EXECUTIVE BOARD MEETING

SM/23/4
Correction 1

February 8, 2023

To: Members of the Executive Board

From: The Secretary

Subject: **Elements of Effective Policies for Crypto Assets**

Board Action:	The attached corrections to SM/23/4 (1/5/23) have been provided by the staff:
Factual Errors Not Affecting the Presentation of Staff's Analysis or Views:	**Pages 4 ("References 40"), 15, 23, 24, 25, 40, 41**
Typographical Errors	**Page 4 (Annexes)**
Questions:	Mr. Ismail, MCM (ext. 35331)

26. Crypto asset platforms with an open architecture could be subject to significant cyber risks as they allow anyone to create malicious protocols or protocols with bugs (errors). Anyone can create open DLT applications in an unregulated manner.[27] Even when the code is publicly available, its complexity means that many applications with bugs become widely used before the bug is discovered. Users have financial incentives to take advantage of bugs at the expense of others rather than report them. Accessing crypto assets through self-custody wallets creates the additional risk of password loss. By their nature, combined with a lack of regulation, recourse is not possible.[28]

Financial Integrity

27. Due to their pseudonymous nature, crypto assets can be attractive to criminals, raising financial integrity risks. Although in most DLT networks transactions are public and therefore visible, linking an address or wallet to an individual can be challenging. While the value of crypto assets involved in most criminal cases detected so far has been relatively small compared to those using traditional financial products and services, some known cases of misuse involve relatively large amounts (FATF 2021). Crypto assets can be misused to commit a range of crimes (e.g., fraud, theft, tax evasion, and terrorist financing) and launder the proceeds of these or other crimes (e.g., corruption). Alnasaa et al. (2022) find that crypto asset usage is significantly and positively associated with higher perceptions of corruption.

Legal Risks

28. The legal classification of crypto assets and the application of existing rules to them pose significant challenges, leading to uncertainty and potential legal risks. In particular, uncertainties in the application of private laws (e.g., insolvency law) could result in the parties to a crypto asset arrangement facing different risks than those envisaged at the time of the transaction.[29] For example, holders of ~~securities~~ crypto assets could face the risk of having their rights recharacterized as unsecured personal claims instead of proprietary rights in the event of the insolvency of an intermediary. This could give rise to financial instability if it occurs on a large scale. If not clearly included in existing financial law classifications, a crypto asset may fall entirely or partially outside the regulatory framework, leading to regulatory arbitrage or inadequate handling of financial stability risks. These uncertainties may also expose the private sector to the risk of unpredictable supervisory actions, curbing financial innovation, while exposing the regulatory authorities to the risk of successful legal challenges due to a broad interpretation of their mandates. Finally, legal risks, including conflict of law challenges, are heightened in cross-border transactions due to differences in legal classification and treatment of crypto assets across jurisdictions.

[27] As with any new technology, operational resilience is an area of concern. DLT is a general purpose technology. Its adoption relies heavily on third-party providers. The lack of consensus on common standards is still prevalent and there is no generally adopted framework for performing quality assurance on core algorithms and code.

[28] For example, one estimate puts the share of Bitcoin lost in wallets at 17-23 percent of all mined Bitcoin, and individual investor losses worth hundreds of millions of U.S. dollars have also been documented.

[29] These risks are even more evident in fragile states with high levels of corruption and weak rule of law, where institutions often lack the capacity to properly enforce and protect contractual and property rights.

responsible authorities clearly designated, and coordination mechanisms among them well defined.[45]

48. Where global standards exist and can be mapped onto crypto assets, authorities should implement these standards into domestic regulation. Currently, global standards ~~are limited to~~have focused on either sectors (banking), issues (financial integrity), or specific products (global stablecoins) and there is an absence of cross-sectoral standards. Annex 2 provides a snapshot of the progress on the development of standards. Where standards exist—for example, the FATF standards on AML/CFT, and the International Organization of Securities Commissions' (IOSCO) guidance on exchanges—these should be implemented. Standards should encompass both the safety of the underlying assets as well as the network that facilitates the transfer of the assets. Guidance may be drawn from CPMI and IOSCO's Principles for Financial Market Infrastructures (PFMI) to address issues related to transfer, governance, and risk management of the infrastructure and networks, or those related to the safe settlement of assets.

Box 3. The Rationale for Comprehensive Regulations

Comprehensive regulations are preferred to blanket bans. Comprehensive regulations should address the specific features of crypto assets that generate externalities, such as those that enable high degrees of anonymity (which could facilitate illicit transactions) or lead to environmental burden (for example, when proof-of-work consensus mechanisms are used). Additionally, regulation, as it relates to consumer protection, is needed to address internalities—cases where consumers do not fully take into account the costs of using or holding crypto assets (e.g., volatility in value, possible losses due to cyber-attacks).[1] Issuing warnings and increasing the availability of information can also be helpful, but it might not be sufficient to address externalities and internalities. Moreover, it can provide legitimacy to the market, facilitating closer links with wider financial services that could generate systemic risks without adequately addressing them.

Blanket bans that make all crypto asset activities (e.g., trading and mining) illegal may stifle innovation and drive illicit activities underground. The crypto ecosystem is undergoing rapid change. There is much uncertainty about the extent to which this change will ultimately materialize as productive innovation. Allowing the system to develop (with proper regulation) will allow policy makers to learn about these potential benefits and better mitigate risks (including financial integrity risks), while bans may inadvertently increase the risk exposure.

Bans can be costly to enforce and increase the incentives for circumvention due to the inherent borderless nature of crypto assets, resulting in potentially heightened financial integrity risks, and can also create inefficiencies. A decision to ban should be informed by an assessment of money laundering and terrorist financing (ML/TF) risks, and other considerations, such as large capital outflows and other public policy aims. Regulations imply that certain forms of crypto assets will still be available in the legal marketplace, and thus the degree of substitutability of illegal versus legal assets is likely to be much larger relative to blanket bans of crypto assets.

When substitute assets are not widely available in legal markets, users may be more motivated to access illegal markets and willing to pay higher prices for these assets, due to the stronger incentives to obtain them. A higher willingness to pay for illegal assets increases the profits to those providing such assets, thus raising the incentives for circumvention. Higher incentives for circumvention imply higher enforcement costs. Moreover, as incentives to circumvent bans are stronger, private sector actors devote more resources to circumvention—an activity that does not produce any socially valuable good or service—and therefore efficiency is negatively affected.

[45] Depending on the domestic legal framework, the type of regulation involved, and the nature of the "product" (such as unbacked tokens or stablecoins), the relevant authorities could include banking regulators, payment system regulators, securities regulators, financial intelligence center authorities, or tax authorities.

Box 3. The Rationale for Comprehensive Regulations (concluded)

Crypto assets that escape bans may generate additional negative externalities (e.g., more crypto asset activity may become linked to the dark web). Moreover, once crypto assets migrate to illegal markets, the ability of targeted regulation to shape their characteristics and guide the types of innovation that occur is lost. Innovation is path dependent, and thus regulations that affect current features can have important long-run effects.

Targeted restriction could be justified to manage specific risks. Where countries experience large capital outflows, significant currency substitution, an unacceptable level of ML/TF risk, and/or risks to consumers and markets, targeted restrictions might be useful. These restrictions might be targeted to certain products (e.g., privacy tokens), activities (e.g., payments in Ukraine), financial promotions (e.g., in Singapore, Spain, U.K.), or products (e.g., crypto derivatives in Japan and the U.K.). Additionally, broader bans could be considered but only over a shorter time horizon. Also, targeted restrictions might be warranted in the short run while countries increase internal capacity (including knowledge and awareness) in anticipation of regulation.

Even when a temporary imposition of restrictions is contemplated, such restrictions should be considered as part of a larger policy framework. Restrictions should not substitute for robust macroeconomic policies and credible institutional frameworks, which are the first line of defense against the macroeconomic and financial risks posed by crypto assets.

_____

[1] Internalities are the costs, often long-term, that an individual may incur as a result of their actions, which are not taken into account by the individual when deciding to take those actions (Reimer and Houmanfar 2017).

49. Conduct requirements should focus on points that are likely to have a direct impact on end users. This is particularly important for key entities, such as exchanges and wallet providers, issuers (where known), governance bodies (where applicable), and regulated financial institutions that participate in crypto asset markets. For example, the administration of wallets must be secure and have clear risk management frameworks. Safekeeping and segregating funds legally and operationally, as well as safeguarding them through, for example, private insurance against cyber risks and other threats, can support consumer protection in stressed market periods. Effective wind-down frameworks where a wallet fails can help manage risks to end users. Exchanges might be required to consider suitability requirements for users, while user education is also an important short-term tool for regulators to protect consumers. Authorities should consider what market abuse rules and surveillance mechanisms should be in place to adequately protect users.

50. Appropriate disclosure and transparency requirements are key. Marketing information should be clear, balanced, and indicate if products are regulated in the local market. White papers form an important part of the disclosure process. They should provide markets and users with clear, accurate, and understandable explanations of the crypto assets issued and other essential information such as key personnel (the importance of which surfaced in the case of FTX and its Alameda Research affiliate). Entities should be transparent about the activities they are carrying out, as well as key operational functions that might impact markets and consumers. In many cases, third party audits can ensure that disclosure is accurate. Regulations should grant the power to establish the scope of external audits and the standards to be followed in performing such audits.

51. When crypto asset service providers provide several core functions, authorities should regulate them based on the risks generated by the entity as a whole and across all of its activities. Conflicts of interest should be addressed where entities carry out several activities within a single group. Additional prudential, conduct, and payment system regulations should reflect the

nature of all risks. Depending on the scope of the activities provided, a regulator or supervisor may establish requirements for crypto asset service providers offering infrastructure-like services such as clearing and settlement. For example, FTX had close financial interlinkages with its affiliates and offered a wide range of services, resulting in conflicts of interest. For further discussion of the FTX case see Annex 3.

52. If designated as systemic, crypto asset service providers should be subject to additional oversight requirements and adhere to the PFMI when they perform payment functions. Designation of a crypto service provider as systemic is at the discretion of authorities whenever certain criteria are met. For financial market infrastructures (FMIs), the key factor is the potential of an FMI to trigger systemic disruptions.[46] For stablecoin arrangements, for example, systemic importance can be determined by domestic regulators based on such factors as size of the stablecoin arrangement (in terms of number of users and value/volume of transactions), nature and risk profile of the stablecoin arrangements' activity, interconnectedness and interdependencies with the real economy and financial system, and availability of alternatives to using the stablecoin arrangement as a means of payment or settlement for time-critical services.[47] The process of identification and designation of crypto service providers as systemically important can be complex, as factors should be viewed holistically by domestic regulators.

53. Authorities should address risks from outsourcing to third parties, including operational failures and cyber incidents. Many authorities require that wallet providers ensure a robust cybersecurity framework to keep custodied crypto assets safe. It is important that key entities that provide core functions have effective incident management procedures in place, including the ability to detect and classify major operational and security incidents. Reporting operational or cyber incidents needs to be timely and accurate to ensure market integrity. Where cyber or operational processes are delegated to third parties, the wallet provider should be responsible for the incidents that occur in the third parties, with clear outsourcing requirements in place. The BCBS Principles on Operational Resilience could usefully be applied to key crypto asset service providers, particularly exchanges and wallets. For stablecoin arrangements that are identified as a systemically important FMI, published guidance on cyber resilience for FMIs needs to be applied.[48]

54. Requirements for stablecoins should be tailored to address risk across the entire ecosystem. This includes, (i) issuance, redemption, and stabilizing mechanisms; (ii) the transfer function; and (iii) access. Depending on the extent and interconnectedness of arrangements, key components of the regulatory framework should be focused on stablecoins' reserve assets to address credit, market, operational, liquidity, concentration risks, and the rights of stablecoin users

[46] More specifically, the PFMI specify that ~~an FMI~~ a payment system could be determined as systemic if it is the sole payment system in a country (or the principal system in terms of the aggregate value of payments); a system that mainly handles time-critical, high-value payments; and a system that settles payments used to effect settlement in other systemically important FMIs.

[47] See guidance on the Application of the Principles for Financial Market Infrastructures to Stablecoin Arrangements (section 2), issued jointly by IOSCO and the Bank for International Settlements' Committee of Payments and Market Infrastructures.

[48] See guidance on Cyber Resilience for Financial Market Infrastructures, issued jointly by IOSCO and the Bank for International Settlements' Committee of Payments and Market Infrastructures.

References

Adrian, T., C. J. Erceg, S. T. Gray, and R. Sahay. 2021. "Asset Purchases and Direct Financing: Guiding Principles for Emerging Markets and Developing Economies during COVID-19 and Beyond." Departmental Paper 2021/023, International Monetary Fund, Washington, DC. [Link]

Adrian, T., F. Grinberg, T. Mancini-Griffoli, R. M. Townsend, and N. Zhang. 2022 "A Multi-Currency Exchange and Contracting Platform." IMF Working Paper 22/217, International Monetary Fund, Washington, DC. [Link]

Agur, I., J. Deodoro, X. Lavayssière, S. Martinez Peria, D. Sandri, H. Tourpe, and G. Villegas Bauer. 2022. "Digital Currencies and Energy Consumption." Fintech Note 2022/006, International Monetary Fund, Washington, DC. [Link]

Akhtaruzzaman, M., A. Sensoy, and S. Corbet. 2020. "The Influence of Bitcoin on Portfolio Diversification and Design." *Finance Research Letters* 37 (November): 101344. [Link]

Allen, J. and others. 2020. "Legal and Regulatory Considerations for Digital Assets." University of Cambridge. [Link]

Alnasaa, M., N. Gueorguiev, J. Honda, E. Imamoglu, P. Mauro, K. Primus, and D. L. Rozhkov. 2022. "Crypto, Corruption, and Capital Controls: Cross-Country Correlations." IMF Working Paper 2022/060, International Monetary Fund, Washington, DC. [Link]

Alvarez, F., D. Argente, and D. Van Patten. 2022. "Are Cryptocurrencies Currencies? Bitcoin as Legal Tender in El Salvador." NBER Work Paper 29968, National Bureau of Economic Research, Cambridge, MA. [Link]

Aramonte, S., W. Huang, and A. Schrimpf. 2021. "DeFi Risks and the Decentralisation Illusion." *BIS Quarterly Review* (December): 21-36. [Link]

Bains, P. 2022. "Blockchain Consensus Mechanisms: A Primer for Supervisors." Fintech Note 2022/003, International Monetary Fund, Washington, DC. [Link]

Bains, P., A. Ismail, F. Melo, and N. Sugimoto. 2022a. "Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Assets." Fintech Note 2022/007, International Monetary Fund, Washington, DC. [Link]

Bains, P., A. Ismail, F. Melo, and N. Sugimoto. 2022b. "Regulating the Crypto Ecosystem: The Case of Stablecoins and Arrangements." Fintech Note 2022/008, International Monetary Fund, Washington, DC. [Link]

Beck, T., M. Janfils, and K. R. Kpodar. 2022. "What Explains Remittance Fees? Panel Evidence." IMF Working Paper 2022/063, International Monetary Fund, Washington, DC. [Link]

BIS (Bank for International Settlements). 2022. "The Future Monetary System." Chapter 3, Annual Economic Report, Bank for International Settlements, Basel, Switzerland. [Link]

Blandin, A. and others. 2019. "Global Cryptoasset Regulatory Landscape Study." University of Cambridge and Nomura Research Institute. [Link].

Bossu, W., M. Itatani, C. Margulis, A. D. P. Rossi, H. Weenink, and A. Yoshinaga. 2020. "Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations." IMF Working Paper 2020/254, International Monetary Fund, Washington, DC. [Link]

Chainalysis. 2022. "The Chainalysis 2022 Geography of Cryptocurrency Report: Everything You Need to Know About Crypto Adoption around the Globe." Chainalysis, New York, NY. [Link]

Carare, A., L. Franco, M. Hadzi-Vaskov, J. Lesniak, D. Vasilyev, and Y. Yakhshilikov. 2022. "Digital Money and Remittances Costs in Central America, Panama, and the Dominican Republic." IMF Working Paper 22/238, International Monetary Fund, Washington, DC. [Link]

DeVries, A., and C. Stoll. 2021. "Bitcoin's Growing E-waste Problem." *Resources, Conservation, and Recycling* 175 (December): 105901. [Link]

FATF (Financial Action Task Force). 2021. "Second 12-Month Review of Revised FATF Standards—Virtual Assts and VASPs." Financial Action Task Force, Paris. [Link]

FSB (Financial Stability Board). 2018. "Crypto-asset Markets: Potential Channels for Future Financial Stability Implications." Financial Stability Board, Basel, Switzerland. [Link]

FSB (Financial Stability Board). 2020. "Enhancing Cross-border Payments: Stage 3 Roadmap." Financial Stability Board, Basel, Switzerland. [Link]

FSB (Financial Stability Board). 2022. "Assessment of Risks to Financial Stability from Crypto-assets." Financial Stability Board, Basel, Switzerland. [Link]

Garrido, J. 2023 (upcoming). "Digital Tokens: A Legal Perspective." International Monetary Fund, Washington, DC.

Garrido, J. M., Y. Liu, J. Sommer, and J. S. Viancha. 2022. "Keeping Pace with Change: Fintech and the Evolution of Commercial Law." Fintech Note 2022/001, International Monetary Fund, Washington, DC. [Link]

Goldstein, A. 2021. "Stablecoins: How Do They Work, How Are They Used, and What Are Their Risks?" Written Testimony of Director of Financial Policy, Open Markets Institute before the Committee on Banking, Housing, and Urban Affairs, United States Senate, December 14. [Link]

Guesmi, K., S. Saadi, I. Abid, and Z. Ftiti. 2019. "Portfolio diversification with virtual currency: evidence from Bitcoin." *International Review of Financial Analysis* 63 (May): 431-437. [Link]

He, D., A. Kokenyne, X. Lavayssière, I. Lukonga, N. Schwarz, N. Sugimoto, and J. Verrier. 2022. "Capital Flow Management Measures in the Digital Age: Challenges of Crypto Assets." Fintech Note 2022/005, International Monetary Fund, Washington, DC. [Link]

IMF (International Monetary Fund). 2015. "Monetary Policy and Financial Stability." Staff Report, International Monetary Fund, Washington, DC. [Link]

IMF (International Monetary Fund). 2018. "The Bali Fintech Agenda: A Blueprint for Successfully Harnessing." IMF Policy Paper, International Monetary Fund, Washington, DC. [Link]

IMF (International Monetary Fund). 2019. "The Fiscal Transparency Code." International Monetary Fund, Washington, DC. [Link]

IMF (International Monetary Fund). 2020. "Digital Money Across Borders: Macro-Financial Implications." Staff Report, International Monetary Fund, Washington, DC. [Link]