Financial Stability Institute

FSI Insights
on policy implementation
No 49

Crypto, tokens and DeFi: navigating the regulatory landscape

By Denise Garcia Ocampo, Nicola Branzoli and Luca Cusmano

May 2023

JEL classification: F30, G18, G28, O38
Keywords: cryptoasset, cryptoasset service provider, decentralised finance, DeFi, DLT, global stablecoin, stablecoin, token, tokenised asset, virtual asset, virtual asset service provider.

BANK FOR INTERNATIONAL SETTLEMENTS

FSI Insights are written by members of the Financial Stability Institute (FSI) of the Bank for International Settlements (BIS), often in collaboration with staff from supervisory agencies and central banks. The papers aim to contribute to international discussions on a range of contemporary regulatory and supervisory policy issues and implementation challenges faced by financial sector authorities. The views expressed in them are solely those of the authors and do not necessarily reflect those of the BIS or the Basel-based committees.

Authorised by the Chair of the FSI, Fernando Restoy.

This publication is available on the BIS website (www.bis.org). To contact the BIS Media and Public Relations team, please email press@bis.org. You can sign up for email alerts at www.bis.org/emailalerts.htm.

ISSN 2522-249X (online)
ISBN 978-92-9259-656-9 (online)

Contents

Crypto, tokens and DeFi: navigating the regulatory landscape[1]

Executive summary

Addressing the risks posed by cryptoassets has become a pressing issue for policymakers. Cryptoasset markets have experienced cycles of growth and collapse, often resulting in large losses for investors. These markets pose risks which, if not adequately addressed, might undermine consumer protection, financial stability and market integrity. While the turmoil experienced in these markets at the end of 2022 has so far not led to wider contagion, the outcome might have been worse had the cryptoasset markets and the traditional financial system been more interconnected.

Policymakers are considering their response to crypto-related risks. Potential lines of action, which are not mutually exclusive, include banning specific activities, isolating cryptoasset markets from the traditional financial system, regulating cryptoasset activities in a manner akin to traditional finance and developing alternatives that improve the efficiency of the traditional financial sector (Aquilina et al (2023)). These lines of action will be contingent on the risks posed to the provision of financial services by the various activities involving cryptoassets and their underlying technology, referred in this paper under the umbrella term of distributed ledger technology (DLT). For lines of action which consider regulating cryptoasset activities, the question depends on policymakers' assessment of which risks posed by cryptoassets and related activities should be captured by regulation and whether those risks are captured by existing regulation or if there are gaps that need to be addressed.

This paper provides an overview of policy measures taken in 19 jurisdictions to address the risks associated with activities that incorporate cryptoassets and DLT programmability capabilities in financial services. [2] In this paper cryptoasset activities are classified into three categories based on the proposed taxonomy by the FSB:[3] (a) issuance; (b) operation of a DLT infrastructure; and (c) service provision (eg wallet, custody, payment, exchange, lending). For the overview of policy measures, initiatives are classified into three categories depending on whether they address the risks associated with (i) centrally managed cryptoasset activities; (ii) community-managed cryptoasset activities;[4] or (iii) users' direct exposures to cryptoassets and related activities.

Different types of policy measure across jurisdictions include bans, restrictions, clarifications, bespoke requirements and initiatives to facilitate innovation. As these measures tend to reflect the evolution of market developments, most current initiatives target centrally managed cryptoasset activities, with a particular focus on service provision.

[1] Denise Garcia Ocampo (Denise.GarciaOcampo@bis.org), Bank for International Settlements, Nicola Branzoli (Nicola.Branzoli@bancaditalia.it) and Luca Cusmano (Luca.Cusmano@bancaditalia.it), Bank of Italy.

The views expressed in this paper are those of the authors and not necessarily those of the BIS, the Basel-based standard setters, the Bank of Italy or the authorities of the jurisdictions covered within it. The authors thank Patrizia Baudino, Carlos Cantú, Stijn Claessens, Emma Claggett, Renzo Corrias, Juan Carlos Crisanto, Nicole Detering, Sebastian Doerr, Tomas Edlund, Daniel Eidan, Johannes Ehrentraud, Jon Frost, Leonardo Gambacorta, Martin Hood, Wenqian Huang, Eva Hupkes, Dooyoung Kim, Ayu Kinanti, Priscilla Koo Wilkens, Anneke Kosse, Theodora Mapfumo, Amelie Monteil, Iota Nassr, Liz Owen, Jermy Prenio, Tara Rice, Hyun Song Shin, Joon Suk Park, Greg Sutton, Jatin Taneja, Toshio Tsuiki, Carolina Velasquez, Oliver Wray, John Yeo, Kean Yong and contacts at the authorities from the jurisdictions covered in this paper.

[2] The jurisdictions covered in this paper are Australia, Belgium, Canada, China, the European Union, France, Germany, Hong Kong SAR, Italy, Japan, the Netherlands, the Philippines, Singapore, South Africa, Spain, Switzerland, the United Arab Emirates, the United Kingdom and the United States.

[3] See FSB (2022c).

[4] These refer to activities managed (ie, operated and governed) by a community of participants in public DLT networks organised under decentralised arrangements.

For centrally managed issuance activities, current regulatory initiatives focus mainly on issuers of security tokens and stablecoins. All the jurisdictions we cover here require issuers of security tokens to comply with securities regulation. Some are developing frameworks for issuers of stablecoins used for payment. The proposed initiatives introduce licensing, capital and reserve requirements but differ across countries in terms of terminology, type of license, redemption rights and standards for governance and risk management practices. Only a small number have adopted a regulatory framework for issuers of stablecoins used for other purposes. Furthermore, only a few have clarified whether securities laws apply to issuers of utility tokens.

Initiatives related to centrally managed infrastructure activities mainly explore the benefits and risks from traditional financial intermediaries' use of DLTs and their programmability capabilities. Some jurisdictions are collaborating in pilot testing use cases of DLT-based infrastructures for the clearing and settlement of payments and securities. Others are facilitating innovation in a controlled environment through bespoke licensing regimes and sandboxes. Only one jurisdiction has issued DLT-specific guidance.

Initiatives related to centrally managed service provision activities often extend the regulatory perimeter to new non-bank centralised intermediaries. Most jurisdictions have introduced authorisation, prudential, anti-money laundering/combating the financing of terrorism (AML/CFT) and consumer protection requirements. Regulatory approaches include establishing bespoke frameworks, introducing specific derogations from the applicable legislation, issuing clarifications on how existing payments or securities regulation apply, and restricting or prohibiting certain activities.

In relation to community-managed activities, policy measures aim at addressing the risks posed by native tokens and DeFi protocols. For activities where native tokens are involved, some authorities rely on a broad interpretation of "rights" attached to a native token to define if it is a security and thus clarify the application of securities regulation. Others use concrete examples for additional guidance. For DeFi protocols, most initiatives were in the form of analytical papers. At present, only one authority in the covered jurisdictions has issued guidance on the adoption of smart contracts. Another has clarified the applicable requirements related to decentralised exchanges and staking activities**.** A few authorities have taken enforcement actions addressing AML/CFT and investor protection risks posed by certain protocols. A small number have introduced initiatives to facilitate the adoption of protocols with certain features by traditional financial intermediaries under a trusted environment.

For risks associated with users' direct exposures to cryptoassets and related activities, initiatives tend to reflect the evolution of cryptoasset markets. All the jurisdictions covered have issued warnings to retail investors about the risks posed by cryptoassets, and some of these warnings target specific types of cryptoasset (eg native tokens, security tokens and non-fungible tokens). A few jurisdictions have banned the distribution of certain cryptoassets to retail investors and others have imposed restrictions on promotional activities. For wholesale investors, no jurisdiction has so far introduced rules to mitigate risks stemming from traditional financial institutions investing in cryptoassets.

Policymakers may face further challenges as cryptoasset markets evolve and DLT programming capabilities are applied to new use cases. Continuous efforts will be needed to understand novel business models and their underlying risks, to build or maintain the skills and capacity to adequately assess potential implications on financial markets and to adjust policy responses promptly. Only with sufficient resources and access to timely and reliable information will authorities be able to assess future risks to the financial system.

The global nature of cryptoassets poses significant challenges that require effective cooperation and coordination among national and international regulators. Jurisdictions cannot entirely mitigate the risks associated with cryptoassets if policy measures are susceptible to gaps and inconsistencies across borders. A coordinated response is essential. In this context, international standards that promote a consistent regulatory framework will play a key role in preventing regulatory arbitrage and a fragmented regulatory environment that could undermine financial stability.

Section 1 – Introduction

1. **Advances in cryptography, computing science and computing power have transformed digital ledgers.** These developments have enabled the creation of technologies, referred to in this paper under the umbrella term of distributed ledger technology (DLT),[5] that allow a network of participants to establish a shared and immutable record of ownership – a ledger with functionalities that go far beyond those of traditional ledgers. DLTs allow participants to share a database of electronic records and build consensus for transaction validity through cryptographic algorithms[6] without a central coordinating entity. Transactions can be recorded by one, some or all participants, regardless of their reliability, according to the rules agreed by the network, and any change is replicated in all copies in minutes or even seconds. Some DLTs also enable the programming or automation of transactions within the ledger.

2. **DLTs have enabled the creation of cryptoassets and decentralised finance (DeFi).** Although the concept of DLT existed before Bitcoin and blockchain (Rauchs et al (2018)), it was not until the publication of Satoshi Nakamoto's whitepaper in 2008 that this technology started to attract attention**.** Cryptoassets emerged when Bitcoin developers combined various technological components to create a new way to represent and transfer value between multiple parties without the need to trust each other. Bitcoin blockchain provided a basic framework which served as the foundation for different types of DLT and DLT-based application. As the technology evolved, some DLTs incorporated new functionalities such as so-called smart contracts. Building on cryptoassets and public permissionless DLTs that support smart contracts, DeFi emerged as an alternative way to offer financial services such as borrowing, lending or investing without relying on a traditional centralised financial intermediary (Auer et al (2023)).

3. **DLTs can also be used to represent and transfer different types of real-world assets.** Aiming to lower costs, increase efficiencies and offer new services, some traditional intermediaries are leveraging the use of DLT programmability capabilities for the representation and transfer of traditional assets.[7] Similarly, several exchanges and market operators are also exploring the use of DLTs as a new type of financial market infrastructure that may enable real-time settlement and automation of processes related to cross-border payments and securities clearing, settlement and trading processes.

4. **Activities that incorporate cryptoassets and DLT programmability capabilities promise to open up opportunities for the provision of financial services but come with risks and challenges.** For example, holding cryptoassets may pose a number of risks for investors including liquidity risk, credit risk, market risk, operational risk (including fraud and cyber risks), money laundering and terrorist financing risk, and legal and reputational risks (BCBS (2019)). Also, economic, legal and technical challenges may arise in relation to transferring assets from traditional ledgers to representations on DLT programmable ledgers (Aldasoro et al (2023)).

5. **Cryptoassets and DeFi ecosystems show structural flaws and pose risks that, if not addressed, might undermine consumer protection, financial stability and market integrity.** The turmoil faced in 2022 (also referred to as the "crypto winter") revealed that cryptoasset and DeFi ecosystems exhibit many of the vulnerabilities familiar from the traditional financial system, such as operational fragilities, liquidity and maturity mismatches, leverage and interconnectedness (Aquilina et al (2023), FSB (2023)). So far, these vulnerabilities have not affected the traditional financial system due to the relatively small size of cryptoasset markets and their limited interconnectedness with traditional

[5] Annex A contains a glossary of terms.

[6] Cryptographic algorithms are the basic building blocks of cryptographic systems. They are mathematical functions or algorithms used to ensure the security, integrity and privacy of electronic records. Examples include hash functions, symmetric and asymmetric key cryptography, digital signatures, Merkle trees and consensus mechanisms. See Rauchs et al (2018).

[7] In the past few years, some banks and international organisations have issued tokenised versions of bonds, including the World Bank, the European Investment Bank, Nomura and Société Générale. Several intermediaries have experimented with the tokenisation of a variety of real-world financial assets (eg JP Morgan, HSBC, Mitsubishi UFJ Financial Group). See OECD (2020).

markets. However, should investor interest not decline following the "crypto winter" and considering that interconnectedness and market concentration in the cryptoasset ecosystem is expected to intensify, a future scenario of turmoil in a larger cryptoasset market could have implications for financial stability (Aquilina et al (2023), FSB (2023)). Moreover, cryptoassets may also pose a threat to the monetary sovereignty of states that are less macroeconomically stable (Aquilina et al (2023)) and may create issues of cryptoisation (ie, the substitution of local currencies with cryptoasset-based ones) (IMF (2021)).

6. **Against this background, discussions among policymakers have intensified over how an appropriate regulatory framework should look.** For new business models that are not yet captured by existing regulatory frameworks, the overarching question is whether they should be inside or outside the regulatory perimeter.[8] If they are inside, the question is how regulatory requirements should apply. For activities or entities that are already subject to existing regulations, the question is whether adjustments can foster innovation that could benefit society while not compromising other policy objectives; or whether stricter requirements are called for.

7. **Regulation of cryptoassets and related activities present policymakers with a number of challenges.** First, cryptoassets and related activities are within the purview of many financial and non-financial authorities, each with its own mandate and policy objectives, requiring enhanced cooperation. Second, the pseudonymous and borderless nature of DLT-based applications deployed in public permissionless networks make it challenging for authorities to identify the applicable legal jurisdiction and the entities or individuals accountable for meeting regulatory obligations. Third, the lack of transparency, consistency and the unreliability of data make it difficult for authorities to monitor and assess risks stemming from these activities and their potential spillovers to the financial system.[9] Fourth, the speed of innovation makes it difficult for regulators to respond promptly to developments in the market.

8. **Cryptoassets have also been at the forefront of the regulatory agenda at the international level.** International standard-setting bodies (SSBs) have undertaken a number of initiatives to capture risks not previously covered in their frameworks, clarify the application of existing principles and promote the development of effective and internationally consistent regulatory frameworks. The BCBS has published prudential standards for banks' activities and exposures related to cryptoassets.[10] The FATF has amended the scope of their standards and recommendations to apply to financial activities involving cryptoassets and cryptoasset service providers.[11] The CPMI-IOSCO has clarified the application of existing principles of financial market infrastructures to stablecoin arrangements primarily used for payments that are considered systemically important financial market infrastructures.[12] The FSB has published high-level

[8] The regulatory perimeter describes the boundary that separates regulated and unregulated financial services activities and determines the type and scope of rules (eg on licensing, safety and soundness, consumer/investor protection and/or market integrity) applicable to firms conducting regulated activities.

[9] According to a recent report by the FSB, data on cryptoasset markets in general, and DeFi in particular, are opaque, inconsistent, and unreliable. This is due to the difficulty of aggregating, reconciling and analysing the vast amount of data available on distributed ledgers; the pseudonymous nature of information on public ledgers, which limits the ability to determine the types of crypto-asset investor involved; the large number of off-chain transactions and other off-chain data; complex ownership structures and loan/investment relationships; and the lack of, or non-compliance with, reporting requirements producing consistent results. See FSB (2023).

[10] See BCBS (2022).

[11] See FATF (2019, 2021).

[12] A stablecoin arrangement (SA) is an arrangement that combines a range of functions to provide an instrument that purports to be used as a means of payment and/or store of value. The CPMI-IOSCO guidance on the *Application of the Principles for Financial Market Infrastructures (PFMI) to stablecoin arrangements* covers systemically important SA primarily used for payments. The transfer function of a SA is comparable to the transfer function performed by other types of financial market infrastructure (FMI). As a result, an SA that performs this transfer function is considered an FMI for the purpose of applying the PFMI and, if determined by relevant authorities to be systemically important, the SA as a whole would be expected to observe all relevant principles in the PFMI. See CPMI (2022).

recommendations for the regulation, supervision and oversight of global stablecoin arrangements[13] and a proposal for the framework for the international regulation and supervision of cryptoassets activities and their markets.[14]

9. **This paper provides an overview of policy measures by financial authorities in 19 jurisdictions and global SSBs.** Policy measures refer to initiatives which aim to address the risks associated with the different activities which incorporate cryptoassets and smart contract functionalities in the provision of financial services (referred in this paper as "cryptoasset activities"). The paper is based on an extensive review of publicly available information[15] of policy measures by authorities in the 19 jurisdictions covered[16] as of end-March 2023 as well as analysis by the authors.[17]

10. **The remainder of this paper is structured as follows.** Section 2 describes the criteria used to classify the policy measures covered in the paper. Section 3 presents policy measures on centrally managed cryptoasset activities. Section 4 describes policy measures on community-managed cryptoasset activities. Section 5 describes policy measures on users' direct exposures to cryptoassets and related activities. Section 6 outlines future challenges and concludes.

Section 2 – Definitions and criteria for classifying policy measures covered in this paper

11. **At present, there is no universal definition of a "cryptoasset".** Authorities covered in this paper use different terms, definitions and taxonomies, which usually depend on the perspective in which these assets are analysed (eg technical, functional, legal). For example, terms such as digital assets, cryptoassets, virtual assets or crypto tokens are often used interchangeably. Also, different terms are used to refer to representations of real-world assets in a DLT and classification of these assets is not uniform.

12. **Similarly, to date there is no universally accepted classification of activities that incorporate cryptoassets and smart-contract functionalities in the provision of financial services.** As in the case of cryptoasset terminology, any analysis of policy measures in this domain is complicated by inconsistencies across jurisdictions regarding the classification of activities considered to define whether an actor is a service provider for regulatory purposes.

13. **Any cross-country comparison of policy and regulatory responses to cryptoassets and related activities is difficult due to the lack of a universally accepted terminology and taxonomy.** This paper uses the definitions proposed by SSBs where possible and classifies policy measures along three dimensions that can encompass the variety of initiatives issued by covered jurisdictions. The first dimension refers to the cryptoasset activity. The second dimension refers to how the activities are managed. And the third refers to the type of cryptoasset involved in those activities. What follows is the description of the terms and categorisations used to classify policy measures covered in this paper.

[13] See FSB (2020).

[14] See FSB (2022b, 2022c, 2022d).

[15] The information was obtained through the BIS Fintech Repository (FinRep). FinRep is an online tool developed by the Financial Stability Institute (FSI) that contains policy and regulatory documents related to financial technology issued by BIS member central banks and supervisory authorities and international standard-setting bodies.

[16] The jurisdictions covered in this paper are Australia, Belgium, Canada, China, the European Union, France, Germany, Hong Kong SAR, Italy, Japan, the Netherlands, the Philippines, Singapore, South Africa, Spain, Switzerland, the United Arab Emirates, the United Kingdom and the United States.

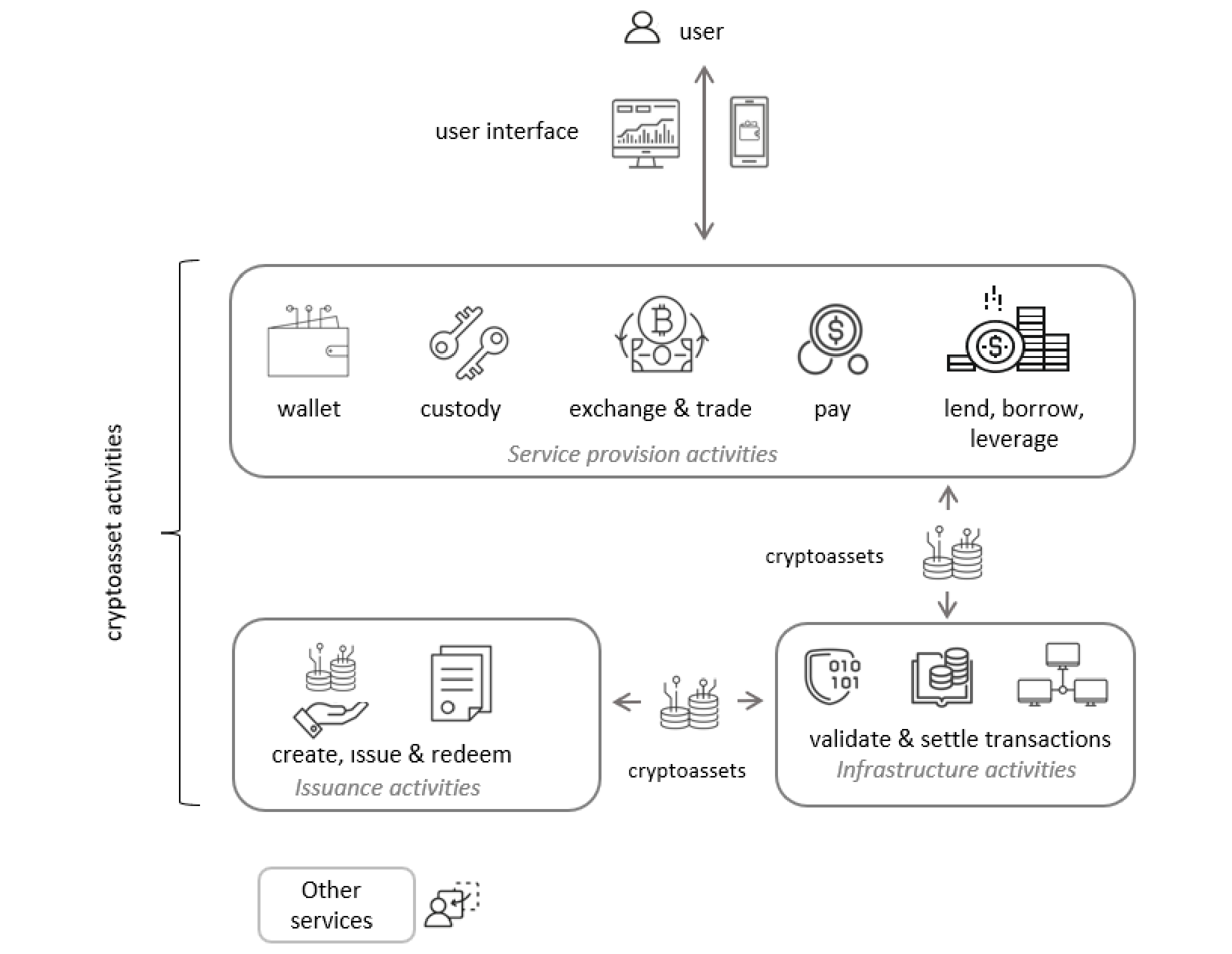
[17] The overview presented in this paper reflects the authors' own views and should not be considered as legal or professional advice. The information presented in this paper is provided on a best-efforts basis and may be subject to errors or omissions. The policy measures covered in this paper are as of end-March 2023 and may not reflect the latest policy responses.

2.1 First dimension: cryptoasset activities

14. **A number of activities incorporate cryptoassets and smart-contract functionalities in the provision of financial services.** Building on the FSB's proposed taxonomy of cryptoasset activities,[18] this paper groups cryptoasset activities in three categories: (i) those related to the issuance of cryptoassets (eg creation, issuance, distribution and redemption); (ii) those related to the operation of a DLT infrastructure (eg validation and settlement of transactions with cryptoassets); and (iii) those related to the provision of services related to cryptoassets (eg wallet, custody, payment, exchange, trading, lending, borrowing or risk management services). There are additional activities, referred to as "other supporting services", which support the three previous categories of activities. These include services such as developing code, providing data external to the network (eg oracles), providing API and cloud services, providing risk advisory services or conducting audits (See Graph 1).

Classification of cryptoasset activities

Graph 1



Source: Authors' elaboration based on the taxonomy of cryptoasset activities proposed by the FSB (2022c).

[18] See FSB (2022c).

2.2 Second dimension: management of cryptoasset activities

15. **Cryptoasset activities can be managed (ie operated and governed) in various ways.** For this paper, we distinguish between policy measures that address risks associated with activities managed by actors organised under centralised operational and governance arrangements ("centrally managed activities") versus those managed by a community of participants in public DLT networks organised under decentralised operational and governance arrangements ("community-managed activities").

2.3 Third dimension: types of cryptoasset

16. **Cryptoassets encompass all digital assets issued by the private sector that depend primarily on cryptography and distributed ledger or similar technology (FSB (2022a)).** Although authorities use different terms and definitions to refer to cryptoassets, they have common elements with the FSB definition in that they refer to cryptographically secured digital representations of value or contractual rights that can be transferred, stored or traded electronically and that use distributed ledger or similar technology to record or store data.

17. **The design and issuance of cryptoassets are contingent on the intended purpose they are meant to serve, with a broad range of objectives guiding their creation.**[19] For example, some are created for a specific use within a particular network, such as providing access to a service (eg FIL grants holders access to a data storage network). These cryptoassets are usually limited in their functionality and are not designed to be used for anything other than their intended use. Other cryptoassets are designed to enable developers to build applications on a particular DLT (eg ETH serves to build applications in the Ethereum platform). These cryptoassets are designed as an essential technical component of the DLT platform and serve as an economic incentive to pay for transaction fees and other services within the platform. Other cryptoassets are issued to represent ownership rights to real-world assets (eg PAXG serves as a digital representation of ownership rights to physical gold). These cryptoassets are usually designed according to agreements that establish the terms and conditions governing the ownership and transfer of the underlying asset, including storage and custody, transfer procedures and redemption mechanisms.

18. **Since cryptoassets have a wide range of intended uses, authorities rely on different criteria to classify them.** Many authorities categorise cryptoassets according to their economic function rather than the creator's intended use. Based on this criterion, authorities classify cryptoassets according to whether they perform a payment or investment function as defined by their regulatory framework or whether they provide another function (eg access to a digital good or service within a network). Another criterion is their technical design. Based on this criterion, authorities classify cryptoassets according to whether they were created as integral part of a DLT platform's operation or not. For cryptoassets that are designed to maintain a stable value by referencing one or more assets, many authorities classify them further according to (i) the type of asset they are referencing (eg fiat currencies, commodities or other cryptoassets); (ii) the type of arrangement by which they are managed (eg centralised or decentralised); or (iii) their potential to become systemically important in and across one or several jurisdictions.

19. **Even though there is no uniform terminology, many authorities refer to cryptoassets as "tokens" for classification purposes.** Many authorities categorise cryptoassets with a view to the economic function performed by a token, using terms such as "payment token", "security token" or "utility token". Other authorities use the term "tokenised asset" to refer to cryptoassets that are digital

[19] Independently of the intended purpose for which a cryptoasset was designed, holders may use them for many purposes: such as means of exchange, means of payment or remittance across borders, collateral in DeFi protocols or store of value.

representations of assets in a DLT.[20] In this sense, authorities may use different terms to refer to a cryptoasset with the same features. For example, a cryptoasset that provides rights and obligations similar to traditional financial instruments such as shares, debt instruments or units in a collective investment scheme may be referred to as an "investment token" or a "security token" or a "tokenised security".

20. **To ensure that this paper covers all types of cryptoasset discussed in the policy documents, it is important to use definitions that are sufficiently broad and inclusive.** Whenever possible, we use the definitions proposed by SSBs. If a SSB definition is not available, we use a general definition that includes most of the features of the cryptoassets covered in this paper. If a more specific definition is needed, it is referenced in the relevant section of the paper. We use the term "token" interchangeably with "cryptoasset". Against this backdrop, the definitions of the main types of cryptoasset covered in this paper are the following:

- **Stablecoin:** cryptoasset that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets (FSB (2022c)).
- **Global stablecoin:** stablecoin with a potential reach and use across multiple jurisdictions and which could become systemically important in and across one or many jurisdictions, including as a means of payments and/or store of value (FSB (2022c)).
- **Security token:** token that provides rights and obligations similar to traditional financial instruments such as shares, debt instruments or units in a collective investment scheme as defined in securities regulation.
- **Utility token:** token which provides users access to a specific good, service or application when they redeem the token.
- **Governance token:** token issued as an incentive, allowing the user the purported opportunity to become a partial owner and decision-maker in a DeFi protocol (FSB (2023)).
- **Native token:** the base token of a blockchain[21] that plays an integral part of the operation of the protocol it is issued on and that is created at its genesis. It is usually used to pay transaction fees (FSB (2023)).

2.4 Classification of policy measures

21. **Building on the previous classifications and definitions, this paper classifies policy measures in three groups.** As shown in Table 1, these refer to policy measures that target risks posed by: (i) centrally managed cryptoasset activities; (ii) community-managed cryptoasset activities; and (iii) users' direct exposures to cryptoasset and related cryptoasset activities. Sections 3–5 explore these policy measures in more detail.

[20] At present there is no uniform definition or classification of "tokenised assets". Tokenisation, under a technical perspective, is the process of creating a digital representation of an asset on a given DLT platform, achieved through a dedicated token contract template (see F Schär (2021) and Auer et al (2023)). The asset being tokenised can be a claim on rights to the issuer's assets, on a reserve of real or financial assets held by the issuer or a custodian, other cryptoassets locked in a smart contract, rights to shares of underlying assets, interest payments or dividends promised by the issuer, a good or a service to be delivered by the issuer, or contractual rights that represent some value for the holder, whether or not they are linked to any underlying asset. For example, some authorities' definitions cover digital representations of all the types of assets and rights described before while other authorities narrow the definition to digital representations of certain types of assets, such as real-world assets.

[21] A blockchain is a form of distributed ledger in which details of transactions are held in the ledger in the form of blocks of information. A block of new information is attached into the chain of pre-existing blocks via a computerised process by which transactions are validated (FSB (2023)).

Classification of policy measures

Table 1

Classification	Description
Policy measures in relation to risks posed by centrally managed cryptoasset activities	These initiatives aim to address risks associated with business models where: a) centralised entities,[22] including traditional financial and other intermediaries, govern and/or operate the issuance of stablecoins, global stablecoins, security tokens and utility tokens. b) traditional financial intermediaries operate a centrally governed DLT (ie private permissioned ledger). c) centralised entities govern and operate service provision activities.
Policy measures in relation to risks posed by community-managed cryptoasset activities	These initiatives aim to address risks associated with the following business models: a) native tokens created on public DLTs (ie public permissionless ledgers) by a community of participants who claim to be organised through decentralised arrangements. b) DLT applications which enable financial functions such as exchange and lending through smart contracts that run in public DLTs and are governed by a community of participants that claim to be organised through decentralised arrangements. Applications with these features are commonly referred to as DeFi protocols.
Policy measures in relation to risks posed by users' direct exposures to cryptoassets and related activities	These initiatives aim to address risks associated with users' direct exposures to different types of cryptoasset and related activity, including both centrally and community-managed activities. These initiatives target risks associated with both retail and wholesale users' direct exposures.

Source: Authors' elaboration.

[22] For this paper, we refer to centralised intermediaries as those organised under centralised organisational structures (eg perform their activities under centralised operational arrangements or take decisions under centralised governance arrangements).

Section 3 – Policy measures on centrally managed cryptoasset activities

22. **This section provides an overview of policy and regulatory responses that aim to address risks posed by centrally managed cryptoasset activities.** It covers policy and regulatory responses targeting entities and actors involved in (i) issuance activities, structuring these responses around issuance of stablecoins, security tokens and utility tokens; (ii) infrastructure activities; and (iii) service provision activities.

23. **In general, for centrally managed cryptoasset activities, authorities' approach aimed at banning, isolating and/or regulating such activities.**[23] Authorities in some jurisdictions, for example China,[24] have introduced comprehensive bans on all activities with cryptoassets, including infrastructure activities (eg mining) and service provision activities (eg trading). Others have introduced bans on certain activities such as the issuance of new stablecoins (eg UAE-DFSA).[25] For service provision activities, authorities in many jurisdictions have modified existing regimes (eg Japan, Philippines and the United Kingdom) or introduced bespoke regulations (eg the EU) to limit potential regulatory arbitrage and address a wide range of related risks.

24. **There is active policy and regulatory activity to address risks associated with centrally managed issuance, infrastructure and service provision activities.** For issuance activities, most jurisdictions covered in this paper have clarified how existing requirements apply to security tokens. Several authorities have announced their interest in establishing a regulatory framework for issuers of stablecoins used for payment and settlement purposes. For infrastructure activities, the authorities' approach aimed at regulating and/or facilitating the experimentation of DLT-based infrastructures to improve trading and settlement processes. For service provision activities, the vast majority of jurisdictions have adopted policy initiatives to address risks associated with these activities by introducing regulatory requirements for their providers.

3.1 Centrally managed issuance activities

25. **On a conceptual level, issuance and redemption activities in centrally managed cryptoasset activities are similar to those in the traditional financial system.** When issuing a cryptoasset, an entity generally provides certain rights, such as the ownership of the asset or the right to receive a stream of payments. For example, stablecoin issuers promise a certain sum (linked to the value of an asset, such as a fiat currency or a basket of assets); issuers of a security token promise a stream of interest payments; issuers of utility tokens commit to provide certain products, services or functions. Issuers influence the value of tokens through the creation of new ones and the destruction of those in circulation.[26]

26. **In general, regulatory responses for issuers of cryptoassets focus mainly on preventing illicit activities, consumer protection and prudential requirements.** The main risks associated with the issuance and redemption of tokens are related to AML/CFT, poor information on the rights of token holders and issuers' (in)ability to fulfil their perceived or legally enforceable obligations.

27. **The authorities' main objectives in this area have been threefold.** First, they aim to prevent issuers from committing financial crimes and diverting resources from socially and economically productive uses. Second, to ensure that token holders have comprehensive, clear and easily accessible

[23] For an analysis of different regulatory approaches to cryptoassets, see Aquilina et al (2023).

[24] People's Bank of China (PBoC) et al (2013, 2017, 2021a, 2021b) and China State Council (2021).

[25] In Dubai, issuance of new payment tokens is forbidden by the DFSA but authorities impose restrictions on (already existing) payment tokens that can be used for providing financial services. See DFSA (2022a, 2022b).

[26] The value of tokens can change either because new or destroyed tokens influence issuers' ability to fulfil their promises or because they change the total amount of tokens in circulation relative to demand.

information on the rights and risks associated with their tokens. Third, to ensure that the issuer is able to fulfil its promises, even under stressed conditions.[27]

28. **Consumer protection safeguards are commonplace in jurisdictions where issuers of stablecoins and security tokens are within the regulatory perimeter.** To protect consumers, authorities typically determine whether certain assets are suitable only for qualified investors, due to their complex characteristics or payoffs, or also for retail consumers. In addition, regulatory interventions often mandate specific disclosure requirements for issuers to enable users to accurately understand the risks associated with token ownership.

29. **By contrast, prudential requirements for issuers vary considerably.** As explained in the following subsections, initiatives in this area have so far mainly focused on issuers of stablecoins that can be used for payment and settlement services and, in particular, on ensuring that an entity creating or destroying this type of cryptoasset is always able to redeem them at their promised value. Issuers of other types of token are generally not subject to prudential requirements.

3.1.1 Issuers of stablecoins

30. **Policy and regulatory responses to stablecoins can be classified according to their economic function.** This type of token can be used as a means of payment or as an investment instrument depending on a number of features, such as the asset(s) to which a stablecoin is pegged (ie asset(s) to which a stablecoin's market value is designed to be linked); whether users have a claim at par value or at market value; and the party who bears the risks associated with fluctuations in the value of the reserve assets. If the issuer assumes the risks, the stablecoin is more akin to a means of payment. However, if they are borne by the holder, the stablecoin is more likely to be regarded as an investment instrument.

(a) Stablecoins used for payment and settlement

Jurisdictional level

31. **Several authorities have publicly expressed interest in developing a regulatory framework for issuers of stablecoins used for payment and settlement.** For example, the Australian Council of Financial Regulators (CFR) is developing options for regulating payment-related stablecoin arrangements. One option being considered is to incorporate stablecoin arrangements into the proposed regulatory framework for stored-value facilities, which is being implemented as part of the government's reforms to the payments licensing framework.[28]

32. **Regulators in the EU, Hong Kong SAR, Japan, Singapore, the UAE (ADGM FSRA and DFSA), the United Kingdom and the United States are pursuing stablecoin regulations.** While these jurisdictions have provided clear indications about their regulatory approach to stablecoins, their initiatives are at different stages of the regulatory process.[29] EU and Japanese legislators have agreed on new legislation that is expected to be published in 2023 (eg Japan) or will enter into force starting from 2023 (eg the EU). The United Kingdom is in the process of agreeing on new legislation. In the United States, authorities have provided official documents that describe in detail the key elements of their forthcoming frameworks. In January 2023, the Hong Kong Monetary Authority (HKMA) issued a conclusion paper to its previous discussion paper on the regulation of stablecoins, confirming its plan to regulate certain activities

[27] While the main risks and responsibilities of an entity that is in charge of creating or destroying cryptoassets are associated with the fulfilment of the promised rights, its actions directly also affect the volatility of the tokens' price, which may have broader implications for the whole cryptoasset market.

[28] See APRA (2022) and CFR (2022).

[29] It should be noted that the initiatives discussed in this section, except for those in the UAE (ADGM FSRA and DFSA), have not been formally agreed. Some proposals, which are currently under consultation, may undergo significant changes.

relating to stablecoins under a risk-based approach and indicating the expected regulatory scope and key regulatory requirements.[30] Singapore's proposed stablecoin regulatory framework has been consulted and is currently being reviewed, taking into account consultation feedback, for finalisation. In the UAE, the ADGM FSRA clarified the regulation applicable to stablecoin issuers in September 2022 while the crypto token regime issued by the DFSA entered into force in November 2022. A summary of the rules that have been introduced or will soon be introduced in these jurisdictions is shown in Table 2.

[30] See HKMA (2023).

Table 2

Licensing and ongoing requirements for issuers of stablecoins used for payment and settlement

	Status of the initiative as of March 2023	Licensing (Admissible entities)	Capital requirements	Reserve requirements
EU – EMT (1)	Final draft agreed by co-legislators	• banks • e-money institutions	As required for banks and e-money institutions	Funds must be invested in secure, low-risk assets denominated in the same currency as the one referenced by the e-money token
Hong Kong	First round of consultation concluded. Further consultation will be conducted on the more granular information about the regulatory regime	• banks • non-bank institutions	More granular parameters of the regulatory regime will be drawn up by the HKMA, including but not limited to financial resources requirements	The value of the reserve assets of a stablecoin arrangement should meet the value of the outstanding stablecoins at all times. The reserve assets should be of high quality and high liquidity. Stablecoins that derive their value based on arbitrage or algorithm will not be accepted
Japan	New regulatory framework will come into force by June 2023	• banks • fund transfer service providers (2) • e-money institutions • trust companies (3) • JFSA can designate equivalent arrangements	As required for the issuer type	• banks: as required by applicable regulation • fund transfer service providers: money deposits with official depositaries, bank guarantees, or segregated safe assets (eg bank deposits, government bonds) • trust companies: bank deposits
Singapore	Consultation concluded. Proposed framework is being reviewed, taken into account consultation feedback, for finalisation	• banks • major payment institution	Proposed capital requirements for stablecoin issuers would be higher than the ones applicable to current digital payment service providers (depending on the type of licence they apply for – Standard Payment Institution or Major Payment Institution Licence)	Reserves must be: • valued on a marked-to-market basis daily, and be equivalent to at least 100% of the par value of the outstanding stablecoins in circulation at all times (including those held by the issuer) • held in the form of cash, cash equivalents, or debt securities with no more than three months residual maturity and issued by (i) the central bank of the pegged currency; or (ii) organisations that are of both a governmental and international character with a credit rating of at least AA–; • denominated in the same currency as the pegged currency • held in segregated accounts with regulated entities providing custodial services in Singapore
UAE (4)	DFSA – Consultation concluded and regime entered into force in November 2022 ADGM FRSA – Final guidance published in September 2022	In Dubai, issuance of new payment tokens is forbidden by the DFSA and authorities impose restrictions on (already existing) payment tokens that can be used for providing financial services In Abu Dhabi, issuers must hold a Financial Services Permission granted by the FSRA of the ADGM.	In Dubai, as required by the issuer's regulatory and supervisory authority In Abu Dhabi, capital requirements are set proportional to operational expenses and may depend on the size, scope, complexity and nature of the activities and operations of the issuer	In Dubai, reserves must: • consist of cash, where only an insignificant proportion (generally, up to 10%) may be held in high-quality liquid assets • be denominated in the reference currency • be held in segregated accounts with properly regulated banks or custodians in jurisdictions that meet the FATF standards • have a value greater than the volume of the payment tokens in circulation at all times In Abu Dhabi, reserve requirements are determined by the Conduct of Business (COB) Client money rules
UK	Legislation introduced into Parliament	• banks • non-bank institutions as authorised by the respective authority	As required by the issuer's regulatory and supervisory authority	Not yet available
US	Draft legislative proposals and public documents by financial authorities	• insured depository institutions (banks and saving associations)	As required for insured depository institutions	Not available

Sources: Authors' elaborations on European Parliament (2022a), HKMA (2023), JFSA (2022), MAS (2022c), DFSA (2022a, 2022b), ADGM FRSA (2022b), UK Treasury (2022a), PWGFM (2021), FSOC (2022).

Notes:

(1): The information provided in the table refers to e-money tokens (EMT), which are defined in the EU MICA Regulation as cryptoassets that aim to maintain a stable value relative to an official currency.

(2): Providers of services to intermediate payments between locations with some distance, without physical transportation of cash between such locations.

(3): A trust company is an arrangement in which a person administers or disposes of property in accordance with a certain purpose (excluding the purpose of exclusively promoting the person's own interests) and conducts any other acts that are necessary to achieve said purpose.

(4): The information provided refers to the initiatives adopted by the Dubai Financial Services Authority and the Financial Services Regulatory Authority of the Abu Dhabi Global Market.

33. **Regulatory frameworks generally adopt different terms for payment tokens.** Japan and the United Kingdom are adopting terminologies based on the word "stablecoin". Specifically, the UK government has decided to formally adopt the terminology "stablecoins" to identify tokens used for payments. The Japanese framework will be based on "digital-money type stablecoins". On the other hand, the EU, UAE and the United States have opted to use the term "tokens" but with varying specifications. For instance, US authorities refer to "dollar tokens", EU co-legislators have introduced the concept of "e-money tokens", and the UAE is centred around "fiat crypto tokens".

34. **Current proposals for regulating issuers of stablecoins used for payments introduce licensing regimes.** Across all covered jurisdictions, authorities require issuers to be regulated institutions. However, the type of licence may differ from country to country. Banks and e-money institutions are generally allowed to issue payment tokens. In the United States, however, only insured depository institutions are allowed to issue stablecoins, which effectively excludes most non-banks that are allowed to issue e-money. In Japan, trust companies are also allowed to issue payment tokens.

35. **Minimum capital requirements for stablecoin issuers are typically determined by the type of licence they hold.** No authorities in the jurisdictions reviewed for this paper have proposed capital buffers that exceed those already established for regulated entities.

36. **Authorities typically impose requirements on the liquidity, denomination and custody of the reserve assets backing the value of payment tokens.** Reserve assets are typically required to be invested in highly liquid assets which may depend on the type of issuers' licence. For example, in Japan trust companies must hold bank deposits, while fund transfer service providers can also hold other safe assets such as government bonds. Some jurisdictions also require reserve assets to be denominated in the same currency as the one referenced by the payment tokens.

37. **Authorities are currently taking a variety of approaches to the regulation of tokens referenced to a basket of currencies.** While tokens that aim to maintain a stable value relative to a single fiat currency are usually classified as payment tokens, initiatives related to multicurrency stablecoins vary. In Singapore these tokens are excluded from the set of tokens that can be used for payments. In the EU, the use of multicurrency stablecoins as means of exchange is limited. In Hong Kong SAR, Japan and the United Kingdom, authorities are seeking to address the risks associated with the use of this type of stablecoin in payments.

38. **Stablecoin issuers are typically required to provide minimum redemption rights.** These can vary depending on two key characteristics: whether tokens can be redeemed at par value or at a different value, and whether holders have a claim directly on the issuer, reserve assets or a third party. Existing proposals across covered jurisdictions differ significantly. In the EU (for e-money tokens only), Japan and the United Kingdom, holders are entitled to a claim at par value. However, in the United States redemption can be close to but not necessarily equal to the nominal value of tokens. Furthermore, in the United States, the claim must be on the issuer, while in the United Kingdom, the legal obligation is with the issuer, but customers could make a claim against a consumer-facing entity where appropriate (eg an exchange platform).[31] In Japan, the type of claim differs depending on the issuer's licence, whether it is a bank, a fund transfer service provider or a trust company (see Table 3).

[31] As described below, in the United Kingdom, issuers of systemic payment tokens can be subject to additional requirements on redemption rights.

Key features of regulated stablecoins used for payment and settlement

Table 3

Jurisdiction	Peg	Redemption rights	Type of stabilisation
EU – EMT (1)	• Single currency	Holders must be provided with a claim at par value on the issuer	Asset-backed
Hong Kong	• Single currency • Multicurrency	Stablecoin holders should be able to redeem the stablecoins into the referenced fiat currency at par within a reasonable period of time.	Asset-backed
Japan	• Single currency • Multicurrency	Holders must be provided a claim at par value. The type of claim depends on the issuer type: • bank-issued stablecoins provide a claim on the issuer bank • fund transfer service providers provide a claim on the issuer's assets • trust companies provide a trust beneficiary right	Asset-backed
Singapore (2)	• Selected single currency (either the Singapore dollar or one of the G10 currencies)	Holders must be provided a claim at par value on the issuer	Asset-backed
UAE (3)	• Single currency	Holders should be able to redeem their tokens at a price within immediate proximity from the peg (generally, up to 10 basis points) for extended periods of time	Asset-backed
UK	• Single currency • Multicurrency	Holders must be provided a claim at par value on either the issuer or, where appropriate, on the consumer-facing entity	Asset-backed
US	• Single currency	Holders can be redeemed at par value or at different value	No specific restriction

Sources: See Table 1.

Notes:

(1): The information provided in the table refers to e-money tokens (EMT), which are defined in the EU MICA Regulation as cryptoassets that aim to maintain a stable value relative to an official currency.

(2): The public consultation explicitly stated that "MAS sees a need to impose higher financial and prudential standards on SCS issuers compared to other payment service providers, given its potential as a provider of a medium of exchange to support the development of the broader digital asset ecosystem. MAS has considered the appropriateness of imposing a risk-based capital framework on SCS issuers at the onset, to account more comprehensively for the risks which the SCS issuer might undertake. However, given that the sector is still in its early phase of development, the compliance cost of such a regime may be disproportionately high. MAS thus proposes to impose a simplified capital regime with necessary restrictions to limit the risks to the SCS issuing entity."

(3): The information provided refers to the initiatives adopted by the Dubai Financial Services Authority.

39. **All covered jurisdictions have introduced restrictions on the types of stabilisation mechanism allowed for stablecoins.** Issuers must maintain a portfolio of assets backing the value of their tokens. These assets can either directly back the value of the token, in cases where the claim is on the reserve assets, or indirectly, in cases where the claim is on the issuer. While tokens that rely exclusively on algorithms to stabilise their value are not generally prohibited (except in the UAE-DFSA), they are usually considered as not meeting the regulatory requirements set forth by the relevant stablecoin regimes.

40. **In some jurisdictions, stablecoin issuers are also subject to specific consumer protection requirements.** Authorities typically establish a minimum set of information that must be disclosed to consumers. For example, under the EU's MICA regulation and Singapore's proposed framework,[32] issuers

[32] The Singapore's proposed stablecoin regulatory framework has been consulted but not finalised. It is currently being reviewed, taking into account consultation feedback, for finalisation.

are required to publish a white paper containing information on, among other things, a description of users' redemption rights and how such rights can be exercised.

41. **Stablecoin issuers are often subject to a number of requirements to improve their risk management practices.** Authorities in jurisdictions covered in this section typically require the presence of a clearly identifiable person to be responsible and liable to the holders of the payment tokens, thereby potentially excluding purely decentralised governance structures. Under the proposed regime in Hong Kong, stablecoin issuers are not allowed to conduct activities that deviate from their principal business(es) as permitted by their relevant licences, or from participating in any other activity that may pose risks to the issuer, including activities related to other cryptoassets (eg trading, lending, staking).[33]

42. **Some authorities have introduced requirements to address systemic risks associated with stablecoins used for payments.** In the EU, legislators have introduced several risk mitigants, such as additional capital requirements, diversification of custodians of reserve assets, additional liquidity risk requirements, and specific plans for an orderly wind-down. In the United States, authorities are considering rules to preserve competition and avoid excessive market power. In the United Kingdom, the Bank of England may consider requiring a direct legal claim on the issuer of systemic payment tokens (Table 4).

Requirements for issuers of stablecoins used for payments to address systemic risks

Table 4

Jurisdiction (1)	Additional requirements for systemic risk
EU – EMT (2)	Several additional requirements, including: additional capital (from 2% to 3%) diversification of custodians additional liquidity risk management requirements (ie resilience under stressed conditions) plans for orderly wind-down
Hong Kong	The HKMA considers it more appropriate to take a risk-based approach, under which the HKMA will calibrate the intensity of regulation with regard to all relevant factors concerning a licensed entity and the specific stablecoin arrangements adopted, instead of seeking to specify at the outset additional requirements for what may constitute "systemic" stablecoins and the corresponding additional regulatory requirements
Singapore	MAS has the power to designate a systemic stablecoin arrangement as a designated payment system (DPS). MAS's regulatory powers over designated payment systems include the ability to regulate access rules for participation, impose restrictions and conditions, establish standards, make regulations, approve and remove chief executive officers and directors, approve substantial shareholders and other controllers, issue directions and inspect its operations
UK	The Bank of England may seek to require a direct legal claim on the issuer to address (systemic) financial stability risks
US	Restrictions on affiliation with commercial entities Interoperability standards

Notes:

(1): For Japan and the UAE, information was not available.

(2): The information provided in the table refers to e-money tokens EMT), which are defined in the EU MICA Regulation as cryptoassets that aim to maintain a stable value relative to an official currency. Requirements shown in this table also apply to issuers of asset referenced tokens (ART) that are classified as significant.

[33] In Hong Kong, it is proposed that the principal business restriction does not apply to banks that are in scope for the purpose of the proposed regulatory regime.

International level

43. **Stablecoins that can be used for payments are the subject of intensive work by SSBs to promote consistent and effective regulation at the international level.** SSBs have issued a number of initiatives in this area. The FATF has published a report on so-called stablecoins;[34] CPMI and IOSCO have published guidance on the application of the Principles for Financial Market Infrastructures (PFMI) to stablecoin arrangements;[35] and the FSB has consulted on the review of its high-level recommendations of the regulation, supervision and oversight of "global stablecoin" arrangements (GSC-HLRs) that were first published in 2020.[36]

44. **In general, SSBs provide high-level standards for the regulation of stablecoin arrangements.** These include not only issuers but also a range of activities related to stablecoins.

- In the *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*,[37] the FATF provides guidance on how the FATF Standards apply to stablecoins and clarifies that a range of entities involved in stablecoin arrangements could qualify as cryptoasset service providers (referred to as virtual asset service providers or VASPs) under the FATF Standards. In addition, the FATF's report to the G20 on so-called stablecoins[38] highlights that, among other things, governance bodies (which in many cases substantially coincide with the issuer) have AML/CFT obligations where they carry out activities of a financial institution or a virtual asset service provider.
- The CPMI and IOSCO clarified the application of existing principles of financial market infrastructures to stablecoin arrangements that are considered systemically important financial market infrastructures.[39]
- The FSB GSC-HLRs focus on both back-end and user-facing activities of global stablecoins (those with the potential reach and adoption across multiple jurisdictions), irrespective of their economic functions (although the main revisions published in October 2022 target stablecoins that may be used for payments and/or a store of value).

45. **The work by SSBs addresses several regulatory areas, including governance structure and licensing.** In general, the work of SSBs is on a high level so that standards and recommendations can be incorporated into the wide variety of regulatory frameworks around the world. Furthermore, they apply to all global stablecoins, irrespective of the assets to which they are pegged or their economic functions. In relation to authorisation and licensing, the FSB highlights that authorities should require that GSC arrangements meet all applicable regulatory, supervisory and oversight requirements of a particular jurisdiction before commencing any operations. They should also have the powers to effectively prohibit stablecoin activities if necessary and appropriate.

46. **One key focus area of SSBs work is the functioning and reliability of the stabilisation mechanism.** The implementation guidance of FSB recommendation 9 effectively limits purely algorithmic stablecoins. Furthermore, the recommendation stresses that GSC arrangements should be subject to appropriate prudential requirements and to robust requirements for the composition of reserve assets.[40]

[34] See FATF (2020).

[35] See CPMI (2022).

[36] See FSB (2022b, 2022d).

[37] See FATF (2021).

[38] See FATF (2020).

[39] A stablecoin arrangement (SA) that performs the transfer function is considered a financial market infrastructure (FMI) for the purpose of applying the Principles of FMI and, if determined by relevant authorities to be systemically important, the SA as a whole would be expected to observe all relevant principles. See CPMI (2022).

[40] In addition, risks of custodial arrangements for reserve assets should also be adequately managed and addressed.

The key considerations related to Principle 9 of the PFMI highlight that a stablecoin used by a systemically important arrangement should have little or no credit or liquidity risk. In assessing the risk presented by the stablecoin, the arrangement should consider, among other things: (i) the nature and sufficiency of the SA's reserve assets and the degree to which the SA's reserve assets could be liquidated at or close to prevailing market prices; and (ii) the creditworthiness, capitalisation, access to liquidity and operational reliability of the issuer of the stablecoin.

47. **Work at international level has focused on the risks related to poor redemption rights.** The FSB stresses that GSCs referenced to a single fiat currency should have redemption rights that allow holders to redeem at par into fiat. Similarly, CPMI-IOSCO highlights that, when evaluating credit and liquidity risks of stablecoin arrangements, authorities should consider whether the stablecoin provides its holders with a direct legal claim on the issuer.

(b) Stablecoins used for investment

Jurisdictional level

48. **Most authorities have not adopted initiatives for stablecoins used as investments.** Due to their perceived stability, stablecoins may create the perception or expectation among users that they can be used as investment vehicles. However, the specific risks they create and the appropriate regulatory approach remain uncertain due to the limited number of real-world examples. Some authorities have taken a pre-emptive approach, banning the issuance of stablecoins used as investments.

49. **Only a few authorities have adopted specific regulatory initiatives for stablecoins that are used as investments.** For example, FINMA has clarified the regulatory treatment of different categories of stablecoins, which is contingent on the underlying asset(s) and the type of claim. Specifically, cryptoassets pegged to a precious metal with a contractual claim would fall under banking law. Conversely, a stablecoin pegged to a single commodity or security with a contractual claim would be subject to securities regulation. Finally, a stablecoin pegged to a basket of commodities or securities with a redemption claim would be treated as a collective investment scheme.

50. **The EU has introduced a bespoke regime that includes regulation for issuers of stablecoins that can be used mainly as investments.** The new regulatory framework, which labels such tokens as Asset-Referenced Tokens (ART), introduces several requirements for issuers, including those associated with licensing, capital, reserve assets, risk management and provisions for an orderly wind-down. In particular, ART issuers need to be established in the EU, hold own funds whose value should be at least 2% of the reserve of assets that back the value of the ART and maintain the reserve segregated from the issuer's own assets and invested only in highly liquid financial instruments with minimal market and credit risk. In addition, issuers should maintain internal control mechanisms and effective procedures for risk assessment and risk management, including effective control and safeguard arrangements for managing ICT systems. The regulation also introduces rules regarding the content and form of the white paper, which must provide a broad set of information to the public about the token, and introduces additional requirements for significant tokens (including additional capital requirements and risk management requirements).

International level

51. **In 2020, IOSCO published a report on the potential use of stablecoins as investments.** The report analyses this type of cryptoasset from the securities regulators' perspective and highlights that global stablecoin initiatives may, depending on their structure, have features that are typical of regulated securities or other regulated financial instruments. IOSCO members have also concluded that the Policy Recommendations for Money Market Funds and the Principles for the regulation of exchange-traded

funds,[41] among other standards, could apply to global stablecoins if they were classified as securities or other financial instruments.

3.1.2 Issuers of security tokens

Jurisdictional level

52. **Issuers of security tokens are subject to the same regulation as issuers of traditional securities in all covered jurisdictions.** Securities regulators have clarified the applicability of securities regulation to security tokens (also referred to as tokenised securities) focusing on asset characteristics rather than on the technology used to exchange them. In particular, issuers of securities tokens are subject to AML/CFT regulation, transparency requirements (investment prospectus or offering memorandum, audited financial statements) and consumer protection regulation.

53. **Some authorities have exempted issuers of security tokens from the full application of securities regulation.** Such exemptions are in line with the exemptions that exist in typical securities regulation for small-scale issuances. Exemptions are generally related to the content of the investment prospectus or offering memorandum, allowing issuers some flexibility in the information provided or a waiver from the obligation to produce such documentation. Other exemptions, which are usually considered in sandbox initiatives, include limitations on the amount of capital raised through token offerings, the type of potential investor (generally only qualified entities), restrictions or prohibitions from listing and trading tokens on exchanges and time limitations (usually one or two years). However, authorities generally do not provide exemptions from AML/CFT regulation, suggesting that authorities believe that investment tokens may pose considerable AML/CFT risks.[42]

54. **One key area is the regulation of security tokens issued by financial institutions.** In general, our review of regulations at the global level has not identified specific regulatory initiatives for security tokens issued by financial institutions, such as tokenised bank bonds or tokenised shares of investment funds.[43]

International level

55. **The BCBS has clarified some aspects of the prudential treatment of banks' tokenised liabilities.** The BCBS standards,[44] which are focused mainly on banks' exposures,[45] clarify the capital and liquidity treatment of "tokenised traditional assets" issued by banks.[46,] These rules are an important step towards the development of a regulatory framework for banks' funding activities using DLTs. There are,

[41] See IOSCO (2012, 2013).

[42] See eg CSA (2017b).

[43] One exception is the German draft Electronic Securities Act, which was amended in December 2021. The amended draft bill introduces the possibility that certain types of investment fund share can be created on DLTs, although electronic investment fund shares can be registered only in central registers. See OECD (2021a).

[44] See BCBS (2022).

[45] The BCBS standard sets out the prudential treatment of how banks should manage and account for cryptoassets, including tokenised traditional assets, stablecoins and unbacked cryptoassets. For this standard, the term "exposure" includes on- or off-balance sheet amounts that give rise to credit, market, operational and/or liquidity risks. This encompasses various activities, for example holding cryptoassets (either under trading or banking book) or providing services to cryptoasset operators.

[46] Tokenised traditional assets are defined by the BCBS as digital representations of traditional assets using cryptography, DLT or similar technology to record ownership. Traditional assets are those assets that are captured within the Basel Framework that are not classified as cryptoassets. Unbacked cryptoassets are cryptoassets that are neither tokenised traditional assets nor stablecoins. See BCBS (2022).

however, key practical issues that remain to be addressed, including the application of deposit insurance schemes to tokenised deposits.[47]

3.1.3 Issuers of utility tokens

Jurisdictional level

56. **Issuers of utility tokens are generally not subject to specific regulation.** For example, UAE-ADGM FSRA and DFSA have left these tokens out of the scope of its regulation for cryptoassets.

57. **Some authorities have clarified the applicability of securities laws to issuers of utility tokens.** Utility tokens are generally not treated as securities if their sole purpose is to confer digital access rights to an application or service and if the utility token can only be used in this way at the point of issue.[48] In these cases, the underlying function is to grant the access rights, without having any connection with capital markets, which is a typical feature of securities. However, in some cases, utility tokens can have the characteristics of investment assets. For example, some authorities have clarified that offerings of utility tokens involving an investment contract should be treated as security offerings.[49]

3.2 Centrally managed infrastructure activities

58. **On a conceptual level, the programmability capabilities of DLTs might improve infrastructure activities in the traditional financial sector.** The clearing and settlement systems of traditional financial intermediaries might benefit from the efficiencies achieved through programmability capabilities in terms of execution speed and transaction costs. Tokenisation of real-world assets and transaction automation can bring a number of benefits to the traditional financial sector such as atomic/instant trading and settlement,[50] fractional ownership, reduction of end-of-day reconciliations, cost savings and accelerated processing (OECD (2020)).

59. **The adoption of DLT by traditional financial intermediaries might pose a number of risks and challenges.** As with any new technology, DLT raises the potential for operational risks including network stability, exposure to cyber risk, risk of hacking and 51% attacks. Additional risks and implications could arise depending on the use case and features of the DLT network (eg risks related to AML/CFT are particularly high in tokenised markets that are based on public permissionless networks).[51] In addition, the traditional financial sector would face a number of challenges with the migration to a DLT-enabled environment on a large scale. These challenges would include the scalability or interoperability of networks, settlement finality and the legal enforceability of smart contracts, or financial stability risks due to increasing linkages between crypto-asset markets/DeFi, TradFi and the real economy if the tokenisation of real-world assets grows.

[47] See Phillips (2022).

[48] See eg FINMA (2018) and OECD (2021b).

[49] See CSA (2018).

[50] Atomic settlement is the use of a smart contract to link two assets to ensure that the transfer of one asset occurs, if and only if, the transfer of the other asset also occurs (eg to achieve delivery versus payment in a securities transaction or payment versus payment in a foreign exchange transaction).

[51] See OECD (2020) and Bech et al (2020).

Jurisdictional level

60. **Regulatory responses for infrastructure activities focus mainly on supporting innovation that could benefit society while protecting consumers, market integrity and financial stability.** These responses can be broadly classified into three main categories: research, experimentation and initiatives that facilitate the safe adoption of DLT-based FMIs.

61. **Research initiatives have analysed the potential benefits and risks associated with the adoption of DLT by intermediaries, financial market infrastructures or the public sector.** These include working papers and reports by SSBs,[52] international organisations[53] and authorities in some jurisdictions such as the EU,[54] the Netherlands[55] and the United Kingdom.[56]

62. **In experimentation initiatives, authorities are involved in use case pilot schemes.** The aim is to gain practical knowledge of the functioning of DLT-based applications and to test the efficacy of potential solutions for potential risks. Some jurisdictions that have taken this approach are Canada, Singapore and South Africa. Canada has conducted an initiative ("Project Jasper") with the aim of analysing the implications of the use of DLTs in the payments system.[57,58] South Africa has also experimented the use of DLT with the industry (IFWG (2021)). In particular, phase 2 of Project Khokha (or Project Khokha II) has analysed the possibility of issuing, clearing and settling debentures via DLT using tokenised money.[59] Recently, the Monetary Authority of Singapore announced the start of Project Guardian.[60] This is a collaborative initiative with the financial industry to test the feasibility of applications in asset tokenisation and DeFi protocols.

63. **The third category includes regulatory initiatives that facilitate the safe adoption of DLT-based financial market infrastructures.** At present, there are few concrete regulatory initiatives towards facilitating innovation in FMIs. In general terms, these initiatives are aimed at supporting the use of DLT in clearing and settlement of payments and securities in a network of trusted participants. Initiatives have been implemented through bespoke licensing regimes (eg CH, EU), innovation facilitator initiatives (eg United Kingdom) and DLT-specific regulatory guidance (eg AU, UAE):

a. **Switzerland has adopted legislation aimed at regulating the conditions for intermediaries using DLT.**[61] This is done through the introduction of security rights registered on a blockchain, increasing legal certainty in the event of bankruptcy (segregation of cryptoassets), creating a new licence category for DLT/blockchain-based trading systems within

[52] See CPMI (2017).

[53] See OECD (2020, 2021a) and IMF (2022b).

[54] See EIOPA (2021).

[55] See Netherlands Bank (DNB) (2021).

[56] See BoE (2022c).

[57] The project has been carried out by Payments Canada, its member financial institutions, the Bank of Canada and other market participants.

[58] In particular, securities and cash were brought on ledger through the issuance of digital depository receipts (DDRs) by the Canadian Depository for Securities and the Bank of Canada respectively, allowing POC participants to settle simulated securities against simulated central bank cash on the distributed ledger.

[59] In this pilot, industry participants were able to purchase the debentures with a wholesale central bank-issued digital currency (wCBDC) and a wholesale digital settlement token (wToken). The wToken can be seen as a privately issued stablecoin used for interbank settlement. See South Africa Intergovernmental Fintech Working Group (2021),

[60] See MAS (2022b).

[61] See Switzerland Federal Council (2020), Switzerland Federal Department of Finance (2021) and Swiss National Bank (2022).

the framework of financial market supervision,[62] and providing a proportionate response to the risks identified in the area of money laundering and terrorist financing.

b. **In the EU, the Regulation on a Pilot Regime for Market Infrastructures based on DLT aims to support innovation by removing potential obstacles to the application of new technologies and providing a specific regulatory framework.**[63] This regulation seeks to put in place a framework that is tailor-made for DLT, by finding a balance between exemptions to the traditional regulation[64] that DLT market infrastructures can request under specific conditions and additional requirements applicable to DLT market infrastructures to address the new risks related to this particular enabling technology.[65]

c. **The United Kingdom has announced its intent to establish a "financial market infrastructure sandbox".** This initiative includes regulatory action in the field of DLT-based activities.[66] In particular, the Sandbox – which will be run by the Bank of England and the FCA and be operational by 2023 – is designed to enable firms to experiment and innovate in providing the infrastructure services that underpin markets, in particular by enabling DLT to be tested. The government also confirmed that it will initiate a research programme to explore the feasibility and potential benefits of using DLT for sovereign debt instruments.[67]

d. **The Australian Securities and Investments Commission set out guidance for players (start-up or already existing licensees) wanting to operate a market infrastructure or providing financial or consumer credit services through DLTs.** The guidance focuses mainly on the importance of having adequate arrangements and sufficient resources (technological and HR) to understand the technology. It also seeks to ensure that any risks are identified and mitigated, and it requires firms to have and to maintain the competence to properly operate their infrastructure or to provide the financial service covered by the licence.[68]

e. **The United Arab Emirates provided guidelines for institutions that are using or intend to use enabling technologies, with particular reference to DLT.**[69] In this regard, the key principles cover the governance of the application and its design, management and

[62] See Swiss National Bank (2022).

[63] The regulation intends also to support the single European market, given the fact that a DLT Market Infrastructure that has a permission to operate according to the pilot regime can provide its service throughout all Member States. In order to provide legal certainty, the regulation establishes operating conditions for DLT market infrastructures, permissions to make use of them and the supervision and cooperation of competent authorities and ESMA. In particular, the regulation provides common definitions, exemptions and requirements for a DLT Market Infrastructure, differentiating the case between a DLT trading and settlement facility, a DLT Multilateral Trading Facility and a DLT Securities Settlement System and pointing out the limitations in terms of DLT transferable securities that can be admitted to trading on, or recorded by, DLT market infrastructures. See EC (2020b).

[64] See EC (2022a).

[65] For example, DLT market infrastructures must provide detailed information on the differences on their functioning, services and activities from a traditional MTF or CSD; and ensure that overall IT and cyber arrangements related to the use of DLT are adequate.

[66] See UK Treasury (2022b).

[67] Other measures of the UK strategy in crypto include establishing a Cryptoasset Engagement Group to work more closely with the industry; exploring ways of enhancing the competitiveness of the UK tax system to encourage further development of the cryptoasset market; and working with the Royal Mint on a non-fungible token (NFT).

[68] An ad hoc information sheet is designed to help both ASIC and interested parties evaluate whether the use of DLT would allow an entity to meet its regulatory obligations. See ASIC (2017).

[69] See UAE Regulatory Authorities (2021).

monitoring, the anonymity/pseudonymity of users, and issues such as data standardisation, interoperability and business continuity.[70]

3.3 Centrally managed service provision activities

64. **Provision of cryptoasset services includes a wide range of activities.** These are related mainly to the custody and the administration of tokens on behalf of users (ie wallet providers), the exchange of tokens for fiat currencies or other tokens, and the reception, transmission or execution of orders.[71] Non-bank centralised entities such as cryptoasset exchange and trading platforms that provide vertically integrated cryptoasset activities (eg issuance, exchange, trade, payments, lending, borrowing), usually referred to as "crypto conglomerates", have emerged as key players in cryptoasset markets.

3.3.1 Services provided by banks

Jurisdictional level

65. **Service provision activities by regulated entities are generally in scope of existing regulation.** In relation to banks' indirect exposures to cryptoassets, most regulatory initiatives involve the publication of guidelines and clarifications related to their risk management practices.[72] While these initiatives do not introduce new rules, they draw banks' attention to the specific risks associated with indirect exposures to cryptoassets and highlight aspects of the existing regulatory framework that they should consider when measuring and mitigating risks resulting from activities related to cryptoassets. These guidelines cover a number of services, including traditional bank services such as credit, advisory, custody and payment services, and non-traditional services, such as digital wallets, order execution, placement, and receipt and transmission of orders on behalf of third parties of cryptoassets.

66. **In some jurisdictions, supervisors request detailed risk analyses before authorising banks to perform activities related to cryptoasset markets.** For example, in the United States, a bank can engage in certain cryptoasset-related activities, such as cryptoasset custody services for users and custody services for stablecoin reserves, provided it can demonstrate, to the satisfaction of the supervisor, that it has controls in place to conduct the activity in a safe and sound manner. To obtain supervisory non-objection, the bank needs to demonstrate that it has established an appropriate risk management and measurement process for the proposed activities, including having adequate systems in place to identify, measure, monitor and control the risks of its activities.

67. **Authorities have highlighted the need to clarify which cryptoasset activities banks can provide.** For example, US federal agencies are in the process of clarifying which activities related to

[70] For example, institutions should establish an approved and documented governance framework for effective decision-making and proper control of risks arising from the use of DLT; design their DLT Applications to be efficient and effectively secure IT assets and any customer assets; develop permissionless DLT Applications ensuring that users are not anonymous or pseudonymous; ensure their DLT Applications are reviewed and monitored on a periodic basis to evaluate performance, detect technology and security-related incidents, ensure the adequacy of controls and promptly take any remedial action; not maintain personal data on the ledger and such data should be maintained off-chain; and ensure appropriate business continuity planning with respect to DLT, as this covers the potential loss of data and processing capability due to loss of servers or connectivity, and risks such as cyber crime.

[71] Service provision activities include also other activities, such as clearing derivatives and futures of cryptoassets. This is generally a regulated activity independently of the type of underlying assets.

[72] Examples of initiatives in this area include Bank of England (2022b), HKMA and HKSFC (2022), Bank of Italy (2022), FINMA (2018).

cryptoassets conducted by banking organisations are legally permissible and will set out expectations for safety and soundness, consumer protection and compliance with existing laws and regulations.[73]

3.3.2 Services provided by other entities

Jurisdictional level

68. **There are significant similarities between cryptoasset service provision activities and those in the traditional financial system.** As highlighted by the FSB,[74] exchange services in cryptoasset markets generate risks similar to those of the trading and investment services provided by traditional exchanges, broker-dealers and asset management companies. This suggests that the same standards and policies that apply to traditional financial intermediaries should also be applied to cryptoasset service providers, taking into account any novel aspects of these assets. For example, some activities related to the validation mechanism (eg staking) and custody services (eg non-custodian wallets) do not have a direct corollary in traditional finance.

69. **The regulation of cryptoasset service providers is generally determined by the type of activity performed and the regulatory classification of the underlying cryptoasset within a jurisdiction's legal framework.** In the past few years, several authorities have clarified that existing securities regulation applies to entities that do business with cryptoassets that qualify as securities or other traditional financial instruments. Therefore, service providers may not be subject to existing securities regulation if they deal only with cryptoassets that do not qualify as securities or other regulated assets. To address this potential regulatory gap, some authorities have introduced bespoke frameworks for cryptoassets that do not qualify as securities or other regulated assets (eg EU) and others will introduce new licensing frameworks that capture both cryptoassets qualifying as securities and non-securities (eg HK).[75]

70. **In recent years, the vast majority of jurisdictions reviewed for this paper have adopted policy initiatives to address risks associated with cryptoasset service provision activities.** The significant number of policy responses in this area highlights the importance of risks associated with the direct interaction of service providers with retail consumers. For example, some jurisdictions have introduced bespoke frameworks for cryptoasset service providers (eg France[76] and the Philippines[77]) while others have issued clarifications on how requirements under securities laws may be tailored to cryptoasset trading platforms (eg the Canadian Securities Administrators (CSA) and the Investment Industry Regulatory Organization of Canada).[78] Given the large number of initiatives in this area, the remainder of this subsection focuses on the jurisdictions covered in subsection 3.1.

[73] See Federal Reserve, FDIC and OCC (2023).

[74] See FSB (2022d).

[75] In Hong Kong, a new licensing regime for virtual asset service providers (VASPs) will come into effect in June 2023 under the Anti-Money Laundering and Counter-Terrorist Financing Ordinance. Under the new VASP licensing regime, any person who engages in the virtual asset exchange business will be regulated and required to apply a licence from the Securities and Futures Commission. This would bring virtual asset exchanges trading non-securities virtual assets within the regulatory perimeter of the Securities and Futures Commission. See Government of the Hong Kong Special Administrative Region (2022).

[76] France has a legal framework ("PACTE Law" of 22 May 2019) which encompasses a mandatory registration and an optional authorisation for providers of digital asset services and optional approval to ICOs. This national regime would be replaced by the upcoming European MICA regulation.

[77] The Bangko Sentral ng Pilipinas (BSP) regulates virtual asset service providers (VASP) and grants VASP licenses pursuant to BSP Circular No. 1108 (2021). See BSP (2021).

[78] See CSA (2021).

71. **In general, policy measures for service providers fall under four main categories: licensing, prudential requirements, AML/CFT requirements and consumer protection.**[79] Provisions are usually included in regulations related to payment services or financial services. For example, Japan and Singapore regulate cryptoasset activities in their respective payment service legislation.[80] Regulatory initiatives in the EU (ie the EU MICA Regulation) and the United Kingdom (ie the UK Treasury consultation on the future financial services regulatory regime for cryptoassets) are aimed at financial services in general.

72. **Licensing or registration regimes for cryptoasset service providers have been set up in several jurisdictions.** Main authorisation requirements are similar to those of traditional service providers. In the EU, Japan, the Philippines and Singapore,[81] applicants face requirements on the place of incorporation and legal form, sustainability of business plan, minimum paid-in capital, fitness and propriety of management, risk governance frameworks and documentation of the exit strategy.

73. **Cryptoasset service providers, when conducting a regulated activity, generally face the same ongoing prudential requirements as traditional financial institutions.** These requirements can be grouped in five main categories:

- Solvency and liquidity: service providers in the EU, the Philippines and the United Kingdom[82] are subject to (or will become subject to) capital and liquidity requirements, for example in the form of an insurance policy or an equivalent security mechanism (eg cash deposit, bank guarantee).
- Risk management: the EU, Japan, the Philippines, Singapore, the United Kingdom and the United States require providers to properly manage risk exposures (eg AML/CFT risks) or make them subject to bespoke requirements on some specific risks (eg outsourcing).
- Governance: most jurisdictions require senior management to meet professional suitability and experience requirements to perform their functions.
- Operational resilience: most jurisdictions have requirements to ensure business continuity and operational resilience requirements, including in terms of technology-related risks and third-party dependency management. For example, the EU DORA (Digital Operational Resilience Act) sets cross-sectoral uniform requirements to address the operational resilience of a wide range of entities including cryptoasset service providers.
- Reporting: these requirements include reporting the number of holders of cryptoassets, the volume of transactions, reporting of suspicious transactions or of any technical or operational incident that could compromise the continuity of services.

74. **Some jurisdictions cover the full set of prudential requirements, while others focus on specific aspects.** For example, the EU and the consultation in the United Kingdom include all prudential

[79] There are jurisdictions where this categorisation is different. For example, in the United Kingdom, licensing is the stage at which regulators check the other ongoing (ie prudential or conduct or governance) requirements.

[80] In particular, Singapore regulates the "digital payment token service provider", defined as (i) any service of dealing in (ie buying or selling) digital payment tokens; (ii) any service of facilitating the exchange of digital payment tokens. Japan regulates activity in cryptoassets through a Payment Service Act, seeking to "ensure the appropriate provision of payment services, protection of the users and thereof to promote the provision of those services in a sustainable way".

[81] In Singapore's licensing process, exit strategies are not explicitly considered.

[82] See UK Treasury (2023).

requirements. Japan does not cover explicitly capital/liquidity requirements[83] and Singapore focuses mainly on risk management requirements, as shown in Table 5.[84]

Licensing and ongoing requirements for cryptoasset service providers Table 5

	EU	JP	PH	SG	UK	US
A. Licensing regime	✓	✓	✓	✓	✓	✓
1. Governance requirements	✓	✓		✓	✓	
2. Financial requirements	✓	✓	✓	✓	✓	
B. Prudential requirements	✓	✓	✓	✓	✓	✓
1. Solvency and liquidity	✓	✓	✓	✓*	✓	
2. Risk management	✓	✓	✓	✓	✓	✓
3. Governance	✓	✓	✓	✓	✓	✓
4. Operational resilience	✓	✓			✓	
5. Reporting	✓	✓	✓	✓	✓	
C. AML	✓	✓	✓	✓	**	✓
D. Consumer protection	✓	✓	✓		✓	✓

* The MAS regulatory framework does not provide for liquidity requirements for cryptoasset service providers.

** Already regulated by FCA (2019, 2022).

75. **Many jurisdictions have specific requirements on AML/CFT and consumer protection.** The former include mainly obligations to perform customer due diligence, transaction monitoring and suspicious transactions reporting (eg Europe, Japan, Singapore, the United Kingdom and the United States.) The latter requirements generally refer to the prevention of market abuse, the need to act fairly and professionally and in the best interests of the client.

76. **Some jurisdictions have prohibited certain cryptoasset service provision activities.** The type of prohibition varies widely among jurisdictions. Partial approaches are implemented in Belgium, [85] where the promotion of certain crypto-related products to retail investors (eg derivatives based on unbacked cryptoassets) is banned. In the UAE, the DFSA bans any financial activity carried out with "prohibited tokens" (eg privacy tokens or algorithmic tokens) or tokens which are not recognised by the authority.[86] In the case of China, any cryptoassets activity is considered illegal.[87]

[83] As well as safekeeping of clients' cryptoassets and funds and the obligation to establish a complaint handling procedure.

[84] The main policy and regulatory initiatives we used for the analysis are the following: (i) US: Executive Order on Ensuring Responsible Development of Digital Assets; see (US Whitehouse (2022); (ii) EU: MICA Regulation See EC (2020a) and EP (2022b) and DORA EP (2022c); (iii) UK: FCA on AML/CFT regime See FCA (2019 and 2022); UK Consultation on Regulatory Approach (Proposal) See UK Treasury (2021, 2022a) and UK Consultation on the future financial services regulatory regime for cryptoassets. See UK Treasury (2023); BoE Dear CEO letter See BoE (2022b); (iv) Switzerland: Guidance on cryptoassets; Cryptoassets Factsheet May 2022; FinTech License; DLT Federal Act/Ordinance See FINMA (2021, 2022) and Swiss Government (2021); (v) Japan: Payment Services Act Japanese Government (2022); (vi) Singapore: Payment Services Act See MAS, (2019); (vii) Hong Kong: Position paper Regulation of virtual asset trading platforms; Joint circular on intermediaries' virtual asset-related activities See HKMA (2022).

[85] See FSMA of Belgium (2014).

[86] See DFSA (2022a, 2022b).

[87] People's Bank of China (PBoC) et al (2013, 2017, 2021a, 2021b) and China State Council (2021).

International level

77. **SSBs have worked on the development and application of guidelines to promote consistent and effective regulation of service provision activities.** In 2019, the FATF amended its standards (Recommendation 15) to apply AML/CFT obligations to cryptoassets (referred to as virtual assets) and their service providers and regularly reviews the implementation of these standards.[88] The BCBS set out prudential expectations related to the provisions of services related to cryptoassets by banks.[89] The IOSCO published its key considerations for regulating cryptoasset trading platforms[90] and clarified that its standards, including the Objectives and Principles for Securities Regulation, apply to all activities when cryptoassets are considered regulated securities or derivatives instruments. The guidance on the application of the PFMI to stablecoin arrangements by the CPMI-IOSCO reconfirms that service providers involved in the functioning of systemically important stablecoin arrangements are expected to observe all relevant principles of the PFMI.[91]

78. **In 2022, the FSB proposed a new framework for all cryptoasset activities to promote an internationally consistent regulatory approach.** The FSB recommendations,[92] which were developed in close cooperation with international organisations (BIS, IMF, WB) and SSBs (CPMI, IOSCO, FATF) seek to promote the consistency and comprehensiveness of regulatory, supervisory and oversight approaches to cryptoasset activities that may pose risks to financial stability, including front-end activities, and to strengthen international cooperation, coordination and information sharing. They complement the high-level recommendations on global stablecoin arrangements described in subsection 3.1.

Section 4 – Policy measures on community-managed cryptoasset activities

79. **This section provides an overview of policy and regulatory responses that aim to address risks posed by community-managed cryptoasset activities.** These initiatives aim to address the risks associated with two business models. The first one refers to native tokens that are created by a community of participants on a public DLT. The generation of these tokens is governed by participants who claim to be organised through decentralised arrangements. The second business model refers to DLT applications that enable financial functions such as exchange or lending through the implementation of a set of smart contracts that run on public DLTs. These applications are commonly referred to as DeFi protocols and are governed by a community of participants who claim to be organised through decentralised arrangements.

80. **Initiatives related to community-managed cryptoasset activities were mostly in the form of analytical papers.** For activities where native tokens are involved, some authorities rely on a broad interpretation of "rights" to define if a native token is a security and to clarify the application of securities regulation. Others use concrete examples for additional guidance to clarify whether these tokens are

[88] See FATF (2019, 2021, 2022).

[89] See BCBS (2019) Acknowledging that these assets present a number of risks for banks, the Committee expects that some requirements are fulfilled if a bank is authorised and decides to provide cryptoasset services. These requirements are related to due diligence, governance and risk management, disclosure and supervisory dialogue. In relation to the latter, in particular, the bank should inform its supervisory authority of actual and planned cryptoasset exposure or activity in a timely manner and provide assurance that it has fully assessed the permissibility of the activity and the risks associated with the intended exposures and services, and how it has mitigated these risks.

[90] See IOSCO (2020).

[91] See CPMI (2022).

[92] See FSB (2022b, 2022c, 2022d).

subject to regulation.[93] For DeFi protocols, a couple of authorities have issued clarifications on applicable regulation for decentralised exchanges and staking activities and guidance on the adoption of smart contracts. A few authorities have taken enforcement actions addressing AML/CFT and investor protection risks posed by certain protocols. A small number have introduced initiatives to facilitate the adoption of protocols with certain features by traditional financial intermediaries under a trusted environment.

4.1 Native tokens

81. **Native tokens are essential technical components of public DLTs (ie permissionless blockchains).** These tokens are created as part of the consensus mechanism[94] of a given public DLT network and serve to reward specific participants who contribute to ensuring all participants agree on the transactions recorded in the ledger. Native tokens are used to transfer value across participants of a public DLT network without a trusted intermediary. As with any cryptoasset, these tokens are designed for different purposes. For example, some are designed to operate as a peer-to-peer payment infrastructure independently of a central bank or government using cryptography to secure transactions and controlling the creation of new units. These are often referred to as “cryptocurrency” tokens (eg BTC). Others are designed to build applications on a particular public DLT platform. These cryptoassets serve as an economic incentive to pay for transaction fees and other services within the platform (eg ETH) and some authorities refer to them as “exchange” tokens.

82. **Holders of native tokens may use them for economic purposes.** If a native token has a secondary market price, the transferability function could be used to exchange it for something of value. Many consumers buy these tokens in the expectation that their secondary market price will appreciate (ie as a speculative investment). They are also used by some holders to store wealth (ie as a store of value) or to make payments (ie as a means of exchange) (Australian Treasury (2023)).

Jurisdictional level

83. **For native tokens, initiatives in a few jurisdictions are targeting activities involving native tokens rather than the token itself.** These authorities have provided guidelines or clarifications about the conditions in which existing regulatory frameworks apply to activities which involve native tokens.[95] For example, the FSRA ADGM classifies native tokens as “virtual assets” and has issued a guidance that outlines the regulatory treatment governing financial services activities related to these assets.

84. **There are two main issues that authorities consider when assessing the regulatory treatment of activities that involve native tokens.** The first are the relevant characteristics which define whether a cryptoasset qualifies as a security. These characteristics depend on the national legal framework and vary across countries. For example, in the United States, the Howey Test is the key tool for determining whether a token is a security (Gensler (2022)). The second issue is related to the rules applicable to tokens that do not qualify as a security but can be used as investment vehicles by the public.

85. **Some authorities have introduced regulatory requirements that govern entities providing placing services (eg marketing activities) for cryptoassets, including native tokens (commonly referred to as cryptocurrency) that are not considered securities.**[96] These initiatives, as discussed in Section 5, focus mainly on consumer protection issues and impose restrictions or disclosure requirements on entities involved in offering these types of token.

[93] See FSRA ADGM (2022b) and UK Treasury (2023). In both cases, BTC and ETH are mentioned as examples of a specific category of cryptoassets considered in the regulatory framework applicable to CASPs.

[94] The consensus mechanism is the process by which validators agree on the state of a distributed ledger (FSB (2023)).

[95] See FSRA ADGM (2022b) and UK Treasury (2023).

[96] See Bains et al (2022).

4.2 DeFi protocols

86. **DeFi is a new financial paradigm that leverages DLT to offer services such as lending, investing, or exchanging cryptoassets without relying on a traditional centralised intermediary (Auer et al (2023))**. It consists of protocols that implement financial functionalities as a set of smart contracts which run on a public network of computers (ie public DLTs) to automatically manage financial transactions. The underlying ecosystem is competitive as novel intermediaries (eg miners or validators) compete to process and settle transactions.[97]

87. **Several actors play a role in developing DeFi protocols and enabling their operation.** These include creators and developers (the "protocol development group"), investors (including traditional institutional investors, hedge funds and venture capital funds that provide capital to fund the development and deployment of the protocol or retail users that invest in "pseudo-equity" tokens),[98] providers of other services (including oracles,[99] bridges, APIs, cloud services), and networks of miners and validators in the underlying blockchain(s) where smart contracts are deployed and transactions are settled.

88. **Once a DeFi protocol is launched, the ongoing activities are typically governed by a community of participants who claim to be organised through decentralised arrangements.** Participants are usually organised through novel types of technology-mediated structure. These structures are usually unincorporated arrangements or associations, without a formal constitution or registration or a separate legal entity, that make use of cryptoassets and smart contracts for the decision-making process regarding the governance, direction and operation of a DeFi protocol (eg use of governance tokens[100] as enablers of community decision-making). Although some of these structures claim to be decentralised (eg DAOs), at present there is no uniform criteria of the elements that would be considered for classifying a structure or a protocol as decentralised. In the current state of development, the governance of most DeFi protocols retain a level of centralisation in one or more areas such as concentrated ownership and voting power (Aramonte et al (2021)). In many cases, DeFi protocols are subject to centralised data feeds (eg oracles) and can be shaped or influenced by people with "admin keys",[101] or a highly concentrated governance token allocation.

89. **The trustless nature of the public DLTs in which current DeFi protocols are deployed pose a number of risks to its users and the financial system.** Financial functionalities (such as exchanging or lending cryptoassets) implemented by DeFi protocols may be more vulnerable to money laundering, terrorism financing, and other illicit use risks. Access to these functionalities requires only a connection to

[97] See Auer et al (2023) for a detailed technical explanation of the architecture, technical primitives and financial functionalities of DeFi protocols.

[98] In many cases, DeFi protocol creators and developers finance themselves through the issuance of a token that represents a claim on some cash flows produced by the protocol. Many of these DeFi tokens endow token holders with some rudimentary governance rights as well as either implicit or direct claims on cash flows generated through DeFi protocols. These tokens circulate on decentralised financial infrastructure and in some cases on centralised crypto exchanges (Carter and Jeng (2021)). As with initial coin offerings ("ICOs"), depending on the jurisdictions, these more recent types of funding activity may not necessarily have been conducted in compliance with applicable securities laws or may not currently be subject to securities laws in certain jurisdictions (IOSCO (2022)).

[99] DeFi protocols often require information that does not exist on the DLT (eg a cryptoassets market price on a centralised cryptoasset trading platform). Oracles are applications that source, verify and transmit information from the real economy to DeFi protocols. Oracles can be of many forms as long as their outputs are machine-readable: information scraper, human analysts, IoT sensors, public documentation etc.

[100] Governance tokens are tied to a specific DeFi protocol and purport to provide holders with economic rights and/or with voting rights on future changes to certain features of a protocol. They do not, however, provide control over the protocol at the enterprise level. Typically, a single governance token will entitle the holder to a single vote, and votes can also be delegated by those holders who do not wish to participate in voting. Although they can be designed to be user-inclusive, these governance voting systems have been criticised for encouraging plutocratic decision-making (as the amount of tokens one has determines how much voting power one wields) (IOSCO (2022)).

[101] The "admin key" is a private key that holds control over the smart contract containing funds of users. It is used by the developer or founding team to make decisions on the smart contract or perform emergency shutdowns.

a wallet, and some wallets do not require AML/CFT preventive measures for their opening. As such, users can remain fully anonymous or pseudonymous without any link to their identity and with no controls as to the source of funds. Although transactions are traceable and verifiable on the chain, they are so in an anonymous or pseudonymous way, without recourse to the identity of the participant (OECD (2022)). Further, illicit actors are using anonymity-enhancing technologies (eg mixers and tumblers) to obfuscate the details of financial transactions. There are significant risks for those transacting in DeFi that they might engage with a sanctioned counterparty or with cryptoassets sourced through illicit activity (IOSCO (2022)).

90. **In its current state, DeFi has no safeguards.** It lacks protection from criminal conduct or investor fraud and erroneous transactions cannot be undone (Auer et al (2023)). Moreover, DeFi users[102] are exposed to risks related to the legal uncertainty of rights arising from services built on smart contracts. In most jurisdictions, smart contracts are not contracts under civil law, and the interpretation of civil law provisions in the DLT context of events in distributed ledgers remains to be defined. Because there are no recovery schemes or dispute resolution mechanisms, investors run the risk of a total loss in the event of a default. Against this background, DeFi users have no recourse in the event of default or failure of a DeFi protocol and it is frequently challenging to identify a responsible party or central authority that would be in charge of handling consumer concerns.

91. **While the DeFi ecosystem is currently largely separated from the traditional financial system, the ecosystem's growth might present risks to financial stability if there is insufficient regulation and market oversight.** The increase in the use of stablecoins as collateral or bridge between DeFi and traditional finance is a potential channel of risk transmission to the traditional financial markets. Spillovers may also be caused by leverage-driven procyclicality in DeFi lending services, which can arise from changes in collateral value and fluctuations in the associated margins. Due to the largely self-contained nature of DeFi, episodes of rapid deleveraging have thus far had little effect outside the cryptoasset and DeFi ecosystems (FSB (2023)).

92. **Financial stability vulnerabilities may also arise from DeFi concentration risks.** Risks may arise from concentration of (i) the infrastructure used (eg Ethereum blockchain); (ii) critical intermediaries (eg Infura and Alchemy APIs); or (iii) decision-making power in key operations (eg code development, transaction validation, governance) managed by a relatively limited number of people or entities (eg protocol developers, owners of mining hardware, owners of governance tokens) whose true identities may be unknown.

93. **Policymakers around the world are taking a number of steps to address the risks posed by activities implemented through DeFi protocols.** This subsection covers responses in the form of rulemaking, public statements, policy and working papers, enforcement measures and other publications by 25 financial authorities in 11 jurisdictions at the end of March 2023 (Table 6).

[102] DeFi users include service customers and capital providers (Auer et al (2023)).

Regulatory and policy responses to DeFi Table 6

	Rulemaking	Public statement and speeches	Discussion papers and consultations	Reports and working papers	Other*
Canada				✓BoC	
European Union		✓EBA ✓ECB	✓EIOPA	✓EBA ✓ECB ✓ESMA ✓EC	✓ECB
France		✓AMF ✓BdF			
Germany		✓BBK		✓BBK	
Italy		✓BoI			
Japan				✓BoJ	
Netherlands				✓DNB	
Singapore		✓MAS			
United Arab Emirates	✓DFSRA		✓ADGM FSRA ✓DFSRA		
United Kingdom		✓BoE	✓UK Treasury	✓BoE	
United States		✓OCC ✓SEC ✓FED ✓US Treasury		✓GOV ✓FSCO ✓FED ✓PWGFM ✓US Treasury	✓CFTC ✓US Treasury

* = enforcement measures, articles in annual reports, newsletters, bulletins and blogs.

Sources: See list of referenced documents in Annex B. Information as of end-March 2023.

Jurisdiction level

94. **In general, authorities have mostly sought to better understand the dynamics, benefits, risks and challenges of these activities.** Most authorities have released reports and working papers to gain a deeper understanding of the potential benefits of the underlying smart contract functionality and unique risks posed by DeFi protocols as well as to identify regulatory challenges and policy considerations.

95. **At present, clarifications related to DeFi have been issued in only one jurisdiction covered.** As part of its new regulation of crypto tokens,[103] the Dubai Financial Services Authority (DFSA) has clarified that companies established in the Dubai International Financial Centre (DIFC) that are involved in the establishment and running of a decentralised exchange will need to be licensed by the DFSA. Staking will also be allowed in the DIFC, where facilitated or arranged by DFSA-licensed entities, only where such activity is provided to non-retail clients and the purpose of staking is for the borrower to take part in the proof-of-stake consensus mechanism for a recognised crypto token.

96. **A few authorities have taken enforcement measures to address specific risks posed by the use of certain DeFi protocols.** Such is the case of the US Treasury's Office of Foreign Assets Control (OFAC) sanction to Tornado Cash[104] addressing money laundering, terrorism financing, and other illicit

[103] See DFSA (2022a, 2022b).

[104] On 8 August 2022, Tornado Cash was sanctioned by the US Treasury's Office of Foreign Assets Control (OFAC) for its role in laundering more than $7 billion worth of virtual currency since its creation in 2019. These sanctions imply inter alia that all property and interests in Tornado Cash are blocked and that transactions by US persons or within the United States that involve Tornado are prohibited. See: US Department of the Treasury (2022a, 2022b).

activity risks posed by the use of this protocol. Similarly, the US Commodity Futures Trading Commission issued an enforcement action against bZEROx[105] related to the use of this DeFi protocol to illegally offer commodity transactions in digital assets.

97. **Some authorities are introducing initiatives that aim to reap the benefits of smart contract functionalities of DeFi protocols in the traditional financial system within a controlled environment.** Such is the case of the United Kingdom's FCA which has opened its regulatory sandbox to DeFi applications, and MAS which is exploring the feasibility of applications in asset tokenisation and DeFi in a trusted network where guardrails to risks to financial stability and integrity are embedded in the design of the applications.[106]

International level

98. **To address the challenges in the AML/CFT policy domain, in 2021 the FATF updated its guidance for a risk-based approach to Virtual Asset Service Providers (VASPs).** The FATF has clarified that applications based on DeFi protocols (ie DeFi applications) are not a VASP under the FATF standards as these do not apply to underlying software or technology. However, creators, owners and operators (or other persons who maintain control or sufficient influence in DeFi arrangements, even if those arrangements seem decentralised) may fall under the FATF definition of a VASP where they are providing or actively facilitating VASP services. This is the case even if other parties play a role in the service or if parts of the process are automated.[107]

[105] On 22 September 2022, the Commodity Futures Trading Commission issued an order simultaneously filing and settling charges against respondent bZeroX, LLC (bZeroX) and its founders Tom Bean and Kyle Kistner for illegally offering leveraged and margined retail commodity transactions in digital assets; engaging in activities only registered futures commission merchants (FCM) can perform; and failing to adopt a customer identification program as part of a Bank Secrecy Act compliance program, as required of FCMs (US CFTC (2022)).

[106] See MAS (2022a).

[107] See FATF (2022).

Box 1

Potential approaches to addressing the risks associated with DeFi protocols

Traditional regulatory approaches and tools may not be effective, implementable or enforceable for DeFi. Policymakers are analysing various approaches to addressing the different risks associated with DeFi protocols, as set out below.[1]

One approach is to establish a legal framework that recognises the different actors who manage or enable the operation of DeFi protocols. Introducing a legal framework that recognises technology-mediated organisational structures (eg DAOs) as legal entities would make it possible to define entities' and actors' liabilities for their activities (Born et al (2022), OECD (2022), UK Law Commission (2022)). Similarly, introducing a legal framework for the operation of oracles would make it possible to define oracles' liabilities, which would allow some of the safeguards in traditional financial services to be integrated into services provided through DeFi protocols. (EC DG FISMA (2022)). Other approaches suggest considering miners and validators as intermediaries that would be subject to registration and oversight. They would therefore be accountable for extractable value and market manipulation in cryptoasset activities built on public permissionless DLTs (Auer et al (2022)).

Another approach is to impose requirements on regulated entities. One potential line of action is to require legal entities supervised or regulated in traditional markets to disclose and verify their public addresses to dedicated institutions. This would allow policymakers to observe their entire DeFi activity, monitor exposures, and adjust regulatory requirements accordingly. (EC DG FISMA (2022)).

An approach which is currently being tested is the introduction of a "trust layer". The main objective is to establish a trusted environment for the execution of DeFi protocols through a common trust layer of independent "trust anchors". These are regulated financial institutions that screen, verify and issue verifiable credentials to entities that wish to participate in DeFi protocols. This ensures that participants trade only with verified counterparties, issuers and protocol developers (MAS (2022a)).

Similarly, another approach is to "whitelist" protocols. One way to implement this approach is to introduce "approved DeFi protocols". For example, a proposal by the Financial Services Regulatory Authority (FSRA) of the Abu Dhabi Global Market (ADGM) involves assessing the suitability of a DeFi protocol.[2] Various factors would be considered in this assessment, such as the ability to identify participants, the level of transparency regarding the protocol's functionality and governance decisions, and the technology supporting the protocol. Another way to implement this approach is to introduce "institutional grade DeFi protocols". For example, MAS is exploring a technical design that would allow regulatory safeguards and controls to be embedded in DeFi protocols with the aim of preventing market manipulation and mitigating operational risk.[3]

Other approaches are focused on the code used for building smart contracts and DeFi protocols. One option is to establish public-private collaboration for code regulation through ex ante guidelines or ex post code reviews and audits (IMF (2022a). This could be combined with greater disclosure and user education to identify platform-specific risks and close the information gap between retail and institutional investors (OECD (2022)). Smart contract-auditing capabilities could also be used to detect code vulnerabilities (MAS (2022a)). Finally, a regulatory framework could be introduced as part of the code in DeFi protocols which would automatically monitor compliance by reading the market's ledger and reducing the need for firms to actively collect, verify and deliver data (ie "embedded supervision") (Auer (2022)).

Public observatories and voluntary supervisory frameworks are also potential approaches. A public observatory for DeFi activity could be introduced and operated by a public authority. Such an institution would launch public investigations and issue opinions and warnings about specific DeFi protocols, practices and public address activities. While this proposal does not entail enforcement power, it does cover the entire universe of public protocols (EC DG FISMA (2022)). A different approach is to create an open policy framework for the benefits of DeFi services with a view to encouraging voluntary compliance. In such a setting, entities and protocols voluntarily seek to comply with a given set of policy requirements in order to obtain a public stamp of approval and other potential benefits. (EC DG FISMA (2022)).

[1] The potential approaches described in this box have not yet been formulated into formal proposals. [2] See ADGM FSRA (2022b). [3] See MAS (2022a).

Section 5 – Policy measures on users' direct exposures to cryptoassets and related activities

99. **This section provides an overview of policy and regulatory responses that aim to address the risks posed by users' direct exposures to cryptoassets and related activities.** Users of cryptoassets are classified into two groups: retail investors (eg households and non-financial firms) and wholesale investors (eg financial institutions, institutional investors, governments). The subsections below cover policy and regulatory responses targeting these investors.

100. **Policy measures regarding investors' direct exposures to cryptoassets and related activities tend to reflect the evolution of cryptoasset markets.** Most jurisdictions have taken steps to caution retail investors about the potential risks associated with these assets. Some warnings are specific to certain types of cryptoasset, such as native tokens, security tokens and non-fungible tokens. In a few cases, certain cryptoassets have been banned from distribution to retail investors, and some jurisdictions have imposed restrictions on promotional activities. However, no jurisdiction covered in this paper has so far introduced new regulations aimed at mitigating risks arising from traditional financial institutions' investment activities in cryptoassets, specifically for wholesale investors. Nonetheless, several banking authorities have issued statements alerting intermediaries to the potential risks of such exposures and have referenced the BCBS's work in this area.

5.1 Retail investors

Jurisdictional level

101. **Warnings are typically the first type of policy and regulatory response that authorities issue to protect retail users of cryptoassets.** These warnings tend to promote consumer protection and financial education. In general, warnings focus on specific types of cryptoasset (eg native tokens like BTC and ETH), explaining the main features of these assets and warning investors and consumers on the risks associated with them. Responses in the market conduct domain also consist of initiatives to promote financial education such as Q&As,[108] dedicated webpages[109] or reports,[110] explaining what cryptoassets are and the associated risks. In some jurisdictions, distribution of certain products to retail investors is banned. This is the case in Belgium and United Kingdom, which both imposed a ban on the distribution of some derivatives based on cryptoassets.[111,112]

102. **Responses targeting households and firms tend to reflect evolution of market developments.** The market for cryptoassets is evolving rapidly and has given rise to a diverse array of token uses. It began with tokens used for investment purposes and initial coin offerings (ICOs), commonly referred to as equity or security tokens. It also included tokens used as a means of payment or exchange, typically referred to as payment tokens. Recently, stablecoins have emerged as another class of tokens in this market. As market adoption of cryptoassets increased, further waves of warnings were issued by authorities. These took the form of reminders and guidance on applicable regulation. Lately, these reminders have specially targeted promotional practices. The popularity of investments in native and non-

[108] See eg the FAQ on virtual currencies on the website of the Bangko Sentral ng Pilipinas.

[109] See eg information webpage on ICOs on the website of the UK Financial Conduct Authority.

[110] See PWGFM (2021).

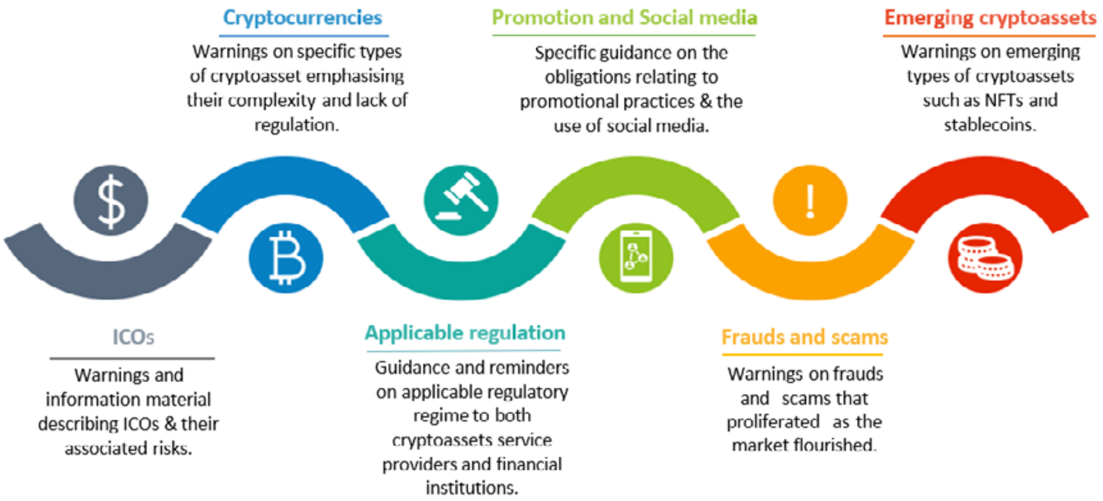
[111] See FSMA of Belgium (2014).

[112] See FCA (2020).

native tokens,[113] including fungible[114] and non-fungible tokens,[115] also led to the multiplication of frauds and scams, about which authorities have attempted to warn investors (see Graph 2).

Policy and regulatory responses to retail investors' exposures to cryptoassets and related activities

Graph 2



Cryptocurrencies

Warnings on specific types of cryptoasset emphasising their complexity and lack of regulation.

Promotion and Social media

Specific guidance on the obligations relating to promotional practices & the use of social media.

Emerging cryptoassets

Warnings on emerging types of cryptoassets such as NFTs and stablecoins.

ICOs

Warnings and information material describing ICOs & their associated risks.

Applicable regulation

Guidance and reminders on applicable regulatory regime to both cryptoassets service providers and financial institutions.

Frauds and scams

Warnings on frauds and scams that proliferated as the market flourished.

Source: Authors' elaboration.

103. **An emerging focus is the aggressive promotion of cryptoassets, especially through social media.** This responds to a growing trend of promoting tokens to the public at large. Examples include warnings against celebrities promoting cryptoassets, or influencers on YouTube or social media.

104. **Some jurisdictions have taken steps to define an advertising framework regulating the promotion of cryptoassets.** In Spain, the National Securities Market Commission (CNMV) has been responsible for supervising advertising practices on these tokens since 2021 and has published rules in January 2022 on the advertising of cryptoassets for investment purposes.[116] In 2021, the Canadian Securities Administrators published a guidance on advertising and marketing activities for cryptoasset trading platforms. In the United Kingdom, all firms marketing cryptoassets to UK consumers, including firms based overseas, will need to comply with the financial promotions regime.[117]

105. **While the cryptoasset markets peaked out at almost $3 trillion in November 2021, the number of fraudulent schemes and scams has also increased exponentially.** This is reflected by the increase in warnings on frauds and scams by financial authorities during 2021. Against this background, some jurisdictions have implemented initiatives to help consumers identify fraudulent trading platforms. These initiatives often take the form of a list of compliant trading platforms published on the financial authority's website.[118] Authorities also communicate on enforcement actions and sanctions against

[113] Non-native tokens refer to tokens that are created and maintained by a smart contract on public or private DLTs with programming capabilities.(Auer et al (2023)).

[114] Fungible tokens refer to tokens that are intrinsically indistinguishable (Auer et al (2023)).

[115] Non-fungible tokens (NFT) refer to tokens that are mathematically unique and unable to be fractionalised (Auer et al (2023)).

[116] See CNMV (2022).

[117] See FCA (2023).

[118] See eg the DNB register or FCA register of authorised crypto service providers.

platforms.[119] More recently, initiatives have started to focus on cryptoassets classified as stablecoins or as non-fungible tokens.

5.2 Wholesale investors

Jurisdictional level

106. **Recent policy initiatives aimed at regulating the exposure of institutional investors to cryptoassets have centred predominantly on banks and investment funds.** There are no specific standards for insurers and pension funds on investing in cryptoasset markets. Yet, they are subject to more general guidelines related to internal controls, risk management and the valuation of assets and liabilities.

107. **For the direct exposure of investment funds to cryptoasset markets, authorities' initiatives have focused on consumer protection risks and compliance with standards related to custody services.** In many jurisdictions, securities regulators have provided guidance on funds' holding of cryptoassets. For example, the Hong Kong Securities and Futures Commission has published a statement including its regulatory framework for virtual asset portfolios managers.[120] The Australian Securities and Investment Commission has published guidance on exchange traded products and investment, which outlines good practices in relation to custody, risk management and disclosure.[121] In Canada, the CSA and IIRO have highlighted a number of issues that funds investing in cryptoassets need to consider.[122] These issues include due diligence on the exchange used to purchase or sell tokens and the need to have proper valuation and quality standards for custody services. On the latter, funds are advised to use custodians that have expertise in holding cryptoassets, including experience with hot and cold storage,[123] security measures to keep cryptoassets protected from theft, and the ability to segregate the cryptocurrencies from other holdings as needed.

International level

108. **Rules to mitigate risks from banks' direct exposures to cryptoassets have been developed at the international level by the BCBS.** In December 2022, the BCBS introduced a set of risk-based classification conditions for cryptoassets and defined the applicable capital treatment for each category. The BCBS prudential standard is due for implementation by 1 January 2025. The taxonomy is structured into two main groups. The first group includes tokenised traditional assets and stablecoins that satisfy a set of conditions, while the second includes all other cryptoassets.

Section 6 – Future challenges and concluding remarks

109. **Cryptoassets and related activities will continue to require authorities' attention in several areas, such as initiatives aimed at addressing risks associated with cryptoassets beyond security tokens or stablecoins.** Most authorities have not yet adopted specific regulatory initiatives for issuers of utility tokens, governance tokens or non-fungible tokens. In future, authorities may consider the introduction of restrictions or specific requirements related to the use of utility tokens as investments.

[119] See eg FINMA, which ascertained illegal activity by envion AG or UOKiK and initiated the first proceedings against pyramid schemes and their advertisers.

[120] See HKSFC (2018).

[121] See ASIC (2021, 2022).

[122] See CSA (2021).

[123] Hot storage is related to custody services that are always connected to the internet, while cold storage uses hardware devices that can keep data offline.

Such limitations could, for example, restrict issuers' ability to buy back such tokens or prohibit exchanges to list such tokens or to provide credit to trade such tokens (ie ban on margin trading). Authorities may also consider placing similar restrictions on governance tokens and any other tokens that are created to perform a different function than those operated by existing financial assets.

110. **Another area that will continue to require authorities' attention is initiatives to address risks related to risk management practices and potential anti-competitive behaviour in centrally managed cryptoasset activities.** While a few initiatives have emerged to limit concentration risks for stablecoin issuers, authorities may consider adopting similar initiatives to limit the risks associated with centralised entities engaging in multiple functions. For example, some trading platforms, besides their primary functions as exchanges and intermediaries, also engage in other services such as custody, brokerage or lending or other activities related to issuance and operation of DLT infrastructures. By vertically integrating multiple functions, these entities resemble a financial conglomerate (FSB (2022c)). For these cases, authorities may restrict the number and type of activities managed by one centralised intermediary; forbid issuers of payment stablecoins from engaging in other cryptoassets activities such as trading; and establish risk management guidelines for intermediaries involved in issuing or servicing stablecoins and operating DLT-based infrastructures. In this respect, a business model analysis can be helpful in providing authorities with a better understanding of an entity's cryptoasset activities. This assessment, which could include an evaluation of governance and decision-making processes, could help identify the actors responsible and accountable for all cryptoasset activities within one entity.

111. **If entities in the traditional financial sector start using public permissionless DLTs to develop applications related to the provision of financial services, this might require authorities to consider how appropriate regulation should look.** Significant operational and technological risks may arise as more use cases are built on top of infrastructures where governance is usually dispersed and it is difficult to identify which participants or entities should be accountable.

112. **Regulatory frameworks may need to take into account additional technical elements that can affect the risk level of applications built on public permissionless DLTs.** For example, two cryptoassets or activities may have the same economic function but the differences in the underlying DLT computing environment in which they run can result in different risks. These differences include factors such as the type of consensus mechanism, the underlying smart contract code or the data reliability of the oracles. These risks might need to be captured in regulatory frameworks and the adoption of a technology-neutral approach may not be appropriate in such cases.

113. **Authorities may need to assess whether there is a need to adjust the regulatory perimeter to include new actors involved in services provided through DeFi protocols.** The risks associated with DeFi are similar to those addressed by existing financial regulations. However, assuming that authorities only need to adjust the regulatory perimeter of different financial activities to include DeFi alongside traditional finance would be incorrect.[124] For example, new actors involved in services provided through DeFi protocols might need to be accounted for. Also, there might be a case for regulating actors who enable financial functionalities implemented by DeFi protocols and have control over (i) the code that replicates those functions (eg developers); (ii) transaction validation and settlement processes (eg miners and validators); (iii) the governance of applications (eg governance token holders); or (iv) smart contract operations by providing key data (eg oracles).[125]

114. **Authorities might also need to develop legal frameworks to enforce agreements coded in smart contracts.** In this context, they may need to determine the liability of participants involved in technology-mediated structures that manage services using tokens with financial functions. Public bodies in some jurisdictions are currently exploring how the law might be adjusted to accommodate these new

[124] See Restoy (2022).

[125] See Auer et al (2022) for discussions on regulation of miners and validators and EC (2022b) on regulation of oracles.

structures;[126] and financial authorities may consider developing guidelines or recommendations for the application of such laws in the financial sector.

115. **Similarly, financial supervisory architecture and legal frameworks might need to be adjusted.** There could be a need to define which authorities will regulate and supervise various entities and activities involved in offering financial services with cryptoassets. In some jurisdictions, multiple authorities regulate and supervise these entities and/or activities, while others have opted to establish a bespoke authority.[127]

116. **Adequate expertise and resources will be critical for addressing the risks posed by cryptoasset and DeFi ecosystems.** These ecosystems are constantly evolving as they incorporate new design features, emerging technologies and market participants. Such is the case, for example, of the use of generative artificial intelligence tools to develop code and smart contracts; the entrance of big techs as providers of DLT infrastructure;[128] the provision of infrastructure and interconnectivity services by oracle providers;[129] or the emergence of new token standards.[130] Therefore, authorities will need to make continuous efforts to understand novel business models and their underlying risks, as well as to develop or maintain the skills and capacity to adequately assess potential implications on financial markets and to adjust their regulatory responses promptly. Authorities will only be able to respond to potential risks to the financial system if they have adequate resources and access to timely and reliable information.

117. **Cooperation and coordination at the national and international level remain essential to address the risks associated with cryptoassets and their markets.** The recent turmoil in cryptoasset markets underscores the critical need for swift and global implementation of international standards. The inherently global nature of cryptoassets lends itself to regulatory and supervisory arbitrage. Jurisdictions cannot fully mitigate their risks as long as they are exposed to weaknesses and inconsistencies across borders. In addition to consistent implementation of international standards, a harmonised framework for the regulation of cryptoassets and related services is key to addressing the related risks.

[126] Examples include the UK Law Commission Call for Evidence on DAOs (2022) and the Council of Arab Central Banks and Monetary Authorities Governors Guidance Note on Adopting Smart Contracts and their Legal Enforceability in Arab Countries (2022).

[127] This is the case of Dubai’s Virtual Asset Regulatory Authority (VARA).

[128] For example, Google Cloud providing node services.

[129] For example, Chainlink providing APIs through Chainlink Functions.

[130] For example, Ethereum’s new token standard ERC-4437.

References

Aldasoro, I, S Doerr, L Gambacorta, R Garratt and P Koo Wilkens (2023): "The tokenisation continuum", *BIS Bulletin*, no 72.

Aquilina, M, J Frost and A Schrimpf (2023): "Addressing the risks in crypto: laying out the options", *BIS Bulletin*, no 66.

Aramonte, S, W Huang, and A Schrimpf (2021): "DeFi risks and the decentralisation illusion", *BIS Quarterly Review*, December, pp 21–36.

Auer, R (2022): "Embedded supervision: how to build regulation into decentralised finance", BIS Working Papers, no 811, May.

Auer, R, Frost J and J Vidal Pastor (2022): "Miners as intermediaries: extractable value and market manipulation in crypto and DeFi", *BIS Bulletin*, no 58.

Auer, R, B Haslhofer, S Kitzler, P Saggese and V Friedhelm (2023): "The technology of decentralized finance (DeFi)", *BIS Working Papers*, no 1066, January.

Australian Treasury (2023): Token Mapping Consultation paper, February.

Australian Prudential Regulation Authority (APRA) (2022): *Cryptoassets: Risk management expectations and policy roadmap*, April.

Australian Securities and Investments Commission (ASIC) (2017): *Evaluating distributed ledger technology*, March.

——— (2021): Crypto-assets, Information sheet, no 225, October.

——— (2022): Exchange traded products: admission guidelines, Information sheet, no 230, November.

Bains, B, A Ismail, F Melo and N Sugimoto (2022): "Regulating the crypto ecosystem: the case of unbacked crypto assets", *IMF Fintech Notes*, September.

Bangko Sentral ng Pilipinas (BSP) (2021): Guidelines for Virtual Service Providers, Circular no 1108.

Bank of England (BoE) (2022a): Financial Stability in Focus: Cryptoassets and decentralised finance, March.

——— (2022b): Existing or planned exposure to cryptoassets, March.

——— (2022c): If a blockchain became more critical to the financial system how should it be governed?, Bank Overground blog, December.

Bank of Italy (BoI) (2022): Communication on Decentralised technology in finance and cryptoassets, September.

Basel Committee on Banking Supervision (BCBS) (2019): Statement on cryptoassets, March.

——— (2022), Prudential treatment of cryptoasset exposures, December.

Bech, M, J Hancock, T Rice and A Wadsworth (2020): "On the future of securities settlement", *BIS Quarterly Review*, March, pp 67–83.

Born, A, I Gschossmann, A Hodbod, C Lambert and A Pellicani (2022): "Decentralised finance – a new unregulated non-bank system?", *ECB Macroprudential Bulletin*, July.

Canadian Securities Administrators (CSA) (2017a): Cryptocurrency Offerings, *Staff Notices*, no 46-307, August.

——— (2017b): Decisions on Token Funder Inc. Initial coin offering, October.

——— (2018): Securities Law Implications for Offerings of Tokens, *Staff Notices*, no 46-308, June.

——— (2021): Guidance for Cryptoasset Trading Platforms: Compliance with Regulatory Requirements, March.

Carter, N and L Jeng (2021): DEFI protocol risks: The paradox of DeFi, SSRN, June.

China State Council (2021): Report of the 51st meeting of the financial stability and development committee of the state council, May.

Comision Nacional del Mercado de Valores of Spain (CNMV) (2022): New guidance on the promotion of cryptoassets for investment purposes, January.

Committee on Payments and Market Infrastructure (CPMI) (2017): *Distributed ledger technology in payment, clearing and settlement*, February.

——— (2022), *Application of the Principles for Financial Market Infrastructures to stablecoin arrangements*, July.

Council of Financial Regulators of Australia (CFR) (2022): Quarterly Statement, December.

Dubai Financial Services Authority (DFSA) (2022a): Consultation paper on the regulation of crypto tokens, no 143, March.

——— (2022b): Feedback statement on CP 143 regulation of crypto tokens, October.

European Commission (EC) (2020a): Proposal for a Regulation of the European Parliament and of the Council on Markets in Cryptoassets, and amending Directive (EU) 2019/1937, September.

——— (2020b): Proposal for a Regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology, September.

——— (2022a): Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology, and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65/EU, May.

European Commission, Directorate-General for Financial Stability, Financial Services and Capital Markets Union (EC DG FISMA) (2022): *Decentralized finance : information frictions and public policies : approaching the regulation and supervision of decentralized finance*, Publications Office of the European Union, June.

European Insurance and Occupational Pensions Authority (EIOPA) (2021): Blockchain and smart contracts in insurance, April.

European Parliament (EP) (2022a): Pilot regime for market infrastructures based on distributed ledger technology, June.

——— (2022b): Proposal for a Regulation of the European Parliament and of the Council on Markets in Cryptoassets, and amending Directive (EU) 2019/1937, Provisional agreement resulting from interinstitutional negotiations, October.

——— (2022c): Digital Operational Resilience Act, November.

Financial Action Task Force (FATF) (2019): Guidance for a risk-based approach to virtual assets and virtual asset service providers, June.

——— (2020): Report to G20 on so-called stablecoins, June.

——— (2021): Updated guidance for a risk based approach to virtual assets and virtual asset service providers, October.

——— (2022): Targeted Update on Implementation of FATF's Standards on VAs and VASPs, June.

Financial Conduct Authority (FCA) (2019), Guidance on Cryptoassets, July.

——— (2020), Policy Statement 20/10: Prohibiting the sale to retail clients of investment products that reference cryptoassets, October.

——— (2022): Anti-Money Laundering and counter-terrorist financing regime, March.

——— (2023): Cryptoasset firms marketing to UK consumers must get ready for financial promotions regime, February.

Financial Services and Markets Authority (FSMA) of Belgium (2014): Regulation of the Financial Services and Markets Authority on the ban on the distribution of certain financial products to retail clients, approved by the Royal Decree, April.

Financial Services Regulatory Authority (FSRA) of Abu Dhabi Global Market (ADGM) (2022a): Discussion paper on Decentralised Finance (DeFi), April.

——— (2022b): Guiding Principles for the Financial Services Regulatory Authority's Approach to Virtual Asset Regulation and Supervision, September.

Financial Stability Board (FSB) (2020): Regulation, Supervision and Oversight of Global Stablecoin Arrangements, October.

——— (2022a): Assessment of Risks to Financial Stability from Cryptoassets, February.

——— (2022b): International regulation of cryptoasset activities: a proposed framework: questions for consultation, October.

——— (2022c): Regulation: Supervision and Oversight of cryptoasset activities and markets: consultative document, October.

——— (2022d): Review of High-level recommendations of the regulation supervision and oversight of GSC consultative report, October.

——— (2023): The Financial Stability Risks of Decentralised Finance, February.

Financial Stability Oversight Council (FSOC) (2022): Digital Assets Financial Stability Risks and Regulations, October.

Gensler, G (2022): Prepared Remarks of Gary Gensler on Crypto Markets, Penn Law Capital Markets Association Annual Conference, April.

Hong Kong Monetary Authority (HKMA) (2022): Regulatory approaches to Authorized Institutions' interface with Virtual Assets and Virtual Asset Service Providers, January.

——— (2023): Conclusion of Discussion Paper on Cryptoassets and Stablecoins, January.

Hong Kong Monetary Authority (HKMA) and Hong Kong Securities and Futures Commission (HKSFC) (2022): Joint circular on intermediaries' virtual asset-related activities, January.

Hong Kong Securities and Futures Commission (HKSFC) (2018): Statement on regulatory framework for virtual asset portfolios managers, fund distributors and trading platform operators, November.

Hong Kong Special Administrative Region (2022): Government welcomes passage of Anti-Money Laundering and Counter-Terrorist Financing (Amendment) Bill 2022, December.

Intergovernmental Fintech Working Group (2021): Press release on the Intergovernmental Fintech Working Group (IFWG) launch of Project Khokha 2, February.

International Monetary Fund (IMF) (2021): "The crypto ecosystem and financial stability challenges", October.

——— (2022a): Chapter 3: The rapid growth of fintech: vulnerabilities and challenges for financial stability – Neobanks and DeFi, April.

——— (2022b): 'DeFi' and 'TradFi' must work together, September.

International Organisation of Securities Commissions (IOSCO) (2012): Policy Recommendations for Money Market Funds, October.

——— (2013): Principles for the Regulation of Exchange Traded Funds, June.

——— (2020): Issues, risks and regulatory considerations to crypto-asset trading platforms, February.

——— (2022): Report of decentralised finance, March.

Japanese Financial Services Agency (JFSA) (2022): Regulatory Framework for Cryptoassets and Stablecoins, September.

Japanese Government (2022): Payment Service Act, January.

Monetary Authority of Singapore (MAS) (2019): Payment Services Act, April.

——— (2022a): MAS Partners the Industry to Pilot Use Cases in Digital Assets, May.

——— (2022b): Speech by Mr Heng Swee Keat, Deputy Prime Minister and Coordinating Minister for Economic Policies, at the Asia Tech X Singapore Summit, May.

——— (2022c): Proposed Regulatory Approach for Stablecoin-Related Activities, October.

——— (2022d): Guidelines on Provision of Digital Payment Token Services to the Public, December.

Netherlands Bank (DNB) (2021): Governance in systems based on distributed ledger technology (DLT): a comparative study, June.

Organisation for Economic Co-operation and Development (OECD) (2020): The Tokenisation of Assets and Potential Implications for Financial Markets, January.

——— (2021a): Regulatory Approaches to the Tokenisation of Assets, OECD Blockchain Policy Series.

——— (2021b): Digitalisation and Finance in Asia.

——— (2022a): Why Decentralised Finance (DeFi) Matters and the Policy Implications, January.

People’s Bank of China (PBoC) Ministry of Industry and Information Technology (MIIT), China Banking Regulatory Commission (CBRC) and China Insurance Regulatory commission (CIRC), China Securities Regulatory Commission (CSRC) (2013): Notice on the prevention of Bitcoin risks, December.

——— (2017): Circular on preventing risks relating to fundraising through token offerings, September.

——— (2021a): Notice on Rectifying Crypto Currency Mining Activities, September.

——— (2021b): Notice on Further Preventing and Disposing of the Risks of Crypto Currency Trading Speculation, September.

Phillips, T (2022): “Tokenized deposits: how I learned to stop worrying and love stablecoins”, SSRN Working Paper, no 4152735.

President’s Working Group on Financial Markets, the Federal Deposit Insurance Corporation and the Office of the Comptroller of the Currency (PWGFM) (2021): Report on stablecoins, November.

Rauchs, M, A Glidden, B Gordon, G Pieters, M Recanatini, F Rostand, K Vagneur and B Zhang (2018): “Distributed ledger technology systema: a conceptual framework report”, University of Cambridge, Judge Business School, September.

Restoy, F (2022): “DeFi prospects and regulatory implications”, *Eurofi Magazine*, September.

Schär, F (2021): “Decentralized finance: on blockchain- and smart contract-based financial markets”, Federal Reserve Bank of St Louis, Review, Second Quarter, April.

South Africa Intergovernmental Fintech Working Group (2021): Project Khokha 2 launched to explore the policy and regulatory implications of tokenisation in financial markets. Press Release, February.

Swiss Financial Market Supervisory Authority (FINMA) (2018): Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs), February.

——— (2019): Guidelines for FinTech licence applications pursuant to Article 1b of the Banking Act, August.

——— (2022): Factsheet on Cryptoassets, May.

Swiss Government (2021): Federal Act on the Adaptation of Federal Law to Developments in Distributed Electronic Register Technology, August.

Swiss National Bank (2022): “Swiss National Bank sets criteria for admitting DLT trading facilities to Swiss Interbank Clearing payment system”, Press Release, March.

Switzerland Federal Council (2020): Federal Act on the Adaptation of Federal Law to Developments in Distributed Ledger Technology, October.

Switzerland Federal Department of Finance (2021): *Blockchain and cryptoassets in the financial sector: Switzerland's pioneering role on the international stage*, December.

UK Law Commission (2022): Call for evidence on DAOs, November.

UK Treasury (2021): UK regulatory approach to cryptoassets and stablecoins Consultation and call for evidence, January.

——— (2022a): UK regulatory approach to cryptoassets and stablecoins: Responses to Consultation and call for evidence, April.

——— (2022b): Government sets out plan to make UK a global cryptoasset technology hub, April.

——— (2023): Future financial services regulatory regime for cryptoassets, Consultation and call for evidence, February.

United Arab Emirates (UAE) Regulatory Authorities (2021): Guidelines for Financial Institutions Adopting Enabling Technologies, November.

US Commodity Futures Trading Commission (CFTC) (2022): CFTC Imposes $250,000 Penalty Against bZeroX, LLC and Its Founders and Charges Successor Ooki DAO for Offering Illegal, Off-Exchange Digital-Asset Trading, Registration Violations, and Failing to Comply with Bank Secrecy Act, September.

US Board of Governors of the Federal Reserve System (Federal Reserve), Federal Deposit Insurance Corporation (FDIC) and the Office of the Comptroller of the Currency (OCC) (2023): Joint Statement on Crypto-Asset Risks to Banking Organizations, January.

US Treasury (2022a): Sanctions Notorious Virtual Currency Mixer Tornado Cash, August.

——— (2022b): Tornado Cash Redesignated with Additional DPRK Authorities, November.

US White House (2022): "Ensuring Responsible Development of Digital Assets", Executive Order, no 14067, March.

Annex A: Glossary

This glossary sets out a (non-exhaustive) list of terms used in this paper. Most definitions are based primarily on previous reports by SSBs. The use of these terms in this paper does not involve a judgment as to their appropriateness in all cases given the rapidly evolving cryptoasset markets.

51% attack: When a malicious actor is able to compromise more than half of the validators on the network, the actor can execute fraudulent transactions (FSB (2023)).

Blockchain: A form of distributed ledger in which details of transactions are held in the ledger in the form of blocks of information. A block of new information is attached into the chain of pre- existing blocks via a computerised process by which transactions are validated (FSB (2023)).

Bridge: A technique used to transfer cryptoassets between ecosystems by, typically, creating a synthetic representation of a blockchain-specific cryptoasset on a different blockchain (FSB (2023)).

Consensus mechanism: In DLT applications, the process by which validators agree on the state of a distributed ledger (FSB (2023)).

Cryptoasset: A type of private sector digital asset that is expressed primarily through cryptography and distributed ledger or similar technology (FSB (2023)).

Cryptoasset trading platform: Any trading platform where cryptoassets can be bought and sold, regardless of the platform's legal status (FSB (2023)).

Cryptography: The conversion of data into private code using encryption algorithms, typically for transmission over a public network (FSB (2023)).

Decentralised autonomous organisation (DAO): In theory, a decentralised application consisting of rules of operation that dictate who can execute a certain behaviour or make an upgrade. Code helps create an organisational structure intended to function without a centralised management structure (FSB (2023)).

Decentralised applications (DApps): DeFi applications offering services such as lending or trading, predominantly between cryptoassets including stablecoins (FSB (2023)).

Decentralised finance (DeFi): A set of alternative financial markets, products and systems that operate using crypto-assets and smart contracts (software) built using distributed ledger or similar technology (FSB (2023)).

DeFi protocol: A specialised system of rules that creates a program designed to perform traditional financial functions (FSB (2023)).

Distributed ledger technology (DLT): A means of saving information through a distributed ledger, such as a repeated digital copy of data available at multiple locations (FSB (2023)). Essentially, it refers to a database that is stored, shared, and synchronised on a computer network. Data are updated by consensus among the network participants. Blockchain is one example, but it does not necessarily maintain its record using the same chain of blocks architecture.

Global stablecoin: Stablecoin with a potential reach and use across multiple jurisdictions and which could become systemically important in and across one or many jurisdictions, including as a means of making payments and/or store of value. (FSB (2022c)).

Governance token: Tokens issued as an incentive, allowing the user the purported opportunity to become a partial owner and decision-maker in a DeFi protocol (FSB (2023)).

Mining: One means to create new cryptoassets, often through a mathematical process by which transactions are verified and added to the distributed ledger (FSB (2023)).

Native token: The base token of a blockchain which plays an integral part of the operation of the protocol it is issued on and that is created at its genesis. It is usually used to pay transaction fees (FSB (2023)).

Oracle: A service that enables smart contracts to access, in real time, relevant external or off- chain data by means of queries typically through cryptoasset exchange application programming interfaces and which provides inputs to smart contracts (FSB (2023)).

Security token: tokens that provide rights and obligations similar to traditional financial instruments such as shares, debt instruments or units in a collective investment scheme, as defined in securities regulation.

Smart contract: A cryptoasset term that refers to self-executing applications that can trigger an action if some pre-specified conditions are met (FSB (2023)).

Stablecoin: A cryptoasset that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets (FSB (2022c)).

Stablecoin arrangement: an arrangement that combines a range of functions to provide an instrument that purports to be used as a means of payment and/or store of value (CPMI (2022)).

Staking: The process of locking up crypto-assets for a set period of time to help support the operation of a blockchain in return for a share of transaction fees (FSB (2023)).

Tokenisation: The process of creating a digital representation (token) of an asset and putting it on a distributed ledger. The information stored in tokenised form can include asset type, ownership details, valuation, legal framework, optionality and settlement requirements, among other elements that enable significant customisation opportunities for issuer and owner to elect (FSB (2023)).

Tokenised traditional assets: digital representations of traditional assets using cryptography, DLT or similar technology to record ownership. Traditional assets are those assets that are captured within the Basel Framework that are not classified as cryptoassets (BCBS (2022)).

Unbacked cryptoassets: cryptoassets that are neither tokenised traditional assets nor stablecoins (BCBS (2022)).

Utility token: tokens that allow users to access specific digital services or perform functions within a given DLT application when they redeem the token.

Wallet: An application or device for storing the private keys providing access to the crypto-asset. Hosted wallets are typically held by a third-party provider, unhosted wallets by the user (FSB (2023)).

Online Annex B: References of regulatory and policy responses covered in Table 6

The Annex B is available as an online appendix and can be found on the BIS website.