

Financial Services Risk

FSB – High-level recommendations for the regulation, supervision and oversight of Crypto-asset activities and markets



Table of content

| | |
|----|--|
| 01 | Introduction |
| 02 | FSB Recommendations - Synopsis |
| 03 | Impact Assessment - Grant Thornton Bharat Analysis |
| 04 | Conclusion / Way forward |
| 05 | Contributors (Authors) |
| 06 | References |



Introduction

In the backdrop of several concerns expressed by G20 in February 2022, primarily around the regulatory and supervisory challenges posed by crypto-assets, the Financial Stability Board (FSB) published a consultative report on regulation, supervision, and oversight of crypto-asset activities and markets, including a set of high-level recommendations on 11 October 2022. The same was open to public comments until 15 December 2022.

In light of several events that further took place in crypto-asset markets in 2022 and early 2023, such as the bankruptcy of FTX, the third largest cryptocurrency exchange, and the resultant collapse of crypto-focused Silvergate Capital Corp bank, the FSB issued a final report solely containing the high-level recommendations to put in place a standardised regulatory framework that addresses supervisory and oversight issues relating to crypto-assets and aid in fostering a safe environment for innovation. These recommendations aim to develop a comprehensive and consistent regulatory and supervisory framework for crypto-asset activities and markets that is technology-neutral and supplements the existing regulatory, supervisory, and oversight frameworks.

The recent past saw significant volatility in the global cryptocurrency market capitalisation ranging from a peak of around USD 3 trillion in November 2021 before crashing to about USD 1.24 trillion as of July 2023. As per the statistical information available on CoinGecko, globally, 10,017 cryptocurrencies are traded over 778 exchanges.

Pursuant to these events, the European Parliament has also recently approved the Markets in Crypto Assets (MiCA) regulation, the world's first comprehensive set of rules that aims to bring in the largely unregulated cryptocurrency markets under government regulation. This regulation covers crypto assets that are not currently regulated by the existing financial services legislation. Key provisions for those issuing and trading crypto-assets (including asset-reference tokens and e-money tokens) cover transparency, disclosure, authorisation, and supervision of transactions. The new legal framework will support market integrity and financial stability by regulating public offers of crypto-assets and by ensuring that consumers are better informed about their associated risks.

Given the global reach and degree of interconnectedness between the traditional financial system and the crypto-asset activities, mitigating the associated financial stability risks associated with crypto-assets and its service providers is imperative. These high-level recommendations issued by FSB provide a reference point to the G20 countries and economies worldwide to build a regulatory framework benchmarked against globally acceptable standards. These recommendations apply to any type of crypto assets in any jurisdiction, including those conducted through so-called decentralised finance (DeFi) protocols, that pose, or potentially pose, risks to financial stability. However, central bank digital currencies (CBDCs) and crypto-asset activities that meet the definition of a Global Stablecoin (GSC) arrangement are out of scope of these high-level recommendations. While these recommendations solely address the potential financial stability risks associated with crypto-asset and its service providers, while drafting a comprehensive framework, the regulators will also have to factor in all other specific risk categories related to crypto-asset activities.

”

Like other stakeholders, we welcome the guidance of the FSB for the regulation of VDAs, VASPs, and other Web3 players. In particular, we applaud the principles based approach that the FSB has taken, that in general, provides enough flexibility for our still nascent industry to innovate and for individuals to experiment. The one exception to this is treating VASPs and crypto assets as analogous to securities, followed by applying “same risk, same regulation” to VASPs – as the risk profile for VASPs is significantly different, and the kind of infrastructure and institutional support required to enable the kind of regulations the FSB suggests must first be created. While we appreciate the many similarities between the two, we still urge caution on painting crypto assets and securities with the same brush.

—— **Kiran Vivekananda, Chief Public Policy Officer,
CoinDCX**

”

The crypto industry has come a long way in terms of integrating governance in their model. The FSB document principles standardise what some of the players have already been doing.

—— **Vivek Iyer, Partner FS Risk,
Grant Thornton Bharat**

Synopsis

In order to promote a comprehensive and greater international consistency of regulatory and supervisory approaches to crypto-asset activities and markets, including crypto-asset issuers and service providers, the FSB has finalised nine recommendations addressing the risks of financial stability



1 Recommendation 1: Regulatory powers and tools

Each jurisdiction should have an independent or collective set of regulatory bodies empowered to regulate, supervise, and oversee crypto-asset activities and markets.

2 Recommendation 2: General regulatory framework

Based on the vulnerability assessment from a financial stability risk standpoint carried out by authorities for their respective jurisdiction, a comprehensive regulatory framework for effective supervision and oversight of crypto-asset activities and markets, including crypto-asset issuers and service providers, shall be put in place. The FSB recommends that the crypto asset regulatory framework may be benchmarked against any of the existing regulations or internal standards that address financial stability risks from a set of activities similar to those of crypto assets. The regulatory framework should be aimed at providing adequate protection to all relevant parties, including the consumers as well as investors.

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

Considering the fact that crypto assets and their activities have a tendency to breach the regulatory perimeter- easily, the FSB recommended the authorities to have an efficient, timely, and effective information-sharing and communication mechanism, both domestically and internationally, with respect to crypto-asset issuers and service providers that are in financial or operational distress. This would essentially aim to mitigate the risk of spillovers of financial instability into other jurisdictions.



4

Recommendation 4: Governance

The FSB recommends that the regulatory framework put in place by the authorities in each jurisdiction should mandate crypto-asset issuers and service providers to have and disclose a comprehensive and robust governance framework proportional to their risk, size, complexity, systemic importance, and the financial stability risk that they pose. Further, irrespective of the complex nature of activities and technology used to conduct the crypto-asset activities, there should be a clear and direct line of responsibility and accountability for all the functions and activities.

6

Recommendation 6: Data collection, recording, and reporting

The regulatory framework shall require the crypto-asset issuers and service providers to have sound policies, procedures, and infrastructure that will aid in collecting, storing, safeguarding, and timely and accurate data reporting to the regulator. The regulatory framework shall focus on the adequacy of infrastructure and controls put in place by crypto-asset issuers and service providers to ensure integrity, security, quality, privacy, timeliness, and completeness of the data collected, stored, and reported.

5

Recommendation 5: Risk management

It is recommended that the regulatory framework put in place by the authorities in each jurisdiction should mandate crypto-asset issuers and service providers to have an effective risk management framework in place that identifies and adequately addresses all material risks associated with their activities. At the bare minimum, this risk management framework should achieve outcomes like those observed in the traditional financial system. In addition to a risk management framework, the FSB also recommends that:

- The management of crypto-asset issuers and service providers should adhere to the 'fit and proper' standards.
- Adequate resources commensurate to the size and scale of crypto-asset issuers and service providers should be deployed to carry out risk management and other control functions.
- The control functions shall be carried out independently of business activities.
- The compliance function shall identify and address any non-compliance issues and deficiencies and ensure adherence to applicable laws and regulations.
- Conflicts of interest should be adequately identified and disclosed to the relevant stakeholders, and crypto-asset issuers and service providers should strive to prevent any conflict of interests in their activities to the extent possible.
- The Crypto-asset issuers and service providers, proportionate to their risk, size, complexity, and systemic importance to the financial stability, should establish contingency arrangements and business continuity plans.
- Further, they should also put appropriate AML/CFT measures in place per the FATF standards.
- To protect and safeguard the customers' rights of ownership, crypto-asset service providers involved in holding or safeguarding crypto-assets will need to have in place adequate controls in the form of segregation and record-keeping, and should be required to implement transparent operating rules for the trading platform.

7 Recommendation 7: Disclosures

The crypto-asset issuers and service providers should be clear and transparent in their functioning, and hence, should disclose the following key elements to users and relevant stakeholders:



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

The regulatory body should continuously monitor and identify any potential financial stability risks emanating due to the inter-linkages between the crypto-asset ecosystem and the broader financial system and address the same by putting in place a robust regulatory and oversight framework.

9 Recommendation 9: The comprehensive regulation of the crypto-asset service providers with multiple functions

The regulatory framework for crypto assets service providers should not only govern, monitor, and regulate the standalone entities' functions but also the functions undertaken by the groups of affiliated service providers. A common practice that is observed in the crypto space is that the responsibility of several functions is bifurcated within a group's affiliate entities under a common brand name. Thus, the regulator must supervise and address the risks arising from the combination of all affiliates' multiple activities and functions. Further, the regulators would also have to evaluate whether combining multiple functions would result in non-compliance with existing regulations or generate acute conflicts of interest that may not be effectively managed. The regulator would need to apply additional prudential measures appropriate to address the additional risks or conflicts of interest from such combinations. Regulators would further need to implement a mechanism for cross-border and cross-sector information about service providers combining multiple functions and operating across borders and sectors in line with Recommendation 3 stated earlier to minimise the financial distress due to spillover into other jurisdictions and sectors.

Impact assessment – Grant Thornton Bharat LLP analysis

1

Recommendation 1: Regulatory powers and tools

- The collapse of a prominent crypto exchange recently, intrinsic volatility and vulnerabilities of crypto assets and its service providers, coupled with the spurt in market capitalisation of global cryptocurrency trades over the years and the interlinkages of the crypto ecosystem with the wider financial system, has made it quintessential for every country to have a regulatory body and an oversight mechanism to govern the crypto-related assets and their service providers from a financial stability standpoint.

- Governments would now need to set up a dedicated regulatory body to develop a regulatory governance framework within which the crypto assets and their service providers shall operate or delegate this responsibility to the existing regulators governing players of a similar domain. Regulators would need to invest adequately in resources from a technology and people standpoint.

- Further, to promote a culture of sound governance in all the activities carried out by crypto asset service providers, these organisations will need to develop robust policies and procedures aligned with the jurisdiction-specific regulatory framework and have a transparent organisation structure to avoid any regulatory non-compliance.

2

Recommendation 2: General regulatory framework

- Drawing an inference from the principle of **'same activity, same risk, same regulation'**, governments will need to develop a regulatory framework akin to the existing regulations governing activities similar to the ones that crypto asset service providers undertake.
- The governments would need to assess the financial stability risks applicable to the crypto asset market and its service providers and determine whether the existing regulatory, supervisory, and oversight requirements adequately address the financial stability risks of crypto asset activities. Additionally, the regulatory framework will have to spell out those crypto-asset activities that may also fall under the supervisory framework's ambit.

- For instance, in India, the government can leverage the rules and regulations put in place by the Securities and Exchange Board of India (SEBI) for stock exchanges around the listing of shares/securities and develop a regulatory framework for listing tokens on similar grounds, considering the financial stability risks the crypto asset market and its service providers possess.

- Given the degree of interconnectedness and complex technological architecture of various crypto activities, this recommendation aims to build a regulatory and oversight mechanism for the crypto-assets and their service providers to a level that can be already observed in the traditional financial system.
- The ultimate objective is to bring in an acceptable level of transparency and protection for all relevant stakeholders in the various crypto-related activities.



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

- In the traditional financial system, we have already witnessed well-established practices of sharing information at a domestic and global level. The nature of information shared ranges from the information related to payments, Know Your Customer (KYC), fraud and security, AML / CFT to credit-related history and past defaults.
- Through this recommendation, the FSB aims to build a similar platform for exchanging critical information at a global level to potentially capture the spillover of financial stability risks into other jurisdictions.
- These will require governments to enter into information-sharing arrangements to identify what type of critical cross-border or cross-sector information shall be shared, along with the periodicity at which such information is shared. While initially, this would be restricted to respective countries, it would gradually transcend boundaries and lead to cross-jurisdiction treaties / agreements for information sharing.
- Such information-sharing arrangement will need to ensure that data privacy and data security measures are in place to avoid any breach of sensitive data.
- What constitutes critical information from a financial stability risk standpoint must be determined and standardised. Indicative parameters that could potentially play a vital role in identifying financial stability risk could be:

01

Details about the **entities or individuals (ultimate beneficial owners)** behind the issuance of crypto assets, including their **identities, track records, and financial standing**, can help evaluate the credibility and risk associated with the assets.

02

Information about the **crypto assets' features, functionalities / product / service offerings**, such as the **underlying technology, utility, governance mechanisms, and token supply**, can shed light on their potential value and usage.

03

Information pertaining to the **distribution of tokens** among holders can highlight potential risks related to the concentration of ownership.

04

Details about the security protocols and measures adopted by issuers and trading platforms.

05

Information relating to wallet addresses that are on the sanctions list.

4

Recommendation 4: Governance

- Owing to the absence of regulatory requirements, the existing crypto asset issuers and their service providers presently operate with a complex organisation structure with overlapping roles and responsibilities that may potentially have a conflict of interest.
- Crypto-asset issuers and service providers would need to implement a robust governance framework with defined roles and responsibilities and accountability for the functions and activities carried out, irrespective of the complexity of technology or the business model adopted to undertake crypto-asset activities.
- Enhanced documentation, a robust process and control framework, more independent audits, frequent internal reviews, effective and well-established three lines of defence would need to be considered to establish, maintain and monitor a robust governance framework.
- Further, from a regulatory point of view for the Indian jurisdiction, the authorities/regulator may benchmark the 'corporate governance framework' applicable to banks and NBFCs while applying the same for crypto-asset issuers and their service providers proportionate to the risk, size, complexity and systemic importance, and the financial stability risk that they pose.

5

Recommendation 5: Risk management

- The crypto-asset issuers and service providers have to put in place a robust risk management framework similar to the ones observed in traditional financial systems.
 - Commensurate to the size, risk, complexity, systemic importance, and financial stability risk that the crypto-asset issuers and service providers pose, an effective risk management framework that identifies all the material risks associated with their activities and the mitigation plan has to be adopted by the organisation.
 - Consequently, an enterprise-wide risk management policy would need to be developed and disclosed by the crypto-asset issuers and service providers. Material risks will have to be identified, measured, evaluated, reported, and controlled in the normal scenario and stress conditions. The FSB has tried to blend in the flavour of the stress testing framework as observed in the traditional financial system.
 - Further, in line with the widely accepted risk management model of three lines of defense in the traditional financial system, the crypto-asset issuers and service providers would be required to segregate and ensure that control functions are carried out independently of business operations. The onus of adherence to applicable laws and regulations and reporting of outlier events lies in the compliance function of crypto-asset issuers and service providers.
- Similar to a recent regulation to this effect in India (applicability of the PMLA to virtual digital asset service providers), the crypto-asset issuers and service providers would now have to adhere to AML/CFT norms in accordance with the FATF standards, and thus, will have to implement a mechanism for continuous transaction monitoring. An effective business continuity plan and effective contingency arrangements for crypto-asset issuers and service providers would act as a key control to address the threats that could disrupt the functioning of the business, which could have a cascading effect on other affiliated players in the economy.
- Further, in line with Recommendation 7 on disclosure, the crypto-asset service providers, which act as custodians on behalf of customers, will need to define, document, and implement robust controls to safeguard the crypto-assets, protect duly, and disclose the customer ownership rights.

6 Recommendation 6: Data collection, recording and reporting

- The crypto-asset issuers and their service providers collect data from several stakeholders in the course of their operations. However, owing to absence of a standardised framework for data management and security, there have been several instances of data security breaches. As per the 'Crypto & DeFi Hacks & Scams Report', as of March 2023, USD 4.5+ billion has been stolen through security breaches since 2011. The FSB recommendations now require the crypto-issuers and their service providers to 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 regulations, including on data retention, data security, and data privacy.
- Further, to enable the ongoing monitoring of crypto-asset activities, they will need to define specific data points and the periodicity for which the regulator shall collect such data. Similar to the approach adopted in the traditional financial system, the crypto-asset issuers and their service providers would now be subject to regulatory reporting and will have to put in place adequate controls to ensure the accuracy, completeness, timeliness, and reliability of the data being submitted.
- The entities would need to invest in data management software or build functionalities in their existing ERP tools to collect, store, process, safeguard and report data accurately. The effectiveness of controls implemented around these functionalities will be important to ensure that reliance can be placed on such data sets extracted for various purposes.
- The regulatory watchdog would now keep a constant eye on the varied crypto asset-based activities to mitigate any potential risks from a financial stability standpoint by obtaining periodic returns of key transactions processed, new tokens listed, audit issues identified, and gaps noted as a part of the internal and external monitoring mechanism implemented.



7 Recommendation 4: Disclosures

- The crypto-asset issuers and their service providers operate in an unregulated space, so the nature and type of information they disclose is the bare minimum and only to very few stakeholders.
- The premise of this recommendation is that the crypto-asset issuers and their service providers will need to be transparent in their functioning and must disclose certain key elements comprehensively and clearly.
- Disclosure with respect to governance framework, operations, risk profiles, financial conditions, and the products they provide and activities they conduct will need to be given and made available to relevant stakeholders, including customers, investors, or shareholders. These elements will be disclosed separately, i.e., through their user agreements/ terms of use or financial statements.
- Further, the crypto-asset issuers and their service providers would need to disclose information on their websites related to the product structure and the operation of their activities.
- Given that the crypto service providers also act as custodians for the users, they are now required to clearly state their terms and conditions of the custodial relationship, the risks that the client could face if the custodian were to enter bankruptcy and the ownership rights of the customers. Such terms and conditions should be made available on their websites/applications, and explicit prior consent of the customer will be a pre-requisite.
- In continuation to the implementation of Recommendation 5 on 'risk management', crypto-asset issuers and their service providers will also be required to disclose material risks associated with their products, technologies and based on the requirements of the jurisdictional laws and regulations, applicable environmental and climate risks and their impact will also need to be disclosed. All the above disclosures would instill a sense of trust and transparency in the operations carried out by crypto-asset issuers and their service providers.

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

- The regulatory framework, on an ongoing basis, would need to identify and evaluate the degree of interconnections within the crypto-asset ecosystem and between the crypto-asset ecosystem and the wider financial system.
- A higher degree of interconnectedness would potentially mean a higher probability of financial stability risk being spilled over from one ecosystem to the other. Thus, this would necessitate closer supervision and oversight over such entities.
- This is in line with the risk-based supervision mechanism adopted for banks, wherein a higher degree of supervision in the form of onsite visits and monitoring is required for banks, subject to a higher degree of risk. A significant amount of specific data is collected across tranches for offsite monitoring, whereby interconnections from financial stability standpoint are evaluated.
- In the Indian context, traditional financial institutions do not offer any other products to crypto exchanges except for payment-related services. However, as and when the crypto markets will evolve in India, the traditional credit-related products may also be on the platter for the crypto players, and hence, in such a scenario, there would be a higher degree of financial stability risk to the wider economy. Such a scenario will entail close supervision and continuous monitoring by regulators of both ecosystems.

9

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

- It is a common practice within the crypto space wherein multiple entities under a common brand name provide and offer their customers various sets of products and services. While the website/application ownership on which the customers register and are onboarded lies with one entity, the various products and services on offer are ultimately owned by several entities within the group that operate under a brand name.
- To address such issues, the FSB recommends that the regulatory framework will be applicable to the crypto-asset service providers and their affiliates that combine multiple functions and activities, thereby resulting in comprehensive supervision and oversight of all affiliated entities to address the risks associated with all the functions as a whole.
- The crypto-asset service provider or group of affiliated service providers must have defined policies and procedures in place to identify, mitigate and manage conflicts of interest and prevent abuse from concentrated control, management, and transparency of related party transactions.
- Further, wherever the regulator is of the opinion that a combination of multiple functions results in non-compliance with the regulations or has the potential to generate conflicts of interest, in such cases, the regulator shall apply regulatory measures to separate a specific set of functions.
- Additionally, implementing Recommendation 3 on cross-border and cross-sector information sharing becomes all the more critical in cases wherein the affiliate service providers operate in different jurisdictions/sectors.



Conclusion

The recommendations issued by the FSB is yet another step in the right direction to regulate and bring crypto-asset issuers and service providers under the ambit of regulatory supervision. While these recommendations are not legally binding, they form a benchmark based on which the G20 countries and other economies can build a regulatory framework that addresses financial stability risk and is based on international standards. While each jurisdiction will build a regulatory framework depending on the degree of interconnectedness of the crypto-asset ecosystem and the traditional financial system, the FSB shall continue to coordinate international regulatory and supervisory approaches for crypto-asset activities to ensure consistency and comprehensiveness at a global level. The FSB will also act as a watchdog to review the implementation of recommendations and will highlight outlier jurisdictions in the process.

Glossary

| | |
|-------|--|
| FSB | Financial Stability Board |
| FTX | Futures Exchange |
| MiCA | Markets in Crypto Assets |
| DeFi | Decentralized Finance |
| CBDCs | Central Bank Digital Currencies |
| GSC | Global Stablecoin |
| AML | Anti-Money Laundering |
| CFT | Combating the Financing of Terrorism |
| FATF | Financial Action Task Force |
| SEBI | Securities and Exchange Board of India |
| KYC | Know Your Customer |
| PMLA | Prevention of Money Laundering Act |
| RBS | Risk-Based Supervision |

References

- High-level Recommendations for the Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets - Final Report issued by the Financial Stability Board dated 17th July 2023
- Crypto & DeFi Hacks & Scams Report - March 2023
- Grant Thornton Bharat LLP Analysis

Contributors from the Financial Services – Risk Advisory team



Vivek Ramji Iyer

Partner and National Leader – Financial Services Risk Advisory
E : Vivek.Iyer@in.gt.com



Vernon Dcosta

Partner – Financial Services Risk Advisory
E : Vernon.Dcosta@in.gt.com



Dharmesh Jadav

Director – Financial Services Risk Advisory
E : Dharmesh.Jadav@in.gt.com



Viraj Parikh

Manager – Financial Services Risk Advisory
E : Viraj.Parikh@in.gt.com



Pranav Panchal

Manager – Financial Services Risk Advisory
E : Pranav.Panchal@in.gt.com

Notes

Notes

Notes

We are Shaping Vibrant Bharat

A member of Grant Thornton International Ltd, Grant Thornton Bharat is at the forefront of helping reshape the values in the profession. We are helping shape various industry ecosystems through our work across Assurance, Tax, Risk, Transactions, Technology and Consulting, and are going beyond to shape a more #VibrantBharat.



Our offices in India

- Ahmedabad ● Bengaluru ● Chandigarh ● Chennai
- Dehradun ● Delhi ● Gurgaon ● Hyderabad ● Kochi
- Kolkata ● Mumbai ● Noida ● Pune



Scan QR code to see
our office addresses
www.grantthornton.in

Connect with us on



@Grant-Thornton-Bharat-LLP



@GrantThorntonBharat



@GrantThornton_Bharat



@GrantThorntonIN



@GrantThorntonBharatLLP



GTBharat@in.gt.com

© 2023 Grant Thornton Bharat LLP. All rights reserved.

"Grant Thornton Bharat" means Grant Thornton Advisory Private Limited, the sole member firm of Grant Thornton International Limited (UK) in India, and those legal entities which are its related parties as defined by the Companies Act, 2013, including Grant Thornton Bharat LLP.

Grant Thornton Bharat LLP, formerly Grant Thornton India LLP, is registered with limited liability with identity number AAA-7677 and has its registered office at L-41 Connaught Circus, New Delhi, 110001.

References to Grant Thornton are to Grant Thornton International Ltd. (Grant Thornton International) or its member firms. Grant Thornton International and the member firms are not a worldwide partnership. Services are delivered independently by the member firms.