EXECUTIVE BOARD MEETING

SM/23/4
Correction 3

February 17, 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) and SM/23/4, Cor. 2 (2/14/23) have been provided by the staff:
Evident Ambiguity	**Pages 22 and 25**
Factual Errors Not Affecting the Presentation of Staff's Analysis or Views	**Page 23**
Questions:	Mr. Ismail, MCM (ext. 35331)

- **Clarify financial law treatment of crypto assets.** This can be achieved in a variety of ways (Blandin et al. 2018). Existing legal and regulatory frameworks can be enforced where activities involving crypto assets fall within the established legal categories (e.g., when a stablecoin arrangement fits into the description of e-money). Another way is to amend existing laws to explicitly cover certain activities related to these assets for specific purposes (e.g., Japan).[42] A third route is for jurisdictions to issue bespoke laws on crypto assets (e.g., the EU's MiCA), or set up a distinct legal framework applied to a set of (typically Fintech) activities of which crypto asset activities are a subset (e.g., Malta, Mexico).[43]

- **Mitigate the tax risk from transactions involving crypto assets**. This requires a transparent and predictable tax law framework, complemented by international cooperation. While tax laws generally apply to crypto assets based on their general legal characterization, tax laws may need to be further adjusted to provide clarity and certainty, and to achieve a country's specific policy objectives.[44] However, the complex and constantly evolving nature of crypto assets requires tax administrations to complement existing tax law frameworks with timely and comprehensive guidance to taxpayers to ensure transparency and predictability of treatment. In addition to clarifying substantive tax obligations, countries should also provide clarity on payment and reporting obligations, including by crypto asset service providers.

E. Element 5: Develop and Enforce Prudential, Conduct, and Oversight Requirements to All Actors

46. This element builds on the premise that comprehensive regulation is preferable to outright bans. For a discussion of the pros and cons of bans versus regulations and targeted restrictions see Box 3.

47. Crypto asset service providers ~~that deliver critical functions~~ should be licensed, registered, or authorized. Entities that provide functions such as storage, transfer, exchange, and custody of reserves and assets should be subject to rules similar to those applied to financial service providers, with additional requirements to reflect their new business models (such as combined exchanges and wallets). Licensing and authorization criteria should be clearly articulated, the

[42] For a summary of the legislative amendments made in Japan's Payment Services Act and other relevant laws to promote financial innovation and to ensure user protection, see Annex IV of the Review of the FSB High-level Recommendations of the Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements: Consultative report.

[43] See Malta's Virtual Financial Assets Act and Mexico's Law to Regulate Financial Technology Institutions.

[44] For instance, where a country's policy objective is to encourage the use of a crypto asset as a means of payment, it will need to consider its tax treatment compared to other potential investment assets. El Salvador, for instance, exempts transactions involving Bitcoin from capital gains tax (Annex 4). A more balanced approach is included in a bill introduced in the U.S. Senate in June 2022 titled the "Responsible Financial Innovation Act." To promote the use of virtual currency in retail transactions, the bill proposes a "de minimis" tax exemption of up to $200 in gains realized from using virtual currency in personal transactions for the purchase of goods or services.

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 have focused on either sectors (banking), issues (financial integrity), or specific products (global stablecoins). International work to establish comprehensive recommendations for crypto assets is being taken forward by the Financial Stability Board (FSB) and international standard setting bodies (SSBs).[46] 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.

[46] In October 2022, the FSB published ~~a~~ proposed frameworks for the international regulation of crypto-asset activities. Further, the BCBS, CPMI and IOSCO, and FATF have provided guidance on the application of existing and new standards to crypto-assets.

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.[47] 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.[48] 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.[49]

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 and capital to address credit, market, operational, liquidity, concentration risks, and the rights of stablecoin users over such reserve assets. In addition, the regulatory framework can take cues from

[47] More specifically, the PFMI specify that 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.

[48] 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.

[49] 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.