiction's regulatory framework. In some jurisdictions, existing regulation cannot be applied to certain crypto-asset activities due to difficulties in categorising the related crypto-assets as payment instruments or financial instruments (e.g., securities, commodities, and/or derivatives) under

---

8 The survey was launched in June 2022. As of 30 June 2022, the survey received responses from 24 FSB members: Argentina, Australia, Brazil, Canada, China, France, Germany, Hong Kong, India, Indonesia, Italy, Japan, Korea, Mexico, Netherland, Saudi Arabia, Singapore, South Africa, Spain, Switzerland, Türkiye, United Kingdom, United States, as well as the European Commission. The 24 participating RCG member jurisdictions are: Belgium, Bermuda, Chile, Colombia, Costa Rica, Denmark, Egypt, Finland, Guatemala, Honduras, Hungary, Ireland, Lebanon, Luxembourg, Malaysia, Mauritius, Norway, Pakistan, Peru, Poland, Portugal, Thailand, Trinidad and Tobago and West African Economic and Monetary Union.

9 1 FSB member and 1 RCG member indicated they had banned all crypto-asset activities in their jurisdictions. 1 RCG member has banned issuing or minting of digital tokens unless they are fully backed by a fiat currency. 1 FSB member and 4 RCG members reported that they had not finalised the regulation or were unable to provide inputs on available regulatory framework. 2 RCG members have issued a comprehensive bespoke regulatory framework for crypto-assets. 4 FSB members and 9 RCG members are members of the European Commission and will implement the Regulation on Markets in Crypto-assets (MiCA), a bespoke regulatory framework which was passed on 30 June 2022.

the jurisdictional regulations.[10] In some jurisdictions, crypto-assets are only regulated under the applicable AML/CFT framework.

While most jurisdictions do not have in place a comprehensive regulatory framework dedicated to crypto-assets, many jurisdictions have provided guidance regarding the application of existing laws and regulations to crypto-assets and related activities or amended existing regulations to adapt them to crypto-asset activities.[11] These amendments or new regulations or policies address financial and conduct risks, as well as help ensure market integrity, investor protection and AML/CFT defences.[12]

The survey results suggest that different regulatory authorities in a single jurisdiction are involved in regulating aspects of the activities that fall within their respective mandates. This requires authorities responsible for payment, securities and markets, prudential, banking, insurance and conduct regulation to cooperate closely in line with their respective mandates. This underscores the importance of cross-sectoral regulatory coordination mechanisms.

A few jurisdictions have identified the need to develop tailored regulatory definitions for crypto-assets[13] within their jurisdiction. Some apply a 'catch-all' definition that includes all crypto-assets as a new form of financial instrument. Others have provided for more granular regulatory definitions in accordance with the underlying economic functions, mainly as payment instruments or securities.[14] Authorities appear to use different terminology, including but not limited to "digital asset", "crypto-asset", "virtual asset" (VA), "virtual currency", and "convertible virtual currency."[15]

2.2.2. Regulatory coverage

The survey reveals variance in regulatory coverage and applicable regulatory approaches across different jurisdictions. Following the introduction of the FATF's guidance in 2019[16],

---

[10] Several jurisdictions reported difficulties in categorising crypto-asset activities under existing jurisdictional financial regulations because the legal and regulatory characterisation of crypto-assets involves a legal analysis of both facts and circumstances and may be complex.

[11] The scope of issued regulatory documents reported by member authorities is defined in a wide measure that includes any documents issued by the national authorities relevant for crypto-assets and activities. Most of the standards refer to a specific activity or are addressed to regulated entities on their participation to crypto-assets (such as banks). Most of these standards are not considered as comprehensive crypto-asset regulatory frameworks.

[12] For example, the Regulation on Markets in Crypto-assets (MiCA) proposes four objectives: (1) to provide legal certainty; (2) to support innovation and fair competition; (3) to instil appropriate level of consumer and investor protection and market integrity and (4) to ensure financial stability.

[13] This includes the definition in a new standard or amended regulations, such as the amendment of payment laws to ensure the applicability to payment tokens with new definitions included in the amended laws.

[14] One jurisdiction plans to extend the definition to cover governance tokens regarded as a digital asset that provides rights, eligibility or access to vote on the management, administration or governance of the affairs.

[15] For example, the French PACTE Law, issued on 22 May 2019, introduced "digital assets". In Mexico, federal anti-money laundering law defines crypto-assets, referred to as virtual assets, as any electronically-stored representation of value, other than fiat domestic or foreign currency or any asset denominated in such currency, used by the public as a means of payment for all kind of actions provided that their transfer can only be carried out by electronic means. The Hong Kong SAR government introduced a bill in July 2022 to amend the AML regulation, under which a definition of "virtual asset" will be introduced. The term "virtual currency" is used in several jurisdictions including China, Indonesia, Netherland and the US. The US Treasury Financial Crimes Enforcement Network (FinCEN) in 2013 issued a guidance on "convertible" virtual currency (CVC), defined as an instrument that has either equivalent value in real currency, or acts as a substitute for real currency.

[16] FATF (2019): *Guidance for a risk-based approach: Virtual assets and virtual asset service providers*, June. (Updated in 2021, See Annex 4).

which requires all countries to introduce AML/CFT requirements for VAs and VASPs, AML/CFT requirements have relatively higher regulatory coverage than other areas, although more efforts are needed to fully implement the FATF Recommendations in the crypto-asset ecosystem.

Of crypto-assets performing different economic functions, those classified as securities are subject to securities regulation and are more widely captured in this way by regulation than other categories of crypto-assets.

Activities cited by respondents with relatively higher regulatory coverage include: operating a centralised trading platform, provision of custody, placement and distribution. Fewer jurisdictions reported to regulate project developers[17], insurance of crypto-assets[18], DeFi trading/lending platforms (DeFi protocols), and the provision of non-custodial wallet services.

More respondents cited prior approval/registration and supervisory or regulatory examinations as applicable regulatory tools. In contrast, most jurisdictions reported that they do not have any resolution planning requirements applicable to crypto-asset service providers.

The survey highlights the extensive challenges facing regulators. The most commonly identified obstacles include: activities conducted through DeFi protocols, “unidentifable entities”, “lack of authority/mandate”, “cross-border cooperation” and “insufficient regulatory infrastructure”.

3. Issues and challenges in regulating and supervising crypto-asset activities and markets

Policy makers identified a range of issues and challenges in regulating and supervising crypto-asset activities and markets, which relate to (i) regulatory powers and their reach as well as potential gaps or challenges in their application; (ii) the extensive use of distributed and decentralised technology in the operations of crypto-asset activities; (iii) the effective regulation and supervision of crypto-asset activities and markets in a cross-border context; (iv) risks related to wallets and custody services; and (v) risks relating to trading, lending and borrowing activities.

3.1. Regulatory powers and coverage

Challenges to regulating and supervising crypto-asset activities and markets arises from the availability and application of existing regulatory powers, specifically in relation to: (i) the treatment of crypto-assets and activities that pose, or potentially pose, risks to financial stability and that may not be within the jurisdictional regulatory perimeter; (ii) enforcement of rules, when activities are in non-compliance with jurisdictional regulations; and (iii) risks associated with certain underlying technologies of crypto-asset activities.

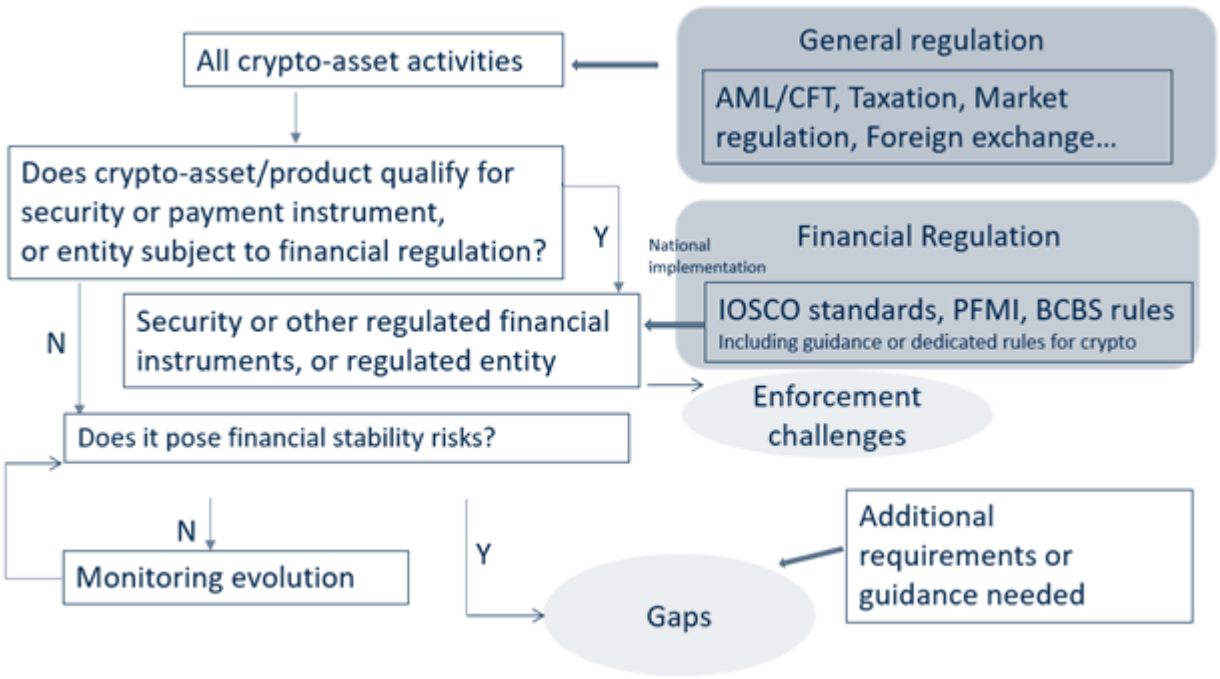
---

17 It is worth noting that project development is traditionally not subject to financial regulation.

18 One possible reason is that the insurance using crypto-assets is very limited and does not exist in most jurisdictions.

Graph 1 depicts an assessment of the regulation applicable to crypto-asset activities in jurisdictional regulatory frameworks. When activities are conducted by a regulated entity or the crypto-asset is classified as payment or financial instrument (e.g., security, commodity, derivative or other), or where the crypto-asset activity is regarded as regulated, they are likely subject to jurisdictional regulatory frameworks aligned to relevant international standards. However, in some cases and in some jurisdictions, crypto-assets or the associated activities fall outside of the existing regulatory perimeter.[19] If that is the case and if the activity poses, or potentially poses, risks to financial stability, there arises a significant regulatory gap. In some other jurisdictions, crypto-asset activities captured by existing regulatory frameworks may be acting in non-compliance with applicable regulations. In these jurisdictions, authorities could face enforcement and supervisory challenges rather than regulatory gaps.

Diagram on the regulation of crypto-asset activities in regulatory frameworks **Graph 1**



3.2. DeFi protocols, non-identifiable entities and governance

The extensive use of distributed and decentralised technology in the operations and/or governance of crypto-asset activities has contributed to opaqueness and a lack of accountability. Identifying the entities or natural persons that should be held accountable for good governance and regulatory compliance may be difficult. Among crypto-asset activities provided within the "Decentralised Finance" (DeFi) ecosystem by DeFi protocols, there exist a variety of governance structures, some of which may obfuscate the identification of a governance body or otherwise impede the application of regulation. In some other cases, there

[19] For example, as per the definitions in the European regulatory framework, only 2% of the outstanding crypto-assets would fall within the scope of the existing MiFID II security regulation. Over 80% of them are crypto-assets that will be assessed by the forthcoming MiCA Regulation.

may be individuals/entities responsible for the operation of an activity that have not adequately disclosed their roles. Such complex and opaque organisational and governance structures pose challenges for regulators. Regulators and supervisors need to look past the labels and marketing around a product or service, and consider the facts and circumstances of each case to establish ways to identify who exercises effective control on the protocol or provides access to the protocol, and to make them accountable under existing or future regulation.

Many crypto-asset issuers and service providers do not have a transparent governance structure with clear accountability. In some cases, governance of a crypto-asset issuer or service provider is dispersed across multiple actors, who each have control or influence only over certain aspects of the relevant operations. A lack of strong governance, which can occur when crypto-asset issuers and service providers are unregulated or operating in non-compliance with applicable regulation, could create or exacerbate financial stability concerns.

3.3. Cross-border cooperation

The cross-border nature of crypto-assets creates regulatory, supervisory and enforcement challenges. These arise from (i) differences in regulatory classification among jurisdictions; and (ii) cross-border cooperation arrangements that may not address the new needs for cross-border and cross-sectoral cooperation and information sharing.

The same crypto-asset may be classified differently in different jurisdictions, or may be regulated in some jurisdictions but not in others. This may create risks of regulatory arbitrage or evasion, in which some actors may be incentivised to structure their businesses to circumvent the application of certain jurisdictions' more stringent regulatory requirements.

Existing cross-border regulatory cooperation arrangements were typically designed for the cooperation of authorities supervising traditional financial institutions and activities and are often sector-specific. These arrangements may need to be reviewed to determine whether they are adequate to support information sharing and coordination related to crypto-asset regulation, supervision and enforcement, even when the subject activities fall into different sectors across jurisdictions.

3.4. Risk management related to wallets and custody services

Wallet services are a key user interface in the operation of all crypto-asset activities and play critical roles in safeguarding the crypto-assets of users.

The provision of wallet services can be custodial or non-custodial. In practice, they have different economic functions and risk-profiles. Many wallet services, in particular non-custodial wallets, are currently unregulated.

- Non-custodial wallets refer to the methods which allow users to independently interact with a blockchain and its services. Non-custodial wallets can include software, or other "hot wallet" services users may download and use on their personal devices, or "cold wallet" services, such as the user's own hardware. Non-custodial wallets enable users to self-custody their crypto-assets and imply that only the users themselves can access or recover their private keys. In general, users are responsible for maintaining their own wallets. However, when the wallet service is disrupted by a hardware failure

or cyber incident, the service provider may bear risks depending on the contractual terms between the provider and the user. As the loss or inaccessibility of cryptographic information will generally result in the permanent and irreversible loss of the crypto-assets,[20] service disruptions may result in the affected users' loss of confidence. Furthermore, as non-custodial wallet users generally are pseudonymous or anonymous, they may pose higher money laundering and terrorist financing (ML/TF) risks. [21] Currently, non-custodial wallets are not regulated in most jurisdictions.

- Custodial wallet providers take custody of private key information for safekeeping. Users do not need to generate and store private keys themselves, and generally log into a system developed by the custodial wallet provider to interact with their crypto-assets. Custodial wallet providers normally are responsible for maintaining access to the crypto-assets.[22] Therefore, the custodial wallet provider has more direct exposure to risks associated with cyber incidents, hacking, fraud and other operational risk events. These wallet providers also face reputational risks and, potentially, their failure could result in a loss of confidence in the market.[23] Custodial wallets also involve higher counterparty risks. If the crypto-assets under custody are not properly segregated from the provider's own liabilities, users may experience investment losses in the event the provider is insolvent or otherwise fails to uphold its obligations.[24] Currently, custodial wallets may be partly regulated if certain functions, such as custody or brokerage, fall within a jurisdiction's regulations. If the crypto-asset is a security or derivative within a jurisdiction, IOSCO Principles for the safe custody of client assets could provide guidance for providers including requirements to segregate client assets and prevention of the inappropriate use of client assets for proprietary trading. In jurisdictions where crypto-assets are not or cannot be categorised as financial instruments (securities or derivatives), custodial wallets may be unregulated unless offered by a regulated financial institution, subject to trust provisions under the general law, or captured by a specific regulation.

---

20 This is unlike similar cases in traditional finance, where options to recover assets are possible in the event of password loss or account inaccessibility.

21 Cold wallets may be easily transferred from one person to another without any records of the transfer of related value.

22 This depends on the contractual agreement between the user and the custodial wallet provider and may vary significantly. In practice, custodial wallets are often offered as an ancillary service by trading platforms that provides trading services to users and are analogous to a combination of the custody and the broker-dealer in traditional finance. The implication of the combinational functions is discussed in the 3.8.

23 In the recent FSB stock-take survey (see Annex 3), some respondents also noted custodial wallets may contribute to risk transmission and amplification, because a failure of custodial wallets could push users to try to recover control over their crypto-assets. When a larger number of users lose confidence in the safety of their crypto-assets, this may trigger sell offs and lead to strains in the crypto-asset market. A few respondents further emphasised that custody services provided in conjunction with risk-taking activities like lending and proprietary trading create financial risks to the wallet provider, potentially entangling user assets if the custodian becomes insolvent. Respondents also noted that when traditional financial institutions provide custody services, they are exposed to reputational risks transmitted from any problems encountered with the custody services.

24 A recent *10-Q filing* with the U.S. SEC by a trading platform offering custody services indicates that "custodially held crypto assets may be considered to be the property of a bankruptcy estate, and that in the event of a bankruptcy, the crypto assets we hold in custody on behalf of our customers could be subject to bankruptcy proceedings and such customers could be treated as our general unsecured creditors."

3.5. Risk management related to trading, lending and borrowing

Trading, lending and borrowing may contribute to financial risk transmission, because these activities create important linkages within the crypto-asset market and between the crypto-asset market and the wider financial system.[25]

Crypto-asset trading services are offered by crypto-asset trading platforms that function as a marketplace similar to an exchange in traditional finance. Trading platforms bring together the orders of multiple buyers and sellers by facilitating crypto-asset users to engage in various transactions, including exchange between different crypto-assets or against fiat currencies, borrowing and lending of crypto-assets, investing in crypto-asset related funds, derivatives or other investment products. The core risks of marketplace trading are comparable to those of traditional exchanges, including operational disruptions, fraudulent or abusive trading, and failed or untimely execution and settlement of transactions. Given the central roles of trading platforms, the materialisation of these risks may lead to market malfunctioning, confidence collapse and liquidity strains in the wider crypto-asset markets. At present, in jurisdictions where crypto-assets are not classified as financial instruments (commodities, securities, and/or derivatives) or payment instruments, many crypto-asset trading platforms are unregulated. In other jurisdictions where crypto-assets are considered financial instruments, platforms may be operating in non-compliance with applicable regulations.

Crypto-asset lending and borrowing has grown rapidly. Many trading or lending platforms promise high returns to attract investors' crypto-asset deposits. To generate these high returns, service providers may engage in or lend assets to complex and risky investment strategies, which can create maturity mismatches and liquidity risk. Liquidity/maturity mismatch is a typical financial sector vulnerability and one of the reasons why activities giving rise to this type of risk are traditionally strictly regulated. However, within the crypto-asset market, most of these activities are not regulated by standards equivalent to banking regulations, nor are they regulated as licensed lending activities, allowing the providers of such activities to engage in unrestricted risk-taking without sufficient resources or appropriate safeguards. In some cases, the providers of such activities may be acting in non-compliance with applicable regulations. Several crypto-asset lenders failed during the recent market turmoil as a result of vulnerability to runs, thin capitalisation, concentrated exposures to risky entities, and risky trading and business ventures. The failure of these entities has significantly impacted many retail investors, and highlighted the potential risks posed to financial stability were interconnections with the traditional financial sector to increase.

3.6. Data management and disclosure

Accurate data on crypto-asset activities may not be available to regulators or to the public because these activities are carried out by unregulated entities that are not subject to any reporting requirements or because the service provider fails to collect and report reliable data in compliance with existing requirements, or because of the lack of specific reporting requirements for traditional regulated entities of their participation in crypto-asset activities.

---

[25] In the recent FSB stock-take survey, many respondents indicated trading platforms, functioning as bridges between investors and markets, may contribute to shock propagation and risk transmission (See Annex 3).

The lack of available and reliable data poses challenges for regulators when monitoring and assessing the financial stability risks of crypto-asset activities. For example, while the recent crypto-asset market strain has not significantly impacted the wider financial system, regulators face challenges in assessing potential spillovers of a similar event in the future due to a lack of reliable data.[26]

Many crypto-asset market participants claim that their activities are fully transparent and reliable because they are stored and accessible on public blockchains. However, certain activities can be obfuscated using privacy enhancing technologies. Many activities and processes are also conducted "off-chain", particularly by centralised trading platforms, meaning that there will not be a public or accessible record of such activities. A recent study indicates that disclosures by crypto-asset trading platforms may not be reliable.[27]

Furthermore, even on-chain data provides only limited information into a transaction, as details are often pseudonymised or anonymised. Thus, it is a challenge to assess and analyse on-chain data due to its complexity and opacity. Many regulatory authorities do not have adequate resources to verify their accuracy and reliability to support monitoring and policy considerations.

Similarly, when crypto-asset issuers and service providers are not subject to disclosure requirements, users and investors lack the tools to assess the risk of their participation. Investors may have very limited information about the product structures or operations. Many crypto-asset service providers (e.g., trading platforms, lending platforms and custodians) do not disclose sufficient information to understand their financial conditions and risk profiles. This means that it is necessary to enhance the transparency and reliability of data on crypto-asset activities to address the data gaps.

3.7. Combination of multiple functions within a single service provider

One prominent feature of the crypto-asset market structure is that service providers often engage in a wide range of functions. Some trading platforms, besides their primary functions as exchanges and intermediaries, also engage in custody, brokerage, lending, deposit gathering, market-making, settlement and clearing, issuance distribution and promotion. Some trading platforms also conduct proprietary trading or allow proprietary trading on the platform by affiliated entities.[28] By vertically integrating multiple functions, these service providers resemble a financial conglomerate.

Similar to a financial conglomerate, these service providers have complex risk profiles. Risks originating from individual functions may be mutually reinforcing and transmit across functions.

---

[26] FSB (2022b): *FinTech and Market Structure,* March. The report suggests a similar issue in the data gaps of Fintech business: "…This leads to a "Catch 22" situation, where risks and systemic importance are key considerations to decide whether to modify the regulatory perimeter or conduct more intensive surveillance, but where the information to assess those risks and systemic importance are only available for institutions falling within the regulatory perimeter".

[27] BIS (2022) indicates that the total number of Bitcoin holdings by Coinbase inferred from on-chain records deviate remarkably from the amount disclosed by the trading platform. BIS (2022): *Banking in the shadow of Bitcoin? The institutional adoption of cryptocurrencies*, May.

[28] Annex 2 provides a detailed overview of activities provided by trading platforms with an analogue to traditional financial activities.

For example, when a trading platform combines the functions of marketplace trading with lending, offering of derivatives, structural products and collective investment vehicles, it may be incentivised to provide products with high risks and leverage.[29] The combination of multiple functions may also give rise to conflicts of interest. For example, a crypto-asset trading platform might conduct market-making on its own platform and impede the fair access of competing market makers. Such conduct may give rise to investor protection, market integrity and conflict of interest issues, such as in the case of a disputed trade with an individual investor.[30]

Traditional financial institutions also have incentives to expand and combine multiple functions. However, existing prudential regulation of financial conglomerates seeks to comprehensively address the corresponding risks, segregate particular functions, and ensure the consolidated group is sufficiently resilient to maintain its operations under stressful conditions. More generally, existing market regulation seeks to mitigate the inherent conflicts of interest and investor risks arising from the combination of services and functions.

Similar to the regulatory approach to financial conglomerates, it may be important to address the risks arising from the combination of multiple crypto-asset related functions within a single entity. In some instances and jurisdictions, it may be appropriate to disallow the provision of certain combination services or functions by a single entity.[31]

4. Proposed recommendations for the regulation, supervision and oversight of crypto-asset activities and markets

4.1. 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. 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 DeFi protocols, that pose, or potentially pose, risks to financial stability, both individually and collectively. 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[32] should also be subject to regulatory and

---

29 According to ECB (2022) *Decrypting financial stability risks in crypto-asset markets*, some trading platforms, including both lending and derivatives, offer to users ways to increase exposures by as much as 125 times the initial investment.

30 In the recent FSB stock-take survey, some members noted that the combination of custody with lending and proprietary trading functions may give rise to conflicts of interests and create market integrity and consumer protection risks. They should be given particular attention. Some jurisdictions are considering specific regulatory requirements, including enhanced disclosure or the separation of functions.

31 In some jurisdictions, such prohibitions exist and certain combinations of functions are not allowed to be carried out by a single entity. For example, there are certain level of segregation requirements between proprietary trading and intermediary services such as deposit-taking or marketplace trading.

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

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 interconnectedness with the traditional financial system. The rapid evolution and international nature of these markets also raise the potential for regulatory gaps, fragmentation or 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.[33] Their aim is to promote a regulatory, supervisory and oversight framework that is technology-neutral and focuses on underlying activities and risks.

The proposed 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 may help to ensure a comprehensive regulatory coverage and reduce the scope for regulatory arbitrage or evasion.

4.2. 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

---

[33] Authorities may also decide to take more conservative regulatory measures and, for example, choose to prohibit certain or all crypto-asset activities.

crypto-asset activities and markets, and will support authorities in implementing the proposed recommendations as crypto-asset activities and markets evolve.

The FSB will, in close cooperation with relevant SSBs, take the appropriate actions to (i) finalise the recommendations by mid-2023 in light of feedback from the public consultation; (ii) continue to coordinate international regulatory and supervisory approaches for crypto-asset activities to ensure they are comprehensive, consistent and complementary, including by considering the findings of the vulnerability analysis work on DeFi and whether additional policy work is warranted; and (iii) conduct a review of the implementation of the recommendations by end-2025 that may help determine whether a further review of the recommendations or development of implementation guidance may be necessary.

Table 2 shows the indicative timelines for this work following the publication of the consultative document.

Table 2: Follow-up work to the FSB consultative report and recommendations

Finalise the recommendations in light of feedbacks from the public consultation	
FSB will, in consultation with SSBs (CPMI, FATF, IOSCO, BCBS) as needed, revise and finalise the proposed recommendations in light of feedback from the public consultation.	By mid-2023
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, the FSB will consider in 2023 whether additional policy work is warranted.	By end-2023
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

4.3. Proposed Recommendations

Recommendation 1: Regulatory powers and tools

Authorities should have the appropriate powers and tools, and adequate resources to regulate, supervise, and oversee crypto-asset activities and markets, including crypto-asset issuers and service providers,[34] 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

[34] Crypto-asset issuers and service providers are defined in the Annex 5 of this document.

crypto-asset activities and markets, including crypto-asset issuers and service providers 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 or appropriate.

Authorities should have the powers and capabilities to enforce applicable regulatory, supervisory and oversight requirements, including authorisation and licensing requirements, the ability to undertake inspections or examinations, and, when crypto-asset issuers or service providers are not complying with applicable laws or regulations, to require corrective actions and take enforcement actions as appropriate, for example, by imposing restrictions on the access by domestic users to foreign crypto-asset activities and markets where they do not comply with applicable domestic regulations.

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 effective regulation, supervision, and oversight to crypto-asset activities and markets – including crypto-asset issuers and service providers – proportionate to the financial stability risk they pose, or potentially pose, 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[35].

Regardless of whether crypto-asset activities are conducted in 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 aims 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, consistent with their respective jurisdictions' laws and regulations. Authorities should use existing cooperation and information sharing arrangements (e.g., supervisory colleges, fora, networks, memoranda of understanding, 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 endeavour to inform each other in a timely manner if they become aware of an adverse situation that may have a wider systemic impact on the financial system and cross-border effects, and should cooperate to mitigate material risks of contagion. Authorities should ensure sufficient information sharing on their enforcement actions against activities in non-compliance or violation with jurisdictional regulations when these activities are operating in multiple jurisdictions.

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 spillover into other jurisdictions.

---

[35] E.g. 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.

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.

Recommendation 4: Governance

Authorities, as appropriate, should require that crypto-asset issuers and service providers have in place and disclose a comprehensive governance framework. 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, such as through DeFi protocols or setting up other 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 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, allocates adequate resources to risk management and other control functions (i.e., compliance and internal audit), and ensures that these functions can exercise their mandates with independence.

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, manage, prevent, and disclose 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 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 consider applying both prudential and market conduct regulatory tools as appropriate. Authorities should pay particular attention to technological risks associated with crypto-asset activities.

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'.

Authorities should supervise and regulate custodial wallet service providers, proportionate to their risk, size, complexity and systemic importance, in order to address operational, reputational, financial and consumer/investor protection risks that may arise from the storage of users' private keys. Regulations and oversight should assess the adequate safeguarding of customer assets, for example, through segregation requirements (including in the case of default/bankruptcy of the custodial wallet service providers).

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 to have in place robust frameworks 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 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[36] 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.

---

[36] 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.

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 should include, if appropriate, information on whether or not client assets are protected and segregated properly.

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.

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 that combine multiple functions and activities, for example crypto-asset trading platforms, 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 requirements regarding separation of certain functions and activities, as appropriate.

Certain crypto-asset service providers, such as some crypto-asset trading platforms, undertake a variety of services, including facilitating transactions, settlement and clearing, non-custodial and custodial wallet provisioning, (including the sale of software and hardware for

non-custodial wallet), market-making, offering investment vehicles, lending and borrowing, proprietary trading and issuance, among others. Relevant authorities should work to ensure that these 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 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 consider whether and, if so, how these combined functions can be appropriately regulated within a single entity. To the extent that such combinations are a result of non-compliance with existing regulations, authorities should enforce their powers and use their tools as appropriate and in line with jurisdictional legal frameworks, including disaggregation and separation of certain functions. In addition, authorities should consider additional prudential requirements if appropriate to address additional risks or conflicts of interest. Authorities should pay particular attention to multiple-function service providers engaging in facilitating custody, trading, settlement, lending, borrowing or proprietary trading, and should apply regulatory measures that are designed for the adequate segregation of risks.

Annex 1: Essential functions, risks and relevant international standards

Function 1: Creation, issuance, redemption, distribution, and underlying infrastructure of crypto-assets

Activities	Service providers and activity/entity pair	Key Regulatory and financial stability risks and vulnerabilities	Potentially relevant international standards and policies
1. Creating, issuing and redeeming crypto-assets (Developing protocols, designing smart contract and choice of the consensus mechanism), placement, marketing and sales	1. Issuers, including those: i) -not incorporated as a legal entity. ii) -incorporated as a legal entity but not licensed or registered by regulatory authorities. iii) -incorporated as a legal entity licensed or registered by regulatory authorities. 2. Project development team 3. An underwriter or facilitator of issuance or in capital formation. 4. An entity undertaking marketing and sales	**(1) Credit risks** The issuer may fail to meet redemptions in stress situations if they have promised redemption to users. **(2) Liquidity risk** The Proof of Stake protocols may lead to concentration of crypto-assets staked in the protocol and affect available liquidity in the market. **(3) Misconduct risk** (insider information, price manipulation, false disclosure); Weak governance related to protocols, consensus mechanism. **(4) Conflicts of interests** in designing the arrangement, selecting participant entities (especially in permissioned DLTs) Some issuance has lack of clear definition of roles and responsibilities of the governing body and lack of effective contractual and accountability mechanisms amongst participating entities. Absence of a clearly identifiable entity that can be held accountable for meeting rights of holders, addressing operational	1. IOSCO Objectives and Principles of Securities Regulation for underwriting 2. CPMI-IOSCO Principles for financial market infrastructures (PFMI) (only if activity is performed by a systemically important FMI) 3. CPMI-IOSCO Guidance on the Application of the Principles for Financial Market Infrastructures to stablecoin arrangements

		risk, and ensuring compliance with AML/CFT standards. **Others: ML/TF risks**	
2. **Operating the infrastructure and validating transactions**	1. **Permissioned DLT**: Entities that perform validation and settlement of transactions. They are normally selected and authorised beforehand. 2. **Permissionless DLT**: Validator nodes (Miners) can be set up by anyone fulfilling the technical requirements and the protocols. 3. **Centralised platforms** (often a trading platform that performs many other functions) that keep records off-chain, hold assets in custody, settle transactions.	**(1) Operational risks (including cyber risks):** Risk from the technology and operations the issuer controls. This includes smart contracts design risks, deficient cyber security resulting in unavailability or hacking of wallets that hold/mint/burn tokens, other operational risk events such as loss of keys, fraud, mismanagement of token supply or trustworthy settlement of transactions, validation and settlement patterns of cross-chain transfer. Operational risk at the issuer level could lead to, e.g., a disruption of users' ability to transfer their tokens, or a loss of value of the tokens. Misconduct such as miners front-running attack in which a miner includes its own transaction in the block instead of someone else's and does not include the original transaction. **(2) Settlement risk** Crypto-assets may have settlement risks when used for payments. **(3) Climate transition risk affecting validation and scalability**: changes of the consensus protocol and validation	1. BCBS Principles for Operational Resilience 2. BCBS Principles for the Sound Management of Operational Risk 3. CPMI-IOSCO Principles for financial market infrastructures (PFMI) (only if activity is performed by a systemically important FMI) 4. CPMI-IOSCO Guidance on the Application of the Principles for Financial Market Infrastructures to stablecoin arrangements 5. CPMI-IOSCO, Guidance on Cyber Resilience for Financial Market Infrastructures (only if activity is performed by a systemically important FMI) 6. IOSCO Objectives and Principles of Securities Regulation 7. IOSCO Principles on Outsourcing 8. FSB Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements 9. FSB Effective Practices for Cyber Incident Response and Recovery

	mechanisms, both voluntary or imposed by legal restrictions for certain type of activities (ban from certain territories and/or climate restrictions. **(4) Concentration risk:** concentration of validators and technology service providers. **(5) Third-party risks** (e.g., a failure that arise in sub-contractors and other centralised entities that keep records or network services). **(6) Others: AML/CFT, financial crime** (e.g., direct exchange of illegal proceeds for mined coins with no transaction history).	

Function 2: Wallets and custody

Activities	Service providers and activity/entity pair	Key regulatory and financial stability risks and vulnerabilities	Potentially relevant applicable standards and policies
3. **Provision of custodial (hosted) wallet and custody services**	**Custody service providers could be** i) **regulated financial institutions;** They manage crypto-assets (i.e., private keys) for retail and institutional customers, usually provided in conjunction with other services such as offline key management services and insurance services as a hedge against loss, in addition to the transfer and exchange of crypto-assets. They may manage crypto-assets administratively or jointly (e.g., using multi-signature) with their customers. ii) **other entities;** They manage crypto-assets (i.e., private keys) on behalf of their customers, but may be exempt from regulation for reasons such as the sole activity of management of crypto-assets are not within the regulatory perimeter in some jurisdictions or they manage crypto-assets jointly	**(1) Operational risks:** cyber security risks leading to unavailability or unauthorised outflow of customers' crypto-assets; This includes technical vulnerabilities including wallet software design and cyber security measures, and operational vulnerabilities such as loss or mismanagement of private keys. Misconduct risk from, e.g., loss of funds due to negligence, fraud/theft, poor administration, inadequate record keeping, or co-mingling of assets. **(2) Concentration risks:** When a small number of service providers, wallet software, or software libraries account for the majority of market share, failures/vulnerabilities in them affect many customers' crypto-assets (e.g., loss of crypto-assets) and spill over to crypto-assets ecosystem. **(3) Third-party risks** (e.g., a failure that arises in sub-custodians and other sub-contractors) **(4) Others: AML/CFT** N.B. Type of custody service varies significantly with different risk features, covering operational, conduct and market knock-on effects, depending on the	1. BCBS Principles for Operational Resilience 2. BCBS Principles for the Sound Management of Operational Risk 3. BCBS Principles for Sound Liquidity Risk Management and Supervision 4. CPMI-IOSCO Principles for financial market infrastructures (PFMI) (only if activity is performed by a systemically important FMI) 5. CPMI-IOSCO, Guidance on Cyber Resilience for Financial Market Infrastructures (only if activity is performed by a systemically important FMI) 6. IOSCO Objectives and Principles of Securities Regulation 7. IOSCO Recommendations Regarding the Protection of Client Assets 8. IOSCO Recommendations for Liquidity Risk Management for Collective Investment Schemes 9. IOSCO Principles on Outsourcing 10. FSB high-level recommendations (Specific to global stablecoin arrangements) 11. FSB Effective Practices for Cyber Incident Response and Recovery

	with their customers and have no controlling authority. In other cases, the actual situation is unclear and it is challenging for authorities to determine whether they are within the perimeter. In addition to this, there are some entities who do not comply with regulations, such as unregistered service providers. **iii) DeFi protocols** They manage users' crypto-assets or information about their interests in crypto-assets using smart-contracts that pool users' crypto-assets, typically as part of DeFi protocol offering exchange or lending activities. **Other entities might provide support services for wallets.**	contractual agreement between the provider and the user.	12. FATF Standards and Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers
4. **Provision of non-custodial (unhosted) wallets**	**i) regulated financial institutions;** To offer solutions for retail and institutional customers or for general public to manage their crypto-assets (i.e., private keys) themselves. Users use unhosted wallets for considerations on cybersecurity, transaction costs, etc. and, they typically use their self-hosted wallets in combination with	**(1) Operational risks:** including cyber security risks leading to unavailability or unauthorised outflow of users' crypto-assets; This includes technical vulnerabilities including wallet software design. Operational vulnerabilities are often due to users (e.g., carelessness, lack of knowledge). **(2) Concentration risks:** When a small number of wallet providers, wallet software, or software libraries account for the majority of market share, failures/vulnerabilities in them affect many	1. BCBS Principles for Operational Resilience 2. BCBS Principles for the Sound Management of Operational Risk 3. CPMI-IOSCO Principles for financial market infrastructures (PFMI) (only if activity is performed by a systemically important FMI) 4. CPMI-IOSCO, Guidance on Cyber Resilience for Financial Market Infrastructures (only if activity is performed by a systemically important FMI)

	regulated entities' services such as exchange of crypto-assets. **ii) others;** They may only develop and sell the hardware/software and are typically not subject to regulations. There may be some entities who do not comply with regulations. **iii) DeFi protocols** They may offer solutions for users or for general public to manage their crypto-assets (i.e., private keys) themselves to promote the use of DeFi protocol. **Other entities might provide support services for wallets.**	users' crypto-assets (e.g., loss of crypto-assets) and spill over to crypto-assets ecosystem. **(3) Third-party risks** (e.g., a failure of hardware/software wallet that arise in sub-contractors) **(4) Others: AML/CFT** (Users can use the wallet without going through KYC, CDD, STR etc)	5. IOSCO Objectives and Principles of Securities Regulation 6. IOSCO Principles on Outsourcing 7. FSB high-level recommendations 8. FSB Effective Practices for Cyber Incident Response and Recovery

Function 3: Transfer and transaction

Activities	Service providers and activity/entity pair	Key regulatory and financial stability risks and vulnerabilities	Potentially relevant applicable standards and policies
5. **Payment for/of goods, services, gifts and remittances**	Payment and settlement providers, including: i) **Traditional FMIs** (both payment and securities systems, e.g., Credit Card provider); ii) **Financial institutions** (including banks); iii) **Other entities**[37], typically centralised trading platforms; iv) **DeFi protocols.**	**(1) Market risks**: excessive volatility, rapid price swings can hamper the use of crypto-assets in transactions, particularly in settlement operations. Sharp depreciation may generate outflows and jeopardise the use of certain crypto-assets. **(2) Counterparty credit risks**: Depending on the mismatch of exposures of the two payment legs. **(3) Operational risks,** in particular for unregulated entities whose records may be less reliable including cyber security risks, and legal risks where uncertainties of the legal status of crypto-assets and their broader ecosystem could expose entities different forms of legal risks. Misconduct by any service provider of the crypto-asset ecosystem, in particular, in unregulated centralised trading platforms; **(4) Reputational risks,** in particular for traditional FMIs that promote or enable the use of crypto-assets in payment transactions, which could face	1. FATF Standards and Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers 2. CPMI-IOSCO, Guidance on Cyber Resilience for Financial Market Infrastructures 3. CPMI-IOSCO Principles for financial market infrastructures (PFMI) (only if activity is performed by a systemically important FMI) 4. CPMI-IOSCO Guidance on the Application of the Principles for Financial Market Infrastructures to stablecoin arrangements 5. BCBS, Principles for Operational Resilience 6. BCBS, Revisions to the Principles for the Sound Management of Operational Risk 7. BCBS, Prudential Treatment of Cryptoasset Exposures (second consultation)

[37] Applicable regulation varies. These institutions may be subject to payment regulation in certain jurisdictions. For instance, many CEXs in the U.S. register as money service business under federal AML/CFT regulations and may be registered money transmitters at a state level.

		reputational risks in the event of payment failure. **(5) Exchange rate risk**. Using for payments or clearing, crypto-assets could substitute local currency, especially in EMDEs and non-reserve currency nations. This can generate volatility and changes in the level of exchange rate. **(6) Settlement risks.** Crypto-assets may have settlement risks when used for payments. **(7) Others:** Investor protection: lack of protection discourages users from use in transactions for payment, in cases of unregulated entities. A specific case relates to lack of legal clarity of single instruments (e.g., whether it is a financial instrument or a crypto-asset), creating uncertainties as to the applicable sectoral regulation. Legal risks are amplified in cross-border transactions; AML/CFT in particular, in cases of unregulated entities. The above-mentioned risks could be amplified in the case of FIs with direct or indirect exposures due to their participation in payment schemes involving the use of crypto-assets.	
6. Facilitate the exchange of crypto-assets: either between crypto-assets or between crypto-assets and	1 They can be	**(1) Market risks**: excessive volatility, rapid price swings can hamper the use of crypto-assets in transactions, particularly in settlement operations.	1. FATF Standards and Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers

fiat-currency, or fiat-currency backed financial contracts	i) **Traditional FMIs** ii) **Traditional financial institutions, broker-dealers, custodians** iii) **Unregulated entities, such as an unregulated centralised trading platform** iv) **DeFi protocols**	Sharp depreciation may generate outflows and jeopardise the use of certain crypto-assets. **(2) Counterparty credit risks**: Depending on the mismatch of exposures of the two payment legs. **(3) Operational risks,** in particular for unregulated entities whose records may be less reliable including cyber security risks, and legal risks where uncertainties of the legal status of crypto-assets and their broader ecosystem could expose entities different forms of legal risks. Misconduct by any service provider of the crypto-asset ecosystem, in particular, in unregulated centralised trading platforms; **(4) Reputational risks,** in particular for traditional FMIs that promote or enable the use of crypto-assets in payment transactions, which could face reputational risks in the event of payment failure. **(5) Exchange rate risk**. Using for payments or clearing, crypto-assets could substitute local currency, especially in Emerging markets and developing economies (EMDEs) and non-reserve currency nations. This can generate volatility and changes in the level of exchange rate. Others: Conflicts of interest associated with exchanges.	2. CPMI-IOSCO, Guidance on Cyber Resilience for Financial Market Infrastructures 3. CPMI-IOSCO Principles for financial market infrastructures (PFMI) (only if activity is performed by a systemically important FMI) 4. CPMI-IOSCO Guidance on the Application of the Principles for Financial Market Infrastructures to stablecoin arrangements 5. BCBS, Principles for Operational Resilience 6. BCBS, Revisions to the Principles for the Sound Management of Operational Risk 7. BCBS, Prudential Treatment of Cryptoasset Exposures (second consultation)

	Use of crypto-assets may compete with fiat currency in EMDES and amplify volatility to non-reserve currencies and currencies of EMDEs. The above-mentioned risks could be amplified in the case of FIs with direct or indirect exposures due to their engagement with crypto-asset service providers (regulated or not).	

Function 4: Investment, lending, insurance, leverage and risk management

Activities	Service providers and activity/entity pair	Key regulatory and financial stability risks and vulnerabilities	Potentially relevant applicable standards and policies
7. Use as collateral to borrow other crypto-assets, including stablecoins	Institutional investors, they can be i) **Centralised investor entity** (e.g., hedge funds, family offices, pension funds, can be either traditional FIs or unregulated entities) ii) **Centralised crypto-asset trading platforms** iii) **DeFi protocols** Other entities providing support services, such as custodian, advisor, asset manager. They can also be any of the three above categories.	**(1) Credit risk:** leverage magnifies potential losses and financial stability consequences of losses (e.g., liquidity impact of unwinding collateralised positions in response to price moves). **(2) Counterparty credit risk:** Collateralisation exposes the lender to the value of crypto-assets. Collateral value and borrower solvency likely to be correlated. **(3) Others**: Risk contagion as losses and liquidity stresses spill over to core part of the financial system. Consumer protection when engaging retail investors Crypto-assets allow for repeated rehypothecation and leverage, creating the possibility of very sharp declines and automated unwinding and liquidation. This hidden leverage may be difficult for regulators to monitor and address.	1. BCBS standards on capital and liquidity 2. CPMI-IOSCO Principles for financial market infrastructures (PFMI) (only if activity is performed by a systemically important FMI) 3. IOSCO Objectives and Principles of Securities Regulation 4. IOSCO Recommendations for Liquidity Risk Management for Collective Investment Schemes
8. Lending in crypto-assets (including direct lending in crypto-assets or facilitator for traditional financial instruments i.e., loans, derivatives, **investment vehicles, etc.)**	Lenders of crypto-assets or lenders that accept crypto-assets in business, they might be: i) **Centralised crypto-asset platforms** ii) **DeFi protocols**	**(1) Liquidity risks,** **(2) Credit and counterparty credit risk**: the risk that the counterparty will fail to meet its obligations in accordance with agreed terms. This risk is particularly relevant in lending operations between users involving	1. IOSCO, Report on Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms 2. BCBS, Prudential Treatment of Cryptoasset Exposures (second consultation)

	iii) **Traditional financial institutions including banks** Other entities providing support services, such as custodian, advisor, asset manager. They can also be any of the three above categories.	crypto-assets: as such, high level of volatility of crypto-assets may amplify this source of risk **(3) Market risk** related to invested assets with proceeds from depositors/investors **(4) Operational risks** fraud, failed process or infrastructure failure. **(5) Others:** Market integrity related to inadequate disclosure, misconduct in sales and promotions. Consumer protection when engaging retail investors Risks may mutually reinforce and give rise to rapid transmission of stress due to tight interconnections. Use of crypto-assets in traditional financial activities may create new risks, such as elevated volatility, technical risks, and sudden price dislocations ("flash crashes") and increases the potential for stress in crypto-asset system to spill over to the traditional financial system.	3. CPMI-IOSCO Principles for Financial Market Infrastructures (PFMI) (only if activity is performed by a systemically important FMI)
9. Insurance	Insurance of digital assets (e.g., crypto-asset wallets), holding of digital assets and underwriting of crypto-related risks. Also includes replacement of fiat currency as a form of payment (premiums and claims). Important to note that there is little to no activity in /	**(1) Credit risk, market risk, liquidity risks** in relation to accepted/invested etc. crypto-assets **(2) Operational risks** for insurer in relation to (i) holding of own assets (custody of keys etc.), (ii) transfers of crypto-assets, (iii) conversions in fiat	IAIS: No specific standards and no specific guidance on insurance based on crypto-assets exist. However, general standards apply, e.g., on risk management and internal controls (ICP 8), valuation of assets and liabilities (ICP 14), and investments (ICP 15) whereby the supervisor requires the insurer to invest only in assets where it can properly assess and manage the risks.

	exposure to digital assets in the insurance industry i) **Traditional insurers** ii) **Centralised platforms** iii) **DeFi protocols** (very rare in practice due to difficulty in pricing the risk)	money and (iv) compliance with AML/KYC regulations	
10. Direct/outright exposures to crypto-assets (including, writing of products, margining, market making, etc.)	1. **Institutional investors, retail investors, banks and insurers** 2. **Centralised crypto-asset trading platforms** 3. **Brokerage firms/ investment advisers** 4. **Settlement provider** 5. **Custodian** They can be i) **Traditional FMIs** ii) **Traditional financial institutions (Bank, insurance, funds)** iii) **Unregulated centralised platforms** iv) **DeFi protocols**	**(1) Market risks,** including basis risks in hedging **(2) Liquidity risks** **(3) Credit and counterparty credit risks** **(4) Operational risks.** **(5) Concentration risk** **(6) Others:** Market integrity/investor protection Holding crypto-assets outright gives rise to the risks outlined above but is also a necessary condition to generating the risks posed by crypto-assets when used as a means of payment or as collateral.	1. IOSCO, Report on Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms (2020) 2. IOSCO, Consultative Report on Principles for the Regulation and Supervision of Commodity Derivatives Markets (2021) 3. IOSCO Recommendations Regarding the Protection of Client Assets 4. IOSCO Recommendations for Liquidity Risk Management for Collective Investment Schemes 5. IOSCO, Risk Mitigation Standards for Non-centrally Cleared OTC Derivatives (2015) 6. BCBS, Prudential Treatment of Cryptoasset Exposures (second consultation) 7. CPMI-IOSCO Principles for Financial Market Infrastructures (PFMI) (only if activity is performed by a systemically important FMI)

11. Synthetic/ derivative exposure to crypto-assets, including exposure to derivatives **referenced by crypto-assets**	1. **Institutional investors, retail investors, banks and insurers** 2. **Centralised crypto-asset trading platforms** 3. **Brokerage firms/ investment advisers** 4. **Settlement provider** 5. **Custodian** They can be i) **Traditional FMIs** ii) **Traditional financial institutions (Bank, insurance, funds)** iii) **Unregulated centralised platforms** iv) **DeFi protocols**	**(1) Market risks**, including basis risks in hedging **(2) Liquidity risks** **(3) Credit and counterparty credit risks** **(4) Operational risks.** In particular misconduct in engaging retail investors and may spillover and have knock-on effects. **(5) Concentration risks.** Derivatives can give rise to virtually unlimited exposure, thereby amplifying losses and liquidity demands to sustain exposures. In addition, given the indirect exposure to crypto-assets it provides, traditional financial system participants who may have concerns with operational resilience of direct holding of crypto-assets are incentivised to hold synthetic exposure to crypto-assets, which would increase interconnectedness between crypto-asset markets and the traditional financial sector	1. IOSCO, Report on Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms (2020) 2. IOSCO Objectives and Principles of Securities Regulation 3. IOSCO, Consultative Report on Principles for the Regulation and Supervision of Commodity Derivatives Markets (2021) 4. IOSCO Recommendations Regarding the Protection of Client Assets 5. IOSCO Recommendations for Liquidity Risk Management for Collective Investment Schemes 6. IOSCO, Risk Mitigation Standards for Non-centrally Cleared OTC Derivatives (2015) 7. The Basel Framework (capital and liquidity standards) 8. BCBS, Prudential Treatment of Cryptoasset Exposures (second consultation) 9. CPMI-IOSCO Principles for Financial Market Infrastructures (PFMI) (only if activity is performed by a systemically important FMI)

Annex 2: Study of features of existing crypto-asset trading platforms and DeFi protocols

This Annex presents a summary based on a functional mapping of the governance structure and activities conducted by existing trading platforms and DeFi protocols. Given the fundamental differences between centralised platforms (which often offer trading, lending and borrowing on one platform) and DeFi protocols (which typically offer their services like trading, lending, and borrowing separately), the findings of the two categories are presented separately. The description provides an amalgamation of facts drawn from existing trading platforms and DeFi protocols and seeks to capture common and most prevalent features and activities pertaining to the two categories, but it does not provide an exhaustive enumeration of all existing activities.

Key takeaways

Centralised platforms generally have a legal and governance structure broadly similar to that of a typical trading platforms/exchanges in traditional finance.

DeFi protocols claim that governance is distributed; however, in reality, governance is often concentrated in a small group of development team members, investors or large governance token holders.

Centralised trading platforms offer an integrated suite of products and services to retail and institutional customers and to other crypto-asset market participants.

DeFi protocols provide different financial services, but the largest share within DeFi include crypto-asset lending, borrowing, or trading facilitated by liquidity pools. They invite users to deposit crypto-assets under various models to ensure adequate liquidity and participation.

Centralised platforms are often not licensed or registered in all capacities; moreover, they may be acting in non-compliance with applicable regulations.

DeFi protocols often have a legal entity behind them, but they are often structured in order to obfuscate the relationship between the two. Some such entities may be licensed or registered in some way, but the related protocols may not be directly regulated or may be operating in non-compliance with applicable regulations.

Centralised trading platforms

Centralised crypto-asset platforms typically provide, directly or through affiliates, an integrated suite of products and services to retail and institutional customers and to other crypto-asset market participants. For example, these platforms facilitate transactions involving fiat currencies and crypto-assets, offer custody services, and themselves engage in proprietary and market making activities. Certain platforms claim that they do not maintain physical headquarters, but typically are registered or licensed in some way in one or more jurisdictions. Table 1 provides a general overview of the different types of products and services offered, together with an initial summary of analogous activities and identified risks.

Table 1: Mapping of activities conducted by crypto-asset trading platforms, with risks and comparison to traditional finance[38]

Activity	Description of Activity	Comparison of Activity to Traditional Finance	Key risks
TRADING	**Purchases, sales and trading of crypto-assets.**		
Marketplace Trading ***Trading Retail*** ***Trading Institutional***	Bringing together the orders of multiple buyers and sellers, including finding a counter-party, discovering prices, and accessing liquidity. Facilitating users (retail/institutional customers) trading between crypto-assets or against fiat currency. Providing routing services for customer order to third party exchanges or other trading venues. Platform generally charges a fee per transaction.	Exchange; issuer distribution (i.e., platform acting as underwriter or participant in primary distribution); broker-dealer; asset management; money transmission.	Fraud, theft, loss of assets; risks of market investor protection and market integrity (e.g., lack of disclosures, lack of rules to promote fair and orderly markets with operational and price transparency, lack of rules to prevent unfair discrimination, lack of listing standards that are subject to regulatory approval).
Prime Brokerage ***Institutional***	Order routing and order management, custody, real-time market data and analytics, and financing products.	Broker-dealer; asset management; lending; data analytics.	Credit risk; liquidity risk; counterparty credit risk; fraud, theft, loss of assets; conflicts of interest; concentration.

[38] The template does not represent a full and comparison to traditional finance or a list of all potential risks.

Activity	Description of Activity	Comparison of Activity to Traditional Finance	Key risks
Offering a trading desk as a Broker-Dealer	Offering a trading desk for execution of trades in various crypto-assets without involving the exchange order book (if it also offers an exchange). The platform may act as a confirming third party in pre-arranged transactions. Generally, there is volume-based pricing and charges a transaction fee for every matched trade.	Broker-dealer; asset management.	Fraud, theft, loss of assets; lack of trade transparency; conflicts of interest; concentration.
Platform Trading Activities	Trading as principal for proprietary accounts (with customers on the other side of trades). Platforms also engage in derivatives activities with their customers and others.	Broker-dealer; derivatives intermediary.	Fraud; Conflicts of interest.
Derivatives Trading	Offer crypto-asset referenced derivatives (may be OTC).	Broker-dealer; derivatives intermediary.	Leverage risk.
ISSUANCE, PROMOTION AND DISTRIBUTION	**Crypto-Asset Offerings and Related Activities.**		
Primary Token Distribution and Token Promotion ***Retail/Institution***	Participating with issuers in offering and selling their tokens through the platforms, including for capital formation transactions. Platforms also make available governance tokens from DeFi protocols and DAOs for trading.	Exchange; issuer distribution (i.e., platform acting as underwriter or participant in primary distribution); broker-dealer; investment adviser;	Information asymmetry; lack of investor and market protections; conflicts of interest; concentration.

Activity	Description of Activity	Comparison of Activity to Traditional Finance	Key risks
	Platform typically receives a commission based on the value of crypto-assets that are distributed to its users.	asset management; money transmission.	
Stablecoin Issuer, Distributor and Trading	Issuing or distribution stablecoins of platform affiliates. Platforms list the stablecoins for trading and provide other returns to customers who hold their stablecoins on the platform or lend the stablecoins to the platform for a promised return.	Exchange; issuer distribution (i.e., platform acting as underwriter or participant in primary distribution); broker-dealer; asset management; money transmission; lending and borrowing.	Information asymmetry; lack of investor and market protection; Conflicts of interest; concentration.
Asset Management Services ***Institutional***	Providing services to asset managers, investment funds and institutional investors to assist in trading and keeping custody of crypto-assets. Offering portfolio management services to investment advisors. A platform may market that they can provide custody, clearing and trade execution services all in one place.	Broker-dealer; underwriter; asset management.	Conflicts of interest; fraud, theft, loss of customer assets.

Activity	Description of Activity	Comparison of Activity to Traditional Finance	Key risks
	Advising on buying and holding crypto-assets.		
STAKING: BLOCKCHAIN VALIDATION	**Participating in blockchain consensus mechanisms.**		
Staking as a Service ***Retail/Institutional***	Offering staking as a service. Platforms generally pool their customers' crypto-assets for staking on the relevant blockchain. They collect the staking rewards for their customers and take a fee. The rewards come from transaction validation on a proof-of-stake blockchain when one of the platform's nodes successfully creates or validates a block. Increasing staking participation increases the changes the platform's nodes will be a validator.	No direct corollary in traditional finance, but can resemble issuers (e.g., of interests in a pooled vehicle or other investment opportunity).	Fraud, theft, loss of staked assets. Lack of investor protections.
Delegated Proof of Stake ***Retail/Institutional***	Participating in a process whereby network participants can designate a certain amount of their crypto-assets on the network as a stake (similar to a security deposit) to validate transactions and be rewarded in kind from the network. Because staking crypto-assets is a technical challenge for most users	No direct corollary in traditional finance, but can resemble issuers (e.g., of interests in a pooled vehicle or other investment opportunity).	Fraud, theft, loss of staked assets. Lack of investor protections.

Activity	Description of Activity	Comparison of Activity to Traditional Finance	Key risks
	requiring a participant to run their own hardware, software, and maintain close to 100% up time, Platform provides a “Delegated Proof of Stake” (DPS) service. DPS allows retail users to maintain full ownership of their crypto-assets while earning staking rewards. Platform earns a commission on all staking rewards received.		
CUSTODY/WALLET SERVICES	**Provide custody (hosted wallets) or unhosted wallets**		
Custodial Wallet ***Retail***	Offering a hosted wallet that allows retail users to interact with their crypto-assets for any management purposes as a custody service.	Broker-dealer; custodian; money transmission; clearing agency; central counterparty.	Fraud, theft, loss of customer assets, conflicts of interest; concentration.
Custodial Wallet ***Institutional***	Offering to institutions the same custody that they offer retail. They market this as being offered by regulated custodians, which they say offers institutional grade audits, governance, digital key management, and physical security.	Broker-dealer; custodian; money transmission; clearing agency; central counterparty	Fraud, theft, loss of customer assets; conflicts of interest; concentration.

Activity	Description of Activity	Comparison of Activity to Traditional Finance	Key risks
	Custody is often marketed as being vertically integrated with the investing platform, providing institutions with access to liquidity and trading services.		
non-custodial wallet Services ***Retail/Institutional***	Offering software to self-custody crypto-assets, separated from the trading platform.	No direct corollary in traditional finance, have some resemblance to broker-dealer; money transmission; depository.	Fraud, theft/hacking, loss of assets through hacking.
INVESTMENT PROGRAMS (IN ADDITION TO TRADING)	**Offering investment programs to customers**		
Yield Programs ***Retail***	Offering program for retail users to use their crypto-assets to earn a yield/reward. These programs may provide returns based on holding stablecoin balances.	Issuer (e.g., of interest on deposit or investment vehicles which could be a security or fund, depending on facts and circumstances).	Fraud, theft, loss of assets; conflicts of interest; concentration.
PLATFORM LENDING AND BORROWING PRODUCTS AND SERVICES	**Platforms may originate fiat consumer and commercial loans as well as crypto-asset loans.**		
Borrowing - Portfolio-backed loans ***Retail***	Allowing retail users to borrow fiat currency against their crypto-asset portfolios.	Non-bank lending activities; issuer; broker-dealer.	Fraud, theft, loss of assets. No retail borrower protections.

Activity	Description of Activity	Comparison of Activity to Traditional Finance	Key risks
	A Platform may offer a portfolio-backed loan allowing retail users to borrow fiat currency using their crypto-assets as collateral. A customer's line of credit is secured by their investment portfolio and they can use the line of credit to access fiat currency while maintaining a "hold" investing strategy.		
Lending - Portfolio-backed loans ***Retail***	Offering retail users the investment products to lend their crypto- assets and earn returns.	Pooled investment program earning a return; broker-dealer; non-bank lending.	Fraud, theft, loss of assets; risk of borrower failure; no investor protections
Borrow & Lend ***Institutional***	Offering credit-based products and services to provide institutional customers access to liquidity for their hedging, speculation, and working capital needs.	Non-bank lending.	Credit risk, counterparty risk, operational risk.
Post-trade credit ***Institutional***	Customers typically need to pre-fund their account and maintain fiat or crypto-assets on the platform in order to participate in the market. Offering institutions post-trade credit or funding, which is an advance of funds and settlement on behalf of credit eligible customers. This is said		

Activity	Description of Activity	Comparison of Activity to Traditional Finance	Key risks
	to allow institutional customers to instantly trade on credit and settle within a few days.		
Margin trading	A Platform also may offer institutions spot trading with margin, allowing significant leverage.	Margin trading.	Market risk, counterparty risk, liquidity risk, compounded risk from high leverage.
MONEY TRANSMISSION SERVICES	**Platforms offer money transmission services to customers.**		
Send & Receive ***Retail***	Offering retail users the ability to send crypto-assets to any user globally on the platform using their email, phone #, or crypto-asset wallet address. Sending and receiving the funds is usually free but some sends incur a small variable transaction fee.	Broker-dealer; money transmission.	Fraud, theft, loss of assets, operational risk, credit risk (including counterparty credit risk) and liquidity risk.
Send & Receive ***Institutional***	Offering institutions the ability to send crypto-assets to any user globally on the platform using their email, phone #, or crypto-asset wallet address. Sending and receiving the funds is usually free but some sends incur a small variable transaction fee.	Broker-dealer; money transmission.	Fraud, theft, loss of assets, operational risk, credit risk (including counterparty credit risk) and liquidity risk.

Activity	Description of Activity	Comparison of Activity to Traditional Finance	Key risks
Electronic Money and Payment	Offering e-money services to customers	Money transmission.	Fraud, theft, loss of assets, operational risk, credit risk (including counterparty credit risk) and liquidity risk.
PREPAID CARDS			
Prepaid Cards ***Retail***	Offering a branded prepaid debit card funded by a customer's crypto-asset balance that allows retail users to swipe or tap to pay for a purchase at any merchant that accepts Visa or another processor. In some Platforms, retailers can use the card to spend, to borrow fiat currency against select crypto-asset balances, or to earn a yield on select crypto-assets. A transaction is shown in local fiat currency and crypto-assets are sold from the customer's crypto-asset wallet or account to fund the purchase. The platform earns a transaction fee based on the transaction volume of each purchase. A platform card also may allow holders to earn crypto-asset rewards.	Prepaid card services; money transmission.	Fraud, theft, loss of assets, operational risk, credit risk (including counterparty credit risk) and liquidity risk.

Activity	Description of Activity	Comparison of Activity to Traditional Finance	Key risks
THIRD PARTY SERVICES	**Platforms offer different data and analytical services to developers and others outside the trading platform.**		
Data and Indices Services and Analytics Tools	Offering blockchain analytics tools and crypto-asset trading data. Platforms also may offer crypto-asset indices. These may be done through APIs.	N/A	Conflicts of interest; concentration; cyber.
Software Supporting Blockchain Application Development	Offering software to make it easier for developers to build applications that work across different blockchains.	N/A	Conflicts of interest; concentration; cyber.
Third Party Development Activities Supporting Particular Products	Supporting third party development activities for particular products, such as particular stablecoins, in order to increase demand and use of those tokens. This includes the development of APIs for payment purposes.	N/A	Conflicts of interest; concentration; cyber.
Wallet Link API	Providing tools to DeFi app (or DApp) developers to connect to and easily accept payments from mobile crypto-asset wallets.	N/A	Conflicts of interest; concentration; cyber.

Activity	Description of Activity	Comparison of Activity to Traditional Finance	Key risks
Cloud Services	Providing infrastructure technology that offers crypto-asset payment or trading APIs, data access, and staking infrastructure. These tools allow companies to build crypto-asset products faster and to simplify how they interact with blockchains.	N/A	Conflicts of interest; concentration; cyber.
VENTURE CAPITAL INVESTING	**Investing in crypto-asset ecosystem**		
Direct Investments	Through their venture capital affiliates, investing in companies and projects focused on growing the crypto-asset ecosystem. These investments may be in early start-ups as well as in more established projects.	Hedge fund, private equity fund, venture capital funds investments	Leverage and risk exposures.

DeFi protocols

General information

A DeFi protocol normally has an identifiable legally entity behind it, often under the name that is similar to the protocol (such as XYZ Lab/Foundation) but may not be exactly the same. The legal and governance relationship between the protocol (platform) and the legal entity may not be readily apparent, and the protocol and/or legal entity may be evasive about whether the legal entity has control over the governance of the protocol. Some legal entities claim that they work as “contractors” or “service providers” to the community composed of users, who are deemed to be the governance body of the protocol. The status and jurisdiction of the entities’ licensing or registration is sometimes unclear and not always adequately disclosed. These entities may not be licensed or registered in any way. In other cases, the entity could be licensed to undertake a given activity, but the DeFi protocol in practice performs additional activities for which it is not licensed. The entity and other participants in the protocol may be acting in non-compliance with applicable regulations.

DeFi protocols are partly enabled by autonomous programs (smart contracts) that facilitate particular activities and tasks and enable users to participate in various trading and other transactions. DeFi protocols purport to rely on decentralised governance, in which stakeholders, usually governance token holders (see below), are in theory responsible for decisions on aspects of the protocol that often take the form of ‘proposals’. Proposals can encompass matters such as, *inter alia*, voter weighting, changes to a parameter in a smart contract, asset listing, risk parameter updates, ecosystem reserve spending, and collateral requirements.

These governance arrangements, often marketed as decentralised autonomous organisations (DAOs), usually operate within communities that communicate off-chain in online fora, for example, on a platform’s official website or on a social media channel. Using these means of communication, the governance token holders typically discuss a proposal to change aspects of the protocol. The decision-making process generally consists of three steps:

- Proposal: To propose a change to the protocol;
- Discussion: To discuss and assess the proposal;
- Vote: To vote on the proposal and enact it if passed.

The actual proposal and voting process differ among protocols. It is a common practice that governance token holders can delegate their proposal power and/or voting power. Depending on the protocol, proposal and voting processes could include a minimum number of voting rounds, voting thresholds, waiting periods, and the like.

Further, some platforms appear to have some mechanism to change proposal and voting processes. For example, a voting threshold may be dynamic and can be subject to change based on the quorum plus differential of votes for/against a proposal. Thus, when the votes against a proposal are more substantial, then the approval threshold can be moved up so there must be an overwhelming approval before the proposal is implemented. There can also be

specific committees with veto power that is claimed by the protocol as a safety mechanism against governance attacks.

Almost all protocols claim to have 'decentralised governance'. However, in actuality governance often appears to be concentrated. In some cases, the implementation of approved proposals appears to lie in the hands of the protocol development team, which includes the founder and management of the registered entity behind it, and the coders and developers it employs. In other cases, governance tokens are concentrated among a small group of related technology companies, venture capitalists and leading private investors[39]. For some protocols, the vast majority of governance tokens are held by a very small number of accounts.[40] Furthermore, because governance tokens may also be traded, it is possible for a protocol development team or the other participant to purchase a controlling share of tokens in order to vote for a favoured proposals and sell the tokens thereafter.

Activities

Governance token issuance

As indicated above, governance tokens play an important role in the governance process. DeFi protocols normally issue a protocol-specific governance token, which (as described above) may be used to propose and vote on protocol changes.

At issuance, governance tokens typically are distributed to community members, development team members, investors and advisors. A portion of the governance tokens also may be retained by the entity behind the protocol, or some affiliate. As that entity is often controlled by the development team members, their shares of governance tokens may grow even larger. Governance tokens of many protocols can be exchanged and bought on centralised trading platforms.

Providing Liquidity

In some cases, token holders can contribute their tokens for a period of time as a way of adding liquidity to the protocol. These tokens may help support trading activities. Token holders who contribute tokens may retain their voting power and may be compensated in some way, e.g., by receiving additional tokens or a percentage of fees collected by the protocol.[41]

Lending/borrowing (depositing or removing collateral)

Lending and borrowing are other predominant activities in DeFi. Users deposit their crypto-asset into a smart contract (if accepted within the protocol) and can receive some form of

---

[39] Available here.

[40] For example, according to the information available on Etherscan, the top 100 accounts hold 86% of the total supply of Aave tokens (13,764,693 out of 16,000,000 tokens). In particular, around 16% of the tokens (around 2,654,536) are held by the top holder aAAVE Token V2. The second largest account is Staked Aave with around 13% of the tokens followed by the Aave ecosystem reserve which holds around 10% of the supply.

[41] The amount to be distributed as rewards is also voted as decided by the protocol. The total distributable amount can be set daily while the distribution may be exercised quarterly.

compensation as a result. Some protocols require users to exchange their deposited crypto-assets into a protocol-specific token, by which compensation is accrued and rewarded. As part of the automated process coded in the smart contract, returns can be dynamic depending on the available collateral pool size and demands. For example, when collateral is abundant, returns are lowered to encourage borrowing. In contrast, greater returns will apply if collateral (of an individual crypto-asset) falls, in order to incentivise repayment of loans and attract additional supply of collateral of that specific crypto-asset from depositors.

Users can withdraw their funds from a collateral pool on-demand, however withdrawal is subject to delay in case of inadequate liquidity in the pools of that specific asset. However, it appears that the conditions on withdraw delays are not adequately disclosed to users.

Exchange of one crypto-asset for another crypto-asset

Some protocols facilitate exchange between two different crypto-assets through what is referred to as an "Automated Market Maker" (AMM). An AMM maintains a liquidity pool for a given token pair and enables trading by users of the AMM at prices set by a formula that uses as inputs the real-time composition of the liquidity pool. A liquidity provider funds the liquidity pool for a given token pair. The liquidity provider may earn a transaction fee from users trading in that liquidity pool. To enhance the efficiency of utilising the pools of all available crypto-assets, some trading platforms recently introduced a revised mechanism to allow liquidity providers to specify a specific price range for their liquidity.

Flash loans

While decentralised crypto-asset lending protocols usually employ over-collateralisation to manage counter-party risk, flash loans allow the borrowing of crypto-assets without the requirement of any collateral. Borrowers are expected to return the borrowed amount, usually accompanied with a fee, within the same blockchain transaction. Flash loans are made possible without the need of collateral because if the borrower fails to repay the loan before the transaction validation is complete, the borrowing will not be validated and the entire transaction will be cancelled, posing no credit risks to the lending party.

Flash loans are mostly used for arbitrage purposes to take advantage of pricing disparities among crypto-assets that are traded on different trading platforms. A user borrows a crypto-asset by exchanging it with another crypto-asset, and then converts it back to the original crypto-asset on a platform with a lower exchange rate to earn a margin, followed by repayment of the borrowed amount and the fees to the lender and platform. However, flash loans can also be used for manipulation and attacks.[42] Flash loan attacks use a variety of techniques, including artificially manipulating the price of a particular exchange using large numbers of tokens to arbitrage with other exchanges, exploiting code vulnerabilities to obtain large numbers of governance tokens under the guise of depositing a large number of tokens, and using large numbers of borrowed governance tokens to pass malicious proposals.

---

[42] Flash loans represent around 30% of the total amount stolen in DeFi exploits. For examples see Qin et al. (2020) "Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit" or Carter, N. and Jeng, L. (2021): DeFi Protocol Risks: The Paradox of DeFi, in Coen, B. and Maurice, D.R. (eds.), Regtech, Suptech and Beyond: Innovation and Technology in Financial Services, RiskBooks.

Annex 3: Summary of stock-take survey feedback

Introduction

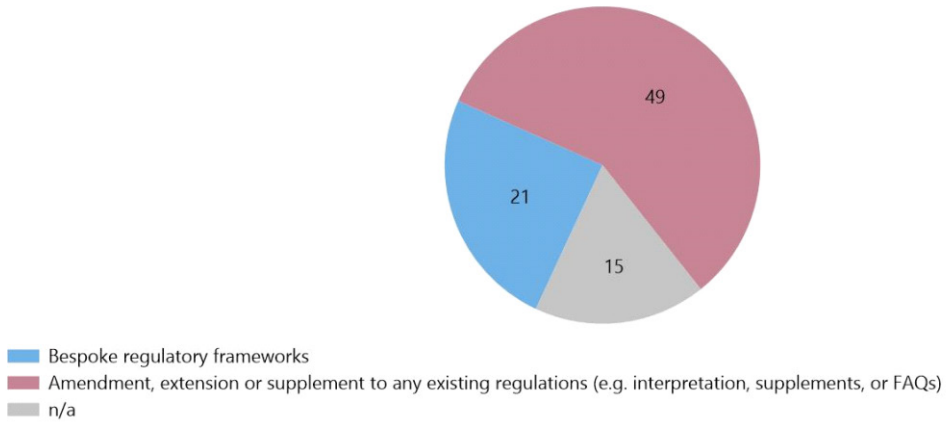
The Crypto-assets Working Group (CAG) conducted a stock-take survey in June 2022 that collects information on regulatory approaches, plans, challenges, as well as views on financial stability implications of crypto-assets. The stock-take received 48 responses from 24 FSB members[43] and 24 RCG members[44].

Regulatory framework and classification

General regulatory framework

15 FSB members and 10 RCG members have issued, or are in the process of issuing, relevant standards to enhance regulation of crypto-assets. Of the 70 issued standards, 49 are amended or adapted from existing standards and 21 are categorised as bespoke standards for crypto-assets (Graph 1).

Regulatory or supervisory standards or guidance issued in each jurisdiction **Graph 1**



Note: n/a reflects that the issued standard or guidance reported by respondents is not classified into either of the two categories.
Source: FSB survey

Regulatory definitions

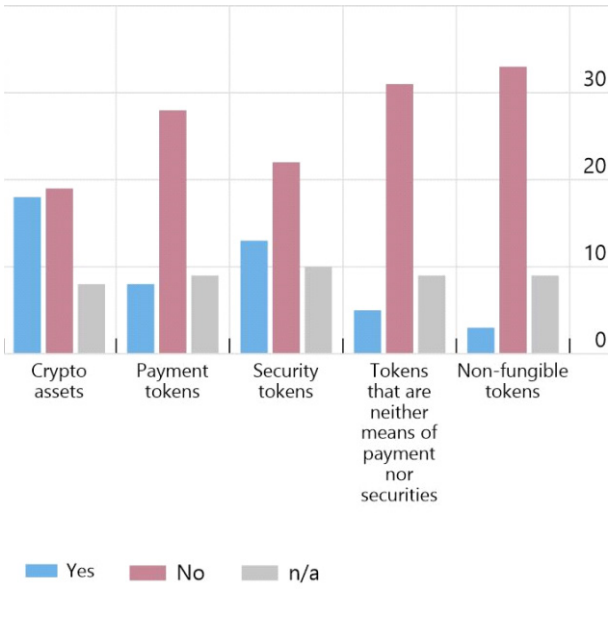
Graph 2 (Left panel) shows that about one-third of respondents have introduced a general regulatory definition of crypto-assets. More granular definitions based on functions are much less. 13 jurisdictions have introduced regulatory definition for security tokens while 8 jurisdictions have introduced definition for payment tokens.

[43] Including 23 national authorities and European Commission.
[44] Including 23 national authorities and one regional consolidated submission.

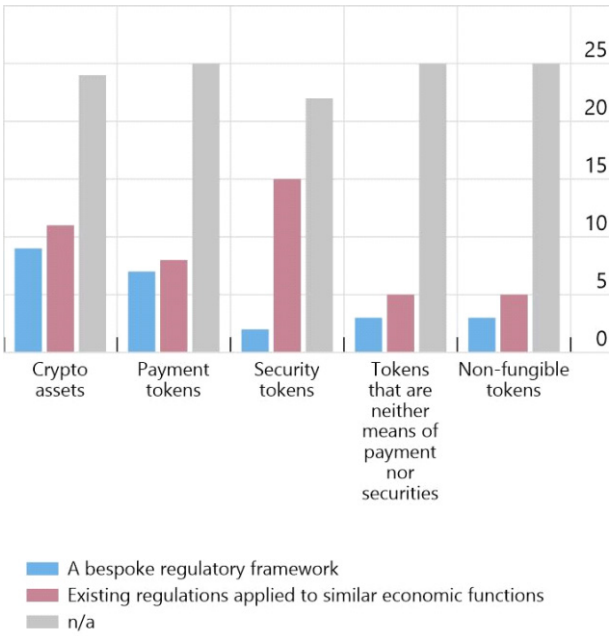
Meanwhile, 7 authorities responded that payment tokens are subject to bespoke regulatory framework while 8 authorities responded that they are subject to existing national payment regulations. As for security tokens these numbers are 2 and 15 respectively (Graph 2, right panel). Intuitively, the total number of jurisdictions with applicable regulations for function-based crypto-assets is larger than reported applicable regulatory definitions. This may indicate that in a minority of jurisdictions, these crypto-assets are captured by existing regulations without introducing specific regulatory definitions.

Regulatory definition of crypto-assets in jurisdictional regulatory framework **Graph 2**

Is this a regulatory/supervisory classification?



Is this category subject to a bespoke regulatory framework, or to existing regulations applied to similar economic functions, e.g., payment, security or derivative laws?



Note: n/a reflects that the respondent did not provide an answer to the question.
Source: FSB survey

Some respondents indicated that, in practice as crypto-assets may perform multiple economic functions, cumulative regulations apply. However, some members emphasised that regulation should not be mechanically divided by the types of crypto-assets. One respondent indicated that as the crypto-asset service providers typically involve different types of tokens, classification-based regulation may lead to an undesirable result whereby a regulator can only supervise part of activities that hampers comprehensive regulation, even leading to regulatory vacuum.

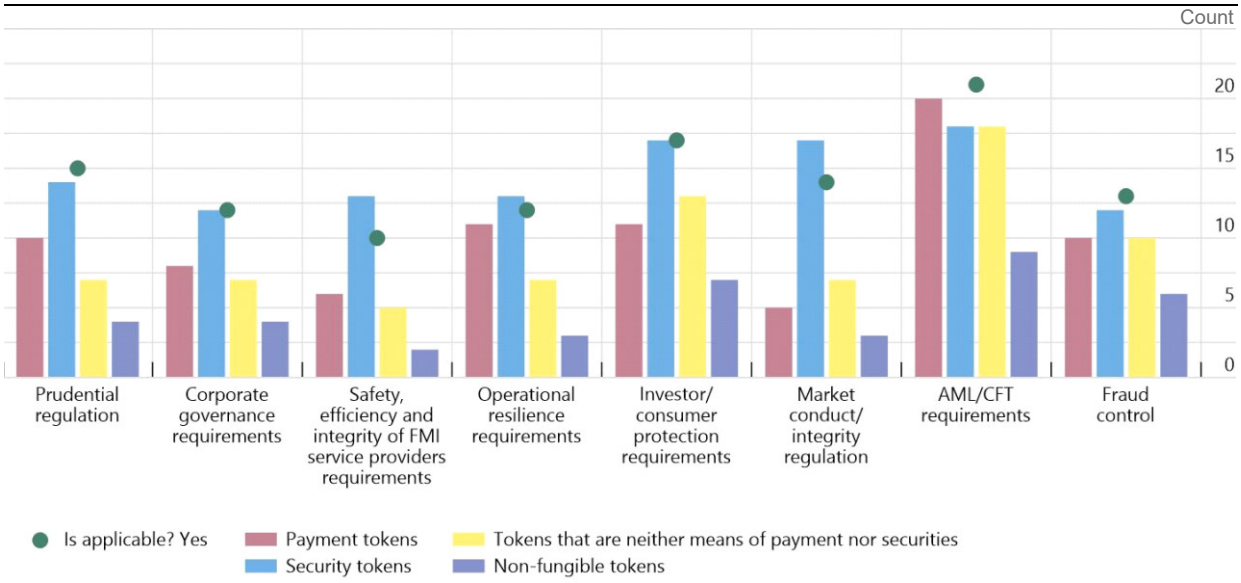
3 FSB members and 1 RCG members reported that they have introduced regulatory definitions other than the 4 categories proposed in the survey template. One of them indicated that it refers to a broader definition of crypto-assets (virtual assets) that include governance tokens and hybrid tokens with multiple functions.

Regulatory measures

Thematic regulation

Graph 3 shows applicable regulations based on 8 common regulatory themes devided by the 4 economic functions. In total, AML/CFT received most counts, followed by investor/consumer protection. The least covered themes are FMI service providers, corporate governance and operational resilience. From economic function perspective, securities tokens are most frequently regulated in all themes except AML/CFT where payment tokens received slightly more positive responses.

Applicable thematic regulation to different categories of crypto-assets **Graph 3**



Source: FSB survey

Regulation of crypto-asset services

Graph 4 depicts the number of jurisdictions that have regulatory measures in place for the 11 essential services and 4 crypto-asset categories. Similar to the outcome of thematic regulation, security tokens are most frequently covered among the 4 economic functions. From service type perspective, centralised trading platform and custody received most votes. The least covered services are developers, insurance and decentralised lending platforms.

Graph 5 summarises appliacable regulatory measures by the 11 essential services and 11 regulatory measures common to traditional financial regulation. The most frequently applicable regulatory measures are prior/approval and examiniation, in particular relation to wallet, custody and centralised trading platforms. On the nexus point, prior registration/approval of custody and centralised trading platforms were most often chosen.

Several authorities highlighted the need to consider scenarios where an entity operates various activities which partially fall within regulatory perimeter and partially outside. In such cases, if a regulatory requirement is entity-based, some authorities apply requirements on the entity by taking into account the entire business of the financial institution. However, some respondents

also indicated that for requirements that are intended to apply on an activity-basis, such as specific conduct requirements, there are challenges to apply them to the unregulated activities and products even if offered by the financial institution.

A few authorities noted self-regulation may support the regulation of crypto-assets, especially given the evolution of the market and technical expertise.

Whether the following crypto-asset activities (by crypto-asset categories) are regulated

Graph 4

Crypto-assets activities	Payment tokens	Security tokens	Tokens that are neither means of payment nor securities	Non-fungible tokens
1. Developing project Total	3	2	3	3
2. Issuing Total	8	17	7	3
3. Placing, distributing and marketing Total	14	14	11	6
4. Wallet provisioning Total	14	10	12	6
5. Providing custody Total	14	14	15	7
6. Facilitating transactions on a centralised trading platform Total	17	15	17	8
7. Facilitating transactions on a decentralised trading platform Total	10	9	8	4
8. Provisioning of centralised lending or on a centralised lending/borrowing platform Total	7	11	6	2
9. Provisioning of decentralised lending or on a decentralised lending/borrowing platform Total	6	8	5	2
10. Operating investment vehicles Total	9	18	10	7
11. Provisioning of crypto-based insurances Total	7	5	5	3

Note: The number in the table reflects total number of respondents who have indicated they have applicable regulation applied to the activity (row) conducted by the category of crypto-asset (column).

Source: FSB survey

What regulatory measures are applicable to the essential crypto-asset activities

Graph 5

Crypto-assets activities	Prior approval/ license/ registration	Prudential requirements	Governance/ management requirements	Restrictive measures	Disclosure requirements	Recovery planning requirements	Regular examination by supervisors	Firm-level data to be collected by supervisors	Risk management requirements	Point-of-sale conduct requirements	Consumer/ user compensation	Others
1. Developing project Total	3	3	3	3	4	3	5	3	4	3	2	2
2. Issuing Total	14	9	11	12	15	6	10	8	10	10	4	5
3. Placing, distributing and marketing Total	15	11	14	13	16	7	17	12	14	12	6	6
4. Wallet provisioning Total	18	8	14	7	8	6	16	10	11	6	3	6
5. Providing custody Total	20	10	17	7	10	6	19	13	15	7	4	7
6. Facilitating transactions on a centralised trading platform Total	21	10	18	11	12	10	19	13	14	9	6	8
7. Facilitating transactions on a decentralised trading platform Total	11	8	9	10	12	8	11	9	10	8	4	6
8. Provisioning of centralised lending or on a centralised lending/borrowing platform Total	9	6	7	6	6	5	8	7	7	5	2	5
9. Provisioning of decentralised lending or on a decentralised lending/borrowing platform Total	8	7	8	7	7	6	7	6	7	5	2	5
10. Operating investment vehicles Total	15	13	13	10	13	9	15	13	14	10	6	3
11. Provisioning of crypto-based insurances Total	6	6	6	5	5	5	6	5	8	6	2	3

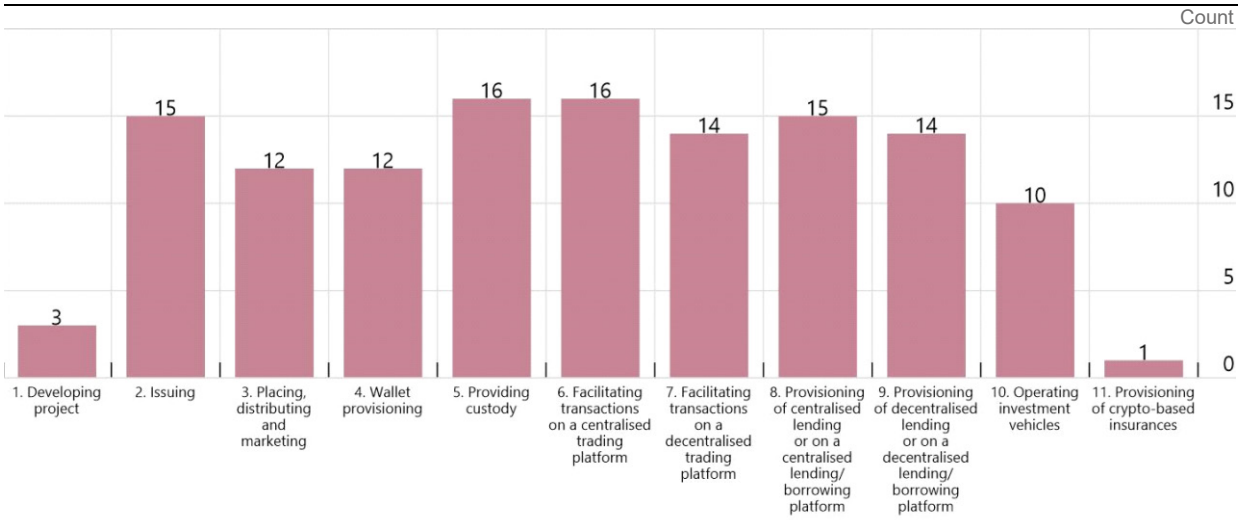
Note: The number in the table reflects the total number of respondents who have indicated the regulatory measure (column) is applicable to the activity (row) in their jurisdiction.

Source: FSB survey

Interconnectedness and risks

Graph 6 presents views on what are critical interfaces that contribute to risk transmission. Among the 11 proposed activities, most selected services are custody, centralised trading platforms, issuing and centralised lending platforms.

What crypto-asset activities are considered as critical interfaces in the crypto-assets ecosystem that are likely to contribute to growing interlinkage with the traditional financial system and could act as risk propagation channel within the crypto-asset ecosystem **Graph 6**



Note: The number reflects the number of respondents who have chosen the activity as a critical interface that is likely to contribute to interlinkage.

Source: FSB survey

Current challenges

Graph 7 presents in a heatmap view of challenges on regulation divided by 7 proposed challenges and 11 services.

On challenges types, cross-border operation, lack of authority and insufficient regulatory infrastructure are the most often chosen. Some authorities indicated that if an activity is unregulated there is no legal basis to either impose regulations or require for data. Some authorities noted that despite that in certain cases the investigative powers could be extended to other entities, certain connections to the financial markets should be necessary. A number of jurisdictions reported difficulties in categorising crypto-asset activities under current regulation. For example, some respondents noted as the current definition of a financial product was written prior to the invention and proliferation of crypto-assets, they may not able to capture a wide variety of novel crypto-assets. One respondent noted that the industry has reported difficulty in determining whether the financial products and services regime or the consumer law regime applies to their products. There is also response indicating that applying legal assessment of the nature of crypto-assets can be complicated and time-consuming. However this may vary remarkbly depending on jurisdictional legal and regulatory framework. Some jurisdictions reported their authorities have adequate enforcement power to bring crypto-asset activities under regulatory orbit by categorising them as securities or commodities.

From the service dimension, decentralised trading platforms and decentralised lending platforms are most often chosen by respondents. A few respondents underscored the significant data gaps related to DeFi that impede a fuller assessment of risks, including how the possible risks to the global financial system may affect the domestic financial system specifically. One authority stressed that going forward, work will be needed to enhance the transparency of institutional investor holdings as crypto-assets and DeFi continue to grow. International effort and co-operation will be essential to remediating these data gaps and monitor risks building across jurisdictions. One EMDE respondent noted that it is difficult to for EMDEs to assess and consider regulations and suggested that it is important for EMDEs to carry out monitoring activities as a basic policy action to assess the magnitude of the financial stability risks of crypto-assets.

Areas of challenges in regulation of essential crypto-asset activities

Graph 7

Crypto-assets activities	Lack of authority/ mandate	Enforcement	Unidentifiable entity	Cross-border operation	Insufficient regulatory infrastructure	Technological limitations	Data gaps
1. Developing project	18	9	10	16	13	8	13
2. Issuing	18	14	10	22	14	10	14
3. Placing, distributing and marketing	14	16	8	18	13	7	12
4. Wallet provisioning	19	10	10	17	17	11	10
5. Providing custody	14	10	10	16	13	9	10
6. Facilitating transactions on a centralised trading platform	14	10	7	17	15	8	8
7. Facilitating transactions on a decentralised trading platform	21	16	20	22	21	13	14
8. Provisioning of centralised lending or on a centralised lending/borrowing platform	18	13	8	16	17	7	12
9. Provisioning of decentralised lending or on a decentralised lending/borrowing platform	21	19	21	21	21	11	17
10. Operating investment vehicles	12	9	9	11	11	5	11
11. Provisioning of crypto-based insurances	16	12	9	12	13	6	11

Note: The number in the table reflects the total number of respondents who have indicated that they encounter the type of challenge (column) in regulating crypto-asset activities (row).

Source: FSB survey

Respondents also provide some preliminary suggestions on addressing the common challenges. This includes to enhance regulation on centralised intermediaries which may offer services in combination with decentralised arrangements, and to assess the scope of entities/bodies with control or influence over the governance or operation of the protocols. One respondent noted that regulation can leverage from the *FATF Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*[45] that scopes in[46] all the creators, owners, operators or persons that maintain control or sufficient influence on decentralised arrangements to the extent that they meet the definition of virtual asset service providers.

Future plans

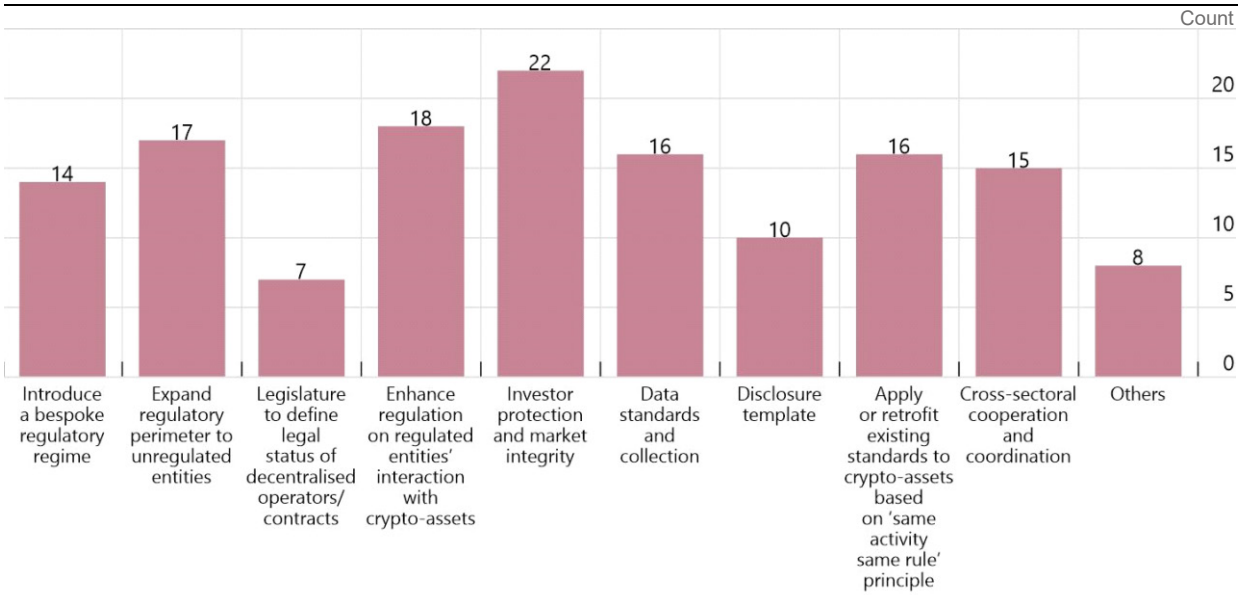
Graph 8 shows what policy considerations are within future plans of national authorities. Graph 9 shows considerations of priorities of jurisdictions which plan to develop a bespoke regulatory framework. Among the 6 members who responded with plans that prirotise certain aspects, a common consideration is to focus on how to develop a bespoke regulatory framework that can be applied to crypto-assets which are not regarded as 'financial products' under current regulations. One respondent reported that national authroties have launched a Fintech Hub joined by the private sector and will draw on this initiative to inform a possible regualtory framework in future. One respondent noted that their priority is to step up initiatives on introducing a bespoke regulatory framework by distinguishing between stablescoins that are mainly used for payment/settlement and other crypto-assets.

[45] Available here.

[46] Virtual asset service provider" is defined as any natural or legal person who is not covered elsewhere under the Recommendations and as a business conducts one or more of the following activities or operations 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; and
iv. Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets;
v. Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

Areas within policy considerations in future

Graph 8

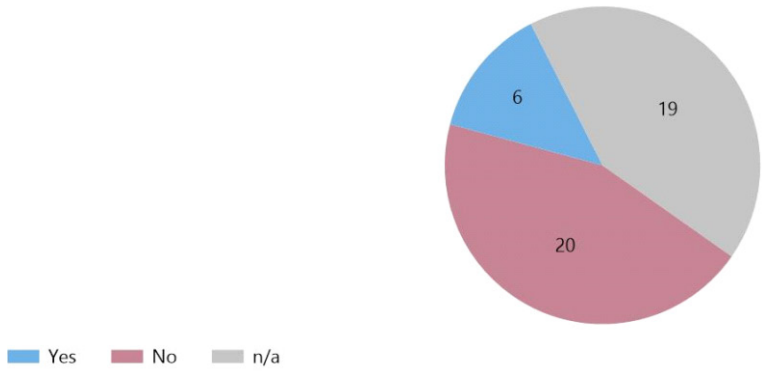


Note: The number reflects total number of respondents who indicated that specific area is within their plan.

Source: FSB survey

Number of jurisdictions that are considering plans to develop a bespoke regulatory framework by prioritising certain categories of crypto-assets

Graph 9



Note: n/a reflects number of respondents who did not provide answer to the question.

Source: FSB survey

Annex 4: Update of initiative of SSBs

Basel Committee on Banking Supervision (BCBS)

On 30 June 2022, the Basel Committee on Banking Supervision issued a second public consultation on the prudential treatment of banks' crypto-asset exposures[47]. The new proposal maintains the basic structure of the proposal in the first consultation, with crypto-assets divided into two broad groups:

Group 1 crypto-assets, which must meet in full a set of classification conditions and are either tokenised traditional assets, or crypto-assets with effective stabilisation mechanisms, and which would be eligible for treatment under the existing Basel Framework with some modifications; and

Group 2 crypto-assets, which include unbacked crypto-asset and stablecoins with ineffective stabilisation mechanisms, which are subject to a new conservative prudential treatment.

The updated proposals provide more detail and include new elements, including an infrastructure risk add-on to cover the new and evolving risks of distributed ledger technologies; limited recognition of hedging for qualifying Group 2 crypto-assets (i.e., Group 2a); and an overall gross limit on exposures to Group 2 crypto-assets exposures.

Given the rapid evolution and volatile nature of the crypto-asset market, the Basel Committee will continue to closely monitor developments during the consultation period, which will end on 30 September. The standards that the Committee aims to finalise around year-end may be tightened if shortcomings in the consultation proposals are identified or new elements of risks emerge and based on the Committee's overall assessment of the risks.

Bank for International Settlements' Committee on Payments and Market Infrastructures (CPMI) and International Organization of Securities Commissions (IOSCO)

In July 2022, the Bank for International Settlements' Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO) published guidance on the Application of the Principles for financial market infrastructures (PFMI) to stablecoin arrangements (SAs).

This guidance, which follows October 2021's proposals for consultation, reconfirms that if a stablecoin arrangement performs a transfer function and is determined by authorities to be systemically important, the stablecoin arrangement as a whole would be expected to observe all relevant principles of the PFMI. The guidance *per se* does not create additional standards for SAs beyond those set out in the PFMI but rather provides clarity and granularity on how systemically important SAs should approach observing certain aspects of the PFMI.

47 BCBS (2022).

Specifically, the report proposes guidance on aspects related to: (i) governance (PFMI Principle 2), (ii) framework for the comprehensive management of risks (Principle 3), (iii) settlement finality (Principle 8) and (iv) money settlements (Principle 9). The report also provides considerations to assist relevant authorities in determining whether an SA is systemically important in their jurisdictions.

While the guidance does not apply to other crypto-assets than stablecoins, some of the discussions presented in it may be useful for other types of crypto-assets.

The CPMI and IOSCO continue to examine regulatory, supervisory and oversight issues associated with SAs and coordinate with other SSBs.

International Organization of Securities Commissions (IOSCO)

Crypto and digital assets have been an IOSCO priority since 2017, with related-work undertaken by IOSCO's former Fintech and ICO Networks and its Board policy committees.

With recent rapid advancements in financial technology and the exponential growth of the crypto-asset market, IOSCO established a Board-level Fintech Task Force (FTF) in March 2022 to develop, oversee, deliver, and implement IOSCO's regulatory policy agenda in this area. The FTF comprises 27 IOSCO Board member jurisdictions. The FTF is also tasked with coordinating IOSCO's engagement with the FSB and other SSBs on Fintech and crypto-related matters.

In its initial 12 to 24 months of operation, the FTF will prioritise policy work on crypto-asset markets and activities, while continuing to monitor trends associated with broader Fintech developments. As published in its roadmap on 7 July, the FTF has formed two workstreams: the Crypto and Digital Assets (CDA) workstream and the Decentralized Finance (DeFi) workstream. Both workstreams will focus on investor protection and market integrity concerns in the crypto-asset space. Recent turmoil in the crypto-asset market has underscored the link between investor protection, market integrity, and the stability of the broader crypto-asset market ecosystem. These developments underpin the importance of the FTF's work to both address potential financial stability issues, taken forward by the FSB, whilst ensuring the same securities market risks are subject to the same regulation.

The CDA workstream is broadly organized into examining (i) fair, efficient and transparent markets, orderly trading, suitability and market manipulation, and (ii) safekeeping, custody and soundness. The DeFi workstream is looking specifically into DeFi, stablecoins, and crypto-assets trading, lending and borrowing platforms, as well as the interactions of DeFi with broader financial markets. It will expand upon and further develop issues discussed in IOSCO's March 2022 Decentralized Finance report.

The FTF aims to publish a report with principles and policy recommendations by end-2023. This will build on IOSCO's earlier work relating to crypto-assets, which includes the following key publications:

Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms - (February 2020)

The report aims to assist IOSCO members in evaluating the issues and risks relating to crypto-assets trading platforms (CTPs). It describes issues associated with the trading of crypto-assets on CTPs, outlines key considerations and provides related toolkits that are useful for each key consideration. The key considerations relate to access to CTPs, safeguarding participant assets, conflicts of interest, operations of CTPs, market integrity, price discovery and technology. These key considerations and toolkits were intended to assist regulatory authorities who may be evaluating CTPs within the context of their regulatory frameworks.

Global Stablecoin initiatives – (March 2020)

The report identifies the possible implications of global stablecoin initiatives for securities markets regulators, including how stablecoins interact with their regulatory remit. Insights from the report contributed to the high-level recommendations for the Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements developed by the FSB RIS, published in October 2020.

Investor Education on Crypto-Assets - (December 2020)

The report identifies an array of possible risks to investors, including lack of market liquidity, volatility, partial or total loss of the invested amount, insufficient information disclosure and fraud. The report then describes methods that regulators can use to provide educational material to retail investors on the risks of investing in crypto-assets and offers guidance on how to (i) develop educational material, (ii) inform the public about unlicensed and fraudulent firms, (iii) use different channels to inform investors and, (iv) form partnerships to develop and disseminate educational materials.

Decentralized Finance Report (March 2022)

The report offers a comprehensive review of the fast-evolving DeFi market, its products, services and principal participants. It highlights the numerous risks to participants, investors and markets arising from DeFi including, for example, the failure of a stablecoin issuer or crypto-asset trading platform involved in a particular stablecoin arrangement. Such a failure could give rise to significant volatility in these assets and thereby impair, among other things, the collateral and liquidity of DeFi protocols and lead to knock-on effects in the broader crypto-asset market ecosystem.

Financial Action Task Force (FATF)

In June 2019, FATF extended its AML/CFT measures to virtual assets (VAs) and VASPs to prevent criminal and terrorist misuse of the sector through its revision of Recommendation 15 and its Interpretative Note (R.15/INR.15)[48]. R.15/INR.15 require countries to either permit and regulate VAs and VASPs or prohibit and effectively enforce this prohibition. For those countries which regulate VASPs, the revised Standards require countries to regulate and supervise

[48] FATF (2019): *The FATF Standards: FATF Recommendations (Amended in 2019)*.

VASPs which undertake activities relating to exchange, transfer, safekeeping/custody and financial services related to the offer/sale of a VA.

Since the adoption of the revised FATF Standards in 2019, FATF has conducted two reviews on implementation of the revised FATF Standards,[49, 50] published its Report to G20 on So-called Stablecoins[51] and published Updated Guidance for a Risk-Based Approach to VAs and VASPs, which provide further clarifications on how the FATF Standards apply to stablecoins, NFTs and DeFi amongst other issues[52]. Through this work, FATF has seen that many countries and the VASP sector have continued to make progress in implementing the revised FATF Standards on virtual assets and VASPs but implementation is still far from sufficient. In a survey of 128 jurisdiction in April 2021, 58 reported that they had introduced the necessary legislation to implement R.15/IN.15, while the other 70 jurisdictions had not yet implemented R.15/INR.15 into their national law. The FATF has also continued to monitor ongoing challenges in implementation of the FATF Standards, including in relation to the challenges posed by decentralised governance and DeFi, peer-to-peer transactions without an AML/CFT-regulated entity and delays in implementation, particularly in relation to the Travel Rule.[53]

Building on this work, in June 2022, FATF produced a targeted update on implementation of its Standards on VAs and VASPs,[54] which outlines country implementation of R.15/INR.15[55] with a focus on FATF's Travel Rule. The report finds a continued need for many countries to strengthen understanding of the ML/TF risks of the VA and VASP sector and to rapidly implement FATF's R.15/INR.15, including the Travel Rule, to mitigate such risks. In particular, the report finds that jurisdictions have made only limited progress over the last year in implementing the Travel Rule specifically despite available technological solutions.[56] Of the 98 jurisdictions that responded to FATF's March 2022 survey, only 29 jurisdictions have passed relevant Travel Rule laws. A smaller subset, just 11 of these jurisdictions, have started enforcement related to the Travel Rule. This demonstrates an urgent need for jurisdictions to accelerate implementation and enforcement of R.15/INR.15 to mitigate criminal and terrorist misuse of VAs. The report also mentioned challenges in cross-border implementation of the Travel Rule such as in relation to the monitoring and risk mitigation measures involving transaction between VASPs and unhosted wallets; interoperability of Travel Rule technological solutions; *de minimis* transaction thresholds for compliance with the Travel Rule; and data protection rules.

---

49 FATF (2020): *12-Month Review of Revised FATF Standards on Virtual Assets and VASPs*, June.

50 FATF (2021): *Second 12-Month Review of the Revised FATF Standards on Virtual Assets and VASPs*, July.

51 FATF (2020): *FATF Report to G20 on So-called Stablecoins*, June.

52 FATF (2021): *FATF Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (Initially published in 2019 and updated in 2021)*, October.

53 The Travel Rule (Recommendation 16) is a key AML/CFT compliance measure, which mandates that VASPs obtain, hold and exchange information about the originators and beneficiaries of VA transfers

54 FATF (2022): *Targeted Update on Implementation of FATF's Standards on VAs and VASPs*, June.

55 FATF's R.15/INR.15 sets the global AML/CFT Standards for VAs and VASPs by clarifying how the FATF requirements apply in relation to VAs and VASPs.

56 The Report also notes that pre-existing technological solutions have some limitations in interoperability with different solutions and insufficient compliance with nuances of national requirements, which means that the private sector needs to further strengthen interoperability between solutions, and to ensure full compliance with the FATF Standards, to enable global implementation.

More broadly, given the remaining challenges in implementation, FATF will continue to promote implementation of FATF's R.15/INR.15, including the Travel Rule. FATF will also monitor additional market trends for material changes, such as in relation to DeFi and NFTs, by engaging with member countries, multilateral fora including G7 and G20, and the private sector. FATF will conduct an updated review on implementation progress by June 2023 with the intention of publishing the main findings. To mitigate ML/TF risks associated with VAs, FATF calls on all FSB member countries and G20 member countries to accelerate compliance with FATF's R.15/INR.15, as well as the Travel Rule, as a matter of priority.

Glossary[57]

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 attached into 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-assets include, but are not limited to, a crypto-asset that is classified as a payment instrument in a jurisdiction and a crypto-asset that is classified as a security in a jurisdiction.

Crypto-asset ecosystem

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

Crypto-asset intermediary

One kind of crypto-asset service provider that performs intermediation functions on a range of economic functions including depositing, saving, borrowing, lending, trading or investment of crypto-assets.

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.

---

[57] The glossary is for the purposes of this document and does not replace other existing taxonomies

Crypto-asset service providers

Individuals and entities that conduct the provision of crypto-asset services, including crypto-asset intermediaries such as crypto-asset trading/lending platforms and wallet providers, among others.

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

Global stablecoin (GSC)

A stablecoin with a 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.

Project developers

Individuals/entities that develop protocols or other essential building blocks of the technological infrastructure to issue a crypto-asset, launch a distributed ledger or distributed ledger-based application, or function as a crypto-asset service provider.

Smart contract

Code deployed in a distributed ledger technology environment that is self-executing and can be used to automate the performance of agreement between entities. The execution of a smart contract is triggered when that smart contract is "called" by a transaction on the blockchain. If triggered, the smart contract will be executed through the blockchain's network of computers and will produce a change in the blockchain's "state" (for example, ownership of a crypto-asset will transfer between market participants).[58]

[58] There are unresolved questions regarding the legal status and enforceability of smart contracts.

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 crypto-asset service where a user's crypto-assets are kept under custody by a service provider on behalf of the user. The user interacts with the service provider, rather than the blockchain, to manage its 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".