FINTECH

NOTES

REGULATION OF CRYPTO ASSETS

Cristina Cuervo
Anastasiia Morozova
Nobuyasu Sugimoto

NOTE/19/03

FINTECH NOTE

Regulation of Crypto Assets

Prepared by Cristina Cuervo, Anastasiia Morozova,
and Nobuyasu Sugimoto
December 2019

INTERNATIONAL MONETARY FUND

Cover Design: IMF Multimedia Services
Composition: The Grauel Group

Names: Cuervo, Cristina, author. | Morozova, Anastasiia, author. | Sugimoto, Nobuyasu, author. | International Monetary Fund, publisher.
Title: Regulation of crypto assets / Prepared by Cristina Cuervo, Anastasiia Morozova, and Nobuyasu Sugimoto.
Other titles: FinTech notes (International Monetary Fund).
Description: Washington, DC : International Monetary Fund, 2019. | FinTech notes. | December 2019. | Includes bibliographical references.
Identifiers: ISBN 9781513520315 (paper)
Subjects: LCSH: Cryptocurrencies. | Electronic funds transfers. | Financial services industry.
Classification: LCC HG1710.C84 2019

Publication orders may be placed online, by fax, or through the mail:
International Monetary Fund, Publication Services
PO Box 92780, Washington, DC 20090, U.S.A.
Tel.: (202) 623-7430 Fax: (202) 623-7201
Email: publications@imf.org
www.imf bookstore.org

CONTENTS

ABBREVIATIONS

AMF	Autorité des Marchés Financiers of France
AML/CFT	anti–money laundering/combating the financing of terrorism
BCBS	Basel Committee on Banking Supervision
BFA	Bali Fintech Agenda
CPMI	Committee on Payments and Market Infrastructures
DLT	distributed ledger technology
FATF	Financial Action Task Force
FINMA	Swiss Financial Market Supervisory Authority
FSB	Financial Stability Board
ICO	initial coin offering
IOSCO	International Organization of Securities Commissions
MTF	multilateral trading systems
PFMI	principles for financial market infrastructures
SAFU	secure asset fund for users
VFAA	Virtual Financial Asset Act

REGULATION OF CRYPTO ASSETS

Introduction[1]

The rapid growth of crypto assets has raised questions about the appropriate regulatory perimeter and the ability of the existing regulatory architecture to adapt to changing conditions (Figure 1). Effective regulation of financial services promotes long-term economic stability and minimizes the social costs and negative externalities from financial instability. The same underlying principles for regulation should apply to nascent products and services based on innovative technologies, notwithstanding design challenges.

The purpose of this note is to identify selected elements of regulation and supervision that authorities should consider when deciding on a regulatory framework for crypto assets. The note is structured in two main sections: the first briefly summarizes some of the most relevant risks related to crypto assets, while the second concentrates on how regulatory frameworks could address these risks. To illustrate the analysis, some country examples are compiled in the Appendix.

The definition of a crypto asset is far from globally uniform and we have therefore opted for a broad approach. In this note, the term *crypto asset* denotes digital assets that use cryptography for security and are coins or tokens of distributed ledgers and/or blockchains, including asset-backed tokens. We also recognize the distinction between "coins" and "tokens" but may use the two terms interchangeably.[2]

The IMF/World Bank Bali Fintech Agenda (BFA) proposes a framework of high-level issues that countries should consider in their policy discussions. The Agenda brings together key considerations for policymakers and the international community into 12 elements, including enabling technologies, ensuring financial sector resilience, addressing risks, and promoting international cooperation. This note aims to provide a discussion into regulatory and supervisory considerations in relation to a specific area of fintech—crypto assets—going deeper into the monitoring, regulation, and supervision elements of the BFA.[3]

While the international regulatory community is actively engaged in discussions around crypto assets, approaches are varied and often only partially address potential risks. The fast-moving pace of fintech challenges authorities and standard setters to develop sound regulatory and supervisory approaches to contain the risks while supporting healthy innovation. This note does not aim to establish standards or to provide prescriptive solutions, but rather to assist policymakers in various jurisdictions in framing the discussion and issues relative to the regulation of crypto assets. The underlying principle is that regulation and supervision are needed when there is sufficient concern that there are potential market failures or externalities that bring risks to financial stability; warrant the need to protect financial markets, consumers, and investors from abuse; or lead to excessive regulatory arbitrage. The need and features of regulation will therefore depend on the characteristics of crypto assets and related products and specific country circumstances.

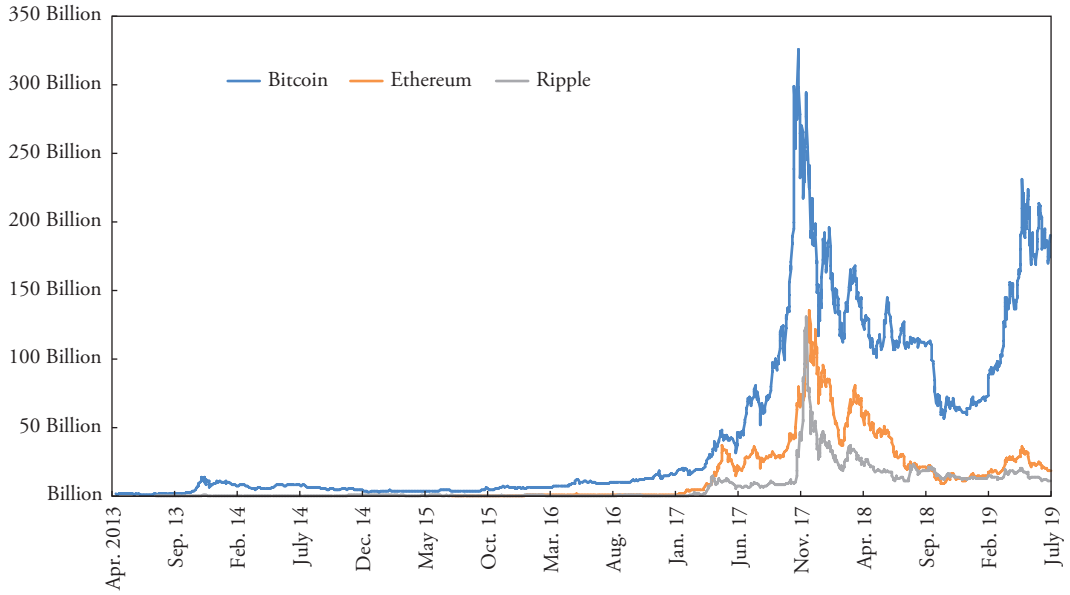
This note therefore does not aim to address comprehensively the regulatory implications of crypto assets but focuses on selected aspects of financial regulation. It addresses some of the most relevant financial regulation issues related to a wide range of crypto-asset features existing today—but not all. For instance, particular features of stablecoins or other newly developed crypto assets may have regulatory implications that are not specifically covered here. In addition, the note does not cover central bank digital currencies or payment

[1]This note was prepared by Cristina Cuervo, Anastasiia Morozova, and Nobuyasu Sugimoto, with inputs from Tamas Gaidosch, Eija Holttinen, David Jutrsa, Richard Stobo and Chris Wilson (all MCM). While detailed discussion of anti–money laundering/combating the financing of terrorism issues is outside the scope of this note, Kristel Poh, Nadine Schwarz, and Jess Cheng (LEG) provided helpful guidance on the topic.

[2]Coins refer to bitcoin and alt-coins, which were issued originally with a main purpose to serve as "currency," that is, with money and payments-related functions. Tokens have more functions than coins, for example, permitting the coin holders to participate in the service provided or the returns offered by the token issuer.

[3]The corresponding elements in the BFA are V—Monitor Developments Closely to Deepen Understanding of Evolving Financial Systems and VI—Adapt Regulatory Framework and Supervisory Practices for Orderly Development and Stability of the Financial System.

Figure 1. The Rapid Growth of Crypto Assets
Market capitalization over time of top three crypto assets



Sources: CoinMarketCap and IMF staff calculations.

system implications related to crypto assets—although these also present challenges to regulators. Moreover, data and privacy issues are not covered in this note, although data use and its regulation could have a significant impact on the network effect of crypto-related services and thus growth of a crypto-asset ecosystem. This paper also aims to cover more imminent issues to the regulatory and supervisory community and thus does not discuss the challenges that could arise in the long term. For example, in June 2019, the Financial Stability Board (FSB) published a report[4] that considers the implications of decentralized financial technologies and concludes that full decentralization seems unlikely to achieve an economically significant scale in the near future. Therefore, in this note we describe regulation with the assumption that some intermediaries will exist for the time being to provide financial services to end users.

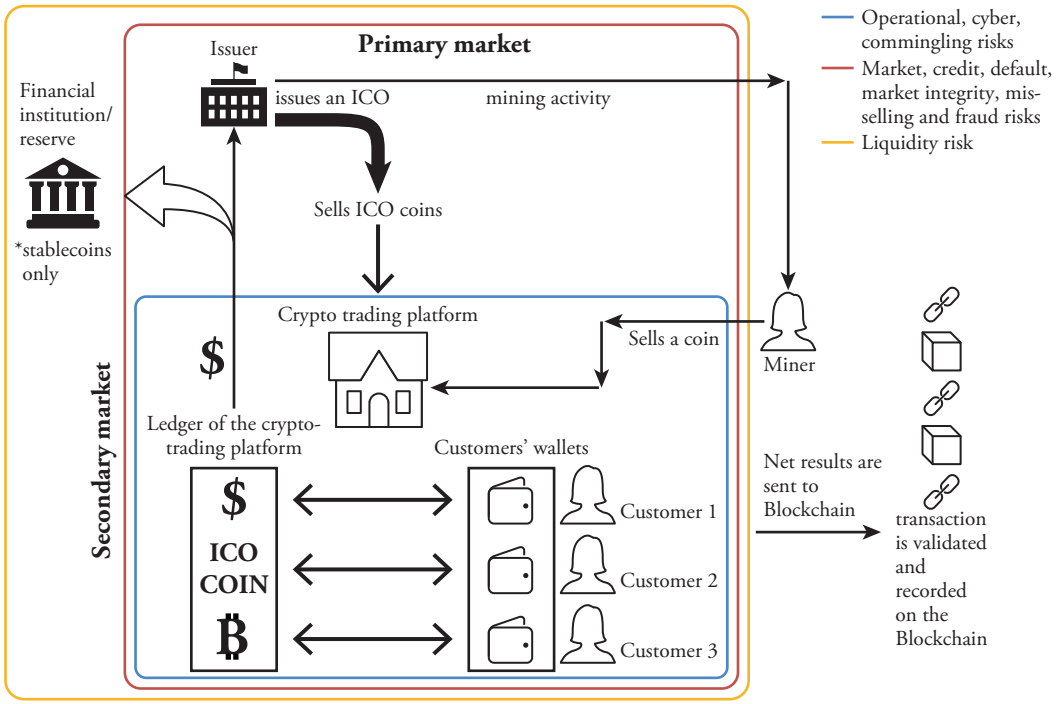
In fact, the risks discussed here are only a starting point for regulatory discussions. The evolving nature of crypto assets will require a continuous assessment of risks and re-evaluation of regulatory approaches. Industry and technological developments may accelerate specific activities (see Box 2), potentially shifting the focus of authorities from some risks to others. As technologies and products evolve, there will be areas where further adaption will be needed, but in all cases, this note takes the approach that similar activities and risks should be regulated in the same way to prevent the development of excessive risk taking, contagion, financial instability, and material regulatory arbitrage.

Finally, given the cross-border and cross-sectoral nature of the activities, closer international cooperation and coordination is needed to address regulatory gaps and prevent potential regulatory arbitrage. Activities related to crypto assets already are and will continue to be more cross-border and cross-sectoral—by design—than traditional financial activities. This requires closer international cooperation and coordination[5] to address regulatory gaps. Consistent regulatory approaches can prevent the potential risk of a race to the bottom by regulators and policymakers and address regulatory arbitrage by financial entities.

[4]Financial Stability Board (FSB). 2019. "Decentralised financial technologies: Report on financial stability, regulatory and governance implications." FSB Policy Paper, Basel, Switzerland. https://www.fsb.org/w-content/uploads/P060619.pdf. IMF staff actively contributed to the analysis and drafting of the report.

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

Figure 2. Market Structure of Crypto Assets
The market structure of crypto assets is simplified and illustrated in the figure. We highlight the risks we address in this paper and illustrate the part of the market chain they relate to in the context of this note.



Source: IMF staff.

The Risks

Crypto-investors and users,[6] as well as crypto-asset service providers, are exposed to high risks. The inherently high volatility of major crypto assets, together with technology features and anonymity, create several significant risks not only to investors but also to service providers. Some of the risks incurred by investors are, for instance, operational and cyber risk of wallet providers and the crypto trading platform; market, credit, and default risk of issuers; comingling risk of assets; liquidity risk of both issuers and service providers; market manipulation; misselling; and fraud. Crypto assets are also vulnerable to misuse for money laundering and terrorist financing. In addition, crypto assets may generate contagion and business model risks, which may potentially become systemic and warrant a prudential response. This section briefly describes these risks. The subsequent sections discuss regulatory challenges and options to address them.

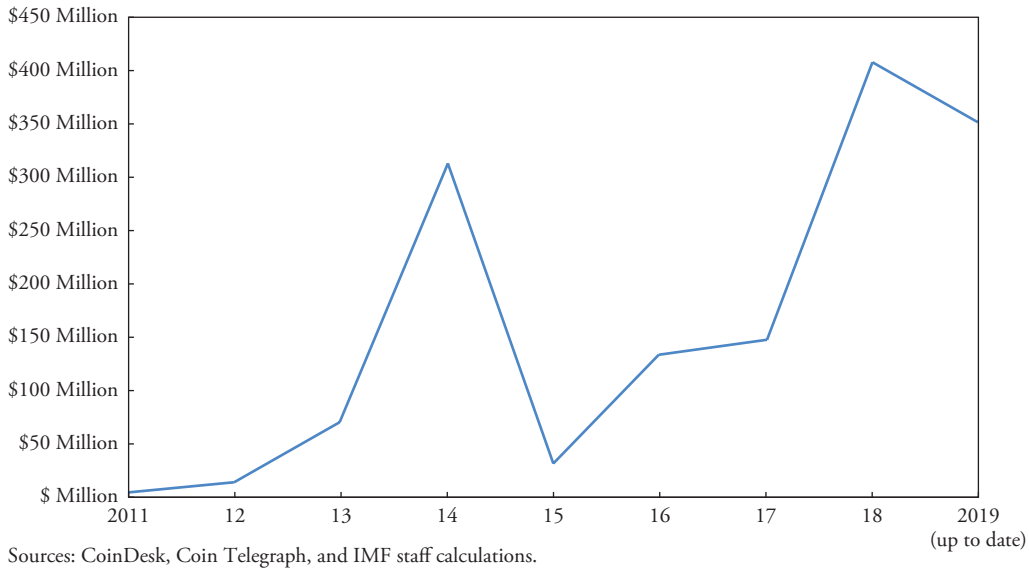
[6]In this note, we will more recurrently refer to "investors," but the term should be understood to also include end users (both wholesale and retail) of crypto assets, where applicable.

Investor Risks

Crypto investors may be exposed to a significantly higher risk of loss than those investing in traditional financial assets. Some of the main risks that investors are facing are illustrated in Figure 2.

- **Operational and cyber risk of wallet providers and crypto-trading platforms.** In the last few years, several crypto-trading platforms and wallet providers, including large and well-known firms, have been hacked and the client coins or tokens have been stolen (Figure 3). Some of the largest loss incidents involved several hundred million US dollars per incident, leaving providers bankrupt and investors at a loss. Even in cases where compensation was ultimately fully paid out within several months, investors were not able to use their hacked coins or tokens over extended periods of time. Some exchanges are trying to mitigate this risk by contracting cyber insurance coverage or by creating separate compensation funds, but there is typically no

Figure 3. Funds Stolen Via Hacks and Cyber Incidents before Major Wallets and Crypto-Trading Platforms



Sources: CoinDesk, Coin Telegraph, and IMF staff calculations.

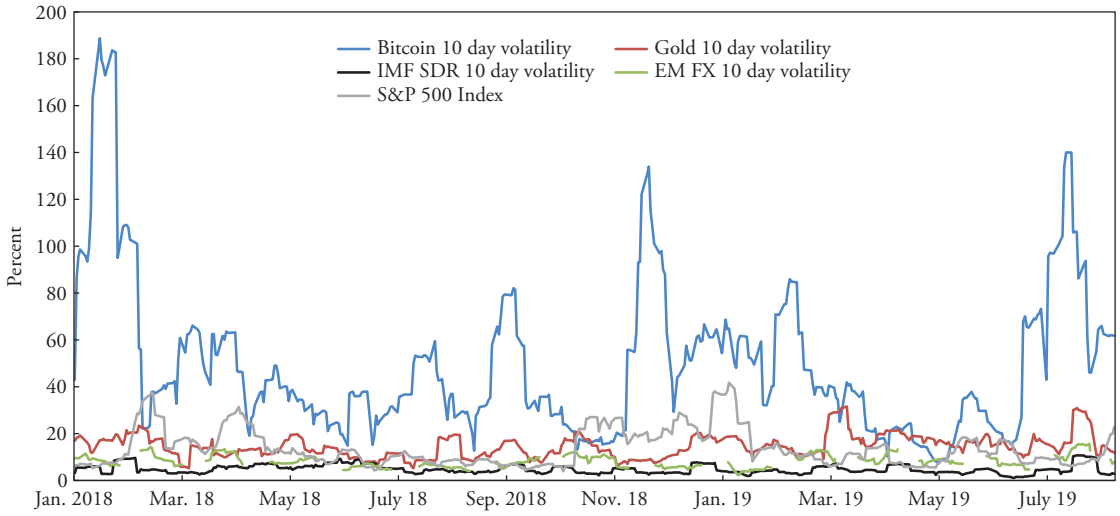
public or other safety net, such as deposit insurance or a liquidity facility from central banks.[7]

- **Market, credit, and default risks of coin and token issuers**. Many crypto assets are highly volatile, and the investors and crypto-trading platforms are exposed to material market risk. Even so-called stablecoins[8] are potentially subject to the credit and default risk of the issuer, as the collateral (such as bank deposits) may not be segregated from other assets of the issuer and thus both could be commingled if the issuer files for bankruptcy. Deterioration of the issuer's credit would be reflected into the price of the issuer's coins and tokens. Issuers of stablecoins also tend to be related parties of crypto-trading platforms. Therefore, there are additional potential conflicts of interest between stablecoin issuers and crypto-trading platform operators (Figure 4). For example, stablecoin issuers may rehypothecate their collateral to the related trading platform operators under favorable conditions.
- **Commingling of assets of service providers**. In the event crypto service providers go bankrupt, their clients' coins and tokens could be comingled with the service provider's other assets, unless there is a clear regulatory framework and robust arrangements to make the client assets bankruptcy-remote. If the service provider is a regulated bank, crypto-asset holdings could make the resolution of the bank complicated, which can, in turn, have wider financial stability implications.
- **Liquidity risk of issuers and service providers**. Issuers may allow redemption (typically very short term, such as daily) by investors and users into other currencies or assets. In addition, even if there is no legal obligation for issuers to respond to redemption requests, investors may expect that they would be able to exchange the coins and tokens with service providers (such as crypto-trading platforms) frequently without material redemption cost. There is a strong incentive for the issuer and service provider to meet such redemption requests from investors, to avoid reputation failure of the coin or token. Such pressure could trigger fire sales of the collateral assets (such as bonds and bank deposits) by the issuers and service providers, which might have a negative impact on the broader financial sector, such as banks and bond markets.
- **Market integrity risk**. Many crypto assets are not backed by tangible assets or other securities (such as

[7]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. Binance established a secure asset fund for users (SAFU) and is reported to allocate 10 percent of all trading fees into it. The SAFU is intended to offer protection to users.

[8]Stablecoins are designed to minimize price volatility versus a fiat currency, currency baskets, commodities, or tangible assets. Most stablecoins are collateralized by the assets they are designed to track. Others use algorithms to stabilize supply and demand.

Figure 4. A Comparison of Volatility: Crypto Assets versus Traditional Financial Instruments



Source: Bloomberg data.

Bitcoin and Ether), and thus have no clear intrinsic value (differently from stablecoins). The price discovery function of the market is inevitably weak and therefore such assets are at high risk of market manipulation.[9] Anecdotal evidence suggests that some large crypto-trading platforms allow investors to conduct wash trades.[10] Also, illiquidity could make markets vulnerable to other forms of market manipulation, such as "whale" trades[11]. Even in cases where assets may be subject to regulation and surveillance by relevant regulated exchanges (because they are considered to fall under the securities supervisory regime, for example), enforcement of market manipulation is challenging due to the often anonymous, cross-border, and decentralized nature of the transactions. This could pose serious risks should asset tokenization become more commonly used and expand to traditional assets in the future.

- **Risk of misselling and fraud in the offer of crypto assets**. The lack of comparable information about the products offered, together with intrinsic technological complexities and hype around innovation, make crypto assets a difficult-to-decipher product for investors. There is, therefore, increased risk of these products being created for fraudulent purposes.

Anti–Money Laundering/Combating the Financing of Terrorism Risk

Crypto assets potentially also create risks of misuse for money laundering and terrorist financing.[12] This is due, in part, to the different levels of anonymity or "pseudo-anonymity" that crypto assets offer that make regulatory action challenging: while the authorities may be able to trace transactions on the blockchain, depending on the level of anonymity that they offer, they may not always be able to establish who the two parties to a transaction are, and, ultimately, who owns the crypto assets. In addition, the fact that they are "internet-based" means that users have the ability to transact globally more rapidly. The use of decentralized technologies also makes it possible for users to transact in crypto assets without going through financial intermediaries (and by extension, bypassing anti–money laundering/combating the financing of

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

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

[11]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.

[12]While a detailed discussion of AML/CFT issues is beyond the scope of this note, it is important to mention that there have been tangible developments in international standard setting by the Financial Action Task Force as described briefly in Section IV (Regulation) of this paper. A dedicated Fintech Note on modernizing legal frameworks including these issues is planned for publication in due course.

Box 1. Crypto-Trading Platforms

Crypto-trading platforms typically execute and receive orders from investors for the "exchange" or secondary market sale or purchase of crypto assets against fiat currency or other crypto assets. Currently, crypto-trading platforms are providing brokerage services to retail investors in a manner similar to that of stock brokerage firms. However, unlike many stock brokerage firms, which can just pass the client orders to a stock exchange, crypto-trading platforms generally need to provide liquidity to support the transactions among their client investors (by selling their own inventories to match purchase orders from their clients). This is similar, for example, to the way US Alternative Trading Systems and Japanese Proprietary Trading Systems work. Such crypto-trading platforms therefore do not work in the same manner as European Union multilateral trading systems (MTFs), because MTF operators cannot trade on their own account in the trading platform they operate.

Crypto-trading platforms may also perform other functions, including custody (similar to wallet providers) and margin lending and provision of liquidity. Many crypto-trading platforms are providing margin trading and financing platforms to investors (for example, Coincheck, Bitfinex). In some cases, this may support considerable leverage, although due to the lack of disclosure it is hard to analyze the size, volume, and associated risks of leveraged trading. Trading platforms also play other important roles, such as underwriters in initial coin offerings, which may raise the risk of market manipulation and insider trading.

terrorism [AML/CFT] obligations). These features, and the fact that, crypto assets currently fall under different regulatory frameworks globally, resulting in uneven or no monitoring and information sharing across jurisdictions, make such assets particularly attractive to individuals who wish to evade existing controls to commit crimes (such as fraud, cyber-crime, and tax evasion, to launder illegal proceeds or even to fund terrorism).

Anonymity enhanced features further complicate authorities' ability to track criminal use of crypto assets. The emergence of more sophisticated mixers and tumblers[13] and anonymity-enhanced crypto assets (such as Monero, Z-cash) aggravate the risks further by obfuscating the source of funds and providing layering services—which can potentially frustrate operational authorities' ability to detect, investigate, and prosecute offenses. Furthermore, new "layers" of application protocols (for example, a lightning network, a second layer technology using micropayment channels aimed at mitigating the scaling problem of the original Bitcoin) and related "netting" arrangements allow offline financial exchanges and further block the visibility of transactions.

[13]Mixers and tumblers are the services which mix coins from different transactions and provide new coins to clients. The services can be used to break the connection between a sending and receiving address and obscure the trail to the original source while simultaneously improving the anonymity of transactions.

Prudential and Systemic Risk

Crypto-asset providers and issuers are increasingly engaging with traditional financial institutions, as well as modifying the competitive landscape, generating prudential risks that warrant a sensible response. Crypto-asset providers (crypto-trading platforms and brokers) are increasingly engaging with traditional financial institutions (through derivatives, providing crypto linked products and cyber insurance). These exposures could trigger contagion risks to financial institutions if the size of the exposures continues to grow in the future or if the risk is not managed properly. If stablecoins become widely used, existing financial institutions would engage with crypto-asset business more actively. Some might issue their own stablecoins (such as JPM Coin) to compete with crypto-asset service providers. In addition, crypto assets and distributed ledger technology (DLT) applications might affect the industry landscape and increase competition in the future, which may, in turn, affect the soundness of the existing financial sector. Digitalization would have a much wider and stronger impact on business models of the existing financial sector, although this is beyond the scope of this note.

While initial assessments by standard setters indicated crypto assets did not pose material systemic risk, technological and market developments are moving fast, and this situation may be changing. In October 2018, the FSB released a report which concluded that

crypto assets did not pose a material risk to global financial stability at that time. The report noted that risks would arise if crypto assets became widely used in payments and settlement (see Box 2). The global fintech survey conducted by the IMF and the World Bank in early 2019 also found that most jurisdictions agree that crypto assets present risks to investors but are not yet a threat to financial stability. The Basel Committee on Banking Supervision (BCBS) released a statement covering crypto assets in March 2019, which highlighted that continued growth of crypto assets has the potential to raise financial stability concerns and increase risks faced by banks. Significant data gaps in information on the extent of leverage in crypto-asset markets, and on direct and indirect exposures of financial institutions pose additional challenges to the assessment and monitoring of systemic risk.

Further institutionalization of crypto-related activities could increase transmission channels between crypto activities and traditional financial institutions. Current transmission channels between the crypto space and traditional financial institutions are restricted to small direct exposures and limited indirect exposures. However, a number of fintech startups and even major financial entities (such as Fidelity Investments) are actively developing solutions to improve the reliability and safety of private key management of crypto assets. If those services become available with competitive pricing, a possible scenario could include much wider use of crypto assets by large institutional investors (such as asset managers, insurance companies, and pension funds). Wider use of crypto-based payment systems (such as for cross-border payments) could also materially increase the number of transmission channels between crypto assets and financial institutions in the future.

Regulation

Although central banks and anti–money laundering authorities initially took the lead in setting a regulatory stance for crypto assets, the emergence of initial coin offerings (ICOs) turned the focus to securities regulators and standard-setting bodies have approached the issue within their mandates. Central banks were mostly the first to react to the emergence of crypto assets—Bitcoin and other cryptocurrencies, in particular—issuing statements and warnings about their potential risks. Many AML/CFT authorities developed or adapted regulation to apply to certain types of crypto assets, with the Financial Action Task Force (FATF) updating its standards to cover virtual assets and virtual asset service providers in 2018. The rapid expansion of ICO activities[14] urged financial sector regulators—and, prominently, securities regulators—to take a position on crypto assets, since it became apparent that many of those assets may meet the definition of a security and therefore should be bound by securities legislation. Many securities regulators then initiated enforcement investigations in relation to crypto-asset activities, which presumably assisted in defining their official position. In the meantime, various standard-setting bodies have discussed potential approaches within their mandate, although very few standards have effectively been set.

What Has Been Done So Far

Many financial sector regulators have already taken a position in relation to crypto assets, although the approach and coverage of the topic is varied. In the absence of international standards or guidance (except in the area of AML/CFT), jurisdictions have taken different approaches and views, often related to the policy stance regarding innovation, the mandates of their regulatory bodies, and the pace and type of crypto-activities in the country.

Warnings. Most jurisdictions have issued public statements warning about the risks of crypto assets (generally referring to investor protection and financial integrity risks), with many also highlighting that some crypto assets could resemble securities and would trigger a securities regulatory approach (for example, the US SEC and the UK FCA).[15]

Prohibition. Several jurisdictions have decided to ban any crypto-asset activity, although it is unclear if enforcement is always feasible and cross-border activities are covered. Some of the jurisdictions that chose this approach are Algeria, Bahrain, Bangladesh, Bolivia, China, Colombia, the Dominican Republic (for regulated financial institutions), Indonesia, Iran, Iraq, Morocco, Nepal, Kuwait, Kyrgyzstan, Macao SAR, Maldives, and Qatar.

[14]ICO activity has since dramatically decreased, both in terms of number of projects and money raised, as pointed out by numerous crypto-related sources. As recently documented by the cryptocurrency analytics firm Long Hash, the total money raised for 2019 is expected to be around $338 million, or 95 percent less than in 2018.

[15]At least 82 countries have issued warnings on digital assets and at least 20 countries have issued warnings on ICOs, specifically.

Box 2. A Special Mention of Recent Crypto Developments: Facebook and Libra

In June 2019, the Libra Association announced a digital currency project, called Libra, led by Facebook and 27 other members. Members of the Libra Association are major payment (Visa, Mastercard, and PayPal), technology (eBay and Uber), telecom (Vodafone), and blockchain (Coinbase and Xapo) companies. In October 2019, a total of 22 members formally signed onto the Libra Association Charter, formalized the Libra Association Council, elected the Board of Directors, and appointed members of the Libra Association Executive Team. The service's target launch is set for the first half of 2020, when it hopes to have approximately 100 members. Facebook is the lead entity in the Libra project and it is relevant to note that there is no banking group among the initial founding members. Each member is to have an equal voting right at each important decision, which would be taken by supermajority among the governance token holders. The association plans to issue two types of coin/tokens, one for the users (payment/user tokens) and one for the governance function (investor tokens). The governance or investor tokens would be subject to a minimum investment threshold of $10 million.

Libra, the digital currency, would be designed to be stable but not pegged to any fiat currency. Libra would be backed by a reserve of real assets. The reserve will be held by a geographically distributed network of custodians with an investment-grade credit rating to limit counterparty risk. The reserve will be made up of a collection of low-volatility assets—bank deposits and government securities in currencies from stable and reputable central banks. The initial set of currencies are reported to be four major hard currencies (British pounds, euros, US dollars, and yen). The association plans to rely on short-dated securities issued by stable governments that are traded in liquid markets to manage the reserve fund. The association may occasionally change the composition of the basket, which would require a supermajority vote by the association's council.[1] Users of Libra would not receive returns from the reserve. The revenue would be used to promote the coins and as a return to governance token investors. It is important that this and other relevant features of Libra (for instance the limits of redemption through authorized entities, see below) should be appropriately and clearly disclosed to the public.

It is not clear how reserve management would be regulated or supervised. The association is established in Geneva, Switzerland, and reported to be subject to Swiss Financial Market Supervisory Authority (FINMA) regulation and supervision. In September 2019, FINMA released a supplement to the initial coin offering guidelines, outlining how to treat stablecoins, and provided the following indications of how Libra would be potentially regulated and supervised: i) the project would require a payment system license from FINMA and requirements that are in line with the Principles for Financial Market Infrastructures (PFMI); ii) the services would clearly go beyond those of a pure payment system and therefore be subject to additional requirements, such as capital allocation (for credit, market, and operational risks), liquidity, and risk concentration, as well as the management of the reserve; iii) bank-like regulatory requirements for bank-like risks; and iv) a condition providing that the returns and risks associated with reserve management are borne entirely by the Libra Association and not—as in the case of a fund provider—by stablecoin holders, as a necessary condition for being granted a license as a payment system. Since stablecoin holders share both downside risk and currency risk, it is not clear if and how the Libra Association, especially its reserve management, would be regulated and supervised.

Conflicts of interest between holders of governance tokens and user tokens would need to be addressed carefully. Since governance token holders are entitled to the return on the reserve investment, they may wish to increase the return to offset operating costs. Therefore, there would be some incentives for them to push yield-enhancing activities, such as securities lending. On the other side, the user token holders would presumably want to minimize volatility and thus would like to see the reserve invested conservatively and in a well-diversified manner. While the initial proposal of the reserve management policy clearly states that "the goal will always be value preservation," each member would have different risk assessments and appetites. Depending on the composition of the members, the association could be under pressure to soften this interpretation of the policy, which may result in a gradual shift toward riskier asset investments in the long term.[2] Therefore, it might be necessary to address the conflicts of interest between the two types of inves-

[1]The council is the Libra Association's governing body. Initially, this group consists of the founding members. All decisions will be brought to the council and major policy or technical decisions require the consent of two-thirds of the members.

[2]The G7 Working Group on Stablecoins also mentioned this issue in its report "Investigating the impact of global stablecoins," issued in October 2019.

Box 2. A Special Mention of Recent Crypto Developments: Facebook and Libra *(continued)*

tors by imposing disclosure requirements and other safeguards (such as a limitation of changes—even with supermajority voting—among the members) to ensure the protection of user token holders' interests.

The ecosystem would rely heavily on crypto-trading platforms for redemption, and that could expose it to liquidity and foreign exchange rate risk. Redemption of the user tokens would be limited to the entities authorized by the association to transact large amounts of fiat and Libra in and out of the reserve. While Facebook seems to be open to banking groups and reportedly encouraged them to become Libra founding members, so far only crypto-trading platforms have joined. Therefore, users would have to sell Libra to those entities (crypto-trading platforms) to cash out to fiat currencies, which would be subject to certain fees (such as foreign exchange conversion and transaction fees). In the case of a run scenario, crypto-trading platforms could be subject to liquidity risk if the association cannot meet redemptions from those entities as quickly as the end users need. Currently, most jurisdictions don't impose prudential requirements (including liquidity requirements) on crypto-trading platforms. It would be useful for the association to have additional reserves and to be able to use such reserves for liquidity provisions to authorized resellers in stressed situations.

Facebook created a subsidiary, Calibra, to serve as the single wallet provider of Libra. It would control all interfaces with the retail users. Calibra would be subject to anti–money laundering/combating the financing of terrorism (AML/CFT) regulation and be licensed as a payment service provider. Transaction data will not be shared with Facebook or any third party without customer consent. However, there are cases where data may be shared with authorities to comply with the law, Calibra indicated. However, arguably, one of Facebook's main motivations for the Libra project could be access to the usage data. It is also uncertain how AML/CFT preventive measures, such as customer due diligence, will be carried out.

Guidance. Many authorities have issued high-level guidance on the treatment of crypto assets. To frame the guidance, some jurisdictions classified the assets according to their main characteristics and economic purpose (for example, the Swiss FINMA, MAS, and UK FCA). The most common classification, inspired by the Swiss approach, refers to (i) securities assets, meaning those that fall within the jurisdiction's definition of a security; (ii) payment assets, for those intended to be used as a means of payment; and (iii) utility assets, which are intended to provide digital access to an application or service. Guidance generally focuses on identifying whether existing legislation and regulations apply to any of these types of crypto assets. Other jurisdictions are not explicitly classifying crypto assets but are identifying the characteristics that would make them securities and thus fall under existing securities regulations.

Tailored regulation. Some jurisdictions are creating specific regulatory frameworks for crypto assets (for example, Malta and Thailand[16]). These provide more details on specific requirements that may apply to the different activities and service providers related to crypto assets, including public offerings and secondary market trading. For instance, the regulation issued by the commodity futures trading supervisory agency under the Ministry of Trade of Indonesia sets out the minimum requirements for crypto assets traders, trading platforms (including futures exchanges), clearing houses, and crypto storage providers (custodians). These requirements include registration and licensing, reporting, systems, organizational structure, governance, certification, security, storage, investor/customer education, transparency, minimum capital, and AML/CFT obligations.

Enforcement. Several authorities are using their enforcement and sanction powers to develop or enforce their position on crypto assets and related activities, on a case-by-case basis (for example, US SEC and CFTC).

Standard setters and coordination/monitoring bodies have also been actively engaged in developing reports and guidance regarding crypto-asset risks, although standards have only been issued by FATF:

- **IOSCO** warned about the risks of crypto-asset offers in January 2018 and created an ICO network for

[16]Japan: Amendment of the Payment Services Act and the Financial Instruments and Exchange Act, 2019; Malta: Virtual Financial Assets Act, 2018; and Thailand: Emergency Decree on the Digital Asset Business B.E. 2561 (C.E. 2018).

its members to exchange information. It also has a standing fintech network in charge of keeping track of fintech developments and identifying policy needs. IOSCO's relevant policy committees will take up any policy development considered necessary. For example, the Committee on Secondary Markets has published a consultative document on crypto-asset platforms (see next bullet).[17]

- **The FSB** issued the report "Decentralised financial technologies" in June 2019, which considered the financial stability and regulatory and governance implications of the use of decentralized financial technologies, such as those involving distributed ledgers and online peer-to-peer or user-matching platforms. The May 2019 report on "work underway to address crypto-asset risks" summarized recent work conducted by international organizations. The reports covered a wide range of issues, including investor protection, market integrity, anti–money laundering, bank exposures, and financial stability monitoring. The report concluded with a recommendation that the G20 keep the topic of regulatory approaches and potential gaps, including the question of whether more coordination is needed, under review. In April 2019, the FSB published "Crypto-assets regulators directory," which provides information on the relevant regulators and other authorities in FSB jurisdictions and international bodies.[18]
- **The BCBS** issued a "statement on crypto assets" in March 2019, and a consultative document in December 2019,[19] in which it set out its prudential expectations related to banks' exposures to crypto assets and related services. The statement highlighted a number of risks for banks, including liquidity risk; credit risk; market risk; operational risk (including fraud and cyber risks); money laundering and terrorist financing risk; and legal and reputation risks. The BCBS is currently collecting data on banks' direct and indirect exposures to crypto assets as part of its end of 2018 Basel III monitoring exercise. BCBS published a discussion paper related to the prudential regulatory treatment of crypto assets in December 2019.
- **The Committee on Payments and Market Infrastructures (CPMI)** and IOSCO joint working group examined the PFMI, discussing whether current initiatives using DLT in clearing and settlement pose challenges for application of the PFMI. In 2018, CPMI issued the two papers: i) cross-border retail payments and ii) central bank digital currencies. The report on cross-border retail payments highlighted that alternative clearing and settlement arrangements are emerging.[20] The CPMI chairman stated that "The emergence and use of cryptocurrencies across borders signals to central bankers that our current payment systems are too expensive and slow. Action is needed to put better arrangements in place."[21]
- **The FATF** adopted changes to its recommendations in October 2018, to explicitly clarify that they apply to financial activities involving virtual assets and to related service providers. In addition, the FATF has since adopted an Interpretative Note to Recommendation 15 in June 2019. The Interpretive Note sets out binding measures for effective regulation and supervision or monitoring of virtual asset service providers. Moreover, In June 2019, the FATF also issued guidance on the application of the risk-based approach to virtual assets and virtual asset service providers.[22]

Considerations for the Development of Regulatory Frameworks

While crypto assets continue to develop and transform, authorities should consider following a proactive and holistic approach to regulation, stemming from a comprehensive consideration of risks. Jurisdictions

[17]https://www.iosco.org/news/pdf/IOSCONEWS485.pdf and Board of the International Organization of Securities and Commissions (IOSCO). 2019. "Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms." IOSCO Consultation Report CR02/2019. IOSCO, Madrid, Spain.

[18]Financial Stability Board (FSB). 2019. "Decentralised financial technologies: Report on financial stability, regulatory and governance implications," June; "Crypto-assets: Work underway, regulatory approaches and potential gaps," May; and "Crypto assets regulatory directory," April.

[19]https://www.bis.org/publ/bcbs_nl21.htm, and https://www.bis.org/bcbs/publ/d490.htm.

[20]Bank for International Settlements (BIS). 2018. "Cross-border retail payments report on cross-border payments." Committee on Payments and Market Infrastructures, February.

[21]BIS. 2018. "Choice and diversity are the key to quicker, cheaper cross-border retail payments." Committee on Payments and Market Infrastructures press release, February, https://www.bis.org/press/p180216.htm.

[22]https://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets-interpretive-note.html and https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html.

should consider monitoring developments to carefully analyze what risks are emerging, identify the most significant vulnerabilities, and determine priorities. There would be merit in an ongoing engagement with the industry to enable authorities to anticipate risks in market developments and proactively seek appropriate measures. The approach chosen by each jurisdiction could be potentially different if micro prudential or investor protection risks are identified, versus an emergence of systemic risk, for instance. Development of regulatory frameworks should be carried out sequentially, based on priorities and resources, but the continuous assessment of risks and strategic planning should be comprehensive and involve all financial sector regulators and other relevant authorities.

Regular and appropriate coordination of all relevant authorities would facilitate a clear allocation of responsibilities going forward. The potential for regulatory arbitrage, scarceness of expertise and resources, existing regulatory framework, and reputational risks would be taken into consideration when determining the responsible authority or authorities for the supervision and regulation of relevant aspects of crypto assets. One or more authorities may be involved and coordination with all other financial sector authorities is, in any case, key.

The chosen approach should aim to enhance investor protection and minimize the potential for regulatory arbitrage while providing enough flexibility to adapt to a changing landscape and risk outlook. Authorities should consider designing a comprehensive plan to address the risks stemming from crypto-asset activities, including any necessary legislative or regulatory actions, and continuous monitoring and coordinated communication initiatives—including investor education programs. When deciding to use or adapt existing regulation to address new risks, efforts should be focused on ensuring that specific crypto-asset features are contemplated as needed to minimize regulatory uncertainty. Authorities should ensure there is clarity and consistency in the terminology used.

The soundness of the legal frameworks is a precondition for a strong financial system in the crypto-asset era.[23] As discussed in the Bali Fintech Agenda, legal certainty helps build confidence in the trustworthiness and reliability of financial products and services. There may be legal aspects that are specific to crypto assets. For example, legal certainty of ownership rights is a precondition for the secure transfer of assets, but the general regime may fall short of providing enough elements to determine who owns a particular crypto asset or whether a transfer can be deemed final. Jurisdictions could consider these issues as part of their overall approach to regulating crypto assets, ensuring that the legal framework evolves with global financial markets and technologies.

In addition, international cooperation in the crypto-asset space will be crucial to ensure risks are appropriately monitored and contained. Authorities would continue to use cooperation networks and standard-setter initiatives to exchange information on developments in the crypto-assets space. Active engagement is needed to identify cross-border considerations and tackle potential regulatory arbitrage. International cooperation in enforcement will, of course, continue to be key for sanctioning and prosecuting crypto-asset-related cases.

Regulation needs to be risk-based and proportional. Based on the analysis in this Note, some relevant crypto-related activities and risks should receive immediate consideration. The public offer of crypto assets raises investor risks due to the potential for information asymmetries, lack of transparency, and plain fraud. Crypto-asset trading also raises several issues, including operational and cyber risks and market integrity. Custodial and wallet services pose investor protection concerns due to segregation and safe handling of client assets. Many crypto-asset activities also involve financial integrity risks and AML/CFT regulation and supervision[24] need to be an integral part of any regulatory framework. Finally, the exposure of the financial sector to crypto assets and the relative size and growth of the crypto-asset market can raise prudential and financial stability risks that should be considered. This section will therefore focus on the following aspects of crypto assets: (i) offering; (ii) trading; (iii) custody; and (iv) exposure to crypto assets. In many cases, crypto-trading platforms have multiple roles. For example, some crypto exchanges issue their own stablecoins and provide trading of the coins. At the same time, they provide a wallet service for the coins and hold some amount of coins as their inventory. If a subject entity provides multiple functions and services, it is

[23]As noted previously, a dedicated Fintech Note on modernizing legal frameworks is expected to be published in due course.

[24]Please understand that this note concentrates on financial regulatory implications of crypto assets and purposely leaves out a detailed evaluation of AML/CFT considerations, which will be discussed in an upcoming Fintech Note.

important to consider applying regulations relevant to each function.

Offering Crypto Assets

The way crypto assets are created and distributed may generate investor protection concerns. The process of mining, by which newly minted assets are distributed ad hoc to those persons as determined by a specific protocol (for example, Bitcoin miners), does not seem to entail major risks to investors at the creation stage, since those acquiring the assets are limited and presumably knowledgeable of their characteristics and risks.[25] However, the distribution of crypto assets that is undertaken as an offer to some investors or to the general public could raise risks to investors that deserve addressing. That would typically be the case when the assets that are the subject of the offer are, or will be, transferable and tradeable in any type of secondary market.[26] In those cases, the public policy need emerges to ensure that investors are able to make informed decisions based on timely and accurate information. A similar consideration can be made for those crypto assets that are not the subject of a public offer but rather made directly available to the public via a secondary market (see later section on trading crypto assets), as investors or users should also be provided with enough information on the issuers and relevant assets before acquiring them.

It is essential to consider financial and technology literacy needs. There are already multiple types of crypto assets and more continue to be developed, with different features, uses, and risks. Yet the understanding of the financial and technology implications of each crypto asset is generally low; this partly stems from the complex nature of the assets and the fast-changing technological environment, but also from the lack of clear and reliable information available to the public. There is a public policy need not only to ensure that the particularities and risks of each crypto asset are clearly and truthfully explained, but also to provide the public with enough education—beyond warnings and regulatory guidance—to be able to make informed decisions. As detailed in the Bali Fintech Agenda, developing adequate financial and technology literacy programs (for example, through initiatives at different education levels, tailored communication and outreach programs, and so on) should be considered a foundational element of any regulatory initiative.

Authorities should consider the need for appropriate disclosure requirements on public offerings of crypto assets. The disclosure of accurate, comprehensive, and timely information about issuers, as well as about the assets themselves, builds sustained investor confidence and allows for an informed assessment of performance and value. Authorities should consider potential requirements for the availability of information on crypto assets, both at the time of the initial offer and on a continual basis, so that investors and users can make informed decisions on the purchase and subsequent sale of the assets. The type of information disclosed may vary depending on the type of crypto asset being offered. Authorities should mandate that disclosure requirements provide a comprehensive description of the features and risks of each asset. For offers of stablecoins, for instance, this would likely include an assessment of the collateral underlying the coins, an explanation of rights governing access to the collateral, and a discussion of their stabilization and governance mechanisms.

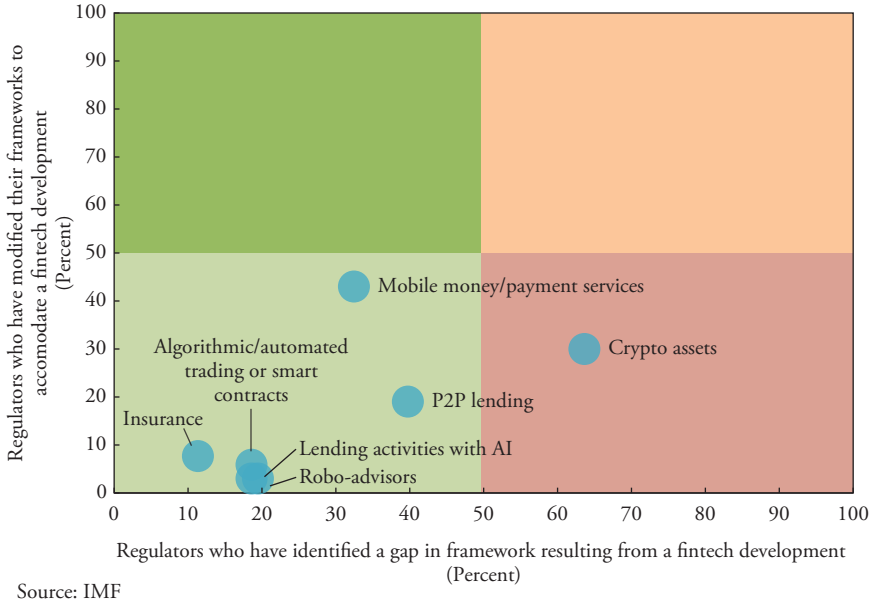
An appropriate disclosure regime would lead to more accurate pricing and enhanced investor protection. Requiring the disclosure of certain information for crypto-asset offerings would significantly reduce the number of investors falling for fraudulent offers, as those could be singled out more efficiently. It would also provide the investor or user the opportunity to make an informed decision on their purchase with adequate data and facts on the risks derived from the features of each crypto asset. Moreover, transparency and disclosure requirements can also assist with market efficiency, allowing for more accurate asset pricing. Finally, jurisdictions may consider the need for requirements to ensure the fair and equitable treatment of crypto-asset investors.

The existing regulatory framework may be too limited to prevent reputational risks to regulators and contain regulatory arbitrage. Some jurisdictions are applying the existing regulatory framework available

[25]The fact that the creation of those assets does not seem to entail risks to investors and may not trigger the application of specific investor protection regulation does not mean other activities related to those same assets are not subject to other risks for which regulation should be considered (for example, trading), as per the following sections. Please note that those assets could be prone to risks arising out of concentration issues (for example, by a small number of miners or agents) potentially vulnerable to manipulation, fraud, or a so-called "51 percent attack," a form of manipulation of a blockchain where a faulty consensus is formed by holding more than 50 percent of mining power.

[26]Some assets may involve initial transferability restrictions or lock-up periods but can become fully transferable and tradeable at a later stage.

Figure 5. Crypto Assets and Other Fintech Areas in a Context of New Frameworks
Crypto asset regulation is identified by respondents as the main (64 percent) gap, which so far has only been addressed by 30 percent of respondents.



Source: IMF

for securities to the offer of some crypto assets (those that meet the jurisdiction's legal definition of security).[27] This approach may be valid as an approximation to the subject, but it falls short of addressing many risks. In fact, many crypto assets would fall outside of the legal definition of a securities but still raise similar investor protection issues. Also, issuers may purposely seek to create crypto assets in such a manner as to escape the legal definition of a security or choose to issue in jurisdictions where that definition is narrower.[28] This jurisdictional approach also implies that the securities regulators will be forced to carry out much of their crypto-asset work through the active use of enforcement powers. Finally, the securities disclosure regime may not be adequate for all crypto-asset offers and authorities may want to consider an approach that can adapt to different asset or issuer features (Figure 5).

Some jurisdictions are already considering moving in this direction, for example:[29]

- In France, the recently approved Loi PACTE provides for a specific voluntary regime[30] for companies seeking to offer their crypto assets publicly (other than those qualifying as securities, which are bound by the securities regulatory regime). Potential

[27]Some examples of jurisdictions that have warned about the application of securities regulatory frameworks to some crypto assets are the Hong Kong SAR, Malta, Singapore, the United Kingdom, and the US SEC.

[28]The definition of a security is specific to each jurisdiction's legal system and it is typically complex and subject to court interpretation. The United States, for instance, has a very broad definition for a security, encompassing—among other things—any note, stock, treasury stock, security future, bond, debenture, evidence of indebtedness, certificate of interest or participation in any profit-sharing agreement, collateral-trust certificate, preorganization certificate or subscription, transferable share, investment contract, and so on—15 U.S.C. §77b(a)(1). The US Supreme Court has also interpreted the term "investment contract" for the purposes of the Securities Act in a broad manner, as it is considered to mean "a contract, transaction, or scheme whereby a person invests his money in a common enterprise and is led to expect profits solely from the efforts of the promoter or a third party" (SEC v. W.J. Howey Co.).

[29]For an in-depth discussion of the treatment of crypto assets in different jurisdictions, please refer to the relevant section of "Fintech: The experience so far" (IMF, Policy Paper No. 19/024 https://www.imf.org/en/Publications/Policy-Papers/Issues/2019/06/27/Fintech-The-Experience-So-Far-47056). The paper points out that some regulators have created special regulatory frameworks for crypto assets while most are taking a case-by-case approach. Only a few jurisdictions have provided specific guidance as to the types of licenses that are required, and the parts of the regulatory framework that are triggered by different types of activities with crypto assets. For most jurisdictions that have stated that securities legislation would apply to securities-like assets, the practicalities remain unclear and many questions unanswered (that is, how and to what extent securities regulation will be applied to each of the aspects of crypto assets issuance, offer, trading, and intermediation is generally not discussed).

[30]Please note that the voluntary nature of the regime can work well to reduce risks to investors but may fall short of an adequate solution to address regulatory arbitrage.

issuers can apply to the French securities regulator (Autorité des Marches Financiers, AMF) for a *visa* by submitting their white paper, which must include some detailed information (for example, a description of the project, rights conferred by the tokens, the legislative court in case of disputes, and the economic purpose and use of the funds collected during the offer).

- The Virtual Financial Asset Act (VFAA), which came into effect in Malta in 2018, also creates a specific regime for crypto assets, including public offering. Malta has created a new regulatory authority for the blockchain sector, the Malta Digital Innovation Authority, and regulates the offer of virtual assets, which are any crypto assets not qualifying as either electronic money, financial instruments (as per respective European Union legal definitions), or virtual tokens (akin to utility tokens).
- Japan's Financial Services Agency introduced a registration requirement to crypto-asset trading platforms in 2017 under the Payment Services Act (PSA) and it led crypto assets designated as payment tokens (such as Bitcoin) and as utility tokens to fall into the PSA scope. Subsequently, the Financial Instruments and Exchange Act (FIEA) (the acts for traditional security platforms) is to be amended to define and regulate crypto assets designated as investment-type tokens, which are regarded as securities. The PSA and FIEA aslo provide more robust frameworks to proote user protection and clarify applicable rules. The revised acts will come into force by June 2020 at the latest.

Trading Crypto Assets

While there are some differences in the way they operate, crypto asset trading platforms and exchanges raise many similar issues to those of securities trading platforms. Crypto platforms differ from securities platforms in two main ways: they typically permit direct access by retail investors and they may also provide custody services. Some crypto asset trading platforms resemble stock trading venues, but others may be directly accessed by clients and therefore resemble more a market intermediary than a trading platform (see Box 1). 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 platforms and from the provision of custodial services.

The work of IOSCO on crypto asset trading platforms is particularly relevant. While still in the consultation phase, IOSCO has put forward a report on the issues, risks, and regulatory considerations relating to crypto-asset trading platforms that examines the main issues surrounding secondary market trading of crypto assets. The document points to the relevant sections of the IOSCO principles and methodology that would be helpful for authorities when considering potential regulation and supervision of crypto-asset platforms. All of the elements considered below are covered by IOSCO's consultation report in more detail and with clear references to other IOSCO materials when relevant.

When building a regulatory framework for crypto-asset platforms, authorities should consider the following elements:

- **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 is added, calling for risk-based capital requirements.
- **Requirements regarding access to the platform**. Protecting the orderly functioning of trading usually requires 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.[31]
- **Requirements for the robustness, resiliency, and integrity of operating systems**. One of the main vulnerabilities of crypto-asset platforms has been cyber-attacks. Adequate processes and controls can help protect them from hacking or theft and provide reassurance that they are otherwise robust and resilient enough to provide trading integrity.
- **Market integrity requirements**. Crypto assets are prone to manipulation, due to their high volatility,

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

potential conflicts of interests/concentration issues, and low level of disclosure. Authorities should consider what market abuse rules and surveillance mechanisms should be in place to adequately protect investors.

- **Transparency requirements**. To promote the efficiency and integrity of trading, it is important to understand the extent of pre- and post-trade information, to whom it is made available, via what 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 FATF standards for AML/CFT.
- **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 and to ensure adequate disclosure to investors and 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 there is a need for regulatory determination of the types of assets that can be accepted for trading or if there is a need to be otherwise involved in the process of product listing.
- **Custody**. Crypto-asset trading platforms may also hold custody of client assets, as opposed to traditional securities trading platforms (see Box 1). Therefore, authorities should consider what measures are required to safeguard clients' assets: to ensure an orderly liquidation and return of client assets in the event the platform closes down, to prevent the use of clients' assets for proprietary purposes, and to facilitate the prompt identification and transfer of positions. See the next section for a discussion on a regulatory approach to custodial services.
- **Clearing and settlement implications**. In addition to custody, crypto-asset trading platforms may also perform clearing and settlement activities (typically carried out by third parties in traditional securities trading). Understanding how legal transfer of ownership of the assets takes effect is key to ensuring smooth functioning of these services. Legal certainty may vary considerably depending on the legal framework of the jurisdiction where the service provider is located. Authorities should also consider what internal record keeping and accounting systems platforms use and whether they are appropriate to ensure that clients are correctly and timely allocated funds and assets.
- **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 and to ensure adequate disclosure to investors and 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 there is a need for regulatory determination of the types of assets that can be accepted for trading or if there is a need to be otherwise involved in the process of product listing.

Custody of Crypto Assets

Custody of crypto assets takes place via wallets. A wallet is a file (or the software used to manage it), in which a unique private key, akin to a password, and the public key, the user's "address" in the form of an alpha-numeric string, are stored for the crypto assets owned by a user. The ownership of crypto assets relies on knowing the private keys stored in the wallet—if a wallet file (and thus private keys) is lost, then the crypto assets "stored" in it are unrecoverable.

Key characteristics of wallets that need consideration from a regulatory perspective are custodianship and type of storage and security of private keys. In terms of custodianship, 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 can also be a third-party service provider. In terms of storage, wallets can be classified as "hot" or "cold"; those that are kept online and connected and those that are kept offline, respectively.

Cold and hot wallets face different types and degrees of risk. Because the function of a wallet is only to store the crypto asset's private key, a cold wallet can be as simple as a paper put in a deposit box or an encrypted file on a thumb drive. In this case, the risks of loss or physical damage to the wallet are greater, but cyber risks are eliminated until the user needs to use the wallet and, thus, change its status from cold to hot. Most users and crypto-trading platforms alike use cold wallets for storing most of their crypto assets and only keep what is needed for transactions in the short term in a hot wallet. Additionally, there is no clear delineation between cold and hot wallet technologies. A hot wallet becomes cold upon disconnecting it from the network and vice versa.

Wallets are the components of crypto-asset systems that are most exposed to cyber risk. Specifically, attackers target the private keys in hot wallets, as obtaining them equates to impersonating the owner and the ability to steal the funds from corresponding wallets. Attacks against cold wallets, while much more difficult, are also possible. Thus, 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. Also, due to the unclear delineation between cold and hot wallet technologies, requirements should not concentrate on this level of technical detail and remain principles based (for example, requiring that wallet protection measures be proportionate at all times with the security risk they are exposed to).

In addition, there is a compelling case for the prudential regulation of third-party wallet service providers to afford a degree of protection for customers and to mitigate contagion risk to other parts of the financial sector. By allowing a third party 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, as well as operational failures or theft or loss of private keys. Therefore, it is recommended to consider if those wallet providers should be subject to some reporting and prudential regulation requirements, such as risk management, including operational and cyber risk, protection of client assets, minimum capital, and liquidity requirements (particularly in case the third-party reuses the customer's crypto assets).

Exposure to Crypto Assets

Currently, there is no global standard for the prudential treatment of exposures to crypto assets for banks or other regulated entities. Most jurisdictions have not yet clarified prudential treatment of crypto-asset exposures, and thus supervised entities might be treating those exposures differently. For example, crypto-asset positions could be classified as intangible assets, cash, or commodities, and depending on the classification, their prudential treatment could be completely different.

Forthcoming international standards are likely to reflect high risks of crypto assets. The Basel Committee on Banking Supervision has issued a statement on crypto assets, noting that "The committee will in due course clarify the prudential treatment of such exposures to appropriately reflect the high degree of risk of crypto assets." The statement also described minimum expectations on due diligence, risk management, and disclosure.[32]

High volatility of crypto assets warrants a conservative treatment on direct exposures. Regulated entities could be vulnerable to high risks from the direct exposures to crypto assets due to their high volatility. It is expected that prudentially regulated financial institutions 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 business and crypto business is desirable, although group-wide and step-in risk would also need to be considered even when crypto businesses are located in a separate entity.

Exposures to stablecoins could incorporate benefits from their collateral only if the issuers are subject to appropriate regulation and supervision. Many stablecoins are reported to be fully backed by safe and reliable collateral, such as hard currencies, bank deposits and government bonds. In principle, good quality collateral could be reflected in the prudential treatment of the exposures. However, many of the issuers are not subject to financial regulation, and there may be legal uncertainty regarding the availability of collateral in a stressed environment. The risk mitigation provided by collateral should only be reflected in the prudential treatment of exposures if robust safeguards are in place, such as prudential regulation and supervision covering

[32]BCBS statement on crypto assets (https://www.bis.org/publ/bcbs_nl21.htm)

the ownership and availability of the collateral by the financial regulator or the central bank.

Financial institutions are encouraged to monitor their indirect exposures. While most financial institutions seem to have conservative investment policies toward crypto assets, they might be exposed to them indirectly. This could be through loans to crypto investors, derivative exposures with crypto-asset trading platforms, cyber insurance to wallet providers, and so on. While such risks brought by indirect exposures are not the same as from direct exposures, they can be strongly correlated with market movement. Financial institutions are therefore expected to monitor their indirect exposures to crypto assets.

Prudentially regulated financial institutions also need to manage risks arising from their role as issuers of crypto assets or crypto-asset-linked products. Some banks have or are planning to issue coins and tokens (such as JP Morgan—JPM Coin; UBS—Utility Settlement Coins; and MUFG Bank—MUFG Coin) for more efficient payments and more effective delivery versus payment of securities settlements. Some financial institutions have already issued structured bonds linked to crypto assets. Some may issue stablecoins for domestic or cross-border payment services or trade financing. Some of those are economically similar to deposit taking activities and thus should be subject to existing prudential regulation, such as the liquidity coverage ratio and net stable funding ratio requirements on those activities. Careful analysis would be needed if a separate issuing entity is established "independently" from prudentially regulated financial institutions. While banks may not be legally obliged to meet redemption requests to the issuing entity, banks may face strong pressure to step in and provide liquidity to the issuing entity if this could cause reputational risk for the group. In any case, financial institutions are expected to manage operational risk (arising from the platform operation of cross-border payment services) and conduct risk when issuing structured bonds). See Box 3.

Handle with Care

Ultimately, developing an adequate regulatory framework for this quickly evolving industry will involve intense monitoring and a flexible approach. Crypto assets are at the core of the fintech revolution, and developments will direct the regulatory and supervisory focus in different directions until the industry matures. 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 for the more traditional 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 thus foster confidence. Regulators need to take a proactive approach to address any risks potentially emerging from industry developments and swiftly build capacity and expertise in new instruments and new technology given the high reputational risks involved. Capacity and resources of supervisory authorities, as well as potential damage to trust in the financial sector will need to be evaluated in each case. Moreover, regulators also need to clearly communicate the role of regulation and supervision to the public, emphasizing the risks which are borne by investors and consumers. That is important to avoid misunderstanding or over-trust in any new regulation or the role of the authorities.

Finally, the cross-sector and cross-border dimensions of crypto assets make domestic and international coordination and cooperation key. In some cases, it may be challenging to determine the geographic location[33] and therefore the jurisdictional powers over some of these assets. While regulation should 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. Given the cross-border and global accessibility aspects of crypto assets, domestic regulatory measures that do not consider cross-border issues and overseas regulatory measures may create opportunities for cross-border regulatory arbitrage. Cross-border transactions may also

[33]While the issuing entity or the main IT system is located in a jurisdiction, the main activities (such as marketing, solicitation) tend to be 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: i) the marketing website was located on a server in Arizona, ii) it was also run primarily by an individual in California, iii) the marketing was almost exclusively targeting US residents, and iv) validating nodes were densely populated in the United States.

Box 3. A Special Mention of Distributed Ledger Technology Adaptations by Financial Institutions: JPM Coin

In February 2019, J.P. Morgan Chase N.A. announced JPM Coin, focusing on its wholesale clients. JPM Coin is based on blockchain technology enabling the instantaneous transfer of payments among JPM group's institutional clients. JPM Coin is a digital coin representing US dollars held in designated accounts at JPMorgan Chase N.A. Other financial institutions have also initiated similar projects and coins, such as Utility Settlement Coins by UBS and others and MUFG Coin by MUFG Bank. This box is focusing on JPM Coin to illustrate how existing financial institutions are adopting new technologies, which might eventually help the existing financial institutions to compete with fintech innovations.

Potential use cases of JPM Coins include i) cross-border payments; ii) delivery versus payment between tokenized securities and the coin; and iii) internal liquidity optimization for large, complex corporate clients. Instantaneous transfer of payments would be available 24 hours, 7 days a week, every day of the year. The coin could be used to settle tokenized securities transactions where simultaneous delivery versus payment could become available. The JPM Coin will be issued on Quorum Blockchain and subsequently extended to other platforms. JP Morgan Chase N.A. states that JPM Coin will be operable on all standard blockchain networks. Finally, corporate clients would be able to minimize liquidity needs within the group significantly when the instantaneous transfer of liquidity is available, allowing complex international groups to centralize their liquidity pool globally.

The holder of the coin can redeem it for the equivalent amount of US dollars, similar to the bank's demand deposit. JP Morgan Chase N.A. plans to extend the coin to other major currencies. Only institutional customers passing the JP Morgan Chase Bank "Know-Your-Customer" standards and onboarded for the JPM Coin can transact with JPM Coins. The prototype test has been successfully completed. The coin would be managed under a private blockchain. As explained, it is limited to wholesale users and, thus, scalability and capacity of the system would not be a binding constraint for the time being. This approach could potentially be expanded to retail payments once new technologies have addressed scalability and capacity constraints, or interbank payment systems have been upgraded.

Risks associated with the JPM Coin are similar to its wholesale bank deposits. Holders of the coin are exposed to the default risk of JPMorgan Chase N.A., unless covered by Federal Deposit Insurance Corporation. Holders might be exposed to operational and cyber risk, while the risk would not be as high as that of other crypto currencies issued under public blockchains. JP Morgan Group would face liquidity, operational, and cyber risks, however those risks would be similar to those of traditional banking operations, both in terms of nature and scale. However, it should be noted that faster transfer of the coins would require an upgrade of liquidity risk management by the individual branch and entity of the JPMorgan Group.

Existing regulations (such as capital and liquidity requirements) could be well fit to the risks to which holders of JPM Coins and JP Morgan Chase N.A. would be exposed. Holders of JPM Coins would treat exposures (such as the risk weight for capital requirement and recognize it properly for the liquidity requirement) as they would for the same amount of bank deposits. JP Morgan Chase N.A. itself would treat the issuance and corresponding assets in the same manner as the assets and liabilities derived from traditional deposit taking activities. Supervisors would address operational and cyber risk of both the coin holders and JP Morgan. If that is the case, there should not be any material regulatory gaps.

cause other challenges, such as undesired complexity in assessing the drivers of capital flows and the diminished effectiveness of domestic policy responses, such as monetary policies and macroprudential measures. To mitigate those risks, it is important for authorities to enhance cross-border cooperation. The need for new mechanisms for regulatory cooperation is likely to increase in the future.

Appendix I. Illustrative examples of crypto assets—related risks

Risk category	Can be realized through….	Example
Investor protection risk	**Operational and cyber risk of wallet providers and crypto-trading platforms**[1]	In May 2019, one of the largest crypto exchanges by trading volume (Binance) suffered from cyber-attacks with a total of $41 million in Bitcoin being stolen.[2] Sixteen million dollars were stolen from digital asset exchange Cryptopia in January 2019.[3] Exchanges CoinBene and DragonEx lost a combined $46 million dollars' worth of Ethereum-based tokens through attacks disclosed in March 2019.[4] South Korean exchange Bithumb was also rocked by its third attack, when $13 million worth of coin was lost in March.[5] Later reports suspected a further $6 million in Ripple had also been taken. Coinbin, another South Korean exchange, was forced into bankruptcy last quarter—roughly $26 million had been lost.[6] Investors in QuadrigaCX, Canada's largest cryptocurrency exchange, were unable to access their funds (about $190 million) after its founder, Gerald Cotten, died in December 2018. According to an Ernst & Young (the bankruptcy auditor) report issued in May 2019, a significant number of clients' assets had been transferred to the founder's private accounts.[7]
	Market, credit, and default risks of coins/tokens' issuers	The New York Attorney General's office has alleged that crypto-exchange Bitfinex, which lost $850 million, subsequently used funds from affiliated stablecoin operator Tether to cover the shortfall.[8]
	Market integrity risk	The majority of crypto asset trading occurs over centralized exchanges (with custody and centralized settling) but decentralized cryptocurrency exchanges (DEXes) allow for more direct trading and are gaining more prominence. Researchers at Cornell Tech recently found that high-frequency trading on these exchanges is using autonomous algorithmic trading programs to take advantage of ordinary users' trading patterns and other market manipulation techniques.[9]
	Commingling risk	In Italy, an exchange called BitGrail that was hacked was also found responsible during the court proceedings to frequently deposit customer funds into wallets directly under Firano's (the exchange's owner) control.[10]
	Market integrity risk	The vast majority of the almost 2,500 crypto assets listed on CoinMarketCap.com are not backed by anything tangible. Only 66 stablecoins—30% of total announced tokens—are actually live and operational.[11] By market capitalization, the top 10 comprise about 90%, of which Tether (the only stablecoin in the top 10) comprises less than 2%. However, it should be noted that by 24h trading volume it comprised 37% of that top 10 group.
	Risk of mis-selling and fraud	The Wall Street Journal conducted an analysis of 3,291 crypto assets white papers and concluded that 16% showed signs of plagiarism, identity theft, and promises of implausible returns. At least 61% contained luring terms such as "nothing to lose," "guaranteed profit," "highest return," "no risk." US state and federal regulators have previously issued cease-and-desist orders on various offerings with similar language.[12]
AML/CFT risk		There have been a number of high-profile money laundering cases, for example, AlphaBay, the largest online criminal marketplace on the Internet, where more than $1 billion was exchanged through crypto assets until the US District Court of Eastern California shut it down in a multinational law enforcement operation. The platform allegedly was 10 times larger than its predecessor, Silk Road.[13]
Prudential and systemic risks	**Prudential risk**	The ECB Crypto-Assets Task Force published a paper in which it provides recommendations for the prudential treatment of crypto assets.[14] It advocates measures such as subtracting crypto assets exposures from CET1 or requiring the segregation of crypto business to ensure FMI's safety. The BCBS issued a statement setting out its prudential expectations related to banks' exposures to crypto assets and related services that will further clarify the prudential treatment of such exposures in the future.
	Business model risk	There is potential blurring of lines between the regulated financial institutions business models and unregulated crypto assets and exchanges as more and more FIs engage with crypto assets. For instance, IBM has signed six banks to issue stablecoins on its Stellar public blockchain. At the same time, multiple banks have announced their interest in issuing stablecoins and JP Morgan has confirmed it is working on a digital coin for payments.
	Systemic risk	BCBS has warned that the crypto industry can potentially "raise financial stability concerns and increase risks faced by banks."[15]

Note: AML/CFT = anti–money laundering/combating the financing of terrorism; BCBS = Basel Committee on Banking Supervision; CET1 = common equity tier 1; ECB = European Central Bank.

[1]Due to the large volume of hacks, it is impossible to provide evidence (albeit it is available in public domain) of the entirety of crypto-exchange hacks and funds lost, therefore, we only cite the most recent incidents.

[2]Lam, Eric. 2019. "Hackers steal $40 million worth of Bitcoin from Binance Exchange." Bloomberg, May 7.

[3]Khatri, Yogita. 2019. "Hacked exchange Cryptopia discloses estimate of stolen crypto." Coindesk. Feb. 27.

[4]Cimpanu, Catalin. 2019. "Cryptocurrency platforms DragonEx and Coinbene disclose hacks." Zero Day Net, March 27.

[5]Zhao, Wolfie. 2019. "Crypto Exchange Bithumb Hacked for $13 Million in Suspected Insider Job." Coindesk, March 30.

[6]Kramer, Melanie. 2019. "Embezzlement, $26 Million Loss Bankrupts Korean Crypto Exchange Coinbin." CNN, Feb. 24.

[7]Alexander, Doug. 2019. "Investigation uncovers mystery of Quadriga's missing cryptocurrencies worth millions." Insurance Journal, June 21.

[8]De, Nikhilesh. 2019. "Bitfinex covered $850 million loss using Tetherfunds, NY prosecutors allege." Coindesk, April 25.

[9]Daian, Philip, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach and Ari Juels. 2019."Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges." ArXiv abs/1904.05234.

[10]Zmudzinski, Adrian. 2019. "Owner of Hacked Crypto Exchange BitGrail Sentenced to Return Funds to Customers." Cointelegraph, Jan. 28.

[11]Boddy, Max. 2019. "Research: Only 30% of Known Stablecoins Are Live and Operational." Cointelegraph, June 28.

[12]Shifflett, Shane, and Coulter Jones. 2018. "A flood of questionable cryptocurrency offerings." The Wall Street Journal, Dec. 26.

[13]Hui, Ada. 2018. "US Government Seizes Lambo and Crypto Millions from Dead Dark Web Kingpin." Coindesk, Sept. 17.

[14]European Central Bank (ECB) Crypto-Assets Task Force. 2019. *Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures*. ECB Occasional Paper 223. Frankfurt am Main, Germany: European Central Bank.

[15]Bank for International Settlements. 2019. "Statement on crypto assets," March 13. https://www.bis.org/publ/bcbs_nl21.htm.