Regulating the Crypto Ecosystem

The Case of Unbacked Crypto Assets

Parma Bains, Arif Ismail, Fabiana Melo, and Nobuyasu Sugimoto

NOTE/2022/007

FINTECH NOTE

Regulating the Crypto Ecosystem

The Case of Unbacked Crypto Assets

Prepared by Parma Bains, Arif Ismail, Fabiana Melo, and Nobuyasu Sugimoto

September 2022

Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Assets

NOTE/2022/007

Parma Bains, Arif Ismail, Fabiana Melo, and Nobuyasa Sugimoto*

RECOMMENDED CITATION: Bains, Parma, Arif Ismail, Fabiana Melo, and Nobuyasa Sugimoto. 2022. "Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Assets." IMF Fintech Note 2022/007, International Monetary Fund, Washington, DC.

ISBN:	979-8-40022-136-1 (Paper) 979-8-40022-158-3 (ePub) 979-8-40022-161-3 (PDF)
JEL Classification Numbers:	D18, E26, E42, F31, G28, G18 , O30
Keywords:	Crypto; crypto asset; cryptocurrency; blockchain; stablecoin; DLT; regulation; Economic sectors; Emerging technologies; Financial crises; Financial sector policy and analysis; Financial sector stability; Financial services; Fintech; Systemic risk; Technology
Authors' email addresses:	PBains@imf.org AIsmail@imf.org FMelo@imf.org NSugimoto@imf.org

* The authors would like to thank Tobias Adrian for his guidance, and Marina Moretti, Agnija Jekabsone, and Cristina Cuervo for their comments and contributions to this note.

Contents

BOXES

FIGURES

TABLE

Acronyms/Glossary

AML ..... Anti–Money Laundering

BCBS..... Basel Committee on Banking Supervision

BFA ..... Bali Fintech Agenda

CFT ..... Combating the Financing of Terrorism

CBDC ..... Central Bank Digital Currency

CPMI ..... Committee on Payments and Market Infrastructure

DeFi..... Decentralized Finance

DLT..... Distributed Ledger Technology

FCA..... Financial Conduct Authority (UK)

FATF ..... Financial Action Task Force

FMI..... Financial Market Infrastructure

FSB ..... Financial Stability Board

IOSCO ..... International Organization of Securities Commissions

NFT ..... Non-Fungible Token

SSB..... Standard Setting Body

VPN..... Virtual Private Network

Executive Summary

The ongoing evolution in the crypto ecosystem is revealing both opportunities and pitfalls. Crypto assets were originally developed to democratize payments but are mostly used for speculation and, in the case of certain types of dollar-denominated stablecoins, also as a hedge against inflation and currency depreciation. Unbacked crypto assets are the oldest and most popular type of crypto assets, relying not on any backing asset for value but instead on supply and demand. These crypto assets offer limited or no rights for the token holder and are usually issued in a decentralized manner. Users treat unbacked crypto assets as speculative instruments rather than as a medium of exchange.

Nevertheless, innovations that have given rise to the crypto ecosystem, including their underlying technologies, could create potential benefits through greater competition and efficiency in some financial services, such as remittance, trade financing, and cross-border payments. Applying decentralized technologies to real use cases, coupled with appropriate regulation, can offer consumers compelling alternatives to traditional finance.

Crypto asset growth has been volatile, and associated financial stability risks in some emerging markets and developing economies are rising. The total valuation of crypto assets reached almost $3 trillion in November 2021 before falling to less than $1 trillion in July 2022, demonstrating relatively high volatility. Although the size of the market itself is not necessarily a financial stability risk, growing interlinkages with regulated financial services and the lack of regulation might be. The October 2021 Global Financial Stability Report revealed that crypto asset exchanges operating in some emerging markets and developing economies have reached trading volumes comparable to those of local stock exchanges and interbank foreign exchange markets. Despite these large retail holdings, many regulatory authorities do not have conduct or prudential regulation, or payments oversight.

Crypto assets were designed to disintermediate financial services, but new types of centralized entities, such as exchanges and wallet providers, offer key functions to users. These require users to trust centralized entities once again, yet they remain largely unregulated. In some instances, a single entity might offer several key services, such as exchange, storage, and clearing, which could require greater prudential and payment system oversight. The growing importance of these entities could lead them to being considered systemic financial market infrastructures (FMIs).

Global standards applicable to unbacked crypto assets are limited and do not currently mitigate these risks and vulnerabilities. Although standard-setting bodies (SSBs) are making efforts to adjust and develop standards, these remain mostly focused on specific products (global stablecoins), issues (financial integrity), sectors (payments, securities, banking), or entities if they are designated by domestic authorities as systemic. As a result, regulatory gaps in many countries remain material, and crypto's cross-sector and cross-border nature limits the effectiveness of uncoordinated national approaches. In particular, gaps exist where crypto assets are issued, exchanged, transferred, or stored by nonbank entities and where a jurisdiction's regulatory framework does not capture crypto assets based on current legal interpretations of financial services and products.

As global standards develop, regulators are encouraged to use all existing tools at their disposal to address rising local risks. The growing systemic implications of crypto assets may warrant immediate regulatory actions, particularly in some emerging markets and developing economies. Regulators should

use existing regulatory powers, guided by the applicable international standards, and should focus on areas of vulnerability, such as hosted wallets, centralized exchanges, and financial institutions' exposures. Actions can range from user education and industry guidance to targeted restrictions. Authorities should ensure that any short-term approach is flexible enough to be adjusted in the future, in line with market developments and future international standards.

Broad bans on crypto assets are likely to be disproportionate and ineffective in the long run, but targeted restrictions could help address immediate challenges while regulatory capacity is being built. Authorities should take a balanced approach to harnessing the benefits of technology-driven innovation in financial services, while ensuring that consumers and markets are protected. Over the short-term, and in the absence of global standards, authorities that face severe and immediate risks may need to restrict certain crypto products or activities (such as derivatives, marketing, or use in payments), while still allowing users to buy and sell crypto. However, such measures should not be seen as a permanent solution, as they are disproportionate, likely to stifle innovation, and there are strong incentives and technological alternatives for circumvention. Authorities need to address the underlying drivers for crypto usage, such as weak macroeconomic conditions, misleading marketing, and a lack of trust in traditional financial services.

Any global standards should be comprehensive and risk-based. Domestic regulation should be guided by cross-sectoral global standards, informed by common taxonomies and available data, and provide a level playing field across the activity and risk spectrum applied proportionately to banks and nonbank entities operating in the crypto asset space. Moreover, the regulatory framework will need to be flexible enough to adapt to a changing landscape and risk outlook.

To achieve a consistent and comprehensive global regulatory framework, the following six elements should be considered:

- To make global standards effective, common taxonomies are needed. These taxonomies should be developed by SSBs and guided by common groupings of risk, structural features, and economic functions as opposed to marketing and the aspirations of developers.
- Access to reliable and consistent data is needed. It can be challenging to get accurate and consistent data in crypto asset markets, although these are needed to identify market risks and to determine regulatory responses while protecting user privacy. A common taxonomy is one foundational step to improving data collection, but greater regulation, oversight, and cross-border collaboration will be required to close data gaps.
- Global standards should be risk-based, with greater requirements on entities and activities that generate more risk. Licensing and authorization criteria should be clearly articulated, the responsible authorities clearly designated, and coordination mechanisms well defined.
- Global standards should be comprehensive and should cover all important activities and entities. Crypto asset service providers that deliver core functions and generate key risks should be licensed, registered, or authorized. These include entities related to the storage, transfer, exchange, and custody of reserves, among others, similar to existing rules for financial service providers. Where crypto asset service providers provide multiple functions, authorities should consider the risks generated across the entity and across multiple activities, and additional prudential, conduct, where appropriate, payment oversight requirements should reflect the nature

of these additional risks. It is important to cover all the entities because regulating one may not be enough and may leave significant risks in the system.

- If entities or activities become systemic, they should be subject to additional requirements. Entities that become systemically important should be subject to requirements comparable to those applicable to systemically important institutions, that is, more intensive supervision, safety and soundness, stress testing, recovery, and resolvability. For example, where entities provide critical services with systemic implications, they could benefit from guidance from the CPMI-IOSCO principles for systemic FMIs
- Regulatory responses should provide a level playing field and address contagion effects. Consistent yet proportionate rules should apply to existing financial entities as well as nonbank crypto asset issuers (where possible) and crypto asset service providers. Authorities should provide clear 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. If regulated entities provide custody services, requirements should be clarified to address the risks arising from that function.

Finally, in addition to the above, Table 1 highlights the potential regulatory responses to key risks. It further underscores that although sector-specific global standards are useful, cross-sectoral coordination is important to achieve an effective regulatory framework for the crypto ecosystem. The Financial Stability Board (FSB) is well placed to take a leading role in coordinating the establishment of global standards to guide the national implementation of regulation of crypto assets while considering sector-specific standards developed by other SSBs.[1] Although this note is focused on unbacked crypto assets, the paper's regulatory considerations on the broader ecosystem may apply to a wider range of crypto assets, including stablecoins.

[1] The FSB (2022) has called for a closer examination of regulatory gaps in association with other SSBs.

Table 1. Recommendations for Prudential and Conduct Regulation of the Crypto Ecosystem: Unbacked Crypto Assets[2]

Policy Objectives	Key Risks	Regulatory Responses
Legal Certainty	Regulatory authorities lack sufficient powers or scope Lack of regulatory resources and expertise	Enhancement of legal powers of regulators Determination of legal classification of crypto assets Establishment of legal basis for domestic regulatory coordination and cross-border cooperation Enhancement of regulatory expertise
Effective Risk Monitoring	No common taxonomy Limited accurate, consistent, and comparable data	SSBs to create consistent global taxonomies Domestic authorities to implement taxonomies consistently Authorities to improve data collection by implementing existing global standards and/or regulating ancillary activities Authorities to require regulatory reporting as part of bespoke regulatory frameworks
Financial Stability	Interlinkage with wider financial system Currency substitution Crypto asset service providers carrying out multiple activities Crypto asset service providers generating systemic risk Third-party risks Market risks	Prudential requirements on bank exposures and active monitoring of indirect exposures Restrictions on regulated entities engaging with certain risky crypto assets Cross-border cooperation and targeted restrictions Prudential requirements commensurate with risk Extension of regulatory coverage to entities with critical functions Wind-down arrangements and resolution Guidance from the principles for financial market infrastructures (for designated entities) IOSCO Principles on Outsourcing
Consumer Protection	Operational failures Cyber attacks Lack of recourse to compensation Volatility Use of leverage	Implementation of BCBS Principles on Operational Resilience (where appropriate) Implementation of BCBS Principles for the Sound Management of Operational Risk (where appropriate) Implementation of FSB practices on cyber incident response and recovery Implementation of CPMI-IOSCO guidance on cyber resilience for FMIs where appropriate Implementation of IOSCO Recommendations Regarding the Protection of Client Assets

[2] Some objectives, such as monetary policy effectiveness, are out of scope of this paper.

		Segregation and safekeeping of consumer funds and appropriate record keeping Clear complaints procedures User education Limits or restrictions on use of leverage Accurate and clear marketing
Market Integrity	Opaque price formation Market manipulation (for example, pump-and-dump schemes, rug pulls) Conflicts of interest	Transparency requirements on crypto asset service providers Governance requirements for issuers (where possible) and crypto asset service providers Requirements for white papers on issuers (where possible) Market abuse rules to be extended to crypto asset service providers Limits to products offered on crypto asset exchanges Minimum set of reporting requirements on crypto asset service providers Implementation of IOSCO recommendations on crypto trading platforms
Cross-border Cooperation	Lack of global standards Regulatory arbitrage	Cross-sectoral global standards to close policy gaps Implementation of existing global standards in domestic regulation Close cooperation between authorities that host crypto asset service providers and jurisdictions where those services are marketed

Introduction[3]

Crypto assets have the potential to generate efficiencies in financial services but also give rise to risks that authorities would need to address.[4] Initially designed to democratize payments, certain crypto assets, and particularly the underlying distributed ledger technology (DLT), have been used in areas such as payments, the issuance of debt and equity, trade financing, and post trade processes.[5] Small-scale experiments conducted by public and private entities have shown the potential of some crypto assets to generate efficiencies in financial services through disintermediation, lowering costs, and speeding up processes. However, crypto assets are diverse, and individual risks and benefits must be considered. Although some crypto assets might develop into tools for investment or decentralizing functions such as storage, lending, or payments, many can bring substantial risks to market integrity, consumer protection, financial integrity and, increasingly, financial stability.

Although decentralization is a key concept of the crypto ecosystem, in practice, most users access their crypto assets through centralized entities that provide easy-to-use interfaces. Many of these entities hold information on their users and can accept or block transactions from certain addresses or can share transaction data with other organizations.[6] These entities include exchanges and wallets and provide an important role in crypto asset markets.

Wallet providers—much like banks and electronic payments wallets—hold assets on behalf of consumers and initiate transfers. When assets are placed with these entities, users are placing their trust in a centralized entity. Likewise, many exchanges—much like stock exchanges—facilitate trading in markets and record transactions taken through their platforms. Here, again, users must trust centralized entities with their data and the exchange of their assets. Many of these entities have grown to offer several products and services as a one-stop shop. Additionally, potential critical service providers might also provide avenues for centralization (Box 2), while holdings of many crypto assets might be concentrated in the hands of a few "whales."[7][8]

The Bali Fintech Agenda (BFA), a guiding framework for fintech developed jointly by the IMF and the World Bank, can help authorities navigate important policy questions on crypto assets. The BFA consists of 12 policy elements to help guide authorities in harnessing the benefits of fintech while mitigating its

[3] Any reference to existing crypto assets and companies in this paper uses publicly available information and does not mean to endorse or analyze features of specific crypto assets or arrangements.

[4] The use of the term *authority* in this paper refers to government bodies, central banks, or financial sector regulators that might be responsible for crypto asset regulation.

[5] The key components of most networks are in fact centralized. Public and permissionless blockchains aim to be open, transparent, auditable, immutable, and decentralized. Nevertheless, crypto asset service providers (like wallets and exchanges) are entities that add points of centralization throughout the value chain. Some crypto assets are also centrally issued, and although this is particularly true of stablecoins, many unbacked crypto assets are issued centrally. This centralization is more pronounced in private and permissioned blockchains. Even in public blockchains, many users access the blockchain through a small number of centralized application programming interfaces call operators, rather than directly interacting with the blockchain.

[6] Self-custody provides an alternative solution, and the famous saying "not your keys, not your crypto" is used as a reminder to users of this centralization.

[7] Ben Mariem and others (2020) estimate that 4.5 percent of entities hold 85 percent of all circulating bitcoins.

[8] The term *whale trade* often refers to the trades where a single trader or entity has a significant position in a particular market and its trades have a significant impact on the market. In the securities market, both wash trades and whale trades are offenses and are prosecuted and sanctioned by securities regulators.

risks. It is a particularly useful framework when considering policy responses to crypto assets. It aims to balance the efficiencies generated by some crypto assets through the promise of embracing the potential of new technologies, while mitigating the diverse risks that some crypto assets create through monitoring new developments and modernizing legal and regulatory frameworks.

This note builds on earlier work by IMF staff to provide a closer look at the prudential and conduct regulatory challenges brought by unbacked crypto assets and is a part of a broader set of publications covering different aspects of crypto assets. A previous Fintech Note discussed various elements of the regulation and supervision of crypto assets (Cuervo and others 2020). It covered a broad variety of crypto topics including risk assessments of various crypto assets and potential regulatory responses. In addition, further Fintech Notes have covered crypto assets and financial integrity (Schwarz and others 2021a and 2021b) and crypto assets and capital flow measures (He and others 2022). Bains (2022), and Agur and others (2022) focus on the underlying technology that delivers crypto assets. IMF has also explored crypto asset risks in blogs exploring both the risks of crypto assets as legal tender[9] and the regulatory implications of the growth of crypto asset markets—calling for a global regulatory framework that provides a level playing field along the activity and risk spectrum.[10]

This note reflects evolving market developments and their associated risks, as well as regulatory and supervisory developments. It also discusses key entities that carry out core functions in the crypto asset ecosystem. The main purpose is to help regulators and supervisors identify key challenges, and so providing high-level guidance for their consideration when designing a regulatory and supervisory approach to address risks, The companion Fintech Note on regulation of stablecoins (Bains and others 2022) complements this note.[11]

Taxonomy and Scope

The FSB defines crypto assets as a type of digital asset that depends primarily on cryptography and DLT or similar technology and unbacked crypto assets as crypto assets that are neither tokenized traditional assets nor stablecoins.[12] Crypto assets have been variously termed virtual assets, digital assets, cryptocurrencies, and digital currencies. This paper refers to DLT in the broadest sense as a set of technological solutions that enables a single, sequenced, standardized, and cryptographically secured record of activity to be safely distributed to, and acted upon, by a network of diverse participants. This record could contain transactions, asset holdings, or identity data. The data are usually distributed, and control of this data is often decentralized to varying degrees. In its popular blockchain form, DLT has a set of defining features such as organizing data in a chain of blocks. Each block contains data that are verified, validated, and then “chained” to the next block. Some blockchains can provide for greater

[9] Adrian, Tobias and Rhoda Weeks-Brown, “Cryptoassets as National Currency? A Step Too Far,” *IMF Blog, IMF*, July 26, 2021, https://blogs.imf.org/2021/07/26/cryptoassets-as-national-currency-a-step-too-far/.

[10] Adrian, Tobias, Dong He, and Aditya Narain, “Global Crypto Regulation Should be Comprehensive, Consistent, and Coordinated,” *IMF Blog*, *IMF*, December 9, 2021, https://blogs.imf.org/2021/12/09/global-crypto-regulation-should-be-comprehensive-consistent-and-coordinated/.

[11] The greater role of BigTech entities in the crypto asset ecosystem is an important development, and Bains and Sugimoto (2022) discuss the unique regulatory considerations required to manage their risks.

[12] See glossaries in https://www.fsb.org/wp-content/uploads/P101018.pdf and https://www.fsb.org/wp-content/uploads/P160222.pdf.

auditability and transparency, as well as immutability, depending on the network design and the types of assets deployed on it.

Unbacked crypto assets are not considered to be money because they do not fulfill the three common functions of money, and regulators have broadly classified them according to their function.[13] Crypto assets are not typically used as a unit of account, a store of value, or a medium of exchange. Many unbacked crypto assets tend to have high price volatility (which makes them a poor store of value and unit of account) with little intrinsic value and are likely to be used as speculative investments akin to gambling. In these cases, users encourage others to "HODL"[14] rather than spend the crypto asset—thereby increasing its price and utility as a speculative tool—when spending would increase its utility as a payment tool. Even where some crypto assets are legal tender, their use as a payment or remittance tool remains very small, they are still not considered a viable medium of exchange, and they are less likely to be used by vulnerable or unbanked consumers despite a focus on financial inclusion (Alvarez and others 2022). Additionally, leveraged trading prevails even among retail users and is offered in both centralized and decentralized exchanges as high as 125 times the initial investment, further increasing utility as a speculative tool.

No internationally agreed taxonomy exists for crypto assets, and this paper will use a classification based on broadly used taxonomies and grouping of common risks (figure 1). A globally consistent taxonomy would help create common regulatory standards and approaches; however, differing legislative and regulatory frameworks and the dichotomy between desired use case (for example, payments) and actual use case (speculation or investment) creates challenges. Absent an internationally agreed taxonomy, this paper will use four broad categories that have been adopted by many financial regulators globally:[15]

- **Unbacked crypto assets.** These crypto assets are transferable, primarily designed to be used as a medium of exchange, and although they are often decentralized, there are examples of unbacked crypto assets that are centrally issued and controlled. Most unbacked crypto assets are currently used for speculation and not for payment purposes. Prominent examples include Bitcoin and Ether (although in some jurisdictions with broad definitions of securities, these might be considered security tokens)
- **Utility tokens.** These tokens 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. For example, a tokenized store card or certain gaming tokens might be considered types of utility tokens.
- **Security tokens.** Although the definition of a security token varies across jurisdictions, these are tokens that provide the holder with rights like that of a traditional security, for example, the right to a share in the profits of the issuer.

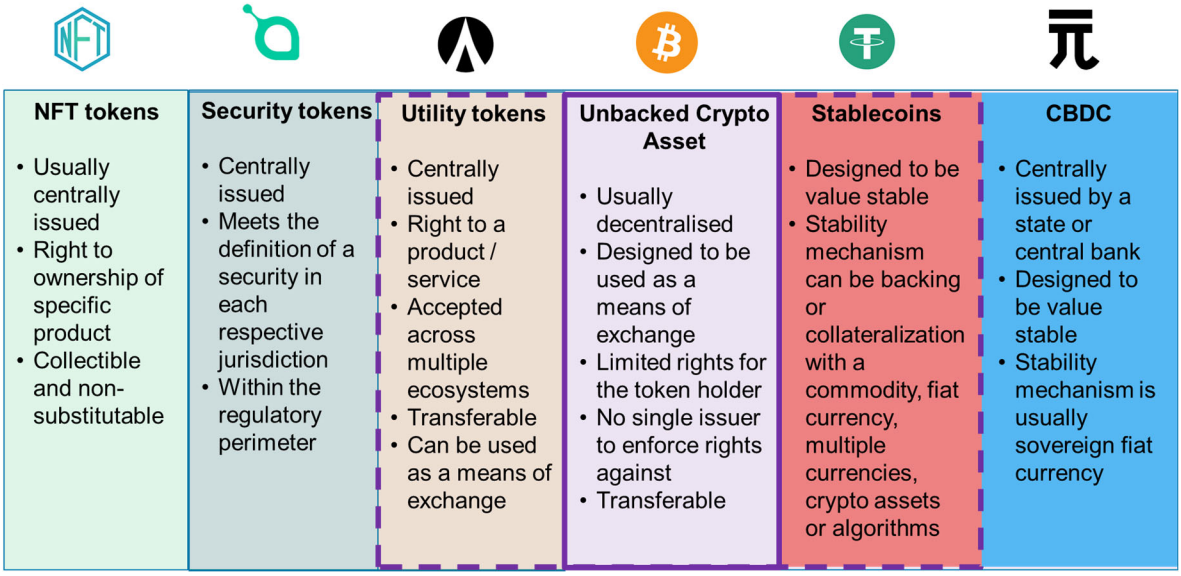
[13] See the glossary in Bains (2022).

[14] HODL refers to a buy and hold strategy in the context of crypto assets.

[15] The four categories delve into the final "cryptocurrency" category introduced by Adrian and Mancini-Griffoli (2019). For further discussion on taxonomies, see BIS (2021).

- **Stablecoins.** This type of crypto asset aims to have a stable price value. This objective is normally[16] pursued by the crypto asset being linked to a single asset or a basket of assets, for example, fiat funds, commodities such as gold, or other crypto assets. Prominent examples include Tether, Binance USD, and USD Coin. Our companion paper, "Regulation of Stablecoins," has a more in-depth discussion on the risks and regulatory responses to stablecoins.

Figure 1. A Taxonomy of Crypto Assets, NFTs, and CBDCs and Scope of This Note



Crypto assets are varied, and this note is focused on unbacked crypto assets, although the paper's regulatory considerations on the broader ecosystem may apply to a wider range of crypto assets.[17] Utility tokens, security tokens, stablecoins, and central bank digital currencies (CBDCs), in their various forms, are out of scope of this paper, as are issues specific to financial integrity, which have been covered by previous IMF Fintech Notes.[18] This note does not cover CBDCs or payment infrastructure issues. Although some CBDCs might be cryptographically secured representations of value deployed on blockchain networks, they are not usually considered a form of crypto asset because the term generally refers to private assets issued by private entities or individuals, whereas CBDCs are instruments issued generally by public institutions such as central banks. That said, in certain CBDC models (so-called "intermediated CBDC"),[19] regulatory issues explored in the note will be relevant for various entities in those ecosystems (for example, wallets). This paper does not explore security tokens because many jurisdictions have taken the approach of extending their traditional securities regulation to them while

[16] Stablecoins can also seek stabilization using a mechanism other than being linked to an asset, for example, through an algorithm. These "algorithmic" stablecoins are mainly used in decentralized finance (DeFi)

[17] Regulatory approaches to DeFi were discussed in other IMF publications and will not be explored in depth. As set out in IMF (2022), regulation should focus on elements of the crypto ecosystem that enable DeFi, such as stablecoin issuers and centralized exchanges. In this sense, the considerations in this paper will also be useful and applicable and can be a conduit for regulatory oversight of DeFi.

[18] Schwarz and others 2021a and 2021b.

[19] Soderberg and others 2022.

experimenting with back-office settlement and record keeping. It also does not discuss non-fungible tokens (NFTs), since they usually fall outside the scope of financial regulation in line with "same activity, same risk, same regulation."[20]

The Growth of Crypto Assets

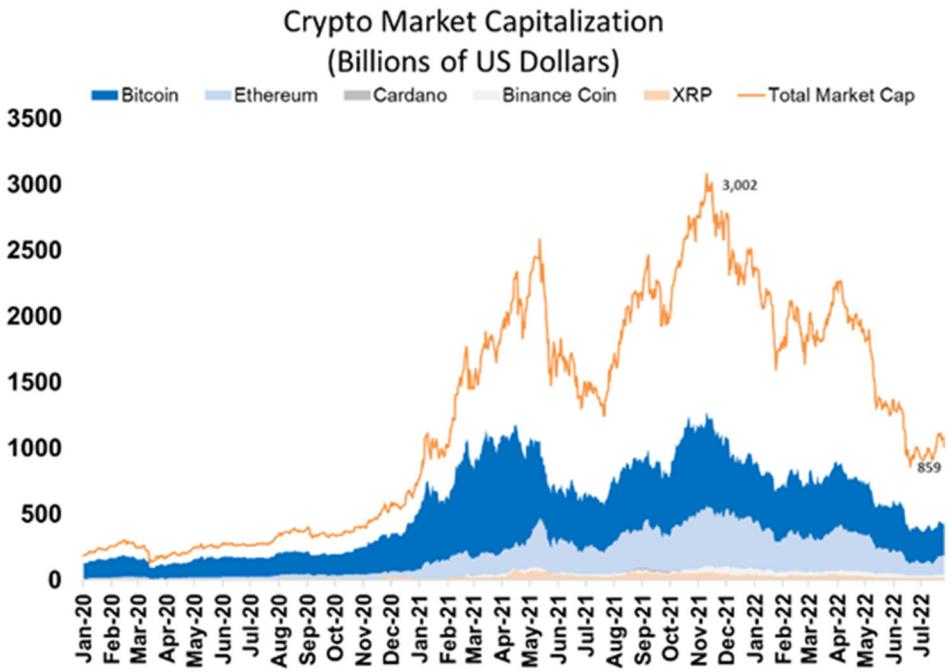
Crypto assets have grown and diversified substantially since Bitcoin was first launched in 2009 and have evolved to serve different purposes and economic functions. After reaching a market capitalization of $1 billion in 2010, the crypto asset market had grown to almost $3 trillion in 2021 before falling to around $1 trillion in mid-2022 (see figure 2), although a considerable amount of wash trades might hide the true figure, which is likely to be substantially lower. This volatile growth has been led primarily by Bitcoin but supported by the increasing proliferation of crypto assets, some of which have grown proportionately quicker.[21] The largest proportion of this market by capitalization are unbacked crypto assets, with stablecoins accounting for roughly $150 billion. The market now supports more than 10,000 different types of crypto assets and, while promoting decentralization and disintermediation, actually creates opportunities for new centralized intermediaries, such as certain issuers, crypto asset exchanges and crypto asset wallet providers, and broader ancillary products like lending and investing (many of which are also carried out by centralized entities). Although most crypto assets are primarily designed to be used as a means of exchange, globally less than 30,000 merchants accept crypto assets as payment.[22] End users are more likely to focus on holding crypto assets as speculative investments, rather than on spending crypto assets as payments. However, some entities are experimenting with different types of crypto assets to improve efficiencies in areas such as cross-border transactions.

[20] Unless they are fractionalized into their constituent parts and their underlying structure or arrangements become similar to financial products or services, for example, collective investment schemes.

[21] "Today's Cryptocurrency Prices by Market Cap," CoinMarketCap, https://coinmarketcap.com/.

[22] "Crypto ATMs and Merchants of the World," Coinmap, https://coinmap.org/view/#/world/14.43468022/-17.22656250/2.

Figure 2: The Growth of Crypto Assets by Market Capitalization



IMF (2021) identified a significant increase in correlation between crypto assets and financial assets during periods of market stress. The correlation between crypto assets and other financial assets has increased over time, driven, in part, by the continued involvement of institutional holders that are affected by common factors (Iyer 2022). Exposure to crypto assets in the banking system and other nonbank sectors[23] is growing, albeit from a low base.[24] Exchange-traded funds linked to Bitcoin futures have been introduced in the United States, which could provide regulatory clarity on investment in such instruments by regulated financial institutions and so broaden the user base, including other institutional users (such as pension funds and insurers). Some regulators have clarified existing requirements for banks, which in turn has facilitated more active engagements by commercial banks in crypto asset businesses (such as custodian services for unbacked crypto assets).

The financial stability risks of crypto assets may not yet be globally systemic, but the growing systemic implications can already be seen in some countries. IMF (2021) noted that risks should be closely monitored given the global implications and inadequate operational and regulatory frameworks in most jurisdictions. FSB (2022) stated that as markets are fast evolving, they could represent a threat to global financial stability because of their scale, structural vulnerabilities, and increasing interconnectedness with the traditional financial system. The Basel Committee on Banking Supervision

[23] According to Coinbase and Goldman Sachs, 10 percent of the 100 largest hedge funds were using their platform to invest in crypto assets as of the second quarter of 2021, 15 percent of family offices have exposures to crypto assets, and close to half of these offices are potentially interested in initiating exposures.

[24] BCBS recently noted that "banks' exposures to crypto assets are currently limited" (BCBS 2022).

(BCBS) (2022) shared the view that the growth of crypto assets and related services has the potential to raise financial stability concerns and to increase risks faced by banks. Furthermore, retail users in emerging markets and developing economies are more likely to own crypto assets than are advanced economies.[25] Trading volumes of crypto exchanges that operate only in emerging markets and developing economies have increased and are comparable to the activity on local stock exchanges and domestic interbank foreign exchange transactions. The growing systemic implications of crypto assets warrants immediate regulatory action in some countries.

I. The Crypto Ecosystem: Risks and Regulatory Responses

This section explores the key components within the crypto ecosystem, the risks that they might generate, and potential regulatory responses. Although the growth of crypto assets has led to the proliferation and diversification of entities within the crypto ecosystem, certain important entities serve key functions within the ecosystem that are both sources of, and vulnerable to, risks. In some instances, these entities might be carrying out multiple activities, which may potentially make them systemic market infrastructures in the future. This section explores risks generated by those entities and regulatory considerations with a focus on issuers (that create or "mint" crypto assets), crypto asset service providers such as exchanges (that facilitate the exchange of crypto assets but can also offer lending and investment services), wallet providers (that store crypto assets and can also be the transfer function), validators or miners (that ensure a consistent, honest, and true ledger), underlying technology (the DLT on which crypto assets are deployed), and regulated financial institutions (that might have exposures to crypto assets). Crypto asset service providers are also carrying out multiple activities, for example, facilitating the exchange of crypto assets, storing client's crypto assets, providing lending and leverage services to the users, offering transfer services, and clearing and settlement for off-chain transactions.

Issuers

The issuance of unbacked crypto assets is frequently decentralized, and often issuers are not known, which raises risks and regulatory challenges. Although decentralization of issuance serves the intended purpose of disintermediating financial services with no central authority and a greater "democratization" of value, it also raises risks for users and broader markets. Decentralization makes it difficult to design a regulatory framework targeted at issuing entities. Most regulators have limited their response to broader consumer warnings and/or user education. The lack of known issuers often results in little information or disclosure on the unbacked crypto assets being issued, and it can be difficult to determine with accuracy the type of technology being used, the intended purpose of the token, or any beneficiaries of profits or income that might be derived from the sale of the token.

[25] Katharina Buchholz, "How Common Is Crypto?," *Statista*, March 17, 2021, https://www.statista.com/chart/18345/crypto-currency-adoption/.

Crypto assets issued on a decentralized public network are less likely to have a single point of failure risk, with nodes and validators potentially spread around the world. This can improve security as well as reduce the need for trust in a single entity. However, such networks are still vulnerable to some cyberattacks (such as 51 percent attacks),[26] and centralized components like crypto asset exchanges and wallet providers are also susceptible to cyber and operational risks. Risks of selfish mining and miner extractable value in certain networks could also lead to risks to market integrity. Even when issuers are decentralized, a governance body might still exist, comprising those with the largest holdings of tokens or tokens with specific governance rights. This can lead to elements of centralization in most crypto assets, which can reintroduce a single point of failure—or require trust in a single entity.

Risks also arise from the different ways in which crypto assets are issued and distributed. There are several ways to create and issue crypto assets, the three most popular being pre-mining, continuous mining, and a hybrid approach. Crypto assets are usually distributed in five main ways: pre-token sale,[27] initial coin offering or token sale,[28] mining, airdrops,[29] and forks. Pre-mining is where all the tokens are created in one batch as a single event, whereas in continuous mining, crypto assets are likely to be created on an ongoing basis or at frequent intervals for either a designated period or until a set deadline. Pre-mining has the potential to create some consumer risk; price manipulation through pump-and-dump" schemes is a key concern.[30] Although all these methods pose some risks to consumers, initial coin offerings have been the most controversial (as covered in Cuervo and others, 2020). However, their level has substantially decreased over the past years.

Crypto asset white papers and other marketing material often lack clarity, and the technological complexities and hype make crypto assets a difficult-to-decipher product for users. The use of white papers in crypto assets dates to the launch of Bitcoin by Satoshi Nakamoto. White papers aim to provide information on the crypto asset, including its developers, objectives, and other technical information. White papers vary in their quality, with many having incomplete or inaccurate information, and in some cases, no white paper exists at all. Marketing of crypto assets often overstates the benefits, while rarely setting out associated risks. The channels for marketing are usually digital, with little oversight or requirement of having these promotions approved by a public authority.

When building a regulatory framework targeting the offering of crypto assets by issuers, authorities could focus on the following elements:[31]

- **Publication of white papers.** White papers form an important part of the disclosure process and should provide markets and users with clear, accurate, and understandable explanations of the crypto assets issued and other essential information such as key personnel and any governance

[26] A 51 percent attack happens when a malicious user in a network acquires control of a blockchain's mining capabilities.

[27] Tokens are sold to interested parties at an agreed price ahead of wider circulation.

[28] A method of fundraising for early-stage crypto asset projects where tokens are sold to speculators in exchange for fiat currency, stablecoins, or more established crypto assets.

[29] Issuers send free tokens to community or broader members as a way of marketing new or existing tokens or to ensure a wide distribution.

[30] This refers to the practice of a group artificially raising the price of relatively illiquid crypto assets through concerted buying. As the price rises, other retail users become interested, which continues to drive up the price. At this point, the initial group will sell all their holdings at the higher price, leaving later investors with a loss as the price falls.

[31] Note the reports and consultation papers published by IOSCO, which contain helpful considerations in regards to retail distribution of crypto assets (https://www.iosco.org/library/pubdocs/pdf/IOSCOPD695.pdf) and investor education in crypto assets (https://www.iosco.org/library/pubdocs/pdf/IOSCOPD668.pdf).

arrangements. The language contained in white papers should be easy to understand and should also provide users with the ability to analyze the technical details behind the crypto asset, the DLT on which it operates, rights conferred by the token, the problem the crypto asset was designed to solve, how it will be issued, associated risks, complaints procedures, and information about the issuing team.

- **Notification.** Some authorities ask to be made aware of white papers through a notification process or as part of a registration or licensing process. Notification can allow authorities to better understand the size of the local crypto asset market and to remain informed on new products and developments. Many authorities also consider proportionality when building a framework for issuance, particularly where the offering is small or restricted to certain users or when it involves unregulated crypto assets such as NFTs.
- **Suitability tests.** Where crypto assets are issued directly to end users, some authorities require issuers to ascertain the suitability of users. Issuers are asked to consider whether it is appropriate to offer their crypto assets to retail users, and if so, how the issuer is taking into consideration the needs and requirements of different users. Suitability tests should help firms understand user risk appetite, education, and capacity to absorb losses.
- **Fair and accurate marketing.** Often, marketing of crypto assets places a disproportionate focus on benefits, with little communication of associated risks. Inexperienced consumers may therefore purchase crypto assets that are not a suitable investment for them. Some regulators have introduced or are considering requirements related to crypto asset marketing (Box 1). These may include requiring that marketing by the issuer reflects information contained in the white paper and is communicated in a way that users can understand. Marketing information should make clear whether the product has any regulatory protections in the local market. Some jurisdictions require marketing related to crypto assets to be approved by the regulator, whereas others have proposed requiring local regulated entities (such as banks) to approve such marketing. This creates new revenue opportunities for these entities, while transferring some of the risk. In some jurisdictions, authorities have banned unregulated crypto asset firms from marketing their materials to domestic consumers, although this can be difficult to enforce.
- **Consumer education.** As detailed in the BFA, developing adequate financial and technology literacy programs (for example, through initiatives at different education levels, tailored communication, and outreach programs) should be considered a foundational element of any regulatory initiative. Some regulatory authorities are already carrying out consumer analysis to determine the level of crypto literacy to better design the appropriate response.

Box 1. Regulating Crypto Asset Promotions

- **United Kingdom:** The UK Crypto Assets Taskforce, consisting of HM Treasury, the Bank of England, and the Financial Conduct Authority (FCA), published a report in 2018 that found that misleading advertising and a lack of suitable information were key consumer protection issues in crypto asset markets. The report found that crypto asset advertising, which is often targeted at retail investors, can often overstate benefits and rarely warns of volatility and risks. The

FCA's consumer research into crypto assets found that 31 percent of crypto asset holders that saw an advertisement were encouraged to buy as a result. In January 2022, the UK Treasury proposed bringing crypto assets within its Financial Promotions Regime. This means the promotion of qualifying crypto assets will be subject to FCA rules in line with the same high standards that other financial promotions such as stocks, shares, and insurance products are held to. The key activities are dealing in securities and contractually based investments, arranging deals in investments, managing investments, advising on investments, and agreeing to conduct specified kinds of activities.

- **Singapore:** In January 2022, the Monetary Authority of Singapore published guidelines to restrict the marketing of crypto assets in Singapore. The guidelines limit the public marketing of crypto assets in areas like public transport, broadcast media, third-party websites, social media platforms (including the use of "influencers"), public events, or road shows. Promotions include the use of crypto ATMs, which are also considered a form of crypto asset marketing. In essence, the Monetary Authority of Singapore's approach limits crypto asset promotions to an entity's own corporate website, official social media accounts, and mobile applications while ensuring such marketing is not "trivialized."
- **Spain:** In January 2022, the National Securities Market Commission published a circular that set out new rules for crypto asset marketing, including the presence of risk warnings as well as ensuring the promotion is "clear, balanced, and fair." These rules apply to the mass marketing of crypto assets.

Crypto Asset Exchanges

Crypto asset exchanges facilitate the buying and selling of unbacked crypto assets and provide much wider services than traditional securities exchanges. Many of the largest and most popular crypto asset exchanges are centralized intermediaries that in practice negate the aim of decentralization and disintermediation that formed the basis of innovation in this space for early crypto proponents. They reintroduce both centralization and trust in a single counterparty.

Although some important differences exist in the way they operate, crypto asset exchanges raise many similar issues to those of securities exchanges. Crypto exchanges differ from securities exchanges in three main ways (although such differences vary across jurisdictions): They typically permit direct access by retail users; they might, in some cases, trade off their own inventory and provide liquidity rather than match buyers and sellers; and they may also provide custody services (through their wallets) to deliver quicker off-chain settlement. Off-chain transactions do not leverage any of the security features of blockchain but instead expose users to credit and counterparty risk of the service provider, which are subject to single point of failure, cyberattacks, and loss of funds. Some crypto asset exchanges resemble stock trading venues, but others may be directly accessed by clients and therefore resemble more a market intermediary. This means that on top of traditional securities trading concerns—operational issues, orderly trading, manipulation, transparency, and so on—authorities may also have to think about specific risks arising from the nature of the exchanges and from the provision of custodial services.

Certain crypto exchanges might also issue their own crypto assets, including stablecoins, which can give rise to conflicts of interest.

Although crypto asset service providers have shown signs of improving their operational and cyber resilience, large and well-known firms have been hacked.[32] The unique features described previously (trading off own inventory and offering both exchange and custody services) can make crypto asset exchanges alluring targets for cybercrime. Some of the largest loss incidents involved several hundred million US dollars per incident, leaving providers bankrupt and users at a loss. Even in cases where compensation was ultimately fully paid out within several months, users were not able to use the tokens that were stolen for extended periods of time. During the two large downturns in the crypto asset market (2018 and 2022), many users could not access their crypto assets to exit their positions because of a combination of operational failures or measures taken by exchanges to block certain crypto asset transactions.[33]

Some exchanges are trying to mitigate cyber and operational risk by contracting cyber insurance coverage, keeping tokens in cold wallets, or creating separate compensation funds.[34] The terms and conditions for crypto asset insurance can vary from policy to policy, with some policies delivering little or no benefit. Operational risks extend further than extreme or stressed events like hacking, as it is well documented that users have found it difficult to withdraw or exchange their crypto assets for fiat currency even in normal times. Most wallet providers keep most of their hosted crypto assets offline in cold storage, but these crypto assets must be connected online before they are able to be transferred. The increased focus on improving security has meant that a smaller proportion of hacking events occur on centralized exchanges and wallets now than in recent years.

The crypto asset market is still relatively new and vulnerable to market abuse risks. Some of the intermediaries, such as wallets and exchanges, are relatively unsophisticated, or they may lack the systems and controls of regulated institutions. This can lead to risks to market integrity through information asymmetries. The price discovery function of the market is relatively weak, and therefore such assets are at high risk of market manipulation.[35] Anecdotal evidence suggests that some large crypto asset exchanges allow users to conduct wash trades, which inflates trading volumes and drives up price.[36] Many of these exchanges are also the largest holders of crypto assets and so might exercise disproportionate control of applications when engaging with networks that use Proof-of-Stake consensus.[37]

[32] Although investment in security has led to a decrease in the number of hacks of centralized exchanges, large hacks still occur. In December 2021, the BitMart exchange was attacked, with hackers stealing $200 million of crypto assets (largely SafeMoon). In January 2022, a hot wallet at the LCX exchange was attacked with losses of approximately $7 million of crypto assets across eight different types of tokens.

[33] IMF, *Global Financial Stability Report: COVID-19, Crypto, and Climate: Navigating Challenging Transitions*, Chapter 2, October 2021, https://www.imf.org/-/media/Files/Publications/GFSR/2021/October/English/ch2.ashx.

[34] Coinbase has insurance coverage of all client positions held in its hot wallet by a large reinsurer. If Coinbase were to suffer a breach of its online storage, the insurance policy would cover any customer funds lost as a result (see How is Coinbase insured?). Binance established a secure asset fund for users and is reported to allocate 10 percent of all trading fees into it. The secured asset fund for users is intended to offer protection to users. See https://academy.binance.com/en/glossary/secure-asset-fund-for-users.

[35] Stablecoin users and investors may be less exposed to market integrity risk.

[36] A wash trade is a form of market manipulation in which an investor simultaneously sells and buys the same financial asset to inflate the volume traded of the asset, thus creating misleading information and activity in the marketplace.

[37] "Bitcoin Rich List," BitInfoCharts, https://bitinfocharts.com/top-100-richest-bitcoin-addresses.html.

Illiquidity could make markets vulnerable to other forms of market manipulation, such as pump-and-dump schemes, and whale trades. Even where trading is subject to regulation and surveillance by regulated exchanges, market manipulation enforcement is challenging because of the often pseudonymous, cross-border, and decentralized nature of the transactions. Market manipulation schemes are more problematic in crypto asset markets given the relative opacity of the market and illiquid nature of many (smaller) crypto assets. This could pose serious risks should asset tokenization[38] become more commonly used and expand to traditional assets in the future.

In many countries, crypto asset exchanges can avoid conduct or prudential regulation by listing only unbacked crypto assets. Existing conduct and prudential regulatory frameworks generally extend to exchanges that list security tokens but not to those that list unbacked crypto assets. Many jurisdictions have not developed conduct or prudential regulatory frameworks specific to crypto asset exchanges because of the small size of the local market, competing priorities, and/or a lack of skilled personnel. The cross-border nature of crypto asset exchanges also creates questions around extraterritoriality, notably when exchanges list only unbacked crypto assets. Some regulatory oversight of exchanges may exist, but generally regulation falls short of a substantive conduct or prudential framework.

The work of IOSCO on crypto asset exchanges is particularly relevant. In February 2020, IOSCO published its final report on issues, risks, and regulatory considerations relating to crypto asset exchanges.[39] A later section in this paper considers the case in which these exchanges might become systemic and offer clearance and settlement services, in which case further oversight is warranted. When building a regulatory framework for crypto asset platforms,[40] the IOSCO report should form the basis for a regulatory response, with additional considerations that reflect local needs, including the following:

- **Governance requirements for platform operators, including prudential requirements.** Robust governance would be established by fit and proper senior management and control functions. In addition, having the necessary resources to run a platform can provide certain assurances on the reliability of the business. Any capital requirements would need to consider whether the operator will function bilaterally, that is, being counterparty to each transaction, or multilaterally by matching buy-and-sell orders. In the first case, counterparty risk on the part of the operator calls for risk-based capital requirements.
- **Requirements regarding access to the platform.** Protecting the orderly functioning of trading usually requires a certain control over who accesses and uses the platform. Crypto asset platforms should have appropriate processes and controls that consider whether the platform allows direct retail access—in which case, the platform would not be able to rely on the due diligence of intermediaries.[41]
- **Requirements for the robustness, resiliency, and integrity of operating systems.** One of the main vulnerabilities of crypto-asset platforms has been cyberattacks. Adequate processes and

[38] This refers to the digital representation of data on DLT that reflects nonnative (that is, non-DLT) assets. These can be physical or digital.

[39] IOSCO 2020.

[40] Some global bodies such as IOSCO and certain authorities use the term “platform” or “trading platform” when referring to crypto asset exchanges.

[41] Securities exchanges are typically accessible only to intermediaries; therefore, members of the platform are regulated entities who, in turn, oversee retail clients’ due diligence requirements (including AML/CFT and suitability).

controls can help protect them from hacking or theft and can provide reassurance that they are otherwise robust and resilient enough to provide trading integrity.

- **Market integrity requirements.** Crypto assets are prone to manipulation because of their high volatility, potential conflicts of interests or concentration issues, and low level of disclosure. Authorities should consider what market abuse rules and surveillance mechanisms should be in place to adequately protect users.
- **Transparency requirements.** To promote the efficiency and integrity of trading, it is important to understand the extent of pre- and post-trade information, its availability, its method of dissemination, and whether it is available on an aggregated basis with other platforms trading the assets. Authorities should consider these elements to determine whether trading information on crypto assets is reliable, timely, and available to the public on a nondiscriminatory basis. Additionally, consideration should be given to the availability and transparency of platform rules and procedures, including order processing and how errors and cancellations are handled.
- **AML/CFT requirements.** Platform operators should be expected to ensure they comply with applicable Financial Action Task Force (FATF) standards for AML/CFT. This monitoring could be developed in-house or might be delegated to a third-party provider; however, in these instances, any regulatory risk should reside with the party offering crypto asset services.
- **Products offered in the platforms.** Platforms may have different approaches to how they determine which assets can be accepted for trading. Authorities need to consider what requirements or criteria are being applied. As discussed in the previous section, to ensure adequate disclosure to users of crypto assets, there should be clear expectations regarding availability of information on products traded, including risks. This is particularly relevant in platforms with direct retail client access. Authorities should consider whether a need exists for regulatory determination of the types of assets that can be accepted for trading or if they should be otherwise involved in the process of product listing.
- **Conflicts of interest.** Where exchanges offer multiple services (such as issuance, exchange, lending, and storage), robust governance framework and disclosure requirements should be put in place to address conflicts of interests. Furthermore, to ensure that conflicts of interest are mitigated, regulatory authorities should consider whether exchanges should have a functional or legal separation of exchange and custody services.
- **Greater prudential requirements for off-chain transactions.** Where crypto asset exchanges conduct significant off-chain transactions, the end users could be subject to greater risks around cyberattacks, loss of funds, and a single point of failure. Here, exchanges might be carrying out several functions that might ordinarily be delivered by the blockchain such as clearing and settlement. In these instances, crypto asset exchange should be subject to greater prudential requirements. Where these exchanges and their activities are considered systemic, the Principles for Financial Markets Infrastructures may also apply.

Wallet Providers

Custody of unbacked crypto assets takes place via wallets that can be varied in their design and operation, with implications for security and risks. The ownership of crypto assets relies on knowing the

private keys stored in the wallet. If a wallet (and therefore private keys) is lost, then the crypto assets "stored" in it are unrecoverable. In terms of custody, a wallet can be managed by the users themselves or delegated to a third-party custodian (that is, a "wallet provider"), which is often a crypto-asset exchange, but it can also be a nonexchange third-party service provider. When the private keys are hosted by a third-party wallet provider, centralization is reintroduced with users no longer in control of their crypto assets, and although the risks of "losing" a wallet are reduced, the risks of cyberattacks, sharing of data, and transactions or accounts being blocked may increase.

Wallets can be classified as "hot" or "cold," with implications for storage and transfer. Hot wallets are kept online, and cold wallets are kept offline. In addition to their role in storing private keys, wallets can also be used as a transfer function for peer-to-peer transactions. Cold wallets can be as simple as a paper put in a deposit box or an encrypted file on a USB drive. Most users and crypto asset exchanges alike use cold wallets for storing most of their crypto assets and keep only what is needed for transactions in the short term in a hot wallet. Hot wallets allow for the quicker transfer of crypto assets in peer-to-peer transactions. There is little real difference between cold and hot wallet technologies. A hot wallet becomes cold upon disconnecting it from the network and vice versa.

The use of hot and cold wallets to store private keys can give rise to a variety of risks. Cold and hot wallets face different types and degrees of risk. Hot wallets can be subject to hacking, particularly in the case of custodial wallets operated by third-party service providers. These wallets are likely to store the private keys of many customers and therefore provide an attractive "honey pot" for hackers. They might also be subject to greater operational risks because there is a reliance on the systems and controls of the third party for the token holder to be able to take control of their private keys. In the case of cold wallets, the risks of loss or physical damage to the wallet are greater than hot wallets, but cyber risks are eliminated until the user needs to use the wallet and so changes its status from cold to hot.

Risks around safeguarding and safekeeping of funds are particularly important in entities with storage and transfer functions. In the event that crypto asset wallet providers go bankrupt, and depending on the contractual arrangements in place, their clients' tokens could be comingled with the service provider's other assets—unless there is a clear legal and regulatory framework and robust arrangements to ensure appropriate separation of client assets and protection from the default of wallet providers. The lack of prudential and conduct regulation means that user funds might not be safeguarded in the same way as other financial products and services, for example, e-money or securities brokerage firms.

Wallets are the components of crypto asset systems that are most exposed to cyber risk, and so security is important. Specifically, attackers target the private keys in hot wallets, as obtaining them equates to impersonating the owner, allowing hackers to steal funds from corresponding wallets. Attacks against cold wallets, although much more difficult, are also possible. The security of the wallet is a crucial factor in the overall security of a crypto asset system. Wallet security requirements should be aligned with best practices in cryptography, with a focus on key protection and key lifecycle management controls. Importantly, because of the unclear delineation between cold and hot wallet technologies, requirements should go beyond technical details and should include principles-based requirements (for example, requiring that wallet protection measures be proportionate at all times to the security risk).

The provision of custody services by wallets is a critical component of the unbacked crypto asset ecosystem, hence regulatory responses should be suitably robust. Many provisions for crypto asset exchanges will be similar for wallet services, although given the role of wallets in storage and transfer,

additional requirements must be considered. When building a regulatory framework for crypto assets, many authorities ask wallet providers to consider the following elements:

- **Segregation and safekeeping of holdings.** In some jurisdictions, wallet providers are required to ensure that user holdings of funds or crypto assets are kept separate from the entity's own funds or crypto assets. Client assets should be restricted from reuse and/or lending without explicit consent from the users and appropriate compensations. This includes ensuring that wallet addresses for users are different to the entity's own wallet address. Funds might be kept in accounts with regulated commercial banks.
- **Operational and cyber resilience.** Many authorities require that wallet providers ensure a robust cybersecurity framework to keep custodied crypto assets safe. There have been many occasions where consumers were unable to access their holdings because of operational failures. Therefore, it is important that wallet providers have effective incident management procedures, which include the detection and classification of 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.
- **Keeping records of holdings.** DLT aims to streamline the administration of custodied assets by keeping a real-time record of holdings on the network. Many regulators require that wallet providers ensure such administration is secure, resilient, timely, and accurate. Wallet providers should be able to share with the user, on request or at regular intervals, any changes in their holdings. Reliance on DLT for record keeping can conflict with existing rules requiring centralized entities for record keeping (for example, the Central Securities Depositories Regulation in the European Union), and some authorities are considering how best to modernize these rules.
- **AML/CFT requirements.** Platform operators are expected to ensure they comply with applicable FATF standards for AML/CFT. This monitoring could be developed in-house or delegated to a third-party provider. However, in these instances, any regulatory risk should reside with the party offering crypto asset wallet services.
- **Minimum set of proportionate reporting requirements.** Authorities should consider subjecting wallet providers to some reporting and prudential regulation requirements, such as regarding risk management (including operational and cyber risk), protection of client assets, minimum capital, and liquidity (particularly in cases when the wallet service provider reuses the customer's crypto assets). Proportionality is an important consideration when developing reporting procedures, but given the risks generated by wallet providers, reporting may need to encompass all necessary information and frequency to mitigate those risks.
- **Adequate safeguards.** Regulatory frameworks might consider the need for wallet providers to have adequate safeguards, such as cyber insurance coverage, in the case of a hacking event, to mitigate risks for consumers. Such insurance could cover a minimum proportion of holdings as determined by authorities. However, authorities should have good oversight over the terms and conditions of such policies as their impact in the event of operational or cyber failure can be limited.

- **Wind-down arrangements and resolution.** Authorities might want to consider effective wind-down arrangements where a wallet fails. Appropriate segregation of client funds can reduce consumer harm in the event of a firm failure, while working with third-party providers and maintaining critical information technology infrastructure is also important. A compelling case can be made for the prudential regulation of third-party wallet service providers to afford a degree of protection for customers in relation to fraud and to mitigate contagion risk to other parts of the financial sector, although there is a significantly weaker case for certain types of protections like deposit insurance when the wallet stores unbacked crypto assets. By allowing a third-party custodian to store private keys, there could be legal uncertainty on the inclusion of crypto assets held in custody in the event of its bankruptcy if the customers' assets are exposed to the risk of comingling with those of other customers or those of the service provider.
- **Conflicts of interest.** Where wallet providers are part of a broader group, they must ensure that appropriate governance procedures are in place to ensure independent decisions on wallet services and no conflict of interest from other group activities within the group. Wallet services should provide for the best interest of wallet service users, and this includes transparency and disclosure requirements where any potential conflicts of interest (such as connections to other businesses, including exchanges) are clearly communicated.

Validators, Miners, and Underlying Technology

The use of DLT in financial services may bring considerable benefits but also unique risks that regulators should consider. When DLT is deployed in an open and permissionless manner, there is no single point of failure, which reduces operational and some cyber risks. DLT in many of its forms is immutable and transparent and can provide a clear audit trail for the transfer of data. Experiments by various market participants and regulatory authorities have shown the potential efficiency that could be leveraged across payments, settlement, and clearing within financial services.[42] However, different forms of DLT can give rise to different risks—including to financial stability. For example, risks are different depending on whether a blockchain is private and/or permissioned or public and/or permissionless. The former ensures that participants who can view and act on the data are known, whereas in the latter model, data distribution is more decentralized.

Private blockchains, especially those created by BigTechs and incumbent financial institutions, could contribute to fragmentation, concentration, and financial stability risks. These risks would be realized by creating closed ecosystems with little interoperability in key areas, such as payments infrastructure, that potentially provide critical services. This could lead to networks that are too big to fail.

Public blockchains, although more resilient to single points of failure, may still be susceptible to certain failures, including 51 percent attacks, selfish miner problems, or miner extractable value (depending on the consensus mechanism employed). Although work is being done to promote cross-network interoperability, most native crypto assets currently can operate only on their native blockchain networks. These cross-network bridges may themselves be single points of failure with $2 billion worth of

[42] Financial Conduct Authority, *Regulatory Sandbox Lessons Learned Report*, October 2017, https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf.

crypto assets being stolen from cross-chain bridges.[43] Even where a crypto asset is offered on separate networks, the crypto assets may not directly be fungible with their cross-chain equivalents. Elements of public blockchains might also be reliant on centralized entities. For example, some hosted nodes on certain public blockchains are reliant on the services of BigTech entities, whereas the networks themselves might rely heavily on common infrastructures for aspects such as the provision of full nodes.[44]

Authorities should consider the regulatory implications of different forms of technology. Global standard-setting bodies and regulatory authorities take a technology-neutral approach to regulation (that is, same activity, same risk, same regulation).[45] However, certain types of consensus mechanisms that underpin blockchains may inherently generate frictions with broader policy objectives and mandates, and a technology-neutral approach may not be sustainable going forward. For example, the use of proof-of-work mining requires significant energy and runs counter to the global aim of transitioning to a low-carbon economy. Other types of consensus mechanisms might generate concerns around security, transparency, or concentration. For example, although the shift from proof-of-work to proof-of-stake would improve energy efficiency and scalability, it could create excessive concentration of decision-making powers on crypto exchanges and wallet services providers, which may increase market integrity risks (Agur and others 2022). Conversely, consensus in private blockchains may be faster and cheaper, but it may centralize the ecosystem, create new entities that could become "too big to fail," and generate concerns around data privacy and protection (Bains 2022). Points of vulnerability, such as cross-chain bridges, should be considered by authorities as part of the unique technology risks of blockchains.

[43] "Vulnerabilities in Cross-chain Bridge Protocols Emerge as Top Security Risk," Chainanalysis, August 2, 2022, https://blog.chainalysis.com/reports/cross-chain-bridge-hacks-2022/.

[44] "Ethereum Mainnet Statistics," Ethernodes, https://ethernodes.org/networkType/Hosting.

[45] FSB 2017.

Box 2. Critical Service Providers

Some elements of the crypto ecosystem provide services that are critical to the ongoing operation of networks. Although marketed as decentralized, important points of centralization are inherent in many blockchains. Centralized entities, such as exchanges and wallets, can be easily circumvented using self-hosted wallets and potentially decentralized exchanges, but other elements are more difficult to avoid. For example, a third of hosted nodes on the Ethereum Network are hosted on Amazon Web Services,[46] 60 percent of all Bitcoin traffic runs through three internet service providers, and Tor routes traffic for roughly half of Bitcoin nodes.[47] Meanwhile, cross-chain bridges and oracles are a growing source of centralization driven by the growth of decentralized finance. The former allows the transfer of a representation of crypto assets between networks, whereas the latter allows decentralized algorithms to connect to off-chain data. Malicious actions, operational failures, or refusal to offer service along these points of centralization could generate significant risks for the smooth operation of blockchain networks.

The policy implications of these critical service providers are broader than financial regulation, but financial authorities should consider regulatory responses where appropriate. Risks generated by these points of centralization might require intervention by governments, competition authorities, or other sector regulators like telecommunications. Within financial services, supervisors will need to make clear regulatory expectations on operations by crypto-critical service providers to ensure they are aligned with applicable international standards. The expectation should help ensure the operational resilience of a crypto-critical service provider is held to the same standards as if provided, for example, by a financial market infrastructure's critical service provider or a third-party critical service provider.

At a minimum, in line with the PFMI (Annex F on oversight expectations applicable to critical service providers) and the Basel Committee on Banking Supervision principles for operational resilience and for sound management of operational risk, expectations on the critical service provider should cover (1) risk identification and management, (2) confidentiality and integrity of information and availability of provided critical services, (3) reliability and resilience of critical services, (4) effective technology planning, and (5) transparent communications with users. It is key that management of exposure to critical third-party and subcontractor service providers includes operational risk management frameworks, clear roles and responsibilities for operational risk management as well as communication lines with the critical service provider, comprehensive information security policies, tested business continuity plans, reliable exit strategies, and tested procedures for managing operational disruptions and incidents, including substitutability of service providers.[48]

Regulated Financial Institutions

Further institutionalization of crypto asset–related activities could increase transmission channels between crypto assets and traditional financial institutions. The BCBS recently issued a second consultative document on the prudential treatment of banks' exposures to crypto assets, which aims to standardize the treatment of crypto asset holdings (BCBS 2022). The proposed standards reflect the high

risk of some crypto assets, while taking a more proportional and technology-neutral approach to those that 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 for traditional assets, whereas 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 1,250 percent risk weight that would be applied to maximum long and short positions.

The high volatility of certain unbacked crypto assets warrants a conservative treatment on direct exposures, but indirect exposures should also be monitored. Regulated entities are vulnerable to loss from direct exposure to unbacked crypto assets because of their high volatility, although data suggest that such exposure remains limited for banks both in terms of number of banks exposed and the size of exposures (Auer and others 2022). Prudentially regulated financial institutions will likely need to follow a conservative approach, such as capital deductions or the imposition of high-risk weights, for their internal risk and capital management purposes. Robust segregation and separation between traditional and crypto business are desirable, although group-wide and step-in risk would also need to be considered even when crypto businesses are located in a separate entity within the group. Financial institutions should also monitor their indirect exposures. This could be through loans to crypto users, derivative exposures with crypto-asset exchanges, cyber insurance to wallet providers, and so on. Although such risks brought by indirect exposures are not the same as from direct exposures, they can be strongly correlated with market movement.

Other prudentially regulated financial institutions (such as broker dealers, asset managers, and insurers) need to manage their risks carefully. Some broker dealers are actively expanding their services toward unbacked crypto assets. Asset managers also provide investment products linked to crypto assets. Crypto-linked exchange-traded funds would need active market making by authorized participants, which are typically prudentially regulated financial institutions. Insurers could potentially increase their exposure to unbacked crypto assets in search for yield. Although those risks may be immaterial at this stage, strong interest among retail users (especially in emerging markets and developing economies) would likely encourage those institutions to offer products linked to unbacked crypto assets in the future. Therefore, authorities should enhance their communication with and monitoring of financial institutions to encourage prudent business decisions and enhanced risk management.

[46] "Ethereum Mainnet Statistics," Ethernodes, https://ethernodes.org/networkType/Hosting.

[47] Trail of Bits, *Are Blockchains Decentralized? Unintended Centralities in Distributed Ledgers*, June 2022, https://assets-global.website-files.com/5fd11235b3950c2c1a3b6df4/62af6c641a672b3329b9a480_Unintended_Centralities_in_Distributed_Ledgers.pdf.

[48] For additional considerations on third- and fourth-party risk management and concentration risk, see the newsletter on third- and fourth-party risk management and concentration risk (https://www.bis.org/publ/bcbs_nl28.htm).

Multiple Functions and Market Infrastructure

Increasing off-chain transactions suggest some centralized entities are taking the role of financial market infrastructures. In principle, in the crypto asset space, traditional financial market infrastructure tasks, such as clearing and settlement, are carried out by the underlying technology in a decentralized manner. Crypto assets were, in fact, designed to operate without traditional FMIs: Technology itself would be responsible for value transfer, record keeping, clearing, and settlement. Nevertheless, the growing importance of "off-chain" transactions through some centralized entities could mean that these entities are playing an important role in the crypto asset ecosystem. For example, such transactions will require that some crypto asset service providers offer clearing services and settlement services.

Additionally, crypto asset service providers are more likely to provide multiple services globally within one entity. In wider financial markets, key functions (such as exchange, custody, clearing, and settlement) have been provided by multiple and dedicated entities. However, in the crypto asset ecosystem, rapid "off-chain" clearing and settlement can occur as, unlike in traditional securities markets where there is separation between exchanges and custodians, these two functions are more likely to be delivered by a single entity. Furthermore, these crypto asset service providers may carry out additional services such as lending and payments, while large crypto exchanges can also operate globally without creating subsidiaries or branches in each jurisdiction.

The potential broadening of offerings and the growth of "off-chain" transactions could lead to crypto asset service providers becoming critical to the crypto asset ecosystem. However regulatory and oversight gaps may remain. To address their critical role, in some jurisdictions, certain crypto asset service providers could be considered or designated as FMIs (although unlikely in relation to unbacked crypto assets). Some differences stand out compared to traditional FMIs. First, traditional FMIs carry out critical non-substitutable services, whereas crypto users could replace one crypto exchange with a competitor or resort to "on-chain" transactions; therefore, the essential services could continue to be provided in the absence of these entities. Second, "off-chain" transactions might be considered "closed loops" which may not trigger FMI oversight. Appropriately addressing oversight of critical service providers remains an important issue.

Where crypto asset services providers carry out multiple activities or offer clearing and settlement services, greater prudential requirements are necessary. Depending on the scope of the activities provided, a regulator or supervisor may want to establish expectations for crypto asset service providers offering infrastructure-like services such as clearing and settlement. The expectations would support the overall objectives of safety and efficiency, including the implementation of greater prudential requirements across the entity that reflect increased risks generated by additional activities. Similar to traditional FMIs, crypto asset service providers can reach a level where they concentrate risk, which, if not properly managed, can contribute to financial system disruption and can trigger shocks throughout financial system. Where the activities of these entities constitute important infrastructure for financial markets or generate risks to broader financial stability, domestic regulators might determine they are systemically important.

Designation of a crypto service provider as systemic is at the discretion of authorities. In the case of FMIs, the key factor is the potential of an FMI to trigger systemic disruptions.[49] For stablecoin arrangements, for example, the systemic importance can be determined by domestic regulators based on such factors as size of stablecoin arrangement in terms of number of users and value or 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.[50] The process of identification and designation of crypto service provider as systemically important can be complex because factors should be viewed holistically by domestic regulators. It is unlikely that crypto asset service providers will reach such a level in most jurisdictions, but if they do, they would be subject to the PFMIs.

II. Building a Regulatory Architecture

Central banks, regulatory authorities, and international standard-setting bodies are looking more closely at regulatory frameworks for crypto assets. Some authorities have provided high-level guidance on their regulatory treatment of crypto assets, while a few have developed bespoke regulatory frameworks. The FATF updated its standards on AML/CFT in 2018 to cover virtual assets and virtual asset service providers. Activities covered by the FATF standards include exchange (between a fiat currency and a cryptocurrency or between cryptocurrencies), transfer, administration and safekeeping, and participation in and provision of financial services related to an issuer's offer and/or sale of virtual assets.[51] Some jurisdictions have since developed or adapted their AML/CFT frameworks to various extents to capture crypto assets and service providers. In the meantime, various standard-setting bodies have discussed potential approaches within their mandates, particularly regarding stablecoins, although few standards have been set on unbacked crypto assets. As noted, the BCBS is consulting on the prudential treatment of banks' crypto asset exposures.

The cross-border nature of crypto assets can make regulation, supervision, and enforcement particularly challenging. Many crypto asset service providers, such as wallets and exchanges, as well as some issuers, operate from offshore jurisdictions while providing services globally. Without a common global approach, entities might relocate to regulation- or tax-friendly jurisdictions and continue offering services to users located elsewhere. Similarly, the use of crypto assets in unregulated exchanges could facilitate circumventing capital flow management measures in individual jurisdictions. Although some authorities may be able to take enforcement actions across borders, most authorities do not have the resources or the mandate. In addition, regulatory actions may take longer to take effect across borders, leaving users exposed to risks. Regulatory frameworks for global financial entities and proposed

[49] More specifically, the PFMI specifies 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.

[50] See CPMI-IOSCO Guidance on Application of the Principles for Financial Market Infrastructures to Stablecoin Arrangements, Section 2.

[51] For details, see Schwarz and others (2021a and 2021b).

frameworks for BigTechs (that is, entity- and activity-based regulation based on a home or host jurisdiction split) could serve as a model to capture some of these cross-border risks.[52] However, in the absence of a global framework, national approaches to manage risks may provide a sensible alternative (Box 3).

The global regulatory framework should provide a level playing field along the activity and risk spectrum. IMF recently called for regulation that works at a global level.[53] This includes ensuring that key entities providing critical functions in the crypto asset value chain are authorized and licensed. Requirements should also be built around the actual economic functions of crypto assets in addition to their technical design and aims. Authorities should also clearly articulate requirements on regulated financial institutions concerning their exposure to crypto assets.

[52] For a fuller discussion, see Bains and Sugimoto (2022).

[53] Adrian, Tobias, Dong He, and Aditya Narain, "Global Crypto Regulation Should Be Comprehensive, Consistent, and Coordinated," IMF Blog, IMF, https://www.imf.org/en/Blogs/Articles/2021/12/09/blog120921-global-crypto-regulation-should-be-comprehensive-consistent-coordinated.

Box 3. Approaches to Unbacked Crypto Asset Regulation

- **European Union:** The Regulation of Markets in Crypto Assets (MiCA) forms part of the European Union's digital finance strategy and encompasses a broad array of crypto assets. Although the focus is on stablecoins, for other crypto assets, MiCA requires the onshoring of issuing entities as well as a notification regime for white papers and marketing. An onshoring and licensing regime is also proposed for key entities delivering critical functions such as exchanges and wallet providers.[1]
- **Japan:** In April 2017, the Payment Service Act was amended, and the Japan Financial Services Agency introduced a bespoke regulation to crypto asset service providers. The main requirements include clients' asset segregation, operational risk and cyber security management, Know-Your-Customer, internal audits, and minimum capital requirement. In May 2019, the law was further amended to expand the crypto regulation to other entities (wallet service providers) and to enhance requirements of crypto asset exchanges, including limitation (up to 200 percent) of the leverage provided to retail customers. The amendment also clarified the application of existing securities laws to security tokens. The Payment Service Act was further amended in June 2020 to introduce stablecoin regulations.
- **Switzerland:** In February 2018, Swiss Financial Market Supervisory Authority (FINMA) issued guidelines for initial coin offering and introduced three categories of tokens—payment tokens, utility tokens, and asset tokens. FINMA also clarified that tradable tokens at prefinancing and presale stage are generally not utility tokens but asset tokens and thus could be treated as securities. In June 2018, the Financial Services Act harmonized prospectus requirements across all securities (including asset tokens). In February 2021, the distributed ledge technology (DLT) amended several civil and financial market laws to enable the introduction of ledger-based securities on a blockchain and to provide rules for the segregation of crypto assets in the event of bankruptcy of crypto custodians.
- **United Kingdom:** In July 2019, the Financial Conduct Authority published its "Final Guidance on Cryptoassets," which sets out that security tokens (crypto assets that provide rights and obligations similar to "specified investments") fell inside its regulatory purview, whereas utility and "exchange tokens" (i.e., unbacked crypto assets) were outside of prudential and conduct regime. Since then, the FCA has conducted significant consumer research to better understand the crypto asset market. In April 2022, the UK Treasury set out its roadmap for crypto asset regulation. Although there was considerable focus on stablecoins, the paper proposed a sandbox regime for blockchain-based FMIs with a longer-term aim to extending the regulatory perimeter to cover crypto assets like Bitcoin. In January 2022, the UK Treasury proposed bringing crypto assets within its Financial Promotions Regime (see Box 1).
- **Albania:** In May 2020, Law no. 66/2020 on "DLT-based Financial Markets" legalized crypto assets in Albania for investment purposes. The law, also known as the "Fintoken Act," regulates the issuance of "Digital Tokens" and "Virtual Currencies" and the licensing, monitoring, and supervision of entities that are engaged in their distribution, trading, and custody. The Fintoken Act entrusts both the Albanian Financial Supervisory Authority (AFSA) and the National Agency

for Information Society (NAIS) as competent authorities as well as the Bank of Albania for stablecoins. The process for licensing crypto asset service providers relies heavily on third-party agents. These agents are themselves licensed as Digital Token Agents when focusing on the regulatory and financial compliance side by AFSA, and as Innovative Service Providers when dealing with technological compliance by NAIS.

- **Nigeria:** In February 2018, the Central Bank of Nigeria (CBN) issued a press release stating that crypto assets are not legal tender in Nigeria. In February 2021, the CBN wrote to regulated financial institutions that dealing in crypto assets and facilitating payments for crypto asset service providers was a prohibited activity. In May 2022, the Securities and Exchange Commission published "New Rules on Issuance, Offering Platforms and Custody of Digital Assets," which outlines that "digital asset offerings" are within the purview of the SEC and imposes requirements on "digital asset offering platforms" and "digital asset offering custodians."

[1] MiCA regulation is in a draft stage. When implemented, it will be combined with the existing e-money and payment services regulatory framework for specific services as well as existing market integrity and conduct for regulated entities.

Broad bans on crypto assets are likely to be ineffective in the long run, but targeted restrictions could help address immediate challenges while regulatory capacity is being built. Some jurisdictions are considering a spectrum of options from total bans to targeted restrictions. Total bans are likely to stifle useful innovation and are unlikely to be effective because unless they are globally agreed upon, implementation will be challenging.

Many crypto asset service providers operate offshore, and users can use virtual private networks (VPNs) to obscure locations, making enforcement of bans on crypto assets extremely difficult. Enforcement can be even more difficult for authorities with limited resources. For example, despite strict domestic restrictions, roughly 2 million Egyptians reportedly hold crypto assets.[54] Likewise, peer-to-peer transactions in crypto assets have grown in Nigeria despite tight restrictions.[55] Data also suggest that significant mining operations exist in China despite a blanket ban on crypto asset activities.[56] Nevertheless, restricting the use of crypto assets for certain cases might be a sensible short-term approach in the absence of the required capacity to regulate. For example, some jurisdictions have restricted the use of derivatives linked to crypto assets (for example, Japan, United Kingdom), whereas others have restricted the use of crypto assets for payments, although users are allowed to buy and sell crypto assets. Restricting or disincentivizing certain regulated institutions to enter crypto markets can have a dampening effect on crypto asset growth that may help authorities address rapidly growing systemic risks and gain time to develop comprehensive regulations. Administrative restrictions should not operate in isolation—they must be embedded in legislation to be enforceable, unauthorized operators should be proactively identified and sanctioned, and the criminal law framework should enable the pursuit of criminal activities involving crypto assets.

[54] Global Cryptocurrency Ownership Data 2021 - TripleA (triple-a.io)

[55] "Local Bitcoins and Paxful Nigerian naira (NGN) Combined Volume," UsefulTulips, https://www.usefultulips.org/combined_NGN_Page.html.

[56] "Bitcoin Mining Map," Cambridge Bitcoin Electricity Consumption Index, https://ccaf.io/cbeci/mining_map.

Considerations for Regulatory Frameworks across Crypto Assets

As crypto assets continue to evolve and transform financial services, authorities should take a proactive and holistic approach to regulation, based on a comprehensive and evidence-based assessment of risks. The BFA provides a general framework for regulators to engage with new technologies in financial services. Particularly relevant in the context of regulating crypto assets are elements V (monitor the developments closely), VI (adapt regulatory framework and supervisory practices), and X (develop robust financial and data infrastructure).

The soundness of the legal framework is a precondition for a strong regulatory framework for crypto assets. The BFA[57] sets out that legal certainty helps build confidence in the trustworthiness and reliability of financial products and services. Some legal aspects are specific to crypto assets. For example, legal certainty related to the nature and the extent of the rights of the holders could be lacking in many of those arrangements, and the general legal regime may fall short of providing the needed answers. Jurisdictions might consider these issues as part of their overall approach to regulating crypto assets, thus ensuring that the legal framework evolves with global financial markets and technologies.

Several steps need to be taken when developing a national regulatory framework for crypto assets:

- Authorities should first monitor developments to accurately gauge the size of the market and to identify areas of risk, which can be challenging given the lack of data available on crypto asset markets to allow authorities to gauge the size of the risks.
- Authorities should consider the risks of unbacked crypto assets as part of their broader regulatory and supervisory duties and determine whether the crypto asset market presents risks to their mandate that would reflect the considerable resources required to regulate and supervise crypto assets.
- Authorities should determine a clear scope for regulation, that is, which entities, crypto assets, and activities will fall within the regulatory scope.
- Regulatory development should be a collaborative effort of financial sector regulators and relevant government departments, taking into account guidance from standard-setting bodies and regulatory approaches in peer countries. Cross-sectoral collaboration is particularly important given the lack of legal clarity in many jurisdictions as well as the hybrid nature of many types of crypto assets. Such collaboration can occur through memorandums of understanding, working groups, standing committees, or joint taskforces such as the UK Crypto Asset Taskforce. Regulation may require authorities to shift from a technology-neutral approach to one that considers the specificities and risk of different technologies.
- Continuous assessment of risks will be needed to identify shifting risks and business models that may require updating regulations to ensure effective protection of markets, consumers, and financial stability. All of this is predicated on the availability and accuracy of relevant data to inform decision-making. Each of these steps is considered in more detail below.

[57] See element VIII of the Bali Fintech Agenda.

Monitoring

The ability to monitor developments effectively and accurately is a core part of the BFA, and the first step in developing a regulatory framework is obtaining information. Some regulators are already assessing the size and composition of their domestic crypto asset market as well as user knowledge and behavior. The crypto asset ecosystem can be monitored through business-as-usual supervision, dedicated horizon scanning tools such as innovation offices, and/or the use of supervisory technology like web scraping. Monitoring can also be done through outreach and engagement, such as consumer and market surveys. Information and analysis should cover the types of crypto asset service providers and types of issuers. For instance, it will be difficult to develop a regulatory framework focused on issuers if most crypto assets within a jurisdiction are issued in a decentralized manner or if crypto asset service providers are located offshore.

Prioritization

Regulators often face stretched resources, competing priorities, and little crypto asset expertise. They will therefore allocate scarce resources depending on their assessment of risks. Where crypto asset markets are small, some regulators have employed an active “wait and see” approach, preferring to focus on other areas of financial regulation, while keeping a close eye on developments using targeted outreach and engagement with the crypto asset community (for example, themed events, drop-in sessions). The resources needed to implement different regulatory approaches vary, and authorities should carefully consider the feasibility of a regulatory approach given their resource constraints. Authorities should also be mindful that developing a regulatory framework for crypto assets has the potential of legitimizing the market—which in turn could spur growth and further stretch regulatory resources.

Scope

The regulatory scope should be clear and focused on the critical functions of the crypto ecosystem. It is important that a clear scope is identified based on the risks generated by different entities and crypto assets. Although it is useful to have regulatory frameworks that cover the entire crypto ecosystem in the long term, in many jurisdictions, economic functions of unbacked crypto assets and certain types of stablecoins are likely to be most prevalent given their use as speculative investments, as access points for other crypto assets, and (for certain stablecoins) as stores of value. In many jurisdictions, those critical functions are supported by centralized entities, such as wallets, exchanges, and existing financial institutions such as commercial banks, brokers, and dealers. Therefore, greater oversight should be given to those entities as well as the exposures that regulated financial institutions (like banks) have to these crypto assets. Conversely, other types of crypto assets like NFTs and certain types of utility tokens remain niche, with unclear use cases that are unlikely to generate systemic risks in the near-term, and so they may not directly affect the mandates of financial regulators in their pure form (see footnote 26).

The scale of adoption and economic function of crypto assets should determine the appropriate regulatory and supervisory approach. Where usage of crypto assets is limited, a regulatory focus on user education and potentially consumer warnings may suffice, as risks to consumers are likely small. For example, consumer research in the United Kingdom has suggested that crypto assets are often used like gambling, but users do not speculate with large amounts or borrowed money (FCA 2020). Where crypto

assets are used purely for speculation—with some similarities to gambling—consumer protection issues may be better addressed by other government agencies, such as those responsible for gambling. In jurisdictions where crypto assets are not widely used as a means of exchange or store of value and regulated institutions do not have large exposures of crypto assets or do not service crypto asset service providers, the risks to financial stability or market conduct might also be small, and so developing bespoke regulation may not be a regulatory priority. However, although some jurisdictions may not deem regulation of crypto assets to be a domestic priority, if they host crypto asset service providers that serve consumers globally, then they should consider developing regulation in collaboration with their regulatory peers, including host jurisdictions. This analysis of economic functions and scale of use can allow regulatory authorities to focus on areas with the highest risks.

The multiple activities carried out by crypto asset service providers can inform and may warrant additional regulatory and supervisory action. Crypto asset service providers often carry out multiple activities that are likely to generate additional cumulative risks. Authorities should determine whether these entities are playing a role akin to a systemic infrastructure provider and should be regulated and supervised as such. Although some authorities may be able to mandate on-shoring of these entities to ensure supervisory oversight, others will need to rely on home regulators setting out strong prudential rules and carrying out robust entity-based supervision. Authorities should regulate all entities that carry out key functions in the crypto asset ecosystem.

Domestic Collaboration

Coordination among financial authorities is important to achieve respective mandates. Many regulators have broad mandates (such as consumer protection, micro- and macroprudential) and different priorities over their mandates. In addition, it is often the case that these mandates are allocated to multiple financial authorities. Therefore, any regulatory framework should be developed as a coordinated effort across financial regulators to achieve various and sometimes competing objectives.

The primary objective of regulation and supervision should be to promote the safety and soundness of the financial system. If the supervisor is assigned broader responsibilities, these should be subordinate to the primary objective and should not conflict with it. Depending on the economic conditions and needs of the local market, some authorities might have lower risk tolerance regarding financial stability, and if so, might allocate more resources to entities and activities that pose higher stability risks. Other markets may have a greater desire to increase financial inclusion and so might be more open to innovation (viewing competition as a way to not only better serve consumers but also to mitigate longer-term systemic risk). In either scenario, regulation needs to be tailored to the risks and to address all important risks discussed in this section.[58]

Close coordination between domestic authorities and other stakeholders can support effective regulation. In many jurisdictions, regulatory frameworks were developed sequentially, based on priorities and resources. Regular coordination among the relevant domestic authorities can facilitate a clear allocation of responsibilities. The potential for regulatory arbitrage, scarce expertise and resources, existing laws and regulations, and reputational risks should all be taken into account when determining

[58] For an example of the variety of regulatory agencies and mandates regarding crypto assets, see the FSB Crypto Assets regulators directory (https://www.fsb.org/wp-content/uploads/P050419.pdf).

which authority or authorities—including those with AML/CFT mandates—should regulate and supervise different aspects of crypto assets. It is also key that the assessment of risks and monitoring involve cross-sector coordination, as well as an ongoing dialogue with the industry and other key stakeholders. This would help authorities better anticipate risks in market developments and proactively seek appropriate responses.

Continuous Assessment of Risks

Although technology neutrality is conceptually appealing, in practice, monitoring and risk assessment will need to adapt to a changing landscape and risk outlook, including technology developments. Technology neutrality is conceptually appealing but difficult in practice as different technologies will have unique benefits and risks. Although most authorities aim to be technology neutral, it is often the case that different regulatory stances are needed depending on specific risks brought by the technology used. Where a specific type of crypto asset, or a DLT underpinning the crypto asset, creates risks to markets and consumers, authorities look to ensure such risks are mitigated. Likewise, where certain types of crypto assets or DLT can help deliver innovation that benefits markets and consumers, some authorities have supported their development. Furthermore, although the concept of same activity, same risk, same regulation is key, the very use of a novel technology (like DLT) can alter the risk profile of traditional assets (for example, through fractionalization, decentralization, availability of greater liquidity) and so unique risks may require bespoke regulatory approaches. Although a technology-neutral approach to regulation might be appropriate, supervisory approaches should consider the unique risks of different methods of delivery and operation, and authorities should be confident in identifying where particular types of technologies might challenge (or support) their objectives.

Understanding DLT networks and inherent risks can help authorities decide if and when a more technology-agnostic approach is needed. Upskilling staff or hiring DLT experts can help authorities better determine the underlying technology used to deliver many types of crypto assets and to accurately understand new risks that might be created. Although frontline supervisors may not necessarily need to review code, they will need to understand important differences that exist between different types of blockchain networks and different types of crypto assets. Many types of DLT work on the basis of fundamental trade-offs, some networks favor security and integrity, some focus on speed and efficiency, and some are designed to be transparent and auditable. Each has relative strengths and weaknesses in different areas of financial services and may be more, or less, suited to existing regulatory frameworks. Better understanding the underlying technology can help authorities determine, for example, risks from high energy consumption, risks of network failure (whether malicious or technological), operational risks, risks to financial integrity, and—if used as scale—risks to financial stability (Bains 2022).

Determining the geographic location[59] of crypto assets and activities is challenging, making international action key in the continuous assessment of risks. Domestic regulatory frameworks will need

[59] Although the issuing entity or the main IT system may be located in one jurisdiction, the main activities (such as marketing, solicitation) are generally conducted in the jurisdictions where the main investors are located. For example, in August 2018, a US district court applied the US Securities Exchange Act in the case of the Tezos Foundation. Although the foundation was established in Switzerland and the subject tokens were claimed to be created in Alderney, an English Channel Island, the court rejected the claim that the transactions occurred outside the United States based on the following four reasons: (1) the

to consider the cross-border and global accessibility nature of crypto assets to minimize regulatory arbitrage. Although regulation specifically targeting crypto assets would need to be tailored to jurisdiction-specific features, a consistent approach and international cooperation will be key to prevent and minimize regulatory arbitrage and potential inconsistencies in the application of laws and regulations. Domestic regulatory measures that do not consider cross-border issues and overseas regulatory measures may create opportunities for regulatory arbitrage. Active engagement is needed to identify cross-border considerations and to tackle potential regulatory arbitrage. International cooperation in enforcement will continue to be key for sanctioning and prosecuting crypto asset–related cases, and authorities should ensure they have the appropriate mechanisms to share information in the context of investigations and prosecution.[60] Finally, specific regulatory and supervisory colleges can help unite authorities in response to product launches and ongoing supervision in multiple jurisdictions at the same time.

Standard-setting bodies and international institutions are playing critical roles to ensure monitoring and assessment of risks, and the IMF can leverage its universal membership to provide guidance and support. Many authorities use cooperation networks and standard-setter initiatives to exchange information on developments in the crypto assets space and ensure they can effectively monitor new and developing risks. Many standard-setting bodies have specific committees that look at the risks of crypto assets (for example, IOSCO Fintech Task Force, FSB Financial Innovation Network, FSB Regulatory Issues of Stablecoins, BCBS Financial Technology expert group, and so on) and membership of such groups can help authorities share new developments and best practices regarding regulatory responses.

Considerations for Data Availability[61]

The fragmented growth of the crypto asset ecosystem coupled with the relative immaturity of the market means data are often unavailable or unreliable. Data in crypto asset markets are currently unreliable, incomplete, or fragmented across borders. As there are few global standards and no common taxonomy, data gaps are substantial. Reporting and disclosure by entities such as issuers, wallets, and exchanges are largely voluntary, lack uniformity, and are sometimes overstated. For most jurisdictions, regulatory data reporting by crypto asset service providers is limited to AML/CFT requirements or no reporting occurs at all.

Crypto asset data are normally limited to what is captured on chain and rely on accurate geolocation capture. Although public distributed systems tend to be transparent and immutable, that transparency extends only to those transactions recorded on chain. Where transactions occur off chain, which is mostly the case in centralized entities such as exchanges and wallets or on certain second-layer applications like the Lightning Network, they may be more difficult to track. Furthermore, the use of VPNs to access these centralized services can make accurate geolocation data more challenging. Most crypto asset issuers have little information about their users' profiles (either retail or institutional) and locations.

marketing website was located on a server in Arizona, (2) it was run primarily by an individual in California, (3) the marketing was almost exclusively targeting US residents, and (4) validating nodes were densely populated in the United States.

[60] Instruments like the IOSCO Multilateral Memorandum of Understanding (MMoU) have proven to be excellent tools to facilitate fast and efficient exchange of information between IOSCO member signatories for the prosecution of securities markets offenses. Experience in the design and use of the IOSCO MMoU could be helpful for the global community when determining potential need to develop mechanisms for the exchange of information in the context of enforcement of crypto asset regulation.

[61] See also the discussion in https://www.fsb.org/wp-content/uploads/P160222.pdf.

Data and insights help regulatory authorities determine whether there are material risks to consumer protection, market integrity, and financial stability. Better tools to understand the crypto ecosystem can help authorities determine whether the development of a regulatory framework for crypto assets should be a priority and how it can be effectively implemented. It can help authorities decide which approach to take, based on solid evidence.

More accurate, granular, and standardized data can help better gauge and manage risks. Data that can help determine domestic market size (such as volume of transactions, number and location of customers and service providers, number of domestic crypto asset issuers and service providers, and so on), consumer and user behavior (type of consumer, size of retail holdings), and composition of market (type of crypto asset entity in local market) can all help authorities better gauge and manage risks.

A common taxonomy can form the foundation of a more coherent and consistent regulatory approach to crypto assets globally. The fragmented approach to categorizing crypto assets is a significant inhibitor to the development of globally consistent standards and can inhibit the reliability and availability of data. Although different legislative frameworks are likely to capture individual tokens in different categories (for example, the broad nature of the Howey Test in the United States used for security tokens), a common taxonomy can ensure authorities have a standardized set of categories to understand the use and impact of crypto assets, identify relevant data, and collect useful information. The absence of common taxonomies and differences in the granularity of data collected mean that data capture might differ across jurisdictions.

In addition to a common taxonomy, data collection can be improved with strong home-host data sharing, extended regulatory coverage, and the use of new technologies. The reporting of crypto asset data is largely limited to voluntary reporting or reporting under the AML/CTF framework. Data collection should be made more consistent across borders, and collected data should be shared among relevant home and host authorities within existing legal frameworks. Extending regulatory coverage for conduct and prudential purposes might help authorities collect more accurate and reliable data from the entities that perform critical functions, such as crypto asset service providers, network administrators, and certain issuers.

Some authorities are beginning to work with blockchain analytics firms to better understand the flow of funds through a crypto asset value chain, and although significant limitations exist (for example, off-chain data collection and the use of VPNs), such an approach is a sensible first step. Some organizations are exploring concepts of embedded supervision that can allow authorities to directly interact with distributed networks, which improves their access to data while enabling them to monitor compliance in real time by viewing blockchain transaction data.[62] Although theoretically appealing, such an approach would initially be limited to authorities with the relevant resources and expertise, and a high initial investment could be required, with ongoing costs of maintenance and training. Furthermore, this investment would be limited to a niche use case that is blockchain regulation and may not warrant highest priority in those jurisdictions where the financial stability and consumer protection risks of crypto assets remain low. Finally, the use of privacy-enhancing techniques, such as zero-knowledge proofs and homomorphic encryption in data collection, might better allow authorities to view these data across borders while protecting individual user privacy and remaining compliant with data protection laws.

[62] See, for example, European Commission (2021) and Auer (2022).

Conclusions

Developing a robust and comprehensive regulatory framework for this quickly evolving industry will involve intense monitoring, a flexible approach, and domestic and global collaboration. The global regulatory framework should provide a level playing field along the activity and risk spectrum. Regulators need to continuously monitor the crypto asset landscape to understand the direction of industry developments. In this sense, ongoing efforts to address data gaps to monitor markets and potential contagion effects to the existing financial sector are welcome. Regulation should not be seen as stifling innovation but rather as building trust. As with the wider financial sector, regulation can instill trust in the business and foster a safer development of the sector by providing clear guidelines that remove uncertainty and foster confidence. Defining a clear scope is important, and the immediate focus should be on key entities that carry out core functions such as exchanges, wallet providers, and other centralized entities.

For crypto assets, it is important that key centralized entities that carry out core functions be licensed and authorized. Regulatory approaches should focus on key components and their functions to ensure those entities are licensed and authorized. Authorities might want to consider any unique risks—from the underlying technology to volatility, market awareness, product knowledge and understanding, and how the crypto assets are used. Although a technology-neutral approach to regulation might be appropriate, supervisory approaches should consider the unique risks of different methods of delivery and operation, and authorities should be confident in identifying where particular types of technologies might challenge (or support) their objectives. Regulators may also want to consider cross-sectoral issues that may need bespoke responses. Where entities are carrying out multiple activities, appropriate prudential requirements coupled with entity-based regulation and supervision will be needed to manage these additional risks. Where these entities are considered systemic, drawing guidance from the PFMI could be appropriate.

In jurisdictions where crypto assets are systemic, immediate action may need to be taken, including strengthening macroeconomic policies, but broad-based restrictions are unlikely to be a long-term solution. In the short term, in certain emerging markets and developing economies where crypto assets might already generate risks to financial stability, authorities should use existing regulatory powers to best manage any risks while a more comprehensive standards are developed at the global level. At the same time, in jurisdictions where residents use crypto assets (in particular, dollar-denominated stablecoins) as a way of hedging against inflation or currency devaluation risk, implementing stronger domestic macroeconomic policies—such as strengthening monetary policy credibility, ensuring central banks have independence from political and industry influence, ensuring traditional financial institutions are held accountable for their failings, and maintaining a sound fiscal position—may help dampen incentives. Restricting the use of crypto assets for certain activities—such as restricting derivatives linked to, or payments in, crypto assets—could also be a short-term solution to dampen crypto asset growth. Broader prohibitions on the creation and use of crypto assets, however, are likely to inhibit innovation and be ineffective given the ability to access them easily across borders. Prohibitions could also trigger even

stronger incentives for regulatory arbitrage and circumvention—rendering the enforcement of such broad bans extremely difficult.

The cross-sector and cross-border dimensions of crypto assets make domestic and international coordination and cooperation key. Activities related to crypto assets already are, and will continue to be, more cross-border and cross-sectoral than many traditional financial activities. This requires close international cooperation [63] to address regulatory gaps and prevent regulatory arbitrage. Consistent regulatory approaches can prevent the potential risk of a race to the bottom by regulators and policymakers and can address regulatory arbitrage by financial entities.

To ensure effective and efficient cross-sectoral and cross-border cooperation, robust international standards are indispensable. Relevant SSBs are making significant efforts to develop their own standards according to their mandates. Although these are important steps, the economic functions of crypto assets are likely to change over time, changing the suitability of sector-specific regulations. Against this background, it will be important for the FSB to take a leading role in coordinating efforts by the sectoral SSBs. Home authorities where crypto asset service providers are domiciled need to coordinate with other relevant authorities where the users of the crypto assets are located. IMF staff are actively contributing to the SSBs' activities to facilitate the development and implementation of robust international standards to ensure consumer protection, market integrity, and financial stability.

[63] Although data, privacy, and tax issues are outside the scope of this note, it is important to address those issues in regard to cross-border and cross-agency cooperation.

References

Adrian, Tobias, and Mancini-Griffoli, Tommaso. 2019. "The Rise of Digital Money." IMF Fintech Notes 2019/001, International Monetary Fund, Washington, DC. The Rise of Digital Money (imf.org)

Agur, Itai; Deodoro, Jose; Lavayssière, Xavier; Martinez Peria, Soledad; Sandri Damiano; Tourpe, Herve; and Villegas Bauer, German. 2022. "Digital Currencies and Energy Consumption." IMF Fintech Notes 2022/006, International Monetary Fund, Washington, DC. Digital Currencies and Energy Consumption (imf.org)

Alvarez, Fernando; Argente, David; and Van Patten, Diana. 2022 "Are Cryptocurrencies Currencies? Bitcoin as Legal Tender in El Salvador." NBER Working Paper 29968, National Bureau for Economic Research, Cambridge, MA. Are Cryptocurrencies Currencies? Bitcoin as Legal Tender in El Salvador | NBER

Aramonte, Sirio; Huang, Wenqian; and Schrimpf, Andreas. 2021. "DeFi risks and the decentralization illusion." *BIS Quarterly Review*, December. DeFi risks and the decentralisation illusion (bis.org)

Auer, Raphael. 2019. "Embedded supervision: how to build regulation into decentralised finance." BIS Working Paper 811, Bank for International Settlements, Basel, Switzerland. Embedded supervision: how to build regulation into blockchain finance (bis.org)

Auer, Raphael; Farag, Mark; Lewrick, Ulf; Orazem, Lovrenc; and Zoss, Marcus. 2022. "Banking in the shadow of Bitcoin? The institutional adoption of cryptocurrencies." BIS Working Paper 1013, Bank for International Settlements, Basel, Switzerland. Banking in the shadow of Bitcoin? The institutional adoption of cryptocurrencies (bis.org)

Bains, Parma. 2022. "Blockchain Consensus Mechanisms: A Primer for Supervisors." IMF Fintech Notes 2022/003, International Monetary Fund, Washington, DC. Blockchain Consensus Mechanisms: A Primer for Supervisors (imf.org)

Bains, Parma; Sugimoto, Nobuyasu; and Wilson Chris. 2022. "BigTech in Financial Services." IMF Fintech Notes 2022/002, International Monetary Fund, Washington, DC. BigTech in Financial Services (imf.org)

Bains, Parma; Ismail, Arif; Melo, Fabiana, and Sugimoto Nobuyasu. 2022. "Regulating the Crypto Ecosystem: The Case of Stablecoins and Arrangements." IMF Fintech Notes 2022/008, International Monetary Fund, Washington, DC.

Bank for International Settlements (BIS). 2021. "Supervising cryptoassets for anti-money laundering." *FSI Insights on Policy Implementation* 31. https://www.bis.org/fsi/publ/insights31.pdf.

Basel Committee on Banking Supervision (BCBS). 2022. "Second consultation on the prudential treatment of cryptoasset exposures." Consultative document. Basel, Switzerland. Second consultation on the prudential treatment of cryptoasset exposures (bis.org)

Ben Mariem, Sami; Casas, Pedro; Romiti, Matteo; Donnet, Benoit; Stütz, Rainer; Haslhofer, Bernhard. 2020. "All that Glitters is not Bitcoin—Unveiling the Centralized Nature of the BTC (IP) Network" *NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium*. All that Glitters is not Bitcoin – Unveiling the Centralized Nature of the BTC (IP) Network | NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium (acm.org)

Cuervo, Cristina; Morozova, Anastassiya; and Sugimoto, Nobuyasu. 2020. Regulation of Crypto Assets. Regulation of Crypto Assets (imf.org)

European Commission. 2021. Strategy on supervisory data in EU financial services. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021DC0798&from=EN

Financial Conduct Authority (FCA). 2021. Research Note: Cryptoasset consumer research. Research Note: Cryptoasset consumer research 2021 | FCA

Financial Stability Board (FSB). 2017. Financial Stability Implications from FinTech: Supervisory and Regulatory Issues that Merit Authorities' Attention https://www.fsb.org/wp-content/uploads/R270617.pdf

Financial Stability Board (FSB), 2018. Crypto-asset markets Potential channels for future financial stability implications Crypto-asset markets: Potential channels for future financial stability implications (fsb.org)

Financial Stability Board (FSB). 2022. "Assessment of Risks to Financial Stability from Crypto-assets." Basel. (https://www.fsb.org/wp-content/uploads/P160222.pdf)

He, Dong ; Kokenyne, Annamaria ; Lavayssière, Xavier ; Lukonga, Inutu ; Schwarz, Nadine ; Sugimoto, Nobuyasu ; Verrier, Jeanne. 2022. Capital Flow Management Measures in the Digital Age Capital Flow Management Measures in the Digital Age: Challenges of Crypto Assets (imf.org)

International Monetary Fund (IMF) and World Bank Group. 2018. "The Bali Fintech Agenda." IMF Policy Paper, Washington, DC. The Bali Fintech Agenda (imf.org)

International Monetary Fund (IMF). 2021. Global Financial Stability Report, October 2021 (imf.org)

International Monetary Fund (IMF). 2022. Global Financial Stability Report | April 2022 (imf.org)

International Organisation of Securities Commissions (IOSCO). 2020. Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms (https://www.iosco.org/library/pubdocs/pdf/IOSCOPD649.pdf)

International Organization of Securities Commissions (IOSCO). 2020. Investor Education on Crypto-Assets FR12/2020 Investor Education on Crypto-Assets (iosco.org)

International Organization of Securities Commissions (IOSCO). 2020. Report on Retail Distribution and Digitalisation CR02/2022 Report on Retail Distribution and Digitalisation (iosco.org)

Iyer, Tara. 2022. Cryptic Connections : Spillovers between Crypto and Equity Markets. Cryptic Connections: Spillovers between Crypto and Equity Markets (imf.org)

Schwarz, Nadine ; Poh, Kristel ; Chen, Ke ; Jackson, Grace ; Kao, Kathleen ; Fernando, Francisca ; Markevych, Maksym. 2021a. “Virtual Assets and Anti–Money Laundering and Combating the Financing of Terrorism (1). Some Legal and Practical Considerations.” IMF Fintech Notes 2021/002. Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism (1): Some Legal and Practical Considerations (imf.org)

Schwarz, Nadine ; Poh, Kristel ; Chen, Ke ; Jackson, Grace ; Kao, Kathleen ; Fernando, Francisca ; Markevych, Maksym. 2021b. “Virtual Assets and Anti–Money Laundering and Combating the Financing of Terrorism (2). Effective Anti–Money Laundering and Combating the Financing of Terrorism Regulatory and Supervisory Framework—Some Legal and Practical Considerations. IMF Fintech Notes 2021/003. Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism (2): Effective Anti-Money Laundering and Combating the Financing of Terrorism Regulatory and Supervisory Framework—Some Legal and Practical Considerations (imf.org)

Soderberg, Gabriel ; Bechara, Marianne ; Bossu, Wouter ; Che, Natasha ; Davidovic, Sonja ; Kiff, John ; Lukonga, Inutu ; Mancini Griffoli, Tommaso ; Sun, Tao ; Akihiro Yoshinaga. 2022. Behind the Scenes of Central Bank Digital Currency: Emerging Trends, Insights, and Policy Lessons Fintech Note 2022/04. https://www.imf.org/en/Publications/fintech-notes/Issues/2022/02/07/Behind-the-Scenes-of-Central-Bank-Digital-Currency-512174

PUBLICATIONS

Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Assets

NOTE/2022/007