EXECUTIVE BOARD MEETING

SM/23/4

January 5, 2023

To: Members of the Executive Board

From: The Secretary

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

Board Action:	Executive Directors' **consideration** (Formal)
Tentative Board Date:	**Wednesday, February 1, 2023**
Issues for Discussion:	Page 33–34
Conclusions:	Page 33
Publication:	Proposed, together with a press release
Questions:	Mr. Ismail, MCM (ext. 35331) Mr. Mancini Griffoli, MCM (ext. 36273)

INTERNATIONAL MONETARY FUND

ELEMENTS OF EFFECTIVE POLICIES FOR CRYPTO ASSETS

January 4, 2023

EXECUTIVE SUMMARY

Crypto assets have existed for more than a decade, but efforts to put in place effective public policies toward them have moved to the top of the global policy agenda only recently. This is partly because crypto assets, after years of being niche products, are now being held and in some instances used more widely. The growth in their market capitalization has been volatile, and their interconnectedness with the financial sector has increased. Amid the decline in crypto asset valuations, the failure of various exchanges (such as FTX) and other actors within the crypto ecosystem, as well as the collapse of certain crypto assets (like Terra USD), have intensified the need for effective policies toward these assets.

This paper aims to address questions by Fund members on how to respond to the rise of crypto assets and the associated risks. To frame the discussion, the paper defines and classifies crypto assets based on their underlying features and describes their purported benefits and potential risks. The paper presents a policy framework for crypto assets that aims to achieve key policy objectives such as macroeconomic stability, financial stability, consumer protection, and market and financial integrity. The framework outlines key elements that are necessary to ensure that these objectives are met. However, such a framework will not fix any underlying crypto design flaws (for instance, the lack of a credible nominal anchor, payments finality, or scalability).

Purported benefits of crypto assets include cheaper and faster cross-border payments, increased financial inclusion, and greater portfolio diversification. Greater operational resilience, and increased transparency and traceability of transactions, are also often presented as benefits. However, a careful consideration of these purported benefits suggests that many have not yet materialized, although the underlying technological innovations could prove useful in the longer term.

There are many risks associated with crypto assets, although the significance and relevance of specific risks differ by country circumstances. These include macroeconomic risks, which encompass risks to the effectiveness of monetary policy, capital flow volatility, and fiscal risks. There are also serious concerns about financial stability, financial integrity, legal risks, consumer protection and market integrity, and contestability. Some risks are inherent to the technology underpinning crypto assets, while others stem from the lack of policies or their enforcement. Enforcement could be

particularly challenging as many crypto asset service providers are located in offshore jurisdictions but market their services globally.

To address the risks of crypto assets, and harness benefits from underpinning innovative technologies, this paper puts forward nine core elements of an effective policy framework:

1. Safeguard monetary sovereignty and stability by strengthening monetary policy frameworks and do not grant crypto assets official currency or legal tender status.
2. Guard against excessive capital flow volatility and maintain effectiveness of capital flow management measures.
3. Analyze and disclose fiscal risks and adopt unambiguous tax treatment of crypto assets.
4. Establish legal certainty of crypto assets and address legal risks.
5. Develop and enforce prudential, conduct, and oversight requirements to all crypto market actors.
6. Establish a joint monitoring framework across different domestic agencies and authorities.
7. Establish international collaborative arrangements to enhance supervision and enforcement of crypto asset regulations.
8. Monitor the impact of crypto assets on the stability of the international monetary system.
9. Strengthen global cooperation to develop digital infrastructures and alternative solutions for cross-border payments and finance.

These elements can help inform a comprehensive, consistent, and coordinated framework for crypto assets. However, it is important to note that individual countries will face different circumstances and capacity constraints that may influence the sequence in which these elements are implemented. Doing nothing is untenable as crypto assets may continue to grow in popularity despite the current downturn. By adopting this framework, policy makers can effectively mitigate the risks posed by these assets while also harnessing the potential benefits of technological innovation.

Approved by
Tobias Adrian, Vitor Gaspar, Pierre-Olivier Gourinchas, Ceyla Pazarbasioglu, and Rhoda Weeks-Brown

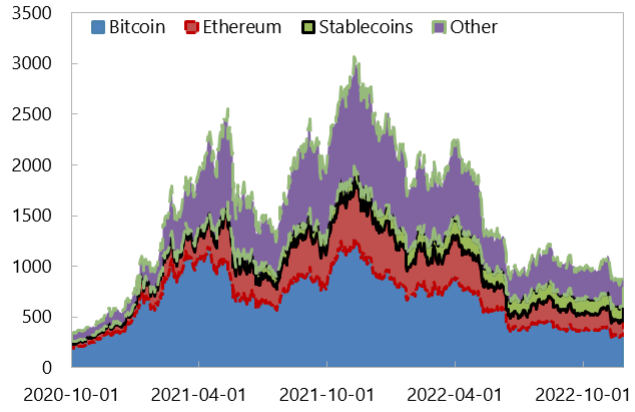
Prepared by an inter-departmental team led by Arif Ismail (MCM), comprising Gerardo Una (FAD); Marianne Bechara, Wouter Bossu, Carine Chartouni, Ke Chen, Ender Emre, Alessandro Gullo, Grace Jackson, Rose Nyongesa, Nadine Schwarz, Karla Vasquez-Suarez, and Christophe Waerzeggers (LEG); Parma Bains, Agnija Jekabsone, Tommaso Mancini-Griffoli, Fabiana Melo, Erica Sandoval, Nobu Sugimoto, and Jay Surti (MCM); Martin Cihak (SPR); and Itai Agur, Soledad Maria Martinez Peria, and German Villegas-Bauer (RES). Overall guidance was provided by Dong He and Marina Moretti (MCM); Ruud De Mooij (FAD); Yan Liu (LEG); Giovanni dell'Ariccia (RES); and Kenneth Kang (SPR).

CONTENTS

INTRODUCTION

1. Crypto assets are not new, but the strong push to design appropriate policies to deal with them is. While crypto assets emerged after the Global Financial Crisis, they were not deemed to pose significant risks until recently (FSB 2018). The volatile rise in their market capitalization, their growing correlation with other financial assets, and their adoption in many emerging markets (IMF 2021a) changed perceptions about the risks of crypto assets and the need for appropriate policies to address them (FSB 2022) (Figure 1). The collapse of some crypto assets and failures of exchanges and other players in the crypto ecosystem, amid the recent slide in crypto valuations, added impetus to this push.[1]

Figure 1. Crypto-Asset Market Capitalization
(In USD billions)



Source: Coingecko, and IMF Staff Calculation

2. Policymakers around the world have been developing a variety of national approaches to crypto assets. Some countries have introduced outright bans on crypto assets, while others are considering more targeted restrictions depending on their use cases. Many jurisdictions have been experimenting with various degrees and combinations of regulation, supervision, oversight, and taxation. On the opposite end of the spectrum, some countries have opted to grant unbacked tokens legal tender status and have introduced more broadly a framework to incentivize their use, including guaranteeing the existence of a convertibility mechanism with a fiat currency.

3. This paper's main objective is to provide guidance to IMF members on key elements of an appropriate policy response to crypto assets. This objective is in line with the IMF's mandate to support economic and financial stability across its membership. This paper addresses questions raised by IMF member countries on the benefits and risks of crypto assets and on how to structure an appropriate policy response. It operationalizes the principles outlined in the Bali Fintech Agenda (IMF 2018) and builds upon the IMF's recent research on regulating the crypto ecosystem and stablecoins (Bains et al. 2022a, 2022b), the effectiveness of capital flow measures in the digital age (He et al. 2022), the energy use of crypto assets (Agur et al. 2022), as well as the macro-financial implications of digital money across borders (IMF 2020).[2]

[1] A nearly $2 trillion decline in the value of crypto assets during the spring/early summer of 2022 took place after the sudden collapse of an algorithmic stablecoin called TerraUSD and its sister token, Luna. Several crypto related firms, such as the hedge fund Three Arrows Capital, the lending firm Celsius, and the crypto exchange FTX Trading, have since filed for bankruptcy.

[2] Additional publications include: (i) Virtual-Assets-and-Anti-Money-Laundering-and-Combating-the-Financing-of-Terrorism-1-463654; (ii) Virtual-Assets-and-Anti-Money-Laundering-and-Combating-the-Financing-of-Terrorism-2-463657; and (iii) Keeping-Pace-with-Change-Fintech-and-the-Evolution-of-Commercial-Law-511100.

4. The paper aims to complement broader efforts by the international community to ensure a comprehensive, consistent, and coordinated policy framework to address the risks associated with crypto assets.[3] Standard-setting bodies responsible for different products and markets have provided varying levels of guidance (Annex 2). For instance, the Financial Action Task Force (FATF) updated its standard on anti-money laundering and combating the financing of terrorism (AML/CFT) to explicitly include crypto assets and their service providers, and issued guidance on a risk-based approach to its implementation. Actions by other standard setting bodies range from broad principles for some types of crypto assets to rules for mitigating exposure risks of regulated entities and setting up information exchange networks. While useful, these efforts have not yet produced a comprehensive framework to manage risks to the macroeconomy, financial and market integrity, financial stability, and consumer and investor protection. The IMF is particularly well-suited to provide guidance on addressing the macroeconomic risks associated with crypto assets.

5. The crypto asset ecosystem is evolving—an important caveat to this paper. Crypto assets come in many forms and will likely continue to evolve, including in response to policy actions. There are major data limitations, with business models still being developed. Therefore, effective policies need to be flexible and able to adapt to new developments. The paper is organized as follows: Section II sets out definitions and classifications of crypto assets; Section III discusses purported benefits and potential risks associated with crypto assets; Section IV puts forward nine core elements of effective policy frameworks that support a comprehensive, consistent, and coordinated framework for crypto assets; Section V concludes; and Section VI raises issues for discussion.

DEFINITIONS AND CLASSIFICATION OF THE CRYPTO ECOSYSTEM

6. There are yet no globally consistent definitions and classification or taxonomy of crypto assets.[4] The internet, advanced cryptography, and distributed ledgers (DLT) underlie crypto assets. DLT is a set of technological solutions that enables a single, sequenced, standardized, and cryptographically secured record of activity to be distributed and maintained by a network of participants. This record could contain transactions, asset holdings, or identity data. DLT may be closed (permissioned) or open (permissionless).[5]

[3] The IMF is playing a key role in international cooperation in this rapidly evolving area. Staff have collaborated with and contributed to the work of bodies and organizations such as the Bank for International Settlements (BIS), the Basel Committee on Banking Supervision (BCBS), the Committee on Payments and Market Infrastructures (CPMI), the Financial Stability Board (FSB), the International Organization of Securities Commissions (IOSCO), and the World Bank. It has also provided policy advice to country authorities in bilateral surveillance and through capacity development.

[4] A taxonomy offers a hierarchical relationship between items while a classification groups items along features or attributes.

[5] Permissioned DLT (also known as "closed DLT") uses a ledger in which the consensus protocol requires participants to be certified by an entity, or a consortium, prior to connecting to the network to read, write, or validate transactions. Permissionless DLT (also known as "open DLT" or "public DLT") uses a ledger in which anyone may participate in the

(continued)

7. To help organize the discussion on purported benefits, potential risks, and policy responses, this paper uses a classification of existing crypto assets based on their key features. The aim is not to provide a definitive categorization of assets that dictates how they should be labelled in order to be appropriately licensed and regulated. The goal is instead to describe today's crypto-asset environment where crypto assets may be defined, classified, and treated differently in each jurisdiction. The legal challenges pertaining to this exercise are captured in Box 1. Moreover, the features of crypto assets will continuously evolve, partly in response to country policies.

8. Crypto assets, a broad term encompassing many different products, are privately issued digital representations of value that are cryptographically secured and deployed using distributed ledger technology. Under this broad definition, three categories stand out: unbacked tokens, stablecoins, and other assets (Annex 1). This paper focuses on unbacked tokens (such as Bitcoin) and stablecoins (such as USDC) because of their much larger scale and associated risks. Public digital money such as central bank digital currencies are not covered by this paper.

- **Unbacked tokens** have no backing assets, are usually issued in a decentralized manner, are transferable, have no redemption pledge, and provide no direct claims on the issuer. With no backing assets, unbacked tokens have volatile prices, and are thus generally not well suited to perform the main functions of money: store of value, medium of exchange, and unit of account.[6] Instead, they are mostly held in the hope that prices will rise.

- **Stablecoins** are centrally or decentrally issued crypto assets that aim to have a stable price through reserve assets or through algorithms that respond to demand and supply.[7] Stablecoins are generally denominated in a monetary unit of account, such as the dollar, and may pledge to redeem into cash at par. The stablecoins that hold very safe and liquid assets as reserves and offer direct legal claims on the issuer may be in a position to do so. However, others may fall short, for instance if they hold risky or illiquid assets as reserves, or if they do not offer a legal claim on the issuer or on the reserve assets. Even if they do, direct redemptions are often constrained by how often withdrawals are allowed, fees, and other conditions, such as a minimum withdrawal threshold. Many algorithmic stablecoins used in decentralized finance have also proven to be volatile.

- **Other tokens include utility and security tokens.** *Utility tokens* are crypto assets that are usually centrally issued and provide the token holder with access to an existing or prospective product or service. These are usually limited to a single network (that is, the issuer), or a closed network linked to the issuer, and have limited transferability. Use cases include loyalty programs and access to pre-launch discounts. *Security tokens* are crypto assets that are usually centrally

consensus protocol, as no central authority can approve or deny participation. Permissionless DLT applications usually rely on monetary incentives.

[6] For example, Alvarez, Argente, and Van Patten (2022) studied a country experiment with bitcoin adoption, finding only a limited potential for this crypto asset to become a medium of exchange. They found that despite a "big push," usage in everyday transactions has been low and concentrated among banked, educated, and young males.

[7] Collateralization could involve a single asset or a basket of assets, including fiat currency, commodities (e.g., gold), or other crypto assets.

issued, transferable, and meet the definition of a security within respective jurisdictions. Their use cases include tokenized equities, fractionalized non-fungible tokens, and initial coin offerings.

Box 1. The Challenge of the Legal Classification of Crypto Assets

Assigning crypto assets to specific legal categories is essential in order to provide clarity on how they will be treated legally. This is important on three levels.

- First, the private law nature of crypto assets is essential for the predictability and enforceability of the rights and obligations of the parties (e.g., whether and how these instruments can be owned, transferred, lent, or pledged, and the rights available to their holders in case of the insolvency of the issuer or the custodian). This, in turn, is key to market confidence and effective risk management and supervision.

- Second, classifying crypto assets under the financial law is necessary for regulating them through existing or new prudential and conduct regulatory frameworks. Specifically, this will be essential to determine (i) the prudential and resolution regime, including the competent authority and eligibility to access financial safety net components; (ii) the market conduct rules; and (iii) the applicability of the legal regime governing financial market infrastructures.

- Third, the tax treatment of crypto assets depends on their legal characterization (whether the asset is treated as a commodity or as a means of payment) and on the country's general tax policy settings. For example, if a country's income tax system broadly defines income and generally taxes capital gains, it would be appropriate to apply this same treatment to income or gains from transactions involving crypto assets.

There are no generally accepted legal definitions of crypto assets. Even with newly adopted laws regulating aspect of digital technologies (such as DLT laws), crypto assets definitions vary and are informed by the purpose of the legislation. A key challenge in defining crypto assets is their diverse, complex, and/or novel features. A few laws have defined the term "crypto assets" (EU's Market in Crypto-assets Regulation; MiCA), while others have adopted it without a legal description (Switzerland). Some countries have chosen to define the broader category of "digital assets" deployed on DLT or similar technologies for general purposes (Liechtenstein and Ukraine) or for specific tax purposes (India), while others have defined specific types of digital assets based on their economic purpose (such as Singapore, which has done so to supplement existing payment laws. For example, the EU and Japan have different definitions of crypto assets that have practical consequences. While the EU's MiCA definition includes stablecoins that are pegged to a fiat currency, Japan's framework appears to exclude them from the definition of crypto assets, allowing them to be issued only by banks and other designated financial institutions.

The private law classification of crypto assets can vary widely. Depending on their design features and in some cases contractual stipulations, crypto assets could be classified as a property, personal claims, or sui generis assets, although no claim exists against an issuer of unbacked crypto assets, such as Bitcoin. The key question is whether crypto assets can be qualified as "property" and thus subject to ownership rights. Some jurisdictions have integrated crypto assets into general property law, while others, where the physical existence of an object is still central to qualify as property, may face complexities. However, even when a crypto asset falls within defined categories, applying traditional rules to these categories may still be challenging due to digital nature of these assets and the use of DLT, particularly in a cross-border context. For instance, DLTs with nodes across borders make it challenging to identify the law of the relevant jurisdiction applicable to crypto asset transactions.

The financial law classification can be equally challenging. Crypto assets could generally be brought under a broad array of existing financial law categories (e.g., such as a deposit, e-money, payment instrument, security, other financial instrument, and commodity). This depends on the type of the asset, its private law nature, design features and intended use, as well as existing financial law categories. Many regulatory authorities apply existing legal categories on a case-by-case basis. While function-based taxonomies by regulatory authorities help understand crypto assets, they do not necessarily provide legal certainty on their classification under financial law.

PURPORTED BENEFITS AND POTENTIAL RISKS

9. There are several benefits and risks that may be associated with crypto assets. The main purported benefits include improved efficiency (higher speed and lower cost) of payments, innovation, resilience, transparency, and financial inclusion. As discussed below, currently the benefits seem to be tenuous, though they could still materialize, including through new designs of crypto assets. Even if crypto assets do not have intrinsic value, the technological innovations underlying them and continually emerging could be of value to society, e.g., smart contracts.[8] At the same time, there are important risks associated with crypto assets, including macroeconomic risks, legal risks, and risks to financial integrity and stability. Some risks are inherent to the technology underpinning crypto assets (for instance, DLT), while others stem from the lack of policies or their enforcement. The significance of specific risks also depends on country circumstances, and some risks may not necessarily be relevant in all jurisdictions.[9]

A. Purported Benefits

10. Crypto assets could achieve cheaper and faster payments by reducing the need for intermediaries through the use of DLT. In online transactions, there is a need to verify that the buyer has the necessary funds available and that these are not spent more than once. In the traditional payment system, centralized intermediaries such as banks and credit card companies perform this verification and typically charge fees for their services. Through decentralization, DLT can do away with the need for centralized intermediaries, since information can be accessed, validated, and updated jointly across a network of nodes. Nevertheless, crypto assets involve a different type of intermediary, known as validators, which may contribute to transaction costs.[10] Moreover, in practice, other intermediaries beyond validators, such as exchanges and custodial wallet providers, play an important role in the crypto ecosystem. Box 2 compares the current transaction costs of unbacked tokens and traditional payment systems.

Box 2. Do Crypto Assets Provide Cheaper Payments than Traditional Systems?

Crypto wallets can be classified into hosted wallets, where a third party keeps the crypto assets for the user, and self-custody wallets, where the user has full control over deposited funds. Hosted wallets do not post all the transactions performed by a user on the blockchain, thus avoiding the transaction costs that such posting entails. Transactions not posted on the blockchain are recorded in the centralized data centers of the wallet providers, in the same way as a commercial bank does when clients transfer funds within the same bank. Commercial banks typically do not charge fees for such internal transactions, and the same is the case

[8] Smart contracts are computer programs stored on a blockchain that run automatically when predetermined conditions are met.

[9] While macroeconomic and financial stability risks become relevant when adoption is significant, other risks such as legal, financial integrity, operational, and consumer protection risks could materialize even if adoption is not high.

[10] Validators in permissionless DLT are incentivized to propose valid transactions through rewards with newly minted coins and transaction fees, both of which result in costs to existing users. In contrast, in permissioned platforms, participants must be certified by an entity or consortium before they can join the network. This introduces ownership and profit-maximization incentives. Fees are a potential way of generating profits.

Box 2. Do Crypto Assets Provide Cheaper Payments than Traditional Systems? (concluded)

for crypto wallet providers.[1] Transactions that are posted on permissionless blockchains incur a network fee,paid to crypto asset miners. The median Bitcoin network transaction fee over the last three years was $2.72 (Statista). According to data from CoinDesk, the median value of Bitcoin transactions is presently $93.61, implying a median transaction fee of 2.9 percent (Kaloudis and Young 2022). This is high compared to most other forms of domestic digital payments and transfers.[2] However, certain types of cross-border transfers, particularly small value remittances, regularly incur larger transaction fees. Beck, Janfils, and Kpodar (2022) calculate the average fee for a $200 remittance at 5.7 percent in 2020, with the 75th and 25th fee percentiles equal to 7.7 and 4 percent, respectively. According to the World Bank Remittances Prices Worldwide database, the cost could be in double digits for certain country corridors. This suggests that crypto assets could be relatively cost efficient for remittances.[3] However, if costs associated with the conversion of crypto to fiat currencies and vice-versa are included, the cost efficiency of crypto for remittances becomes less clear, and is likely to depend on the corridor under analysis. There is evidence that for the US-EU corridor, traditional intermediaries may be more cost efficient than crypto (Goldstein 2021). On the other hand, the use of crypto assets for remittances in other corridors suggest that they may be cost efficient in those cases.[4] Technological advances to reduce crypto costs are being developed (Agur et al. 2022), but their efficacy is yet to be determined.

[1] CoinBase, Binance, Kucoin, and Bitfinex do not charge fees for intra exchange retail transfers. Crypto wallets generally do not charge transaction fees beyond the blockchain network fees (e.g., Guarda, Trust Wallet, and Exodus). CoinBase Commerce charges a 1 percent payment processing fee to merchants, while Bitfinex Pay and Kucoin do not charge fees to merchants. In comparison, credit cards typically charge merchants an interchange fee of between 1 to 3 percent, while the fee is lower for debit cards. Most banks offer credit cards which give cash back rewards of between 1 to 3 percent.

[2] See Carare et al. (2022).

[3] To mitigate the risks and protect the crypto asset markets from misuse, compliance with existing regulations, including AML/CFT regulation, is necessary. But this comes at a cost for intermediaries, especially in cross-border payments where applying customer due diligence measures to foreign parties may be more difficult and time costly. The current trend toward regulating crypto assets may therefore also affect transaction costs.

[4] For example, crypto assets have been gaining market share as a means of remittances on the U.S.-Mexico corridor, as reported by, for example, , Coindesk and Cointelegraph.

11. Crypto assets may spur private sector innovation by relying on DLT with open, programmable, and composable architecture (Wharton 2021). The source code of public blockchains is generally widely available, allowing for the possibility to reutilize code developed by others and to build on top of it to create new financial services. Such diffusion of knowledge has the potential to promote innovation and to increase market competition.

12. DLT systems with multiple copies of the ledger of transactions and nodes performing validation activities may provide higher operational resilience than centralized entities. Even if several nodes become non-operational or malicious, the rest would keep the system running.[11]

13. Crypto assets that rely on an open DLT architecture allow for transparency and traceability of transactions, though not necessarily of users. Crypto assets whose ledger is publicly accessible allow for blockchain analytics that could be used to identify illicit transactions based on automated triggers. "Regtech" and "suptech" can be deployed to enhance regulatory

[11] Higher resilience and transparency, achieved through decentralization, may come at the cost of lower transaction validation speed. This is referred to as "the blockchain trilemma."

compliance and supervision. Challenges that blockchain analytics face include geo-blockers, off-chain transactions, and privacy enhancing mechanisms (He et al. 2022; IMF 2021).

14. Crypto assets' use of DLT may enhance financial inclusion, depending on their ability to increase access and reduce transaction costs. DLT could improve financial inclusion by making it easier for the unbanked population to access payment services and lowering prices and fees. Evidence suggests that this might be the case for small value cross-border transactions along some corridors (see Box 2). However, the high costs to cash in and out, as well as the need for some degree of digital literacy and internet connectivity, likely reduce the financial inclusion potential of crypto assets.[12,13]

15. Unbacked tokens have been used to enhance portfolio diversification, but this potential use has decreased over time.[14] The prices of these tokens have become more correlated with other financial assets as they have become more mainstream and held by financial institutions (FSB 2022; Iyer 2022). This has reduced their usability for diversification purposes.

B. Potential Risks

Macroeconomic

16. The widespread adoption of crypto assets could threaten the effectiveness of monetary policy. The transmission of monetary policy would weaken if firms and households prefer to save and invest in crypto assets that are not pegged to the domestic fiat currency (IMF 2020).[15] The risk of currency substitution ("cryptoization") is particularly pertinent for countries with unstable currencies and weak monetary frameworks.[16] Cryptoization is more likely to be associated with the adoption of stablecoins denominated in foreign currencies which, relative to other crypto assets, can offer a less volatile alternative to the domestic currency. The decentralized and anonymity features of certain crypto assets, which make their regulation challenging, ease their accessibility and their potential use for circumventing existing capital control measures. This may incentivize substitution to crypto assets rather than to reserve currencies like the dollar or euro, even though the latter might still represent a safer alternative to domestic currencies. The adoption of crypto assets as official currency or legal tender may further incentivize their adoption and weaken monetary policy effectiveness.

17. Crypto asset usage could also have implications for capital flows' volume and volatility. If crypto assets have lower cross-border transaction costs than existing asset classes, they may create

[12] Households with bank accounts can more easily switch their holdings from fiat to crypto than those without (Shy 2021). Most Bitcoin ATMs charge fees typically above 10 percent to buy Bitcoin with cash (see CoinATMradar).

[13] Despite the legal tender status in El Salvador, bitcoin adoption has not improved financial inclusion (Kapsoli and Ponce, forthcoming).].

[14] See Guesmi et al. (2019) and Akhtaruzzaman et al. (2020).

[15] Monetary transmission refers to the extent to which policy-induced changes in monetary instruments (e.g., the nominal money stock or the short-term nominal interest rate) can affect macroeconomic variables.

[16] As noted in October 2021 *Global Financial Stability Report*, "cryptoization" refers to both currency and asset substitution.

additional incentives for investors to allocate capital across borders. Gross capital flows could increase as a result, as could capital flow volatility, given the large price volatility of unbacked tokens and the potential for herding behavior by investors across borders.[17] Although global crypto asset trading volumes remained relatively small as compared to other financial market transactions, crypto-related capital flows could be significant for countries where local adoption of crypto assets is relatively high (Chainalysis 2022).[18]

18. The adoption of crypto assets could erode the effectiveness of capital flow measures (CFMs), which may limit countries' ability to counteract capital flow volatility.[19] First, crypto assets may not be covered by existing CFM laws and regulations and authorities may not have a mandate and powers to control their use. Second, particularly for pseudonymous crypto assets, prosecution and sanctioning may be difficult.[20] Third, crypto asset trades may not involve any intermediaries or service providers that can be held responsible to comply with CFM laws and regulations and that can verify the identities of transacting parties and the nature of transactions. Lastly, crypto asset service providers might not be regulated. As existing CFM regulations are typically enforced through regulated entities, this limits their effectiveness (He et al. 2022).

19. A potential rapid proliferation of crypto assets can affect the international monetary system. Crypto assets, as noted, have been mostly held in the hope that prices will rise, with only limited use as a medium of exchange. Despite this, the strong correlations between payment currency and reserve currency shares suggests that the adoption of crypto asset for payment purposes might eventually lead to a demand for crypto asset reserves. However, a significant increase in crypto efficiency and payment usage would be necessary before we see a material change in the existing reserve configuration.[21] Illustrative network-model analysis suggests that crypto asset-induced shocks could result in substantial reserve losses across the international monetary system, leading to increased demand for Global Financial Safety Net resources.

20. The spread of crypto assets can increase fiscal risks for public finances. New fiscal risks[22] can arise from the financial sector's exposure to the crypto assets ecosystem, the lack of clarity of tax regimes, and the extra-territorial nature of crypto assets. The wide adoption of crypto assets in a

[17] Stablecoin issuers and their custodians can move from one jurisdiction to another at a very low cost, potentially being an additional source of capital flows and their volatility.

[18] According to Chainalysis (2022), the top 20 countries where the most people are putting the biggest share of their money into cryptos are Vietnam, Philippines, Ukraine, India, United States, Pakistan, Brazil, Thailand, Russia, China, Nigeria, Türkiye, Argentina, Morocco, Colombia, Nepal, United Kingdom, Ecuador, Kenya, and Indonesia.

[19] Even without considering flows related to crypto assets, there is no consensus on the level of effectiveness of capital flow measures (Magud et al. 2011; Forbes et al. 2015; Landi and Schiavonne 2021)

[20] Not all crypto assets are pseudonymous. Some stablecoins require clear identification of the user. Pseudonymous crypto assets shield the identity of the user by using a pseudonym (e.g., a crypto wallet address) instead of the real name.

[21] The demand for currencies to be held in reserves is closely related to strong legal and macroeconomic frameworks and these factors do not change rapidly over time.

[22] Fiscal risks are factors that may cause fiscal outcomes to deviate from expectations or forecasts. These factors comprise potential shocks to government revenues, expenditures, assets, or liabilities, which are not reflected in the government's fiscal forecasts or reports (IMF 2019).

weakly regulated environment could increase the likelihood of facing explicit and implicit fiscal risks from the financial sector. In turn, crypto assets, particularly if pseudonymous, can affect tax revenue collection and compliance, even when not adopted as legal tender. The use of withholding taxes and third-party information is challenging for crypto assets. Decentralized peer-to-peer (P2P) activities increase the reliance on voluntary compliance and self-reporting. Even if supervised institutions are required to report crypto-related activities to tax authorities, some institutions may fall outside of the scope of such regulations (e.g., because they are still unregulated or reside abroad).

21. Granting a crypto asset official currency or legal tender status has far-reaching consequences for monetary stability. If a crypto asset were granted official currency or legal tender status, creditors would be required to accept it in payment of monetary obligations, including taxes, similar to notes and coins (currency) issued by the central bank. Governments can also enact legislation to encourage the use of crypto assets as an official currency, serving as both a unit of account for monetary obligations and a mandatory means of payment for everyday purchases. But there are consequences. If goods and services are priced in both an official currency and a crypto asset, households and businesses would spend significant time and resources choosing which money to hold as opposed to engaging in productive activities. And domestic prices could become highly unstable. Even if all prices were quoted in, say, Bitcoin, the prices of imported goods and services would still fluctuate massively, following the whims of market valuations.

22. Granting a crypto asset official currency or legal tender would also amplify fiscal risks. If a crypto asset that is not pegged to the domestic fiat currency, or whose peg may not be sustainable, is adopted as an official currency or granted legal tender status, government revenues may be exposed to exchange rate risk if taxes or non-tax revenues[23] are quoted in advance in a crypto asset while expenditures are primarily made in the local currency. Moreover, contingent liabilities arise if convertibility to fiat currency is guaranteed by the government. and if the operationalization of such convertibility is through the establishment of public digital e-wallets and trust funds held in public development banks. In addition, the adoption of a crypto asset as official currency or legal tender could affect a government's social policy objectives, particularly for unbacked tokens, as their high price volatility could affect poor households more. The adoption of a crypto asset as a legal tender, which would allow the government to use it as a means of payments, could also significantly impact public financial management.[24] Finally, taxpayers may be able to gain a tax advantage where the application of tax laws to crypto asset transactions is uncertain or otherwise incomplete. The risk of tax avoidance and evasion is heightened in the case of cross-

[23] There are two main categories of non-tax revenue in the public sector. The first is non-tax revenue generated by royalties, such as those from extractives sectors and dividend payments from state-owned enterprises. The second is non-tax revenue from fees for good and services provided by government agencies, such as passport issuance, port fees, agricultural services charges, police fines and penalties, as well as some health and education services. Crypto assets as a legal tender could affect mainly the first category.

[24] The utilization of crypto assets as a legal tender could impact the functioning of the treasury single account (TSA), an essential element of treasury management, by adding numerous e-wallets over existing subaccounts/bank accounts. This can weaken active cash management practices, tangle liquidity management, and require significant investments to adjust the TSA design and operationalization. For fiscal reporting, measurement of value and registration issues may arise in accounting due to high volatility in the price of unbacked crypto assets. This can affect the value of payments and, depending on the timing of crypto assets conversion, impact the reliability of fiscal reports.

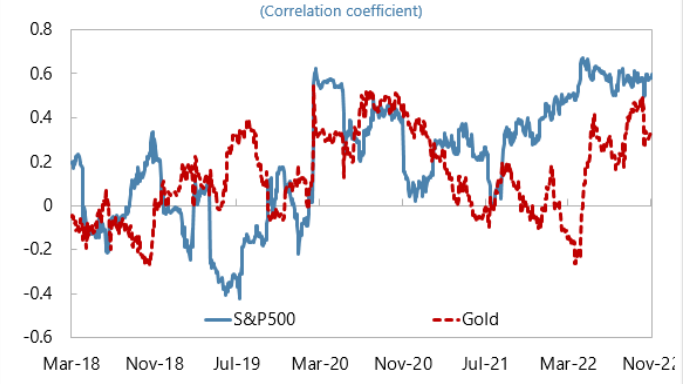
border transactions due to potential differences in classification of crypto assets by different jurisdictions.

23. Granting a crypto asset official currency or legal tender status could raise significant macro-critical legal issues. Legal tender status requires that a means of payment be widely accessible. However, internet access and technology needed to transfer crypto assets remains scarce in many countries, raising issues about fairness and financial inclusion. Moreover, the official monetary unit must be sufficiently stable in value to facilitate its use for medium- to long-term monetary obligations.[25] And changes to a country's legal tender status and monetary unit typically require complex and widespread changes to monetary law to avoid creating a disjointed legal system.

Financial Stability

24. Unbacked tokens and stablecoins without credible backing may pose financial stability risks. Sharp declines in crypto asset prices can have large negative effects on the balance sheets of investors. Financial institutions may hold crypto assets directly to pursue trading, custodial, or market-making activities. They may also be exposed to crypto asset volatility indirectly if they provide credit or other financial services to crypto asset trading platforms and wallet providers, institutional or retail investors in crypto assets, or if they accept crypto assets as collateral for lending. Moreover, a rapid adoption of crypto assets may pose financial stability and credit provision concerns due to changes in bank funding models.[26] Spillovers may materialize if financial institutions are closely connected. Figure 2 is an illustration of interdependencies with traditional financial market.

Figure 2. 60-Day Moving Correlations of Bitcoin and Other Asset Price Changes



Sources: Coingecko; Federal Reserve Economic Data (FRED); IMF staff calculations.

25. Some forms of crypto assets come with risks to ecosystem governance. DLT allows for governance rights to be decentralized through governance tokens (Aramonte et al. 2021). As governance tokens are traded on the market, an attacker who gathers enough voting rights may impose policies that allow him or her to drain funds from users (Wharton 2021). Due to the current lack of regulation, the draining of funds is currently not penalized.

[25] This raises several macro-critical issues. For unbacked crypto assets, how can monetary obligations be expressed in a monetary unit with high volatility? For private stablecoins, what would be the effect on the discharge of monetary debt when the stablecoin is delivered in payment and its market value is "below par"? And what happens with debt discharge if the stablecoin subsequently ceases to exist?

[26] Banks typically rely on retail depositors to fund their operations. If crypto adoption rises, banks might have to pay higher rates on deposits or see their funding shift from stable, low-cost deposits to more expensive, less stable wholesale funding. Banks might respond by taking on greater risks to support profits.

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 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.

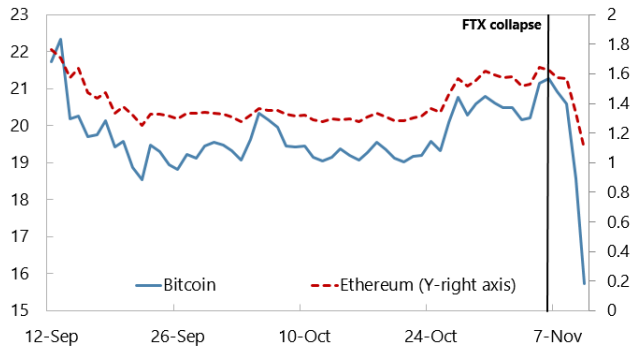
[29] These risks are even more evident in fragile states with high levels of corruption and weak rule of law, where institutions often lack the capacity to properly enforce and protect contractual and property rights.

Consumer Protection

29. Consumer protection risks arise when consumers and investors are unaware or do not fully comprehend the risks associated with crypto assets. Risks to consumers stem from inadequate governance, opaque decision-making processes, and limited recourse when there is insufficient regulation. Consumer protection risks may also arise from price volatility, fraud, or cyber-attacks.[30] The filing for bankruptcy protection in November 2022 by FTX, a major crypto exchange, revealed risky investments, inadequate governance, and opaque corporate interlinkages. The run on FTX exerted significant spillovers on major crypto assets and also impacted decentralized finance and stablecoin markets, ultimately impacting investors (Figures 3 and 4). Similarly, the fallout of the third largest stablecoin, TerraUSD (UST), in May 2022 highlighted significant risks to investors. The stablecoin experienced significant redemptions culminating in the breakdown of the entire Terra ecosystem.

Figure 3. Price of Bitcoin and Ethereum After FTX collapse

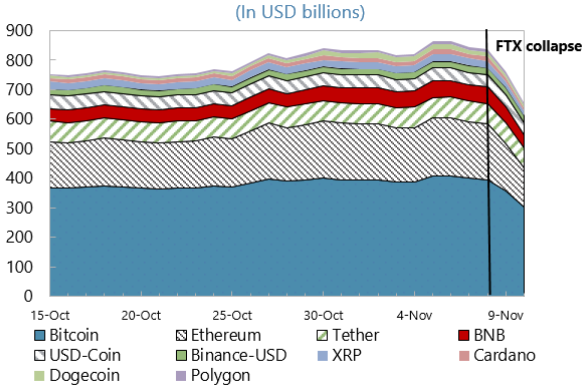
(In USD thousands)



Source: Coingecko.

Figure 4. Market Capitalization of Crypto Market

(In USD billions)



Source: Coingecko.

Market Integrity and Contestability

30. Crypto assets can suffer from market contestability issues. Permissionless crypto assets' scalability constraints may cause congestion, leading to high transaction costs and fragmentation (BIS 2022).[31] The presence of multiple blockchains may generate interoperability problems. Instead, for permissioned DLT, the value of networks and returns to scale make the market prone to concentration risks and market power. Permissioned platforms, including for digital currencies issued by "big techs," could use their networks to shut out competitors and monetize information, using proprietary data on customer transactions.[32]

[30] For a listing of some of the largest crypto frauds, see https://alts.co/cryptos-biggest-scams-of-all-time).

[31] Scalability constraints can make it difficult to withdraw and transfer funds during runs, and may also cause transaction fees to skyrocket. On April 21, 2021, Bitcoin transaction fees peaked at $62.79 (Statista).

[32] In permissionless blockchains, consensus mechanisms may favor concentration. For instance, under proof-of-stake, richer individuals or entities with more crypto assets to stake are more likely to be selected to validate and thus to receive compensation in newly minted crypto assets (Bains 2022).

31. Crypto assets are also prone to manipulation and therefore to fraud and market integrity risks. In permissionless DLT, users can set the fees of their own transactions to rank higher or lower in the settlement queue and obtain financial gains. Large validators could congest the blockchain with artificial trades (Bains 2022), raising the fees that other users pay them (Aramonte, Huang, and Schrimpf 2021). Moreover, illiquidity of certain exchanges or crypto assets may facilitate price manipulations - to trigger liquidations and purchase liquidated collateral at a discounted price or short the collateral asset (Werner et al. 2021).[33]

32. Additional risks inherent to some forms of crypto assets include uncertainty in payment finality and environmental risks. Many types of consensus mechanisms that underpin public blockchains can only deliver probabilistic settlement due to the possibility of forks in the blockchain, which might cancel earlier transactions (Bains 2022). In addition, crypto assets based on proof-of-work consensus mechanisms are highly energy intensive and generate large amounts of e-waste (De Vries and Stoll 2021).[34]

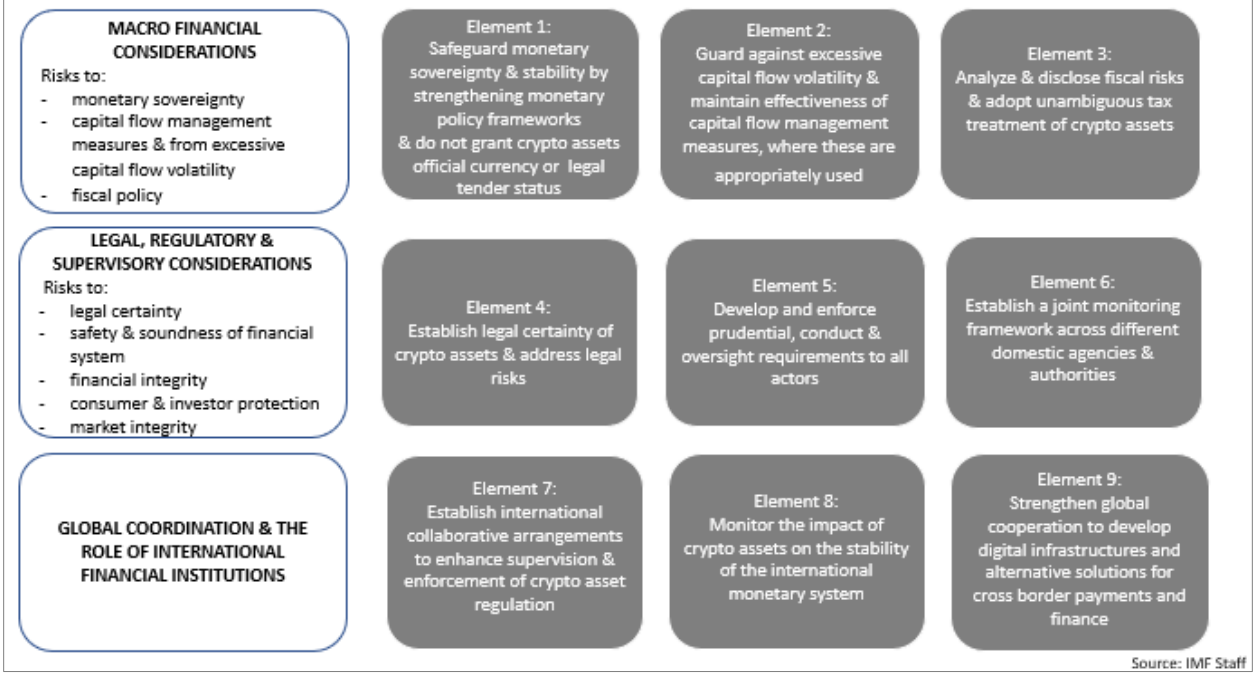
POLICY AND REGULATORY RESPONSES

33. The paper proposes a policy framework comprising nine elements to address the risks and harness the potential benefits of crypto assets. The first three elements relate to macrofinancial risks, while the next three address risks to legal certainty; safety, and soundness of the financial system; financial integrity; consumer, and investor protection; and market integrity and contestability. Elements seven to nine address the importance of enhanced global coordination and collaboration, given the extra-territorial nature of unbacked tokens and stablecoins. They also envision the use of technological innovations for public policy purposes, such as enhancing cross-border payments. Country circumstances and capacity constraints may condition the sequence of implementing the elements of this framework.

[33] Other examples include matching orders, that is, the buying and selling of the same asset to increase trading volume and interest in the asset. DeFi allows for other forms of attacks, including attacks exploiting smart contract vulnerabilities and attacks executed within a single transaction (Werner et al. 2021).

[34] However, other consensus mechanisms are much more energy efficient than proof-of-work, and if properly designed, DLT may be more energy efficient than existing payment systems (Agur et al. 2022).

Table 1. Mapping Risks to Responses: Nine Elements of an Effective Crypto Policy Framework



Source: IMF Staff

A. Element 1: Safeguard Monetary Sovereignty and Stability by Strengthening Monetary Policy Frameworks and Do Not Grant Crypto Assets Official Currency or Legal Tender Status

34. Robust macroeconomic policies and credible institutional frameworks are the first line of defense to protect monetary sovereignty and stability. A lack of credible domestic institutions and policies is the most common root cause of substitution pressures into foreign fiat currencies, and the same is the case for the pressures to substitute into crypto assets. A weak monetary policy framework (MPF), combined with large fiscal deficits and government pressures for central bank financing, are likely to undermine monetary credibility and instigate currency substitution (Adrian et al. 2021; IMF 2020). Therefore, the most effective way to limit substitution into crypto assets is to develop effective monetary frameworks and fiscal and monetary policies that maintain monetary credibility.

35. An effective MPF safeguards monetary sovereignty by being transparent, coherent, and consistent (IMF 2015; IMF 2021b; Unsal, Papageorgiou, and Garbers 2022). A MPF encompasses elements of the design, implementation, and communication of monetary policy as well as the legal foundations for the independence and accountability of the central bank. A transparent MPF helps the public understand the MPF and monetary policy actions (IMF 2020). A coherent MPF incorporates desirable features or principles, such as having a forward-looking policy strategy and timely and regular communications. A MPF is consistent when the central bank's policies and operations are in sync with its communications. A transparent, coherent, and consistent MPF helps

anchor market expectations, curb currency substitution, and ensure the effectiveness of monetary policy.[35]

36. Avoiding large deficits and high debt levels would also protect monetary sovereignty, especially in the context of weak MPFs. In countries where fiscal deficits are large and debt levels are high, governments are more likely to put pressure on the central bank to provide monetary financing and not to tighten monetary policy, in order to avoid raising the cost of sovereign borrowing. The inflationary consequences of this fiscal dominance could increase pressures toward currency substitution.[36]

37. To protect monetary sovereignty and stability, crypto assets should not be granted official currency or legal tender status. Almost all monetary laws recognize that the issuance of officially recognized means of payment is a task of the State, and therefore only recognize "high quality" public means of payment (banknotes and coins issued by the Treasury or the central bank) as "currency" (Bossu et al. 2020). In this light, and considering the fundamental risks they pose, unbacked crypto assets and privately issued stablecoins should not be recognized as "currency." This would be different for crypto assets backed by a public institution, such as the State itself, a central bank, or a monetary institute.

38. Financial stability considerations also support the argument against granting official currency or legal tender status to crypto assets. Crypto assets with official currency or legal tender status could increase adoption and exposures of banks and other regulated financial institutions, thereby amplifying many of the risks noted in the prior section. Moreover, significant financial and reputational risks could arise if a country decides to use a crypto asset for financial relations with the formal international financial system (e.g., correspondent banks, including relations with the IMF, and other central banks). Due to the risks and concerns about destabilizing impacts on the IMS, central banks should not hold unbacked crypto assets or privately issued stablecoins as part of their official reserve assets.

39. In cases where a crypto asset is granted official currency or legal tender status, governments should minimize their exposure to fiscal and operational risks. Governments should minimize their use for official payments. Government revenues would be exposed to high variations if taxes are quoted in crypto assets and if operations of e-wallet are handled by state-owned enterprises (SOEs). Guarantees on the convertibility of crypto assets to fiat currency should be avoided so the ministry of finance does not become exposed to contingent liabilities. Risks to fiscal management operations (such as budget execution, treasury management, fiscal reporting,

[35] IMF (2015) provides guidance on key elements of effective monetary policy frameworks for low- and lower-middle income countries. Unsal et al. (2022) provide a multidimensional characterization of monetary policy frameworks across three pillars—independence and accountability; policy and operational strategy; and communications—for 50 advanced and developing countries between 2007 and 2018.

[36] Catão and Terrones (2001) and Agur et al. (2022) present evidence of a non-linear association between fiscal deficits and inflation, showing a large and significant impact on inflation among developing countries and countries with high inflation. Vieira, Holland and Resende (2012) show that higher debt levels and default risk are associated with higher levels of dollarization.

internal/external audits, and rent seeking) should also be clearly identified and managed with adequate safeguards, controls, and procedures.[37]

B. Element 2: Guard Against Excessive Capital Flow Volatility and Maintain Effectiveness of Capital Flow Measures

40. Policy makers should contemplate various measures to counter the erosion of capital flow measures (CFMs) arising from crypto asset adoption This includes clarifying the legal status of crypto assets and ensuring that CFM laws and regulations cover crypto assets and are effectively applied to the various actors in the crypto ecosystem, ideally also abroad. Moreover, by addressing data gaps and applying new regulatory and supervisory technologies, authorities can create anomaly detection models and red-flag indicators that can facilitate timely risk monitoring and CFM implementation (He et al. 2022).

41. Greater exchange rate flexibility may be needed if CFMs become less effective. The trilemma of international finance implies that countries face a tradeoff between maintaining monetary autonomy, exchange rate stability, and financial openness. Many developing economies employ CFMs and maintain both a degree of monetary autonomy and (partially) fixed or managed exchange rate regimes. If the use of crypto assets leads to a greater circumvention of CFMs, and efforts to reestablish the traction of such measures prove insufficient, authorities may face a choice between gradually shifting toward increased exchange rate flexibility and relinquishing a degree of monetary autonomy.

42. Managing an increased risk of sudden capital outflows could involve a recalibration of international reserves. Holding international reserves comes at an opportunity cost to a central bank, because the safe assets in which such reserves are commonly held have low returns. However, the main benefit of international reserves is that they can provide a buffer against the sudden onset of a balance of payments crisis. When the risk of sudden capital outflow episodes increases, as could occur with a greater use of crypto assets, even if regulated, the benefit of holding international reserves becomes more prominent and central banks may judge that the optimal level of reserves has risen. If so, the macroeconomic policy mix may require adjustments, such as tighter monetary and/or fiscal policies.

C. Element 3: Analyze and Disclose Fiscal Risks and Adopt Unambiguous Tax Treatment of Crypto Assets

43. Fiscal risks in the financial sector generated by the adoption of crypto assets should be analyzed, quantified, disclosed, and monitored as part of government fiscal risk management. The exposure of the government to fiscal risks emerging from crypto assets should be properly quantified and monitored in a timely fashion. The spread of the crypto assets ecosystem and its wide

[37] Audit functions would also need strengthening for oversight of crypto assets operations in the public sector, including audit of transactions, nodes, and e-wallets. If these procedures are not adopted, rent-seeking risks could materialize by delaying the settlement timing between the e-wallets and treasury information systems in a context of high volatility of crypto asset prices.

adoption in a weakly regulated environment could amplify government exposure to financial sector risk. Monitoring and identification of risks generated by highly volatile assets, recognizing the challenges this poses, can increase the government's ability to mitigate and respond to them, thereby underpinning fiscal credibility and the sustainability of public finances.[38] In addition, this information should be included in the government's fiscal risk statement as part of the budget documentation submitted to law makers to promote fiscal transparency (IMF 2019).

44. Tax policy should ensure an unambiguous tax treatment of crypto assets, while tax administrations must reinforce tax compliance. Specific regulations are required to clarify the tax treatment of crypto assets, both for income/wealth and value-added taxes.[39] Tax administrations should exploit opportunities to use third-party information where feasible, e.g., where intermediaries are involved, such as exchange providers, brokers, and dealers, or where trade in assets is settled centrally. Fostering collaboration on cross-border information sharing and financial regulations in this area is critical for tax compliance. This could involve following the recently developed Crypto Asset Reporting Framework (CARF) proposed by OECD (2022). T To complement these efforts, there should be improvements in institutional capacity, including investments in specialized data infrastructure and analytics to support risk analysis and tax audits related to crypto assets operations, as well as prioritizing training and the technical capabilities of tax administration staff to understand and implement the relevant procedures.

D. Element 4: Establish Legal Certainty of Crypto Assets and Address Legal Risks

45. To establish legal certainty, jurisdictions should consider three actions. The following are not mutually exclusive and may involve law reforms, and should be developed with private sector participation and in line with international organizations' guidance: [40]

- **Modernize private law through targeted legislative reforms (Garrido et al. 2022).** Private law may need to be modernized to clarify the classification of crypto assets and the rules governing their transactions. Legislative reforms targeting the areas of friction between private law and new technologies might be best (such as the reforms in Switzerland, Liechtenstein, and Germany) to avoid delays and inconsistencies with the broader framework (Allend 2020).[41]

[38] The IMF Fiscal Transparency Code provides a set of principles and practices to enhance transparency of fiscal risks analysis and management, in addition to fiscal reporting, fiscal forecasting and budgeting, and resource revenue management areas (IMF 2019).

[39] Taxation might also play a corrective role to complement regulatory interventions. The most obvious correction relates to externalities from energy use in proof-of-work mechanisms. In the absence of appropriate carbon pricing, for instance, mining activities could be subject to a corrective tax or, at least, be denied income tax deduction for energy costs.

[40] One example of international cooperation in this area is the ongoing initiative on Digital Asset and Private Law Principles by the International Institute for the Unification of Private Law.

[41] Targeted legal amendments are often more desirable than a complete overhaul of the private law system. However, it is important for jurisdictions undergoing a major overhaul to also consider the inclusion of provisions for crypto assets.

- **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 are limited to 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 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 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 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.

over such reserve assets. In addition, the regulatory framework can take cues from similar products and business in the market, such as commercial banking, e-money, FMIs, and money market funds, while addressing novel risks. A regulatory approach that combines conduct, payment, and prudential regulation, and models it on similar products and activities in the market, may be a sensible approach.

55. Clear and robust governance requirements are essential, especially for stablecoin arrangements. Governance should cover "fit and proper" senior management, resources and control functions, and identifiable decision-making structures that promote safety and efficiency of the arrangement. For example, in case of FTX, the governance framework and its interconnectedness with other affiliates was opaque. Where redemption depends on third parties, the governance body of the arrangement must have clear plans to ensure redeemability in case of failure of the third parties. When stablecoin issuers are non-banks and engage with lending services, conflict of interests should be carefully managed or otherwise prohibited. Third party audits of reserves should be mandatory to show proof of reserves.

56. Where stablecoin arrangements become systemically important, authorities should analyze and adjust the regulatory framework to address new risks.[49] Authorities should apply requirements comparable to those applicable to systemically important banks, such as more intensive supervision, safety and soundness measures, stress testing, recovery planning, and resolvability, to stablecoin providers, taking into account differences in business models (especially where stablecoins do not offer maturity transformation). Access to the financial safety net could be considered when stablecoins reach a systemic scale and when commercial banks issue their own stablecoins or tokenize their deposits, subject to safeguards.

57. Authorities should provide clear prudential requirements on regulated financial institutions (such as banks and insurers) concerning their exposure to, and engagement with, crypto assets. For example, banking, securities, insurance, and pensions regulators should stipulate capital and liquidity requirements and limits on exposures. Financial institutions should also monitor their indirect exposures. This could be, for instance, through loans to crypto users, derivative exposures with crypto asset exchanges, and cyber insurance to wallet providers. While such risks brought by indirect exposures are not the same as from direct exposures, they can be strongly correlated with market movement.

Financial Integrity

58. To address financial integrity risks, countries should implement the FATF standards on AML/CFT. The standards explicitly address crypto assets, which they refer to as virtual assets (VA). They notably require countries to identify and assess the ML/TF risks associated with VAs and take appropriate steps to manage and mitigate those risks. This means ensuring that (i) the relevant laws, including criminal laws, cover VAs; (ii) the relevant authorities have the necessary powers to pursue potential crimes involving VAs, sanction the perpetrators, and freeze, seize, and confiscate VAs when warranted; (iii) unless they are banned, the VA-related services listed in the FATF standards are

[49] This includes contagion risks arising from stablecoin activities to other parts of the financial sector.

regulated and their providers are subject to AML/CFT obligations (including customer due diligence, transaction monitoring, and reporting of suspicious transactions) and supervised for AML/CFT purposes; and (iv) all stakeholders (e.g., AML/CFT supervisors, law enforcement agencies, and the private sector) work in a coordinated manner. Authorities may prohibit the listing of certain types of crypto assets, such as those that use technology to completely mask any form of user identification.

59. Countries need to monitor and mitigate the ML/TF risks related to decentralized finance (DeFi) projects and peer-to-peer (P2P) transactions. P2P transactions do not involve intermediaries or other AML/CFT obliged entities. Likewise, an intermediary may not be present or may be difficult to identify in the context of DeFi. In these contexts, the lack of intermediaries means that traditional AML/CFT regulation, in which AML/CFT requirements are imposed on the private sector and compliance is monitored by supervisors, cannot be applied. The potentially substantial volume of P2P transactions and the rise of DeFi calls for creative risk mitigation.[50,51] To address these issues, countries may consider measures such as requiring intermediaries to apply enhanced AML/CFT measures when dealing with unhosted wallets, and identifying intermediaries in the DeFi context that can be regulated and held accountable for AML/CFT controls.[52] Continual monitoring of P2P transactions and the DeFi space by countries and the FATF is needed to ensure that the associated risks are adequately mitigated and that guidance is provided as appropriate.

60. If properly used, digital tools can help improve the effectiveness of AML/CFT measures taken by the public and private sectors, but they are not silver bullets. When relying upon proper technology, and adequate governance, processes, and procedures, new solutions such as digital ID can facilitate the implementation of effective AML/CFT controls. Likewise, blockchain-based regtech and suptech can greatly help the private sector and the authorities to trace flows and detect suspicious transactions. However, there are important limitations to this approach. For example, off-chain transactions might not be traceable, and the use of anonymity enhancing features or mechanisms to hide critical information will significantly hinder the ability to implement certain measures that address financial integrity risks (such as customer due diligence).[53]

[50] The FATF found that a significant amount of certain crypto assets is transferred on a P2P basis and the proportion has remained largely stable between 2016 and 2020.

[51] One study suggests that in 2021, more VA was stolen from DeFi protocols than any other type of platform, and that centralized exchanges decreased in popularity as a destination for stolen funds. This is likely due to AML/CFT procedures adopted by major exchanges.

[52] DeFi platforms are not always as fully decentralized as they claim to be. There may be some parties such as creators, owners, operators, or other persons who maintain control, or have sufficient influence, in the DeFi arrangement and therefore are qualified as VA service providers subject to AML/CFT regulation. The FATF has also recommended that in cases where there is no intermediary, countries may consider requiring the involvement of a regulated intermediary in activities related to the DeFi arrangements. Nonetheless, oversight of DeFi platforms is still very limited in practice.

[53] Examples of anonymity enhancers include mixers and multiple layers of encryption, stealth addresses, and ring signatures. Hidden critical information may include the location of the customer or the counterparty, or the value of the transaction.

F. Element 6: Establish a Joint Monitoring Framework Across Different Agencies and Authorities

61. Establishing joint monitoring between authorities may be a good first step to better understand developments in the crypto ecosystem. Whilst comprehensive regulation is the first best option, unique jurisdictional challenges may warrant a "constrained best solution" (Box 4 highlights implementation challenges). Irrespective of approach, authorities with different mandates may all equally have interest in developing a deeper understanding of crypto developments. Existing regulatory and supervisory framework (e.g., for AML/CFT purposes), if any, remain an important mechanism to aid understanding of crypto asset activities in a jurisdiction and can help obtain information useful for other regulatory purposes. In addition, frequent engagements with the crypto industry to understand the different actors and their emerging activities could help authorities grasp the extent of developments. Innovation hubs and regulatory sandboxes have been deployed by many countries to understand the innovation, risks, actors, and use cases involved.

Box 4. Potential Implementation Challenges

Authorities will face practical challenges during implementation of recommendations. Countries face several constraints, and it may not be feasible to implement all recommendations comprehensively and immediately. The main constraints include:

- **Lack of sufficient and appropriate resources:** Many authorities are experiencing a shortage of resources and expertise. Authorities need to choose and allocate these scarce resources to areas with highest priority or highest risk. For instance, the effective implementation of the FATF standards on AML/CFT requires a sound assessment and understanding of the ML/TF risks associated with crypto assets, which in many instances remains limited and underdeveloped, sometimes due to resource shortages. Authorities should consider implementing some elements with higher importance, including those with fiscal impact, and defer implementing others.

- **Lack of data**: Due to a lack of comprehensive and comparable data, most authorities struggle to accurately assess the scale and types of risks posed by the misuse of crypto assets, and to identify appropriate regulatory responses. Furthermore, differences in taxonomies can hinder data comparisons across jurisdictions.

- **Fragmented implementation:** While standard setting bodies are developing recommendations, guidance, and standards in relation to crypto assets, a lack of a common taxonomy can limit the timeliness of implementation. Also, as evidenced from the implementation of the FATF standard on AML/CFT, the speed and level of implementation can differ across jurisdictions, creating opportunities for regulatory arbitrage. Furthermore, some global standards are tailored toward advanced economies and might not reflect the challenges facing emerging and developing countries (such as risks of cryptoization).

- **Cross-border nature**: Many crypto asset service providers are located in offshore jurisdictions with limited capacity or history of international cooperation. However, these crypto asset service providers market their services globally, providing significant challenge to the authorities where the users are located, with possible scope for tax avoidance or evasion. This presents a major obstacle to effect regulations. Some jurisdictions require onshoring of these entities to subject them to regulation, but this can be challenging and difficult to enforce. Others are creating public communication channels to ensure the public is aware of which entities are licensed domestically and which are unlicensed and foreign. This helps to inform the public about the lack of recourse to compensation when dealing with foreign crypto entities. Fostering collaboration on cross-border sharing is also critical for tax compliance.

Box 4. Potential Implementation Challenges (concluded)

- **Legal challenges:** A critical challenge when adopting legal reforms is maintaining a level of flexibility to allow for the rapidly evolving technology in the crypto ecosystems, while still providing sufficient legal certainty.
- **Challenges with novelty:** Some requirements may be difficult to implement. For instance, the so-called Travel Rule[1] in the FATF Standards on AML/CFT raises implementation challenges that require greater technological knowhow and collaboration to be overcome.

Authorities should implement the necessary elements in a pragmatic manner, taking into account jurisdictional contexts and idiosyncratic constraints. Authorities face various constraints and need to explore a "constrained best solution." In most instances, the constrained best solution is likely to be bespoke national frameworks that are guided by global standards and best practices, supplemented by a mix of targeted restrictions where global standards have not been completed and supervisory capacity is lacking. Public communication and other soft measures can help supplement and fill outstanding gaps.

Authorities that are faced with rapid uptake of crypto assets may prioritize select elements. The nine elements work together to create a holistic framework, but some may be more important than others depending on the rate of adoption. A starting point is establishing legal certainty within both private and public law. Following legal clarification, comprehensive and consistent regulations are preferable, but under specific circumstances, targeted restrictions may be considered as an alternative (as discussed in Box 3).

[1] FATF's Travel Rule requires crypto asset service providers and other financial institutions to share relevant originator and beneficiary information alongside virtual asset transactions, therefore helping to prevent criminal and terrorist misuse.

62. Authorities should also collaborate on data collection and analysis to improve monitoring capacities. Consistent and reliable data are important for monitoring and enforcement. The fragmented approach to categorizing crypto assets can inhibit the reliability and availability of data. The FSB and other standard setters are well placed to develop common global taxonomies. At present, the reporting of crypto asset data is largely limited to voluntary reporting or reporting under AML/CFT frameworks. Gaps in reporting exist, including off-chain transaction data from the entities that perform critical functions, such as crypto asset service providers. Some authorities are beginning to work with blockchain analytics firms to better understand the flow of funds through a crypto asset value chain, and where significant limitations exist (for example, off-chain data collection and the use of virtual private networks).[54] Finally, data collection should be made more consistent across borders, and collected data should be shared among relevant home and host authorities.

63. To support consistent recording in macroeconomic statistics across economies, there is a need to develop a data collection framework. Work is ongoing on the development of a statistical methodology on the recording of crypto assets in macroeconomic statistics, in the context of the ongoing update of international statistical standards.[55] Also, the new G20 Data Gaps Initiative,

[54] In addition, some organizations are exploring concepts of embedded supervision (i.e., suptech) that enable authorities to directly interact with distributed networks. This will improve access to data and allow authorities to monitor compliance in real time by viewing blockchain transaction data.

[55] See Guidance Note F.18 on The Recording of Crypto Assets in Macroeconomic Statistics.

recently welcomed by the G20 leaders,[56] includes a recommendation for the development of a data collection framework for crypto assets.

G. Element 7: Establish International Collaborative Arrangements to Enhance Supervision and Enforcement of Crypto Asset Regulations

64. The borderless nature of the crypto-assets ecosystem limits the effectiveness of national approaches to regulation. For instance, crypto asset service providers have incentives to register in "regulatory friendly" locations from which they provide platforms for crypto asset transactions to a global market (e.g., FTX was domiciled in The Bahamas but offered crypto related services across the globe). Jurisdictions wishing to regulate crypto services may not have sufficient information or powers to enforce restrictions and need to cooperate with crypto exchanges' home regulators. International collaboration and information sharing are required to minimize regulatory arbitrage and ensure the continued effectiveness of regulatory policies. A comprehensive, consistent, and coordinated regulatory approach to crypto assets is a prerequisite for effective international collaboration, but it may not be sufficient.

65. Mechanisms need to be developed for domestic authorities to authorize and regulate crypto service providers legally domiciled in foreign jurisdictions. Under the FATF recommendations, virtual asset service providers (VASPs)[57] should be registered or licensed at least in the jurisdiction where they are created (as legal persons) or where the place of business is located (for natural persons) and supervised for AML/CFT purposes. The borderless nature of crypto assets means that customers in a given country can easily access services of a service provider not authorized by that country. Countries may, therefore, need to develop ways to authorize and regulate providers that offer services in their jurisdiction, even if the providers are legally domiciled elsewhere. Enforcement, however, may be challenging for regulators with capacity or technological constraints.

66. Furthermore, a clear legal basis must underpin the exchange of information and cooperation, including between AML/CFT competent authorities, even for countries that have restricted or banned virtual asset-related activities. Given that specific VASPs may be subject to the AML/CFT framework of multiple jurisdictions, cooperation between AML/CFT supervisors is critical, and establishing AML/CFT supervisory colleges can facilitate the information sharing and exchange of views among supervisors of VASPs operating in multiple jurisdictions. Sharing of information and knowledge among countries is critical for improving understanding of ML/TF risks related to crypto assets at the global and country levels. Many countries have not yet implemented

[56] See IMF Press Release No. 22/410.

[57] The FATF defines VASPs as "any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conduct 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; iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset." It defines a virtual asset as "a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations."

the FATF standards related to crypto assets, and amongst those that have, many are struggling to implement them effectively. The uneven and inconsistent implementation creates opportunities for regulatory arbitrage as well as challenges in the implementation of certain requirements, such as those governing the transfer of virtual assets.[58] Considerably more efforts are needed globally to implement the FATF standards effectively.

67. International collaborative arrangements should be adapted for crypto assets. Existing cooperation protocols among regulatory authorities in different jurisdictions—such as bilateral memoranda of understanding (MoUs), multilateral MoUs, and supervisory colleges for systemically important financial institutions—are well established and should be expanded to cover the crypto ecosystem. To better understand cross-border risks and find common solutions, new supervisory colleges can be created where an entity wants to launch a potentially globally systemic crypto service.

H. Element 8: Monitor the Impact of Crypto Assets on the Stability of the International Monetary System

68. Policymakers need to step up to the challenges and opportunities posed by crypto assets in the complex global environment. Central bankers, regulators, and other policymakers can help ensure a strong international monetary system by taking decisive action to renew commitments to international cooperation and multilateralism, and reinforce progress made in integrating the global economy.

69. To ensure the success of this upgraded effort, it is essential to continuously monitor the impact of crypto assets on the international monetary system. The international monetary system (IMS) may be entering a chapter with major challenges, such as excessive fragmentation, large and volatile capital flows, and new risks to financial stability and integrity. Crypto assets could amplify existing vulnerabilities and pose new risks to global financial stability and the IMS on multiple fronts. The areas that need close and ongoing monitoring include: (i) crypto assets' impacts on gross and net cross-border capital flows; (ii) changes in financial intermediation, currency substitution, and international currency use; (iii) effects of exchange rate and capital account regimes as well as capital flow management measures; (iv) financial integrity risks; and (v) demand for and supply of Global Financial Safety Net resources. The close monitoring will help inform appropriate regulation and cross-border cooperation among policymakers and international standard setting bodies and institutions.

70. The IMF will help by monitoring macrofinancial and spillover risks. The IMF can do so by actively engaging with member countries through surveillance, lending facilities, and capacity

[58] Preventing and detecting ML/TF requires VASPs to know the originator and beneficiary of transactions. To ensure compliance with regulatory requirements, certain information, such as the identities of both parties involved, must be transmitted along with the VA in a manner similar to how it is conveyed in a bank wire transfer. This practice, known as the "travel rule," must be adapted to suit the specific characteristics of VA transactions. When transferring VAs, VASPs must therefore obtain, hold, and transmit required originator and beneficiary information.

development support. The IMF, with its worldwide membership and technical assistance, can also help bridge the digital divide by supporting countries with their technical challenges.

I. Element 9: Strengthen Global Cooperation to Develop Digital Infrastructure and Alternative Solutions for Cross-Border Payments and Finance

71. In addition to putting in place an effective policy framework for crypto assets, the public sector should take advantage of progress in digital technology to enhance public policy objectives. Some of the underlying technologies of crypto assets could be used to facilitate the development of digital infrastructures and address existing inefficiencies in financial services. Digital public infrastructure, such as interoperable digital platforms, digital identification systems, digital payments, and trusted data sharing, can help solve problems, such as persistent inefficiencies in cross-border payments.

72. Cross-border payments often face a range of inefficiencies, including high fees, slow transaction times, lack of transparency, and limited accessibility for some individuals or businesses. In response, G20 finance ministers and central bank governors endorsed a "roadmap" in October 2020 to enhance cross-border payments (FSB 2020). The roadmap splits necessary improvements into 19 building blocks (BBs) that the IMF and other institutions are actively developing. In particular, the last three BBs are aimed at "exploring the potential role of new payment infrastructures and arrangements," including considering the feasibility of new multilateral platforms and arrangements for cross-border payments (BB17), fostering the soundness of global stablecoin arrangements for cross-border payments (BB18), and factoring an international dimension into central bank digital currency design (BB19).

73. The policy framework proposed in this paper can help create the conditions to improve cross-border payments. It sets out the key elements for authorities to consider that create an environment that allows for innovation in digital money while managing the risks. Of particular importance are the macroeconomic, regulatory, and oversight requirements to ensure the safety of the international monetary system. A consistent legal basis and coherent policies, including for fiscal, monetary, and regulatory purposes, are also essential. Moreover, standards for technology interoperability are necessary to allow for cross-border flows and to ensure sufficient competition. Finally, policies must ensure that capital flow measures and the monitoring of capital flows remain effective even when transactions shift to digital money.

74. But the public sector's role can go beyond providing a robust policy framework. For example, the public sector can build, operate, or supervise digital infrastructure to facilitate cross-border payments. Although not exclusively the domain of the underlying technology of crypto assets, tokenization, encryption, and programmability, new networks and platforms could improve the efficiency of transactions (Adrian et al. 2022). As a final point, it is important to consider the possibility that the public sector might issue central bank digital currency, utilizing technologies developed by crypto asset programmers. While this could offer numerous benefits, it also raises a range of complex policy and technical issues that are beyond the scope of this paper.

CONCLUSION

75. The paper proposes nine elements along three dimensions that inform a comprehensive, consistent, and coordinated policy framework for crypto assets. This framework will serve as the foundation for staff's efforts to provide policy advice and capacity development to country authorities, as well as their participation in discussions at the standard setting bodies.

76. The first dimension of the framework raises the importance of macro-financial considerations, including monetary, capital flow management, and fiscal. Where widely adopted, crypto assets could instigate currency substitution. The first line of defense is ensuring sound and effective monetary and fiscal policy, and not declaring privately issued crypto assets as national currency.

77. The second dimension lays a path to establishing domestic regulatory, supervisory, and oversight requirements, and the effective implementation of existing standards (e.g., the FATF standards on AML/CFT). A starting point is establishing legal certainty within both private and public law. Once legal clarity has been established, it is generally best to implement comprehensive and consistent regulations. In certain circumstances, targeted restrictions may also be necessary to address specific risks or challenges that cannot be effectively addressed through more general regulations. In line with developing comprehensive regulations, the paper provides a set of recommendations on the prudential, conduct and oversight requirements. Developing consistent domestic approaches is important to avoid duplication and prevent arbitrage.

78. The third dimension addresses the criticality of global coordination, recognizing the extra-territorial nature of crypto assets, but also the potential for technological innovations to be leveraged for public policy purposes. Global coordination, monitoring the impact on the international monetary system, and developing alternatives for cross-border payments are highlighted as priorities. The public sector should play a strong catalyst role in leveraging emerging technologies to foster the improvement in cross-border payments.

79. Finally, the paper acknowledges the heterogeneity across jurisdictions, including different initial conditions and constraints. A "constrained best solution" and pragmatic approach to regulation is recommended. Country circumstances and capacity constraints may affect the pace and the sequence of implementation. Moreover, regulations and broader policies toward crypto assets will not fix any underlying design flaws such as the lack of a credible nominal anchor, payments finality, or scalability.

ISSUES FOR DISCUSSION

- Do Directors agree with the purported benefits and potential risks described in paragraphs 9–32?
- Do Directors agree with staff's proposal on nine elements to inform a comprehensive, consistent, and coordinated policy framework for crypto assets?

- Do Directors agree that this framework should be used to guide staff's policy dialogue with country authorities and capacity development activities, and participation in discussions with standard-setting organizations?

Annex I. Classification of the Crypto Asset Ecosystem

	CRYPTO ASSETS			
	UNBACKED TOKENS	**STABLECOINS**	**OTHER**	
Characteristic		Includes algorithmic stablecoins	Utility tokens	Security tokens
Privately issued? Deployed on distributed ledger technology? Pseudonymous?[59]	√	√	√	√
Centralized (known issuer) or decentralized issuance?	Usually decentralized	Centralized or decentralized	Usually centralized	Usually centralized
Claim or no claim on the issuer?	No claim	Depends on design	Depends on design	Depends on design
Redemption pledge (at face value)?	None	Fixed/variable	None[60]	None (equity instruments) Fixed (debt instruments)
Backed assets?	No backing assets	Safe or varied Collateralized (off chain) assets (e.g., fiat, commodity, commercial paper) or uncollateralized but could be backed (on chain crypto assets)	N/A	Can represent real world securities
Stable or volatile price?	Volatile	Dampened price volatility (fluctuates around peg; de-pegs likely)	N/A	N/A

[1] Not all stablecoins are pseudonymous.

[2] May differ on case-by-case basis.

Use cases?	Speculation Remittances Potential usage as a payment instrument	Access to crypto ecosystem, including other crypto assets and DeFi USD-denominated stablecoins might be used as a hedge against inflation or store of value in some EMDEs Potential use as a payment instrument	Loyalty programs, access to pre-launch discounts,	Tokenized equities, fractionalized non-fungible tokens, initial coin offerings

Annex II. Crypto Asset Standards and Guidance by Standard-Setting Bodies

- **Basel Committee on Banking Supervision (BCBS):** In December 2022, the BCBS finalized its standard on prudential treatment of crypto assets, which was endorsed by the Committee's oversight body, the Group of Governors and Heads of Supervision. This included the final standard that the Committee agreed to implement by January 1, 2025. The proposed standard reflects the high-risk of some crypto assets, while taking a more proportional and technology neutral approach to those which are anchored on real-world assets. The BCBS proposed splitting crypto assets into two categories: lower-risk anchored crypto assets and higher-risk "traditional" crypto assets, like Bitcoin. The first category was further distinguished between tokenized assets and stablecoins. Credit and market risk capital requirements for tokenized assets would be similar to those of traditional assets. For stablecoins, the proposal considered a possible lower risk weight based on certain conditions. For traditional crypto assets—which include unbacked crypto assets—the BCBS proposed a conservative prudential treatment based on a 1250 percent risk weight that would be applied to maximum long and short positions.

- **Committee on Payments and Market Infrastructures (CPMI)**: In 2022, the CPMI and IOSCO published a guidance note on the application of the Principles for Financial Market Infrastructures to stablecoin arrangements (SAs). The PFMI is particularly relevant for stablecoin arrangements primarily used for payment purposes, as it would help ensure the safety, efficiency and resilience of these infrastructures. The guidance defines the SA's transfer function as the transfer of coins between users, and typically entails the operation of a system, a set of rules for the transfer of coins between or among participants, and a mechanism for validating transactions (similar as for other FMIs). The guidance aims to provide more clarity on a subset of principles (i.e., governance, framework for the comprehensive management of risks, settlement finality, and money settlements) but SAs will be expected to observe all of the relevant principles. Further work is expected on issues specific to stablecoins denominated in or pegged to a basket of fiat currencies (i.e., multicurrency SAs) and stablecoins with non-cash reserve assets as well as the PFMI Responsibilities.

- **Financial Action Task Force (FATF)**: In 2018, the FATF defined virtual assets (VAs) and virtual assets service providers (VASPs). The entire FATF standards apply to activities involving VAs, but in 2018 and 2019, several provisions were introduced specifically to address VAs and VASPs, including the FATF Glossary, Recommendation 15 on "New Technologies," and its Interpretive Note. To facilitate implementation, the FATF also issued an Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers.

- **Financial Stability Board (FSB):** In October 2020, the FSB published high-level recommendations to promote coordinated and effective regulation, supervision, and oversight of global stablecoin arrangements. In February 2022, the FSB published an assessment of risks to financial stability posed by crypto assets. While the FSB concluded that crypto assets are not globally systemic, they noted that stablecoins in particular may have the potential to be systemic in the future. In October 2022, the FSB revised their high-level recommendations on global

stablecoins to reflect new products and trends in the market. They also consulted on high-level recommendations on the regulation, supervision, and oversight of broader crypto asset activities and markets. In comparison to the Fund's proposed elements of an Effective Policy Framework, the FSB high-level recommendations on the Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements do not address macro-financial considerations.

- **International Organization of Securities Commissions (IOSCO):** In February 2020, IOSCO published its final report on issues, risks, and regulatory considerations relating to crypto asset exchanges. When building a regulatory framework for crypto asset platforms, the IOSCO report sets out that authorities should consider the following elements: (i) governance requirements for platform operators, including prudential requirements; (ii) requirements regarding access to the platform; (iii) requirements for the robustness, resiliency, and integrity of operating systems; (iv) market integrity requirements; (v) transparency requirements; (vi) AML/CFT requirements; and (vii) criteria to accept products to be offered in the platforms. In 2022, IOSCO published a fact-finding report on key risks and considerations on DeFi.

Annex III. The FTX Debacle: Strengthening the Case for Consistent and Comprehensive Regulation

FTX, a major crypto exchange once valued at $32 billion, filed for bankruptcy protection on November 11, 2022. Although contagion to the wider financial system appeared to be limited, the run on FTX exerted significant spillover effects on major crypto assets and impacted decentralized finance and stablecoin markets. The prices of Bitcoin and Ether dropped 23 and 43 percent respectively and the total value locked (TVL) of DeFi dropped by around 17 percent to 45 billion.

The FTX debacle highlights several vulnerabilities arising from the provision of multiple crypto asset activities:

- First, the lack of basic information of crypto exchanges, such as the corporate structure and financial information (for example the composition of reserves including exposure to self-issued tokens), makes it difficult to assess the extent of interconnections, as well as the robustness of governance and risk management arrangements.
- Second, the nature and magnitude of financial interlinkages between affiliates were opaque. Intra-group transactions were significant—FTX reportedly lent more than half of its customer funds to fund risky investments by its trading arm, Alameda Research, which in turn held a significant value in claims on FTX through its holdings of the unbacked self-issued token, FTT. Financial interconnectedness on such scale points to severe governance and risk management failures, as well as consumer protection concerns.
- Third, the multiple functions and activities (such as brokerage, trading, and custody services) of crypto service providers are not subject to regulation and oversight. In the case of FTX, these integrated offerings led to leveraged lending to consumers, creating liquidity mismatches, and the subsequent inability to fulfill higher demands for withdrawals.
- Fourth, crypto asset providers and their affiliates are often domiciled in multiple jurisdictions with different reporting requirements (where applicable). These disparate reporting requirements compounds the opacity and increases the lack of transparency of providers activities.

The recommendations of this paper should help address similar vulnerabilities in the crypto ecosystems. The recommendations emphasize in particular the importance of transparent and robust governance and risk management frameworks; the criticality of segregation of customers' assets; in the case of integration of trading, storage, and brokerage services, the importance of each activity to have clear and distinct regulatory requirements; greater transparency and disclosure requirements, and the importance of independent third-party audits.

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]

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]

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. 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]

IMF (International Monetary Fund). 2021. "The Crypto Ecosystem and Financial Stability Challenges." In *Global Financial Stability Report*, Chapter 2. Washington, DC: International Monetary Fund. [Link]

IMF (International Monetary Fund). 2021. "The Rise of Digital Money: A Strategic Plan to Continue Delivering on the IMF's Mandate." Staff Report, International Monetary Fund, Washington, DC. [Link]

Iyer, T. 2022. "Cryptic Connections: Spillovers Between Crypto and Equity Markets." Global Financial Stability Note 2022/001, International Monetary Fund, Washington, DC. [Link]

Kaloudis, G., and S. D. Young. 2022. "A Brief Overview of Crypto Payments in 5 Charts." Coindesk's *Payments Week* series. [Link]

Landi, V.N., and Schiavone. A. 2021. "The Effectiveness of Capital Controls."Open Economies Review, 32 (June): 183-211. [Link]

OECD (Organisation for Economic Co-operation and Development). 2022. "Public Consultation on the Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard: Comments by B. Michel and T. Falcao." OECD, Paris. [Link]

Schwarz, N., K. Chen, K. Poh, G. Jackson, K. Kao, F. Fernando, and M. Markevych. 2021. "Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism (1): Some Legal and Practical Considerations." Fintech Note 2021/002, International Monetary Fund, Washington, DC. [Link]

Schwarz, N., K. Chen, K. Poh, G. Jackson, K. Kao, F. Fernando, and M. Markevych. 2021. "Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism (2): Effective Anti-Money Laundering and Combating the Financing of Terrorism and Supervisory Framework—Some Legal and Practical Considerations." Fintech Note 2021/003, International Monetary Fund, Washington, DC. [Link]

Terrones, Marco and Catão, Luis. 2001. "Fiscal Deficits and Inflation: A New Look at the Emerging Market Evidence." Working Paper 2001/074, International Monetary Fund, Washington, DC. [Link]

Unsal, F. D., C. Papageorgiou, and H. Garbers. 2022. "Monetary Policy Frameworks: An Index and New Evidence." IMF Working Paper 22/022, International Monetary Fund, Washington, DC. [Link]

Shy, O. 2021. "Digital Currency, Digital Payments, and the 'Last Mile' to the Unbanked." Federal Reserve Bank of Atlanta Policy Hub. [Link]

Vieira, Fabrício A.C., Holland, Márcio, Resende, Marco F. 2012. "Financial Dollarization and Systemic Risks: New Empirical Evidence." Journal of International Money and Finance, Volume 31, Issue 6 (October) 1695-1714. [Link]

Werner, S. M., D. Perez, L. Gudgeon, A. Klages-Mundt, D. Harz, and W. J. Knottenbelt. 2021. "SoK: Decentralized Finance (DeFi)." [Link]

Wharton (Wharton Blockchain and Digital Asset Project). 2021. "DeFi Beyond the Hype: The Emerging World of Decentralized Finance." Produced by the Wharton Blockchain and Digital Asset Project, in collaboration with the World Economic Forum. [Link]