FSB FINANCIAL STABILITY BOARD

Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements

Final Report and High-Level Recommendations

13 October 2020

The Financial Stability Board (FSB) coordinates at the international level the work of national financial authorities and international standard-setting bodies in order to develop and promote the implementation of effective regulatory, supervisory and other financial sector policies. Its mandate is set out in the FSB Charter, which governs the policymaking and related activities of the FSB. These activities, including any decisions reached in their context, shall not be binding or give rise to any legal rights or obligations.

Contact the Financial Stability Board

Sign up for e-mail alerts: www.fsb.org/emailalert
Follow the FSB on Twitter: @FinStbBoard
E-mail the FSB at: fsb@fsb.org

Table of Contents

Executive summary 1

Glossary 5

Introduction 7

1. Characteristics of global stablecoins 9

    1.1. Stabilisation mechanism 9

    1.2. Combination of multiple functions and activities 10

    1.3. Potential reach and adoption across multiple jurisdictions 12

2. Risks and vulnerabilities raised by global stablecoins 12

    2.1. Potential risks to financial stability from a GSC 13

    2.2. Vulnerabilities arising from the functions and activities of a GSC arrangement .. 14

3. Existing regulatory, supervisory and oversight approaches and challenges 17

    3.1. Findings from the FSB Stocktake 17

    3.2. International standards that could apply to GSC arrangements 19

4. Cross-border regulation, supervision and oversight 23

    4.1. Cross-border challenges 23

    4.2. Issues for cross-border cooperation and coordination 23

    4.3. Role of existing standards on cooperation, coordination and information sharing 25

5. High-Level Recommendations for the effective regulation, supervision and oversight of GSCs 27

    5.1. Objectives 27

    5.2. Scope 27

    5.3. Follow-up and review 28

    5.4. High-level Recommendations 29

Annex 1: Different operating models for stablecoin arrangements 37

Annex 2: Examples of vulnerabilities, regulatory tools, and international standards by activity of a GSC arrangement 38

Annex 3: Summary of stocktake responses 46

Annex 4: Details from standard-setting bodies on work underway 54

Annex 5: Potential elements that could be used to determine whether a stablecoin qualifies as a GSC 69

Executive summary

So-called "stablecoins" are a specific category of crypto-assets which have the potential to enhance the efficiency of the provision of financial services, but may also generate risks to financial stability, particularly if they are adopted at a significant scale. While such financial stability risks are currently limited by the relatively small scale of these arrangements, this could change in the future. Stablecoins are an attempt to address the high volatility of "traditional" crypto-assets by tying the stablecoin's value to one or more other assets, such as sovereign currencies. They have the potential to bring efficiencies to payments (including cross-border payments), and to promote financial inclusion. However, a widely adopted stablecoin with a potential reach and use across multiple jurisdictions (so-called "global stablecoins" or GSCs) could become systemically important in and across one or many jurisdictions, including as a means of making payments.

The emergence of GSCs may challenge the comprehensiveness and effectiveness of existing regulatory, supervisory and oversight approaches. The activities associated with GSCs and the risks they may pose can span across banking, payments, and securities/investment regulatory regimes both within jurisdictions and across borders. GSCs also can give rise to specific vulnerabilities. For example, depending on the facts and circumstances, specific money-laundering/terrorist financing risks may emerge; the decentralised nature of GSC arrangements could pose governance challenges; stabilisation mechanisms and redemption arrangements could pose market, liquidity, and credit risks; and, the infrastructure and technology used for recording transactions, and accessing, transferring and exchanging coins could pose operational and cyber-security risks. Ensuring appropriate regulation, supervision and oversight within jurisdictions and internationally will therefore be important to prevent any potential gaps and avoid regulatory arbitrage.

The G20 mandated the FSB in June 2019 to examine regulatory issues raised by GSCs and to advise on multilateral responses as appropriate, taking into account the perspective of emerging market and developing economies (EMDEs). In February 2020, the G20 reiterated the importance of evaluating and appropriately addressing the risks of GSCs before they commence operation and supported the FSB's efforts to develop regulatory recommendations with respect to GSCs. The FSB carried out an analysis of financial stability risks raised by GSCs and conducted a comprehensive survey of regulatory, supervisory and oversight approaches to stablecoins amongst FSB members and non-FSB members represented on FSB Regional Consultative Groups (RCGs). A report with proposed recommendations to address the regulatory, supervisory and oversight challenges raised by GSCs arrangements was issued for public consultation in April 2020.[1] The FSB also carried out a series of virtual outreach meetings with representatives from regulated financial institutions, financial technology firms, academia and the legal field.

---

[1] *Addressing the regulatory, supervisory and oversight challenges raised by "global stablecoin" arrangements: Consultative document*
Public responses received*: Public responses to consultation on Addressing the regulatory, supervisory and oversight challenges raised by "global stablecoin" arrangements*

This final report takes account of the feedback from the public consultation and the outreach. It sets out ten high-level recommendations that seek to promote coordinated and effective regulation, supervision and oversight of GSC arrangements to address the financial stability risks posed by GSCs, both at the domestic and international level, while supporting responsible innovation and providing sufficient flexibility for jurisdictions to implement domestic approaches. The recommendations call for regulation, supervision and oversight that is proportionate to the risks, and stress the value of flexible, efficient, inclusive, and multi-sectoral cross-border cooperation, coordination, and information sharing arrangements among authorities that take into account the evolving nature of GSC arrangements and the risks they may pose over time.

The recommendations are addressed to authorities at jurisdictional level and focus on privately-issued GSCs predominately intended for retail use. Although the recommendations are aimed at global stablecoins, they could be used for other stablecoins, including those that may pose risks to financial stability only in some countries or regions, and, potentially, other crypto-assets that could pose risks similar to some of those posed by GSCs because of comparable international reach, scale and use.

The report is intended to primarily address risks to financial stability and therefore does not cover important issues such as AML/CFT, data privacy, cyber security consumer and investor protection and competition, which however could have consequences for financial stability if they are not properly addressed. It therefore stresses the importance of addressing these issues as part of a comprehensive effective supervisory, regulatory and oversight framework.

The recommendations complement and are intended to inform any potential updates to international sectoral standards and principles. Authorities should rely on sectoral standards and principles, wherever GSC arrangements perform the same economic function and pose the same risks as existing regulated activities covered by these standards. The recommendations acknowledge the important role of the standard-setting bodies in reviewing, and where appropriate adjusting their standards to take into account the novel features of GSCs in order to further promote international cooperation and reduce the risk of arbitrage or regulatory underlaps. The report provides a guide for regulatory authorities of relevant international standards and potential tools to address vulnerabilities arising from GSC activities.

GSC arrangements are expected to adhere to all applicable regulatory standards and address risks to financial stability before commencing operation, and to adapt to new regulatory requirements as necessary. Authorities agree on the need to apply supervisory and oversight capabilities and practices under the “same business, same risk, same rules” principle. In some jurisdictions, some GSC functions may not fit within existing regulatory and supervisory frameworks, such that existing approaches might need clarification, adjustment, or new regulation.

The performance of some functions of a GSC arrangement may have important impacts across borders. It is therefore important for authorities to take a holistic approach to regulation, supervision and oversight, and to engage in close international cooperation and information sharing. Relevant authorities should, where necessary, clarify regulatory powers and address potential gaps in their domestic frameworks to adequately address risks posed by GSCs. This will help achieve common regulatory outcomes across jurisdictions and reduce opportunities for cross-sectoral and cross-border regulatory arbitrage, and enable appropriate regulation and supervision of GSC arrangements as a whole.

The establishment of effective regulatory, supervisory and oversight approaches for GSC arrangements will support the implementation of a key building block of the roadmap to enhance cross-border payments commissioned by the G20.[2]

To keep pace with the evolution of GSC arrangements and market developments, the FSB will, in close cooperation with relevant SSBs, review its recommendations on a regular basis in order to identify any potential gaps, and update them if needed to ensure that they remain relevant and continue to promote effective regulation, supervision and oversight of GSC arrangements across jurisdictions.

Table 3 shows the indicative timelines for this work, as set out in the roadmap.

[2] https://www.fsb.org/2020/10/enhancing-cross-border-payments-stage-3-roadmap/

FSB High-Level recommendations to address the regulatory, supervisory and oversight challenges raised by GSCs arrangements

1. Authorities should have and utilise the necessary powers and tools, and adequate resources, to comprehensively regulate, supervise and oversee a GSC arrangement and its associated functions and activities, and enforce relevant laws and regulations effectively.[3]

2. Authorities should apply comprehensive regulatory, supervisory and oversight requirements and relevant international standards to GSC arrangements on a functional basis and proportionately to their risks.

3. Authorities should cooperate and coordinate with each other, both domestically and internationally, to foster efficient and effective communication and consultation in order to support each other in fulfilling their respective mandates and to ensure comprehensive regulation, supervision, and oversight of a GSC arrangement across borders and sectors.

4. Authorities should ensure that GSC arrangements have in place a comprehensive governance framework with a clear allocation of accountability for the functions and activities within the GSC arrangement.

5. Authorities should ensure that GSC arrangements have effective risk management frameworks in place especially with regard to reserve management, operational resilience, cyber security safeguards and AML/CFT measures, as well as 'fit and proper' requirements.

6. Authorities should ensure that GSC arrangements have in place robust systems for collecting, storing and safeguarding data.

7. Authorities should ensure that GSC arrangements have appropriate recovery and resolution plans.

8. Authorities should ensure that GSC arrangements provide users and relevant stakeholders with comprehensive and transparent information necessary to understand the functioning of the GSC arrangement, including with respect to its stabilisation mechanism.

9. Authorities should ensure that GSC arrangements provide legal clarity to users on the nature and enforceability of any redemption rights and the process for redemption, where applicable.

10. Authorities should ensure that GSC arrangements meet all applicable regulatory, supervisory and oversight requirements of a particular jurisdiction before commencing any operations in that jurisdiction, and adapt to new regulatory requirements as necessary.

[3] This report recognises that establishing powers and tools for authorities is the province of individual jurisdictions' governing legislatures and any change would require legislative support.

Glossary[4]

Algorithm-based stablecoins

A stablecoin that purports to maintain a stable value via protocols that provide for the increase or decrease of the supply of the stablecoins in response to changes in demand.

Asset-linked stablecoin

A stablecoin that purports to maintain a stable value by referencing physical or financial assets or other crypto-assets.

Crypto-asset

A type of private digital asset that depends primarily on cryptography and distributed ledger or similar technology.

Digital asset

A digital representation of value which can be used for payment or investment purposes. This does not include digital representations of fiat currencies.

Global stablecoin (GSC)

A stablecoin with a potential reach and adoption across multiple jurisdictions and the potential to achieve substantial volume.

Stablecoin

A crypto-asset that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets.

Stablecoin arrangement

An arrangement that combines a range of functions (and the related specific activities) to provide an instrument that purports to be used a means of payment and/or store of value. When discussing a stablecoin arrangement, reference is made to:

- **Activity**

  Typical activities in a stablecoin arrangement are: (i) establishing rules governing the stablecoin arrangement; (ii) issuing, creating and destroying stablecoins; (iii) managing reserve assets; (iv) providing custody/trust services for reserve assets; (v) operating the infrastructure; (vi) validating transactions; (vii) storing the private keys providing access to stablecoins (e.g., using a wallet); and (viii) exchanging, trading, reselling, and market making of stablecoins.

- **Function**

[4] The glossary is for the purposes of this document and does not replace other existing taxonomies.

Functions in a stablecoin arrangement are: (i) governing the arrangement; (ii) issuance, redemption and stabilisation of the value of coins; (iii) transfer of coins; and (iv) interaction with users for storing and exchanging coins.

- **Governance body**

  A body responsible for establishing and monitoring the rules governing the stablecoin arrangement which would cover, among other issues, the types of entities that could be involved in the arrangement, the protocol for validating transactions, and the manner in which the value of the stablecoin is "stabilised".

- **Provider of function/activity**

  An entity that provides a particular function or activity associated with that function in a stablecoin arrangement.

- **User**

  A person or entity that uses a stablecoin as a means of payment or store of value.

- **Validator node**

  An entity on a network which validates transactions. In the context of distributed ledger technology, a node will commit transaction blocks to the ledger once they are validated.

- **Wallet**

  An application or device for storing the private keys providing access to stablecoins. Hosted wallets are typically held by a third party provider, unhosted wallets by the user.

Introduction

So-called "stablecoins" are a type of crypto-asset or, more broadly, digital asset.[5] Stablecoins may be used for different purposes. Some stablecoin projects have the stated ambition to facilitate payments, especially cross-border retail payments, which have remained relatively slow and expensive. A stablecoin, particularly if linked to a fiat currency or a basket of currencies, may become a widely used store of value. The use of stablecoins can evolve over time, particularly so that a stablecoin initially intended to be used as means of payment could also be increasingly used as a store of value.

While so-called "global stablecoins"[6] have the potential to contribute to developing new global payment arrangements, they could present a host of challenges to the regulatory, supervisory, oversight and enforcement authorities. This is because such instruments may have the potential to pose systemic risks to the financial system and significant risks to the real economy, including through the substitution of domestic currencies. Risks may relate to (i) challenges for financial stability; (ii) consumer and investor protection; (iii) data privacy and protection; (iv) financial integrity, including compliance with rules governing anti-money laundering and countering the financing of terrorism and proliferation (AML/CFT); (v) tax evasion; (vi) fair competition and anti-trust policy; (vii) market integrity; (viii) sound and efficient governance; (ix) cyber security and other operational risks; (x) the safety, efficiency and integrity of financial market infrastructures (FMIs) (e.g. payment systems); and (xi) resolution and recovery considerations.[7]

No existing, operational stablecoins or other crypto-assets currently appear to have reached a scale that could pose financial stability risks. However, existing stablecoins or those at the development or testing stage could potentially scale quickly if such stablecoins were offered to and used by a large, existing customer base, though the factors and conditions that could drive such potential mass adoption may require further analysis.

Against this backdrop, the G20 mandated the FSB in June 2019 to examine regulatory issues raised by "global stablecoin" arrangements (GSCs) and to advise on multilateral responses as appropriate, taking into account the perspective of EMDEs. In February 2020, the G20 reiterated the importance of evaluating and appropriately addressing the risks of GSC arrangements before they commence operation and supported the FSB's efforts to develop regulatory recommendations with respect to these arrangements. In April 2020, the FSB issued a report with a proposed set of high-level recommendations for public consultation.[8] The report drew on analysis undertaken within the FSB of potential financial stability risks and on a comprehensive survey of regulatory, supervisory and oversight approaches to stablecoins amongst FSB members and non-FSB members represented on FSB Regional Consultative Groups (RCGs). In the following months, the FSB also carried out a series of virtual outreach meetings with representatives from regulated financial institutions, financial technology firms, legal experts and

---

5 This document refers to stablecoins as a category of crypto-assets rather than using the broader reference to digital assets. The reference to crypto-assets was chosen for consistency with the FSB's prior publications.

6 Please refer to Annex 5 for elements that could be used to determine whether a stablecoin qualifies as a "global" stablecoin.

7 For a high-level overview of the risks posed by stablecoins, see the October 2019 G7 Report, *Investigating the impact of global stablecoins*.

8 FSB (2020), *Addressing the regulatory, supervisory and oversight challenges raised by "global stablecoin" arrangements: Consultative document*, April

academia. This final report takes into account feedback from the public consultation and the outreach.

In line with the G20 mandate, this report:

1. describes GSCs and how they may differ from other crypto-assets and other stablecoins (Section 1);

2. identifies the potential risks raised by GSCs (Section 2);

3. considers existing regulatory, supervisory and oversight approaches to GSCs and identifies issues that regulators, supervisors and overseers should address (Section 3);

4. considers the specific challenges arising in a cross-border context, including the value for cross-border cooperation and coordination (Section 4); and

5. sets out high-level recommendations for regulatory supervisory and oversight responses to GSCs, including beneficial multilateral actions (Section 5).

The focus of this report is on regulatory, supervisory and oversight issues relating to privately-issued GSCs primarily used for retail purposes, as defined in Section 1, but it may be relevant for other types of stablecoin, including stablecoins used for wholesale market purposes and those that may pose risks to financial stability only in some countries or regions. This report may also be relevant for other crypto-assets that could pose risks similar to some of those posed by GSCs because of comparable international reach, scale and use.

In line with the mandate of the FSB, the report does not address the consumer and investor protection, cyber security, data privacy, competition, market integrity taxation as well as Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) issues related to GSCs. However, a comprehensive supervisory and regulatory framework for GSC arrangements needs to effectively address AML/CFT, data privacy, consumer and investor protection, competition and market integrity in addition to financial stability risks. The wider monetary policy, monetary sovereignty and currency substitution questions, the issue of public versus private provision of digital money and payment services and issues related to central bank digital currencies are also outside the scope of the report. The G20 asked the IMF to consider the macroeconomic implications including monetary sovereignty issues in IMF member countries, taking into account country characteristics, and the Financial Action Task Force (FATF) to consider AML/CFT issues.

The FSB has been working closely with the IMF, World Bank, FATF, the Basel Committee on Banking Supervision (BCBS), the Committee on Payments and Market Infrastructures (CPMI), and the International Organization of Securities Commissions (IOSCO) as well as the other SSBs and international organisations to ensure that the work underway is coordinated and mutually supportive. Effective regulatory, supervisory and oversight approaches for GSC arrangements will support ongoing work to enhance cross-border payments. The FSB has, in coordination with relevant international organisations and SSBs, developed a roadmap called

for by the G20 to enhance cross-border payments.[9] Authorities are exploring the potential role of new payment infrastructures and, as part of this, concur that appropriate risk management within GSCs, and sound legal underpinnings, as a basis for the use of stablecoins in multiple jurisdictions, constitute one important building block.

1. Characteristics of global stablecoins

The term *stablecoin* commonly refers to a crypto-asset that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets. In turn, the value of these assets typically determines or affects the market value of a stablecoin. A stablecoin may also employ algorithmic or other means to stabilise or impact its market value by, for example, automatically adjusting its supply in response to changes in demand.

There is no universally agreed definition of stablecoin. The term stablecoin does not denote a distinct legal or regulatory classification. Importantly, the use of the term "stablecoin" in this report is not intended to affirm or imply that its value is necessarily stable.[10] Rather, the term is used here because it is commonly employed by market participants and authorities.

The attribute *global* refers to a stablecoin with a potential reach and adoption across multiple jurisdictions and the potential to achieve substantial volume, thus posing financial stability risks, rather than a specific legal or regulatory concept.

This section describes three characteristics that may distinguish a GSC from other crypto-assets and other stablecoins, and the potential importance of such distinctions. The first two (the existence of a stabilisation mechanism and a specific combination of multiple functions and activities) distinguish stablecoins from other crypto-assets. The third, the potential reach and adoption across multiple jurisdictions, differentiates GSCs from other stablecoins.

1.1. Stabilisation mechanism

A stablecoin arrangement seeks to stabilise the value of the stablecoin through the use of some kind of stabilisation mechanism. Stablecoins can be categorised according to the different types of stabilisation mechanisms.[11] Stablecoin designs currently reflect two broad types of mechanisms: asset-linked and algorithmic, with some approaches being a hybrid of the two:

- Asset-linked stablecoins purport to link the stablecoins at issue to physical or financial assets (including crypto-assets), in order to maintain a stable value relative to its

---

9 FSB (2020), *Enhancing Cross-border Payments: Stage 3 roadmap*, *October*

10 In fact, alternative terms such as private asset-linked tokens may characterise more accurately the technical nature of such instruments.

11 See for example: Bullmann, D. / Klemm, J. / Pinna, A., *In search for stability in crypto-assets: Are stablecoins the solution?*, ECB Occasional Paper No. 230, August 2019, distinguishing between stablecoins that are backed by funds ('tokenised funds'), stablecoins that are backed by assets ('collateralised stablecoins') – either traditional asset classes that require a custodian for their safekeeping ('off-chain') or backed by (crypto-)assets – and algorithmic stablecoins that are "backed by users' expectations about the future purchasing power of their holdings, which does not need the custody of any underlying asset"; Moin/Gün Sirer/Sekniqi, *A Classification Framework for Stablecoin Designs*, 2019, classifying stablecoins by collateral (type and amount), mechanism, price information, and pegging.

reference asset(s). They can be further differentiated into currency-based, financial instrument-based, commodity-based and crypto asset-based stablecoins. The mechanism by which a stablecoin's value is maintained in relation to the referenced asset may vary and includes the use of creation and redemption structures, arbitrage, and direct rights to receive underlying reserve assets. Depending on the structure, stablecoin holders may or may not have a redemption right against the issuer or direct claim on the reserve assets. Reserve assets may or may not be available to be used in case of a redemption request and may or may not benefit from consumer and investor protection arrangements or other guaranty schemes. Additionally, there may not be any assets in reserve if the stablecoin merely references another asset as a peg.[12]

- Algorithm-based stablecoins attempt to maintain a stable value via protocols that provide for the increase or decrease of the supply of the stablecoins in response to changes in demand. While the amount to be increased or decreased may be based on an algorithm, the actual issuance or destruction may not be automatic.

1.2. Combination of multiple functions and activities

To be useable as a means of payment and/or store of value, a stablecoin arrangement typically provides three core functions: [13]

(i) issuance, redemption and stabilisation of the value of the coins;

(ii) transfer of coins;

(iii) interaction with coin users for storing and exchanging coins.

Considering these functions, stablecoins could share functional similarities with payment systems or financial services or products, such as deposit liabilities or securities (including collective investment schemes), and therefore be subject to the same risks. However, they may also pose new risks, depending on the design of the stablecoin arrangement.

Each of these functions involves a number of constituent activities. For instance, the issuance, redemption and stabilisation of the value of the coins typically involves creating and destroying coins, as well as managing the corresponding reserve assets and providing custody/trust services for those assets. The transfer of coins typically entails the operation of a suitable infrastructure and a mechanism for validating transactions. The interaction with users typically occurs through devices or applications that operate as "wallets", which store the private keys providing access to stablecoins, as well as applications that enable the exchange of coins against fiat currencies or other crypto-assets. Considering this range of activities performed, a

---

12 For example, in some cases, maintenance of the stablecoin's value involves the use of reserve assets in addition to referencing another asset as a peg; in some other cases, the stablecoin may merely reference another asset as a peg without reserve assets. Generally, the value of a stablecoin could be more stable if it is pegged to a widely accepted stable reference asset and when the underlying reserve asset is highly correlated with the referenced asset (e.g. when the reserve asset is held in cash in the same currency as the reference asset).

13 G7 Working Group on Stablecoins, *Investigating the impact of global stablecoins*, October 2019.

stablecoin arrangement is generally understood as an arrangement comprised of different, interrelated functions and activities that can be provided by one or several entities.

The operating model employed may differ considerably across stablecoin arrangements (see Annex 1 for examples). The core system can be a book of records that registers ownership of coins and changes therein. It can be built as a shared ledger that operates in a decentralised way, for example by using distributed ledger technology (DLT) and that allows for transactions to be processed without a trusted third party.

Depending on the design and operating model, one or more entities may perform the activities, or design protocols or codes to perform them. Moreover, other variants and ways to perform the activities are emerging. In particular, technological innovation, such as developments in DLT, may enable the increased use of decentralised processes. Table 1 summarises, in a stylised manner, how the core functions of a stablecoin arrangement relate to activities and operational design elements.

Table 1: Functions and activities in a stablecoin arrangement

Functions	Activities	Operational design elements
Governance of the arrangement	Establishing rules governing the stablecoin arrangement	The rules covering, among other issues, the types of entities that could be involved in the arrangement, the protocol for validating transactions, the mechanism for stabilising the value of the stablecoin, and the arrangements for the management and ownership of the reserve assets. Generally, a governance body is essential to a stablecoin arrangement and also may have a role in promoting adherence to common rules across the stablecoin arrangement.
Issuance, redemption and stabilisation of value of coins	Issuing, creating and destroying stablecoins	The mechanism through which stablecoins may be issued or created, and subsequently destroyed by one or more entities or software protocols designed by these entities.
	Managing reserve assets	The activity of managing the assets that are "backing" the value of a stablecoin, where a stablecoin fully or partially maintains its value or confidence in its value based on real or financial assets or other crypto-assets. This may involve buying and selling assets based on an investment policy. The activity may also be undertaken by using software protocols that adjust the composition of the reserve through smart contracts and algorithmic decision-making.
	Providing custody/trust services for reserve assets	The activity of holding the assets that are "backing" the value of a stablecoin. The entity or entities issuing the stablecoin or other entities may hold the reserve assets.
Transfer of coins	Operating the infrastructure	A DLT protocol determining roles in and access to the system. Access may be permissioned (access, including the ability to hold and transfer stablecoins, is controlled with defined access conditions) or permissionless (anyone can access and transfer the stablecoins peer-to-peer, directly to other wallets).
	Validating transactions	Mechanism by which a transaction is authorised and validated by validator nodes.

Interaction with users	Storing the private keys providing access to stablecoins (wallet)	Cryptographic wallets storing private and public keys which are used to digitally sign transaction instructions performed by the stablecoin arrangement. Wallets can be custodial (hosted), where a third party operates the wallet and holds the private keys on behalf of the users, or non-custodial (unhosted), where the users hold the private keys directly. Multiple different parties can develop wallets, based on a set of specifications provided by the stablecoin arrangement.
	Exchanging, trading, reselling, and market making of stablecoins	The activity of purchasing/exchanging a stablecoin with fiat currencies, or a stablecoin with other stablecoins or crypto-assets.

1.3. Potential reach and adoption across multiple jurisdictions

As with many financial services that utilise the internet, the technological infrastructure underlying stablecoin arrangements is not limited in its geographic scope. If a stablecoin arrangement combines such infrastructure with features that may be attractive to a broad range of users across multiple jurisdictions, its user base may rapidly grow, i.e. it may become a GSC.

The potential reach and adoption of stablecoins across multiple jurisdictions and the potential to achieve substantial volume differentiates a GSC from other stablecoins. A framework to identify a GSC arrangement could seek to measure the global systemic importance of the arrangement. The criteria to be considered in determining whether a stablecoin is a GSC need to take into account the extent of the stablecoin's potential use as a means of payment or store of value in multiple jurisdictions. The likelihood that a stablecoin becomes a GSC also depends on a range of factors, including competition dynamics, which in turn would reflect network effects, access to data, the openness of the GSC arrangement or its integration with other digital services or platforms.

Annex 5 sets out elements that could be used by authorities to determine whether a stablecoin has the potential to expand reach or be adopted across multiple jurisdictions and has the potential to achieve substantial volume.

Individual jurisdictions on their own may not be able to monitor stablecoin adoption and materiality of risks in a comprehensive manner. For example, a stablecoin that may not pose systemic risk in any one jurisdiction may nonetheless pose such risk globally if it has a presence across multiple jurisdictions and therefore has linkages to the global financial system. It is therefore important for relevant authorities in jurisdictions, where stablecoin arrangement functions and activities occur, to coordinate and cooperate closely when monitoring stablecoin use across borders.

2. Risks and vulnerabilities raised by global stablecoins

Financial stability risks from existing stablecoins are presently limited. This is largely due to the relatively small scale of these arrangements and their current limited use cases, mainly around facilitating trading in other crypto assets. However, the use of stablecoins as a means of payment or a store of value might significantly increase in the future, possibly on a large scale and across

multiple jurisdictions. In addition, the different activities within a stablecoin arrangement, in particular those related to managing the reserve assets, may considerably increase linkages to the existing financial system. Such developments could change the current assessment.

This section describes the channels through which GSCs may adversely affect financial stability and discusses how the specific activities performed within a GSC arrangement, and their interaction, may affect these channels. Linking activity-specific risks to the financial stability outcomes provides the basis for considering which functions and activities of a GSC arrangement may warrant particular attention by regulators, supervisors and oversight authorities.

2.1. Potential risks to financial stability from a GSC

GSCs could pose financial stability risks through certain key channels.

If a GSC were widely-used as a common store of value, even a moderate variation in its value might cause significant fluctuations in users' wealth. Such wealth effects may be sizeable enough to affect spending decisions and economic activity. Wealth effects may be particularly pronounced in EMDEs where the likelihood of GSCs becoming a mainstream store of value may be higher than in advanced economies (AE).

If widely used for payments, any operational disruption in the GSC arrangement might have significant impacts on economic activity and financial system functioning. If users relied upon a stablecoin to make regular payments, significant operational disruptions could quickly affect real economic activity, e.g. by blocking remittances and other payments. Large-scale flows of funds into or out of the GSC could test the ability of the supporting infrastructure to handle high transaction volumes and the financing conditions of the wider financial system.

Exposures of financial institutions might increase in scale and change in nature – particularly if financial institutions played multiple roles within a GSC arrangement (for example as resellers, wallet providers, managers or custodians/trustees of reserve assets). This may be a source of market, credit and operational risks to those institutions and, eventually, may end up having systemic implications.

The large-scale use of GSCs might magnify confidence effects. A greater sensitivity to confidence effects could also reflect the extent of the use of a GSC as a store of value and/or means of payment. Moreover, closer linkages to financial institutions might also expose a GSC to adverse confidence effects, such as when a financial institution that acts as reseller/market-maker of the GSC arrangement comes under financial distress. The reverse may also be true – the potential failure of a GSC might expose the financial institutions involved in the GSC arrangement to adverse confidence effects.

These channels may also interact. For example, disruption to payments may cause further decline in confidence, which in turn could prompt further redemptions and decline in the GSC's value, compounding wealth effects. The significance of these channels and their impact on financial stability depend on how widely and for what purpose a GSC is used, and whether linkages to the financial system increase. For example, if a GSC were adopted as a widespread means of payment, but not as a store of value, its potential implications for financial stability may

be narrower. If, however, a GSC also became adopted as a significant store of value by some of its users, other channels – including those pertaining to confidence effects, interlinkages to financial institutions and macroeconomic stability – may become more prominent.

Macrofinancial risks may arise particularly if, over time, households and businesses in some economies (e.g. EMDEs) come to hold substantial portions of their wealth in GSCs, rather than in local currencies. During periods of stress, households in some countries might come to regard GSCs as a safe store of value over existing fiat currencies and exacerbate destabilising capital flows. Volatile capital flows can have a destabilising effect on exchange rates and on domestic bank funding and intermediation.

2.2. Vulnerabilities arising from the functions and activities of a GSC arrangement

While the significance of the individual channels discussed above depends on what a GSC is used for and how widely it is used, the vulnerability of the GSC itself to shocks depends on how the functions and activities of the GSC arrangement are designed and performed. A scenario analysis conducted by the FSB identifies three main types of vulnerabilities. This scenario analysis focuses on asset-linked GSCs that have reserve assets and where the user has the ability to redeem the GSCs:

Market, liquidity and credit risks

The first type of vulnerability relates to traditional financial risks – market, liquidity and credit risk – in a GSC arrangement. Of key importance in this regard is the choice and management of the GSC reserve assets, particularly the degree to which they could be liquidated at or close to prevailing market prices. Otherwise, large-scale GSC redemptions might result in "fire sales" of reserve assets that could reduce the "stable" value of the GSC relative to the reserve assets absent secondary guarantees. Such loss of value could impair user confidence in the resilience of the GSC arrangement as a payment mechanism, the financial institutions and the markets in which such assets were invested. Large-scale redemptions of GSCs might lead to large-scale sales of other assets and stress transmitted to wider financial markets. Also, significant changes in the composition of the reserve assets, in the absence of large-scale redemption of GSCs, might trigger spillover effects to the wider financial system. The ability of GSC arrangements to sell reserve assets in large volume at (or close to) prevailing market prices would depend on the duration, quality, liquidity and concentration of the GSC's reserve assets. The degree of transparency as to the nature, sufficiency and liquidity of these reserve assets might also affect confidence in the GSC. Other design features of a GSC arrangement may add to financial stability risks. For instance, the withdrawal of liquidity provision by resellers/market makers might cause a sharp reduction in the liquidity of the GSC and dislocation in its price, which might in turn undermine user confidence and prompt further redemption. Moreover, users' loss of confidence could be more pronounced for GSCs which are not fully backed by reserve assets.

Operational risk (including cyber risks) and risk of loss of data

A second type of vulnerability concerns potential fragilities in the governance, operation and design of the GSC arrangement's infrastructure, including its ledger and the manner of validating

users' ownership and transfer of coins. This vulnerability could crystallise for example due to an operational incident at a custodian or a compromised ledger resulting from a design defect, a cyber incident, or a failure of validator nodes. A lack of network capacity to validate – and subsequent delays in processing – large volumes of transactions might amplify users' loss of confidence, and trigger further redemption requests. In the event of a disruption in the GSC arrangement, ambiguity about rights and protection afforded to users could amplify confidence effects. In particular, if users do not have redemption rights or a direct claim on the underlying assets, confidence could be undermined. The degree of vulnerability would be impacted by the effectiveness of the GSC arrangement's governance and controls. The clarity of the roles and responsibilities of the GSC arrangement's governance body – including in respect of setting and enforcing the rules on establishing the GSC's value and on the functioning of the infrastructure – could affect users' confidence.

Vulnerabilities arising from applications and components within the GSC arrangement

The third vulnerability relates to the applications and components on which users rely to store private keys and exchange coins. Such vulnerabilities could crystallise due to an operational incident at a wallet or exchange, for example. The scope of affected users might depend on the market share of the associated provider, and the degree to which it, for example, serves users in different jurisdictions.

The degree of vulnerability of a GSC to shocks also depends on the operational resilience arrangements for wallets and exchanges, including stand-in and fall-back arrangements that ensure continuity of service to users, and on the continued liquidity of the secondary market for coins.

Table 2 summarises, in a stylised way, the above types of vulnerabilities, their main determinants, and the functions and activities of a GSC arrangement that are particularly relevant in this regard.

Table 2: Examples of vulnerabilities and related functions and activities in a GSC arrangement (stylised presentation)

Type of vulnerability	Main determinants	Functions and activities primarily concerned
Financial exposures in the GSC arrangement, giving rise to market, liquidity and credit risks.	• Choice, composition and management of the GSC reserve assets • Robustness of liquidity provision by GSC resellers/market makers • Ability of actors in the GSC arrangement to employ leverage	• Governing the GSC arrangement • Issuing, creating and destroying GSCs • Managing reserve assets • Exchanging, trading, reselling and market making of stablecoins
Weaknesses in the GSC infrastructure, giving rise to operational risk (including cyber risks) and risk of loss of data.	• Reliability and resilience of the GSC's ledger and validation mechanism, including validator nodes • Capacity of network to validate and process large volumes of transactions • Reliability of custodians/trustees	• Governing the GSC arrangement • Operating the infrastructure • Validating transactions • Providing custody/trust services for reserve assets •
Weaknesses in those parts of the GSC arrangement on which users rely to store, exchange and trade GSCs, including operational or fraud risk	• Effectiveness of governance in preventing fraud • Operational resilience • Clarity and robustness of claims that users have[14] • Robustness of liquidity provision by GSC resellers/market-makers	• Governing the GSC arrangement • Storing of private keys providing access to GSCs • Exchanging, trading, reselling, and market making of GSCs

The resilience of a GSC arrangement depends on the proper functioning of a range of different activities and processes. Weaknesses in the interlinkages that exist between the various functions and activities in a GSC arrangement may add to vulnerabilities. For instance, a design failure in the validation process used for coin transfers could undermine confidence in the payment mechanism, but also in the performance of GSCs as a store of value and eventually of the GSC arrangement as a whole. Additionally, some of the functions of a given GSC arrangement may be shared with other existing GSCs or crypto-assets (e.g. the infrastructures used to transfer coins or interact with users), resulting in vulnerabilities potentially triggering spillover effects to or from other GSCs or crypto-assets.

[14] Including whether or not users have a right to redeem at par in fiat.

3. Existing regulatory, supervisory and oversight approaches and challenges

3.1. Findings from the FSB stocktake

To take stock of existing regulatory, supervisory, and oversight approaches, the FSB surveyed FSB and RCG member jurisdictions. The survey included questions on current approaches with respect to the regulatory classification of stablecoins and stablecoin arrangements and activities, as well as potential regulatory gaps. See Annex 3 for a summary of the survey findings.

Coverage under existing regulatory, supervisory and oversight approaches

The survey findings highlight that most jurisdictions do not currently have regulatory regimes specific to crypto-assets in general or stablecoins in particular. The findings also show that, in most jurisdictions, existing regulatory, supervisory and oversight approaches, while not specific to crypto-assets or stablecoins, apply in whole or part and address some of the risks associated with stablecoins or with entities that are part of the stablecoin arrangement. The most common approach is to identify the activity performed by a stablecoin arrangement and the participants involved, and apply the relevant existing regulation to that activity or entity according to the "*same business, same risks, same rules*" principle.

Several authorities reported that they planned to clarify how existing regimes apply to stablecoins and their providers, and that some adaptation of their regulation may be necessary, while others indicated that their current frameworks apply to stablecoin arrangements. Some jurisdictions have already provided guidance on how to apply existing regulation to crypto-assets and/or stablecoins. This guidance has typically sought to help stablecoin providers understand which regulatory requirements apply and how to ensure compliance. Others are currently developing new legislation or regulation to address the risks posed by crypto-assets, including stablecoins. Some jurisdictions have chosen to issue warnings to the public, highlighting the risks of these investments and/or that some of these activities are not licensed or regulated. In a few cases, jurisdictions have chosen to prohibit crypto-assets (including stablecoins).

Functions and activities within GSC arrangements are often, at least partly, covered by multiple relevant regulations in AEs, while some are not covered by any regulations in EMDEs. In general, the functions and activities that are most frequently covered include the issuance and redemption of stablecoins; managing reserve assets; providing custody/trust services for stablecoin reserve assets; exchanging and trading stablecoins (including reselling to retail users) and storing the private keys providing access to stablecoins (wallets). The survey indicates that jurisdictions were less likely to regulate the governance of the stablecoin arrangement, the operation of the infrastructure of a stablecoin arrangement and the validation of transactions.

The type of regulatory coverage of stablecoin activities varies. For example, in many jurisdictions AML/CFT regulations seem to apply to stablecoin activities generally. In a few jurisdictions, other types of financial regulation, such as market integrity, investor and consumer protection regulations, also apply to stablecoin activities like issuance, exchanging and trading of stablecoins. See the table in Annex 2 on potential vulnerabilities arising from stablecoin activities

and the regulatory authorities, relevant international standards and potential tools to address such vulnerabilities.

Potential regulatory classification

There is currently no common and consistent regulatory classification of the nature, functionality, structure and rights associated with stablecoins across jurisdictions. In different jurisdictions, a stablecoin could fall within one or multiple regulatory classifications, depending on the design of the stablecoin and how it is offered and sold. In AE jurisdictions, stablecoins were most frequently classified as e-money and a collective investment scheme (CIS), followed by deposits, a security other than CIS and derivatives. For EMDEs, the most common classifications were e-money and payment instrument.

Most respondents note that stablecoins or activities of stablecoin arrangements could be classified under more than one regulatory category, and that the classification could change as the nature and use of a stablecoin evolves. Which existing regulatory regime applies typically depends on the specific design features and characteristics of a stablecoin or of the entities that are part of the stablecoin arrangement. The application of existing regulatory regimes is subject to a case-by-case assessment. For instance, whether a "stablecoin" qualifies as e-money may depend on the nature of the claim of a stablecoin holder against the stablecoin issuer or its assets. Stablecoins that do provide a claim may also fall under the definition of a collective investment scheme or deposit. A change in the features of the stablecoin or the activities of the stablecoin arrangement over time may lead to a change in the applicable regulatory and supervisory regime.

Potential gaps in existing approaches

The FSB stocktake did not reveal regulatory or supervisory gaps that are common to all jurisdictions. Several authorities noted that their existing frameworks provide an adequate coverage of stablecoin arrangements and that they did not identify any gaps in their regulatory, supervisory and oversight regimes. Some authorities identified potential gaps in existing regimes that they indicated should be addressed. One source of gaps may be an unanticipated *bundling* of attributes that existing regulations, in particular those designed to be applied by sector, may not fully capture. For instance, legal frameworks in some jurisdictions may not allow stablecoins to fall under multiple regulatory classifications, so certain activities may not be captured at present (e.g., if a GSC falls exclusively under securities regulation in a jurisdiction, activities related to the transfer of coins may not be covered). Another source of gaps may be the *unbundling* of activities in a stablecoin arrangement. As a consequence, some of the activities in a GSC arrangement may fall outside of traditional regulatory boundaries.

Based on the survey findings, potential gaps in existing frameworks at domestic level may include:

(i) potentially incomplete or non-existent implementation of the revised FATF standards on virtual assets and lack of inclusion of all activities of a GSC arrangement (e.g. peer-to-peer transfers of stablecoins may not be addressed) under the revised FATF standards;

(ii) inability to effectively supervise and oversee a GSC arrangement if the legal classification of a stablecoin falls outside an existing regulatory framework (e.g. e-money or a security);

(iii) incomplete regulatory coverage of the functions and activities under a GSC arrangement that are economically similar to those that would fall under the remit of existing regulation, but as a result of their particular design, are not within the perimeter of existing regulation (e.g. exchange and trading, wallet services used for storing keys, unhosted wallets) with a range of risks not or not fully addressed (e.g. market integrity, consumer or investor protection, cyber security, data privacy);

(iv) insufficient risk mitigation tools within a regulatory framework applicable to a given activity (e.g. no specific capital or liquidity requirements for issuing stablecoins or managing the reserve assets, incomplete measures addressing cyber security, and operational risks of the underlying technology used for operating the infrastructure, validating transactions or storing keys in wallets, absence of safeguards for users holding unhosted wallets; lack of legal certainty regarding the consumer or investor protection safeguards, the recovery of funds and legal remedies);

(v) lack of adequate competition policies that grant rights and safeguards to consumers and businesses to join a GSC arrangement (e.g., by requiring interoperability protocols), and facilitate appropriate competition among market participants.

3.2. International standards that could apply to GSC arrangements

Several international financial standards could potentially be applicable to the activities of a stablecoin arrangement, including standards for prudential regulation as well as AML/CFT regulation depending on the specific design of the stablecoin arrangement and regulatory regime of each jurisdiction. Standard-setting bodies – BCBS, FATF, CPMI, and IOSCO – are undertaking work to review whether and how existing international standards can apply to stablecoin arrangements.

Basel Committee on Banking Supervision (BCBS)

Banks could be subject to a range of direct and indirect exposure channels in a GSC arrangement, including as an issuer, investor, lender, custodian/wallet provider and market maker of stablecoins. Such exposures would in principle be subject to prudential capital and liquidity requirements.

However, the current Basel framework does not specify the prudential treatment for banks' exposures to crypto-assets at large or crypto-assets that make use of stabilisation tools. The BCBS is considering the appropriateness of a global prudential standard and other approaches. The BCBS issued a discussion paper that outlines a set of general principles and considerations to guide the design of a prudential treatment of banks' exposures to crypto-assets, including an illustrative example of potential capital and liquidity requirements for exposures to high-risk

crypto-assets.[15] Building on the feedback to the discussion paper, the BCBS is currently taking a broad and holistic approach to proceed with work on the prudential treatment of crypto-assets, and will consult on any specific measures.

Banks having a role in a GSC arrangement could be subject to cyber, fraud, and other operational risks as well as legal, third-party and implementation risks. The BCBS *Principles for the Sound Management of Operational Risk* should help address those risks by calling a strong control environment, appropriate internal controls and business resilience and continuity plans.[16]

Moreover, as noted in the March 2019 BCBS statement on crypto-assets, one of the first steps in analysing the impact of crypto-assets on banking institutions is to assess the permissibility of a banking institution to engage in such activity.[17]

Financial Action Task Force (FATF)

The FATF, as the global standard setter for AML/CFT, set out in June 2019 how the FATF standards should apply to virtual asset activities and Virtual Asset Service Providers (VASPs).[18,19] It set out recommendations that require countries to assess and mitigate the money laundering and terrorist financing risks associated with virtual asset activities and VASPs; license or register such providers; subject them to supervision or monitoring; and require that they implement all of the AML/CFT preventive measures under the FATF recommendations just like other financial institutions, including customer due diligence, record-keeping, suspicious transaction reporting, and screening all transactions for compliance with sanctions.

In October 2019, the FATF clarified that both global "stablecoins" and their service providers would be subject to the FATF standards either as virtual assets and VASPs or as traditional financial assets and their service providers, and that stablecoins should "never be outside of the scope of anti-money laundering controls".[20] Accordingly, the FATF has made clear that countries should effectively implement the FATF standards as part of their domestic regulatory and supervisory regimes for virtual assets, including stablecoins and VASPs.

In July 2020, the FATF further expanded on these findings in its report to the G20 on so-called stablecoins.[21] The FATF has found that so-called stablecoins share many of the same potential money-laundering/terrorist-financing (ML/TF) risks as some virtual assets, in virtue of their potential for anonymity, global reach and layering of illicit funds. Depending on how they are designed, they may allow anonymous peer-to-peer transactions via unhosted wallets. These features present ML/TF vulnerabilities, which are heightened if there is mass-adoption. When

---

15 BCBS (2019), *Designing a prudential treatment for crypto-assets*, December

16 BCBS (2011), *Principles for the sound management of operational risk*, June

17 BCBS (2019), *Statement on crypto-assets*, March

18 On 21 June 2019, the FATF issued an Interpretive Note to Recommendation 15 on New Technologies (INR. 15) that clarifies the FATF's previous amendments to the international Standards relating to virtual assets and describes how countries and obliged entities must comply with the relevant FATF Recommendations to prevent the misuse of virtual assets for money laundering and terrorist financing and the financing of proliferation.

19 The terms "virtual asset" and "virtual asset service provider" are used by FATF according to the definitions available at http://www.fatf-gafi.org/glossary/u-z/.

20 FATF (2019), *Money laundering risks from "stablecoins" and other emerging assets*, October

21 FATF (2020), *FATF Report to G20 on So-called Stablecoins*, June

reviewing current and potential projects, so-called stablecoins appear better placed to achieve mass-adoption than many virtual assets, if they do in fact remain stable in value, are easier to use and are under sponsorship of large firms that seek to integrate them into mass telecommunication platforms.

In line with its previous statements, the FATF found that the revised FATF Standards clearly apply to so-called stablecoins. Under the revised FATF Standards, a so-called stablecoin will either be considered to be a virtual asset or a traditional financial asset depending on its exact nature. A range of the entities involved in any so-called stablecoin arrangement will have AML/CFT obligations under the revised FATF Standards. Which entities will have AML/CFT obligations will depend on the design of the so-called stablecoin, particularly the extent to which the functions of the so-called stablecoin are centralised or decentralised, and what activities the entity undertakes.

Committee on Payments and Market Infrastructures (CPMI) and International Organization of Securities Commissions (IOSCO)

The CPMI and IOSCO have carried out a preliminary analysis on the application of the Principles for Financial Market Infrastructures (PFMI) stablecoin arrangements and their activities. The PFMI include 24 high-level principles applicable to systemically important FMIs. Principles include the existence of a well-founded legal basis, clear governance promoting safe and efficiency and supporting stability of the broader financial system, risks management, and operational resilience. Responsibility E of the PFMI provides the framework for cooperation among central banks, market regulators, and other authorities for promoting the safety and efficiency of systemically important FMIs.

In this preliminary analysis, the CPMI-IOSCO established that the PFMI apply to systemically important stablecoin arrangements that perform systemically important payment system functions[22] or other financial market infrastructure (FMI) functions that are systemically important. Further to their preliminary analysis, CPMI-IOSCO intend to determine which factors authorities may consider for assessing whether a stablecoin arrangement is systemically important. To the extent that systemically important stablecoin arrangements perform additional functions not covered by the PFMI, they will be subject to relevant standards for those functions in addition to the PFMI.

In their preliminary analysis, the CPMI-IOSCO considered that, while it may be challenging for systemically important stablecoin arrangements, in particular for those that are partly or highly decentralised, to comply with the standards of the PFMI, systemically important stablecoin arrangements need to adapt to comply with them. In this regard, CPMI-IOSCO intend to further identify the main issues for systemically important stablecoin arrangements to comply with the PFMI. The CPMI and IOSCO are considering the need for some clarification or interpretation to help explain how systemically important stablecoin arrangements may comply with the PFMI, but such clarification or interpretation would not change the underlying principles that apply to

---

22 The PFMI note that a payment system is "…a set of instruments, procedures, and rules for the transfer of funds between or among participants; the system includes the participants and the entity operating the arrangement." The instruments could potentially be the tokens issued by a stablecoin issuer, the procedures could be the payments made between token holders (or to participating retailers), and the rules would likely be set out by the stablecoin issuer (and codified on the blockchain).

systemically important stablecoin arrangements. The CPMI and IOSCO also intend to analyse whether stablecoin arrangements present additional risks not appropriately addressed by the PFMIs. The CPMI and IOSCO are carrying out further work building on the preliminary analysis before a definitive statement on applicability of each of the individual PFMI principles to stablecoin arrangements can be made.

International Organization of Securities Commissions (IOSCO)

IOSCO is reviewing the applicability of IOSCO standards and principles to GSC initiatives and published a report on 23 March 2020.[23] The report assesses the implications that global stablecoin proposals could have for securities market regulators. It concludes that GSCs may, depending on their structure, present features that are typical of regulated securities or other regulated financial instruments or services. It then engages in a lifecycle analysis of a hypothetical stablecoin used for domestic and cross-border payments. The hypothetical stablecoin uses a reserve fund and intermediaries to try to achieve a stable price vis-a-vis a basket of low volatility currencies.

The report concludes that several principles and standards could apply to the hypothetical stablecoin offering. These include (i) IOSCO's *Policy Recommendations for Money Market Funds* (2012); (ii) *Issues, Risks and Regulatory Considerations for Crypto-asset Trading Platforms* (2020); (iii) the *Principles for the Regulation of Exchange Traded Funds* (2013); and (iv) the IOSCO work on market fragmentation including the *Cross Border Regulation Task Force Report* (2015) and the work of the Follow-Up Group on Cross-Border Regulation to address potential regulatory arbitrage as well as IOSCO work on Cyber Resilience and Client Assets. These findings may equally apply to stablecoin arrangements other than the hypothetical stablecoin offering, subject to a facts and circumstances assessment of the individual proposal at hand. The report also sets out considerations of broader issues of relevance to securities market regulators and contains the CPMI-IOSCO's preliminary analysis of the applicability of the PFMI to GSCs. A more detailed summary of the report's findings along with the CPMI-IOSCO analysis are both set out in Annex 4.

Future IOSCO work will expand the functional analysis in the published report to look at other structures of GSCs offerings and how they might interact with the perimeter of securities markets regulation, as well as supplementing the analysis with any relevant additional information, if and when GSC proposals come to market.

The table in Annex 2 maps the activities in a stablecoin arrangement to the associated vulnerabilities and highlights appropriate regulatory, supervisory and oversight tools as well as international standards that could be relevant.

---

[23] IOSCO (2020), *Global Stablecoin Initiatives*, March

4. Cross-border regulation, supervision and oversight

4.1. Cross-border challenges

Cross-border challenges are inherent to GSC arrangements. The ease with which stablecoin arrangements and entities providing various functions and activities within the arrangements can operate across borders and reorganise or relocate their activities challenges the effectiveness of regulation, supervision, oversight and enforcement at jurisdictional levels. A stablecoin issued in one jurisdiction may be easily accessible online to users in another jurisdiction. Operational and cyber security risks related to the technology and infrastructure used in a stablecoin arrangement may affect the operation of GSC arrangements across multiple jurisdictions. The governance arrangements underpinning the operations and infrastructure should therefore be of interest to regulators in all jurisdictions where the stablecoin arrangement has activities.

Jurisdictions generally seek to apply their rules and regulations to activities taking place in their jurisdiction, including in situations where stablecoins are offered to local users from abroad. However, the effective application and enforcement of a jurisdiction's rules may be difficult as users access services on the Internet and authorities cannot easily locate the provider of the services. It may be further complicated by the fact that different regulatory classifications of stablecoins and hence different regulatory, supervisory and oversight approaches are adopted across jurisdictions. Different jurisdictional approaches could give rise to regulatory arbitrage and fragmentation.

These cross-border challenges may be particularly significant for EMDEs. The use of stablecoins as a means of payment and/or store of value may be more widespread in EMDEs, for example due to the substitution of local currency, than in AEs with developed financial systems. At the same time, the activities of a stablecoin arrangement may typically be performed by entities that are located outside EMDE jurisdictions. Taken together, EMDEs may face a combination of relatively high systemic relevance of a stablecoin and constraints in regulating and supervising the arrangement.

4.2. Issues for cross-border cooperation and coordination

Addressing the cross-border challenges requires effective cross-border cooperation, coordination and information sharing amongst the relevant authorities. Establishing effective cooperation arrangements requires an understanding of how a specific stablecoin arrangement is organised and operates and how the individual activities are interconnected and generate contagion channels. Authorities also need to understand the scope of application of their respective regulatory frameworks and how they interact. They then need to determine the level and nature of cross-border cooperation needed to avoid any regulatory underlap or gaps and ensure an effective holistic oversight. The level and nature of cross-border cooperation needed may depend on:

- *Use and systemic importance* – what the GSC is used for and where users are located;
- *Governance* – where the decisions across the GSC arrangement are made and policies set and enforced;

- *Issuance and redemption of coins, reserve management* - where the issuance and redemption of coins and the management of reserve assets occurs; the jurisdiction whose currency or assets (e.g. government bonds) are included in reserve assets;

- *Transfer mechanisms* – how transfer mechanisms are operated and how stablecoins are exchanged, traded and resold, for example, whether or not these are centralised processes operated by a designated entity or decentralised processes operated by multiple entities; where data and records are located (whether transaction records and other data are centralised or decentralised);

- *User-facing elements* – where wallet and platform providers are located, whether they operate cross-border, and whether there is vertical integration between operators of the functions and activities of the GSC arrangement.

Challenges could arise around the ability to supervise and oversee stablecoin arrangements holistically, rather than in a piecemeal fashion based on individual functions and activities. There are different approaches for cross-border supervision and oversight: for prudentially regulated financial institutions, cross-border cooperation builds on principles for comprehensive consolidated supervision.[24] The "home supervisor', that is the supervisor in the jurisdiction where the head office or parent entity of a financial institution is headquartered, is responsible for the supervision of the group of related institutions on a consolidated basis. In this case, effective consolidated supervision requires the home supervisor to cooperate with supervisors in jurisdictions where subsidiaries or branches are located ("host supervisors"). In the case of FMIs, a FMI's competent authority ("lead overseer" which could be compared to the "home supervisor") is designated as the coordinator of the cooperation arrangement. A wide set of relevant authorities is identified and engaged in the cooperation, taking into account the features and the services that the FMI provides on a cross-border basis.

In both cases, the objective of the "home supervisor" and of the "lead overseer" is to gain sufficient knowledge of the operations of the financial group or FMI, both domestic and foreign, as a whole so as to monitor and assess risks and vulnerabilities faced by the group or FMI. Host supervisors may have different interests in relation to the supervision of the group or FMI as a whole, depending on whether the group or FMI has material risk exposures in the host jurisdiction and whether it poses a systemic risk to the host jurisdiction.

A stablecoin arrangement could be different from a financial group or FMI. Unlike a financial group, a stablecoin arrangement may be a network of unrelated entities conducting different functions and activities usually from various jurisdictions that may only be held together by common policies, standards and agreements about their respective roles. At the same time, a stablecoin arrangement may involve functions that extend beyond those of a traditional financial group or FMI. Each part, whether entity, policy, process, or technology, of a stablecoin arrangement can affect the other parts. Depending on the specific features of the stablecoin arrangement, there is a risk that a stablecoin arrangement is not subject to sufficiently robust

[24] See for example BCBS (1992), *Minimum standards for the supervision of international banking groups and their cross-border establishments*, July

governance and controls that are enforced through policies, standards, and contractual obligations over its entire network of functions, activities and participants.

Whereas the objectives of comprehensive consolidated supervision are relevant in the context of a GSC arrangement, the concepts of "home" and "host" cannot in certain cases be easily transposed to GSC arrangements that are operated through a loose network of entities and dispersed ownership and control structures. This is the case in particular if there is no entity responsible for the governance of the GSC arrangement or if the back-end core functions (governance, issuance of coins, stabilisation mechanism, or transfer mechanism) of the GSC arrangement are performed by different entities in different jurisdictions. There may also be different options for determining a "home jurisdiction".[25] Given these inherent limitations to the "home-host" concept, certain cross-border supervisory and oversight models existing outside the consolidated supervision context may be more relevant.

Existing cooperation mechanisms between sectoral authorities can help support cooperation and coordination, possibly with some adaptations (e.g. through Memorandums of Understanding (MoU)).

4.3. Role of existing standards on cooperation, coordination and information sharing

Despite the particularities of GSC arrangements, existing international standards and principles governing cooperation, coordination and information sharing amongst authorities should help inform cross-border cooperation for GSC arrangements. Given the multi-functional and multi-jurisdictional nature and "loose network structure" of GSC arrangements, new forms of cooperation may need to be established or adapted from existing approaches.

In addition to the overarching international standards referred to in Section 3.2 that could apply to GSC arrangements, existing international standards and principles that focus on cross-border cooperation, coordination and information sharing may also be adapted to apply to GSC arrangements. These include principles related to cooperation, which underscore the importance of collaboration and information-sharing, such as:

- *Responsibility E of the PFMI* which provides that "central banks, market regulators, and other relevant authorities should cooperate with each other, both domestically and internationally, as appropriate, in promoting the safety and efficiency of FMIs." Responsibility E, together with its Key Considerations, provides a strong basis for cooperation among authorities responsible for oversight at cross-border level. Where a stablecoin arrangement may have other features and provide services in addition to those of an FMI, Responsibility E also foresees that overseers identify and engage with potentially broader set of authorities. CPMI-IOSCO is currently considering whether

[25] For example, the FATF standards require licensing or registration of virtual asset service providers where they are incorporated and leave individual jurisdictions to decide whether it should also be required where the service provider has management, back office presence, or a substantial customer base.

additional considerations would be helpful to achieve appropriate cooperation among relevant authorities.

- *BCBS standards relating to cross-border supervisory cooperation*: Supervisors overseeing international banking groups involved in GSC arrangements would build on the Committee's principles related to supervisory cooperation, which underscore the importance of collaboration and information-sharing.[26] These include the Basel Concordat[27], the Core Principles for effective banking supervision, home-host information sharing arrangements and the Principles for effective supervisory colleges.

- *FATF standards*: The FATF standards on AML/CFT apply whether GSCs are classified as virtual assets or as other traditional financial assets. The FATF standards on virtual assets finalized in June 2019 require licensing or registration of virtual asset service providers in at least the jurisdiction where they are created if a legal person or where they are located, if a natural person. The standards also include optional further licensing and registration in jurisdictions where service providers offer products and/or services to customers in that jurisdiction or conduct their operations from that jurisdiction. The FATF standards further require various forms of cross-border cooperation among authorities, include mutual legal assistance and information sharing.

- *The IOSCO Principles[28] covering Cooperation in regulation* (Principles 13 to 15), *IOSCO's Multilateral MoU Concerning Consultation and Cooperation and the Exchange of Information[29], the Enhanced Multilateral MoU Concerning Consultation and Cooperation and the Exchange of Information[30], the IOSCO Principles regarding Cross-Border Supervisory Cooperation of May 2010* and the cross-border regulatory and supervisory cooperation aspects of the IOSCO 2015 Cross-Border Regulation Task Force Report as well as of the work of the Follow-Up Group to address potential regulatory arbitrage; and

- The cross-border regulatory and supervisory cooperation aspects of the *Joint Forum Principles for the Supervision of Financial Conglomerates* (2012).

In addition, bespoke oversight arrangements, such as the arrangement governing the international cooperative oversight of SWIFT[31] or of CLS[32], may provide a reference point for

---

26 See respectively, BCBS *Principles for the supervision of bank's foreign establishments* (1983), *Core Principles for Effective Banking Supervision* (2012), *Home-host information sharing for effective Basel II implementation* (2006), and *Principles for effective supervisory colleges* (2014).

27 BCBS (1983) *Principles for the supervision of bank's foreign establishments*, May

28 See *Objectives and Principles of Securities Regulation*, May 2017.

29 See https://www.iosco.org/about/?subsection=mmou.

30 See https://www.iosco.org/about/?subsection=emmou.

31 The National Bank of Belgium, as the lead overseer, conduct the oversight of SWIFT in cooperation with the other G10 central banks, i.e. Bank of Canada, Deutsche Bundesbank, European Central Bank, Banque de France, Banca d'Italia, Bank of Japan, De Nederlandsche Bank, Sveriges Riksbank, Swiss National Bank, Bank of England and the Federal Reserve System (USA), represented by the Federal Reserve Bank of New York and the Board of Governors of the Federal Reserve System. The relationship between the NBB and those other cooperating central banks has been laid downs in bilateral MoUs.

32 Similarly, a cooperative oversight arrangement is established for the oversight of CLS, which is conducted by the Federal Reserve System, which includes both the Board of Governors of the Federal Reserve System and the Federal Reserve Bank of

establishing cooperative arrangements that can help ensure comprehensive oversight and supervision of a GSC arrangement operating across sectors and borders.

5. High-Level Recommendations for the effective regulation, supervision and oversight of GSCs

5.1. Objectives

These high-level recommendations seek to promote consistent and effective regulation, supervision, and oversight of GSCs across jurisdictions to address the potential financial stability risks posed by GSCs, both at the domestic and international level, while supporting responsible innovation and providing sufficient flexibility for jurisdictions to implement domestic approaches.

The recommendations are intended to be high-level and flexible so that they can be incorporated into the wide variety of regulatory frameworks potentially applicable to GSCs around the world. They aim to promote a regulatory, supervisory and oversight framework that is technology neutral and focuses on underlying activities and risks.

The recommendations are addressed to financial regulatory, supervisory and oversight authorities at a jurisdictional level. They should be applied by individual authorities to the extent they fall within the authorities' remits.

Grounded in an assessment of a GSC arrangement's economic functions and the principle of "same business, same risk, same rules", and focused on regulatory objectives and outcomes, authorities should apply and, if necessary, develop effective regulatory, supervisory and oversight approaches and cross-border cooperation mechanisms within their respective mandate and legal frameworks.

At the same time, the recommendations set out expectations for providers of services and activities within the GSC arrangements and can serve as a basis for authorities' active engagement with stakeholders on GSC-related risks and how these are addressed.

5.2. Scope

The recommendations focus on addressing risks to financial stability and therefore do not comprehensively cover important issues such as AML/CFT, data privacy, cyber security consumer and investor protection, competition policy, taxation, monetary policy, monetary sovereignty, currency substitution, and other macroeconomic concerns. However, they acknowledge that a comprehensive supervisory and regulatory framework for GSC arrangements should effectively address AML/CFT, data privacy, consumer and investor protection, competition and market integrity in addition to financial stability risks.

New York, in cooperation with the G-10 and other central banks of issue of CLS-settled currencies. A protocol for cooperation has been established (see https://www.federalreserve.gov/paymentsystems/cls_protocol.htm).

The recommendations apply to any GSC in any jurisdiction and help authorities to address activities and services within GSC arrangements that may fall outside the traditional regulatory perimeter. Consistent application of these recommendations by all relevant authorities in jurisdictions in which GSC arrangements are active may help to ensure comprehensive regulatory coverage and reduce the scope for regulatory arbitrage.

While focusing on GSCs that may be widely used as a means of payment and/or store of value for consumers and businesses, the recommendations could also be relevant for:

- stablecoin arrangements that may pose risks to financial stability only in some countries or regions;
- stablecoin arrangements used only for wholesale transactions among financial institutions;
- stablecoin arrangements that are anticipated to become GSC arrangements; and
- other crypto-assets that could pose risks similar to some of those posed by GSCs because of comparable international reach, scale and use.

The high-level recommendations complement and are intended to inform any potential updates to international sectoral standards and principles. Authorities should rely on sectoral standards and principles for cross-border cooperation relevant to the supervision and oversight of GSC arrangements, where they perform the same economic function as existing regulated activities covered by these standards. These include, for example, the IOSCO *Principles regarding Cross-Border Supervisory Cooperation*, the CPMI-IOSCO *Principles for Financial Market Infrastructures*, including the Responsibilities of Authorities and particularly Responsibility E, the FATF standards, in particular Recommendation 15, and the relevant principles applicable to cross-border banking supervision and crisis management of the BCBS and the FSB. Efforts by the standard setting bodies to review, and where appropriate adjust their standards to take into account the novel features of stablecoins can further promote international consistency and reduce the risk of arbitrage or regulatory underlaps.

5.3. Follow-up and review

The FSB will, in close cooperation with relevant SSBs, take the appropriate actions in the next few years to (i) ensure that any relevant international standard-setting work is completed, (ii) take stock of the implementation of international standards, including on cooperation, coordination and information sharing among authorities, and (iii) review and assess the need to update the recommendations in this report and refine or adapt international standards (including providing further guidance). Table 3 shows the indicative timelines for this work, as set out in the roadmap.

Table 3: Follow-up work to the FSB report and recommendations	
Completion of international standard-setting work, by reviewing existing standards and principles, and assessing the need for further guidance in accordance with the FSB recommendations	
SSBs (CPMI, FATF, IOSCO, BCBS), as needed, to make any revisions to standards and principles or provide further guidance supplementing existing standards and principles in light of the FSB report and following their review of their existing frameworks, including on cooperation, coordination and information sharing amongst authorities.	By December 2021
Implementation of international standards in national jurisdictions, including effective cooperation, coordination and information sharing arrangements to support the comprehensive regulation, supervision and oversight of GSC arrangements across borders and sectors, in accordance with the FSB report	
National authorities to consider establishing or, as necessary, adjusting, for any existing GSCs and stablecoin arrangements that have the potential of becoming a GSC, cooperation arrangements consistent with international standards and principles, and the FSB report.	By December 2021, and as needed depending on the emergence of cross-border GSC arrangements
National authorities to consider establishing or, as necessary, adjusting regulatory, supervisory and oversight frameworks consistent with the FSB recommendations and international standards and guidance.	By July 2022, and as needed depending on the emergence of cross-border GSC arrangements
Review of the implementation and assess the need to refine or adapt international standards	
FSB to review in consultation with other relevant SSBs and international organisations the recommendations in the FSB Report and how any gaps identified could be addressed by existing frameworks, and update recommendations if needed.	To be started in January 2022 – completed by July 2023

Beyond 2023 and to keep pace with evolution of GSC arrangements and market developments, the FSB will carry on reviewing its recommendations on a regular basis in order to identify any potential gaps, and update them if needed in order to ensure that they remain relevant and continue to promote effective regulation, supervision and oversight of GSC arrangements across jurisdictions.

5.4. High-level Recommendations

1. **Authorities should have and utilise the necessary powers and tools, and adequate resources, to comprehensively regulate, supervise, and oversee a GSC**

arrangement and its associated functions and activities, and enforce relevant laws and regulations effectively.[33]

Authorities within a jurisdiction, either independently or collectively, should have and utilise the appropriate powers and capabilities to, as applicable, regulate, supervise, oversee and, if necessary, prohibit effectively stablecoin activities being conducted and services being offered to users in or from their jurisdiction and the attendant risks that these services and activities may pose. This may include, for example, activities and services related to the governance and control of the stablecoin arrangement, operating the infrastructure of the stablecoin arrangement, issuing and redeeming stablecoins, managing stablecoin reserve assets, providing custody or trust services for stablecoin reserve assets, trading and exchanging stablecoins, or storing the keys providing access to stablecoins.

Authorities' powers should extend to entities that are engaged in GSC activities in their jurisdictions and fall within the scope of their authority and mandate. Authorities should evaluate, identify and clarify which authorities have responsibility for each activity of a GSC arrangement, as appropriate.

Authorities should identify and address material gaps in their regulatory, supervisory and oversight frameworks through changes in regulations, or policy, as appropriate. In some jurisdictions, legislative changes may be necessary to address those gaps.

Authorities should ensure appropriate monitoring of GSC activities (and any significant change to the way those activities are performed) and ensure timely access to relevant information sufficient to conduct effective regulation, supervision and oversight.

Authorities should have the powers and capabilities to enforce applicable regulatory, supervisory and oversight requirements, including the ability to undertake inspections or examinations, and, when necessary, require corrective actions and take enforcement measures. To do so, authorities should be provided with or obtain sufficient information regarding the technology and legal obligations underpinning the GSC arrangements.

Authorities should be able to identify the legal entities responsible for the relevant activities and to assess the ability of the GSC arrangement to implement corrective actions.

Authorities should have the ability to mitigate risks associated with, or prohibit the use of certain or specific stablecoins in their jurisdictions where these do not meet the applicable regulatory, supervisory, and oversight requirements.

2. **Authorities should apply comprehensive regulatory, supervisory and oversight requirements and relevant international standards to GSC arrangements on a functional basis and proportionate to their risks.**

[33] This report recognises that establishing powers and tools for authorities is the province of individual jurisdictions' governing legislatures and any change would require legislative support.

To promote a technology neutral approach that enables comprehensive oversight of GSC's functions and activities and mitigates regulatory arbitrage, authorities should focus on the functions performed by the GSC arrangement and risks posed and apply the appropriate regulatory framework in the same manner as they would apply it to entities performing the same functions or activities, and posing the same risks ("same business, same risk, same rules").

Authorities should apply rules and policies, including applicable international standards, as appropriate and to the extent that the GSC arrangement provides the same functions and poses the same risks as other financial service providers. This includes the relevant regulation, standards and rules for e-money issuers, remittance companies, financial market infrastructures including payment systems, collective investment schemes, and deposit-taking and securities trading activities. This also includes market integrity, consumer and investor protection arrangements, appropriate safeguards, such as pre- and post-trade transparency obligations, rules on conflicts of interest (including for different service providers such as e.g., the reserve asset custodian and coin issuer, the coin issuer and an exchange platform), disclosure requirements, robust systems and controls for platforms where the GSC is traded, rules that allocate responsibility in the event of unauthorised transactions and fraud, and rules governing the irrevocability of a transfer orders ("settlement finality").

Authorities should assess whether existing regulatory, supervisory and oversight requirements adequately address the risks of GSC functions and activities, and consider the potential effects of requirements not applying to aspects of a GSC arrangement. Authorities should, if necessary, clarify or supplement financial regulations that do not adequately capture the risks of GSC functions and activities and to develop and implement regulations to address uncaptured risks as needed.

There should be cooperation and coordination regarding how jurisdictions' rules apply to the different aspects of the GSC arrangement's functions and activities operating across borders, as with other types of financial arrangements.

3. **Authorities should cooperate and coordinate with each other, both domestically and internationally, to foster efficient and effective communication and consultation in order to support each other in fulfilling their respective mandates and to ensure comprehensive regulation, supervision, and oversight of a GSC arrangement across borders and sectors.**

   Cooperation arrangements should be flexible, efficient, inclusive, and multi-sectoral, and take into account the complexity and the potential evolution of the GSC arrangement and the risks it poses over time. They may take different forms (e.g. supervisory colleges, fora, networks, memorandums of understanding (MoUs), ad-hoc arrangements). They should also consider the distinctive nature of GSC arrangements as usually consisting of multiple and oftentimes unrelated entities that interact and have varying roles and responsibilities.

   Cooperation arrangements may be underpinned by bilateral and/or multilateral memoranda of understanding for cooperation and information sharing, and for crisis management and resolution, and complemented with mechanisms with a single focus,

e.g. regarding AML/CFT or cyber security. These arrangements should also consider the potential need to seek cooperation from authorities in other jurisdictions to achieve regulatory objectives, e.g. in implementing recovery and resolution plans, or halting activities based in one jurisdiction having an adverse impact in another.

In establishing a cooperation arrangement, authorities should consider how to ensure that the arrangement takes into account the interests of each of the jurisdictions and sectors in which GSC arrangements may be operating or seeking to operate, jurisdictions where the governance body, the providers of GSC functions and activities and the GSC arrangement's users are located, where (spillover) risks reside, and the potentially differing impacts of GSC arrangements across jurisdictions and between AEs and EMDEs.

4. **Authorities should ensure that GSC arrangements have in place a comprehensive governance framework with a clear allocation of accountability for the functions and activities within the GSC arrangement.**

   An adequate governance framework that conforms with relevant international standards needs to be in place for the entire network of GSC activities, functions and participants, given each part of the network can affect the other parts. The governance structures and accountabilities should have a sound legal basis and be clear, transparent, and disclosed to users and other stakeholders. Such disclosures should include how governance and accountability is allocated and how potential conflicts of interest are addressed among different entities in different jurisdictions, as well as clarify the limits of accountability and legal liability in any one jurisdiction. This should be the case for all functions and activities of the GSC arrangement, including but not limited to, setting rules and standards for participants of the GSC arrangement, operating the stabilisation mechanism, in particular the investing of the reserve assets as appropriate, providing the custody or trust services for reserve assets, and providing user-facing services such as exchanges and wallets.

   GSC arrangements may vary in the degree of decentralisation of their governance design. This notwithstanding, authorities should ensure that there are one or more governance bodies or an equivalent mechanism and that the functions and activities of the GSC arrangement are subject to appropriate oversight, governance and safeguards. Fully permissionless ledgers or similar mechanisms could pose particular challenges to accountability and governance and authorities therefore need to ensure that appropriate regulatory, supervisory, and oversight requirements can be effectively applied to such arrangements.

   Where a GSC arrangement relies on a third-party, the GSC governance body should provide a comprehensive assessment of how its reliance on the third-party does not impede its ability to meet regulatory requirements and expectations for performance, resilience, security, development and maintenance, and regulatory compliance.

5. **Authorities should ensure that GSC arrangements have effective risk management frameworks in place especially with regard to reserve management, operational resilience, cyber security safeguards and AML/CFT measures, as well as "fit and proper" requirements.**

Authorities should ensure that GSC arrangements have in place policies that set out how all functions and activities within the GSC arrangement are subject to risk management measures that are appropriate to and commensurate with the specific risks that GSC arrangements pose. If the risk from the fluctuation in the value of the underlying assets is borne, partially or totally by the GSC operator, the relevant prudential framework (e.g. market risk framework) should be applied to the GSC operator.

Authorities should ensure that GSC arrangements conduct proper due diligence (for example, by applying 'fit and proper' standards) into individuals involved in the management and control of the GSC arrangement, as well as those who exercise significant power or discharge significant responsibilities in relation to GSC activities.

Authorities should ensure that GSC arrangements have in place policies that address heightened risks for GSC arrangements, such as operational risks, money laundering/terrorist financing risks, and cyber risks, and provide for appropriate consumer and investor protection, in line with legal obligations in jurisdictions where a GSC arrangement operates. Risk management measures and technical standards should cover relevant activities performed by providers of activities in the GSC arrangements, paying particular attention to compliance by permissionless or anonymous networks.

Authorities should ensure that GSC arrangements conduct continuous risk assessments, contingency preparedness, and continuity planning. Authorities should ensure that GSC arrangements conduct a robust assessment of how their technology model and the rules for transferring coins provide assurance of settlement finality.

Authorities should consider requiring GSC arrangements to adopt strict rules on reserve assets management and have adequate capital and liquidity buffers to absorb credit, liquidity and market risks, as well as risks related to legal, operational and cyber risks relevant to the stabilisation mechanism. Provisions for capital and liquidity should ensure that GSC arrangements that include redemption rights have taken into consideration their ability to properly handle risks of large-scale redemption demands in cases of stressed and extreme market conditions, including through scenario analysis for example.

There should be particular attention to the degree of risk-taking in terms of duration, credit quality, liquidity and concentration of a GSC's reserve assets. In addition, asset-linked stabilisation mechanisms should have sufficient controls to ensure that GSC issuance and destruction are sufficiently matched by a corresponding increase or decrease in reserve assets and that such increases or decreases are managed to avoid adverse impacts on the broader market.

6. **Authorities should ensure that GSC arrangements have in place robust systems for collecting, storing and safeguarding data.**

GSC arrangements should implement and operate data management systems that record and safeguard in a discoverable format relevant data and information collected and produced in the course of their operations, while conforming to all applicable data privacy requirements. Adequate controls should be in place to safeguard the integrity

and security of both on-chain and off-chain data and conform to applicable data protection regulation.

Authorities should be able to obtain timely and complete access to relevant data and information to enable them to implement adequate regulatory, supervisory, and oversight approaches that capture the functions and activities of the GSC arrangement, in accordance with the level and nature of the risks posed.

7. **Authorities should ensure that GSC arrangements have appropriate recovery and resolution plans.**

   Authorities should ensure that GSC arrangements have in place appropriate planning to support an orderly wind-down or resolution under the applicable legal (or insolvency) frameworks, including continuity or recovery of any critical functions and activities within the GSC arrangement.

   Authorities should consider how such plans are implemented through effective contractual obligations among the entities in the GSC network, and address the potential involvement of authorities in all of the jurisdictions that the entities operate in.

8. **Authorities should ensure that GSC arrangements provide users and relevant stakeholders with comprehensive and transparent information necessary to understand the functioning of the GSC arrangement, including with respect to its stabilisation mechanism.**

   Features of GSC arrangements that should be transparent to users and relevant stakeholders should include: the governance structure of the GSC arrangement; the allocation of roles and responsibilities assigned to operators or service providers within the GSC arrangement; the operation of the stabilisation mechanism; the investment mandate for the reserve assets; the custody arrangement and applicable segregation of reserve assets; available dispute resolution mechanisms or procedures for seeking redress or lodging complaints, as well as information on risk relevant for users.

   Authorities should ensure that GSC arrangement makes appropriate disclosures to users and the market regarding the design of the stabilisation mechanism (e.g. asset-linked or algorithm-based), and the mechanism by which the stablecoin's value is maintained.

   Information to be disclosed to users and counterparties should periodically cover the amount of GSC in circulation and the value and the composition of the assets in the reserve backing the GSC. Information pertaining to the amount of GSC in circulation and the value and the composition of the assets in the reserve backing the GSC should be subject to independent audit, and disclosed on a regular basis in a comprehensive and transparent manner. Other information relevant to the functioning of the GSC arrangement, such as e.g. a list of available exchange platforms, wallet providers, should be made available whenever possible.

   GSC arrangements should put in place mechanisms to ensure the protection of the interests of users and counterparties, when a potential modification of the arrangement could have a material effect on the value, stability, or risk of the GSC.

9. **Authorities should ensure that GSC arrangements provide legal clarity to users on the nature and enforceability of any redemption rights and the process for redemption, where applicable.**

Authorities should require GSC arrangements to provide appropriate information to users on the nature and enforceability of redemption rights, where available, and of any claims that users and intermediaries may or may not have on the underlying reserve assets or against the issuer or guarantors, including how claims may be treated in insolvency or resolution. The GSC arrangement should also provide adequate information on the process for redemption and the enforcement of any claims by users, where applicable, and how the GSC arrangement ensures smooth execution of such processes, including under stressed circumstances. Authorities should consider implications, including for "run" risks, of GSC arrangements' decisions to grant users and/or intermediaries a direct legal claim against the GSC issuer or its reserve.

The GSC arrangement should provide adequate information on the recovery avenues that are available to users that lose access to their wallet or private key for example because of a cyber-attack or other operational incident.

Where a stablecoin is used widely for payment purposes, authorities should assess whether safeguards or protections consistent with similar instruments are appropriate. Where a GSC arrangement for such a stablecoin offers rights to redemption, such redemption should be at predictable and transparent rates of exchange, including, where authorities consider it appropriate, at par into fiat money consistent with similar instruments used widely for payment purposes. Authorities should ensure that such GSC arrangements follow prudential standards comparable to those required for financial institutions performing the same economic functions and posing similar risks.

10. **Authorities should ensure that GSC arrangements meet all applicable regulatory, supervisory and oversight requirements of a particular jurisdiction before commencing any operations in that jurisdiction, and adapt to new regulatory requirements as necessary.**

Authorities should not permit the operation of a GSC arrangement in their jurisdiction unless the GSC arrangement meets all of their jurisdiction's regulatory, supervisory, and oversight requirements,[34] including affirmative approval (e.g. licenses or registrations) where such a mechanism is in place.[35]

GSC arrangements should have the ability to adjust their operational features, processes and mechanisms as necessary to maintain compliance with regulatory requirements and international standards if these evolve.

Before launching the arrangement and the provision of services to users in a particular jurisdiction, entities and individuals involved in the management and control of the GSC

---

34 Including taking into account prevailing policies of authorities.

35 This would not prevent the establishment of proof-of-concepts or limited scale experiments under the adequate supervision of relevant authorities in jurisdictions concerned.

arrangement intending to engage in GSC functions and activities should make themselves aware of the regulatory requirements that apply. Where regulations of more than one jurisdiction may apply, they should make themselves aware of which jurisdictions' rules are applicable to different aspects of the functions and activities of the entities performing them and should engage proactively with authorities.

Annex 1: Different operating models for stablecoin arrangements

Stablecoin arrangements could take on a variety of structures and operating models, including from a technical perspective. The following four hypothetical examples can be used to illustrate the diversity in current and proposed stablecoin arrangements.

	Stablecoin A	Stablecoin B	Stablecoin C	Stablecoin D
Issuer	Single issuer	Multiple issuers	Single issuer	Smart Contracts
Liability **- Who or what is the claim on, and are there conditions?**	Claim on issuer	Claim on issuer, subject to holder meeting compliance requirements	Claim on approved intermediary; users have no rights or claims on underlying reserve assets	Interest in an equivalent amount held in the reserve assets
- Is it directly redeemable by the user, and if not, by whom?	Directly redeemable	Directly redeemable	Not directly redeemable; only approved participants can redeem coins with issuer	Directly redeemable
- What is it redeemed for, and are there conditions?	Redeemable for USD only at high ticket size, > $100K	Redeemable for USD (> $100)	Redeemable for local fiat currency	Redeemable for another crypto-asset
Stabilisation mechanism	Fiat currency – backed	Fiat currency – backed	Fiat currency – backed	Crypto-asset backed
Reserve assets	USD bank deposits	USD bank deposits	Bank deposits and short-term government securities in the referenced currencies	Another crypto-asset
Transaction permission	Permissionless	Permissionless	Permissionless below threshold	Permissionless
Medium of record	Multiple public blockchains	Single public blockchain	Single private blockchain	Single public blockchain
Ledger model	UTXO[36] or account depending on the blockchain	Account	Account	Account
Network permissions	Permissionless	Permissionless	Permissioned; validator nodes operated by approved parties	Permissionless

[36] The Unspent Transaction Output (UTXO)-based model records the ownership of the coins, and transfers occur through updating the ownership records of coins. The account-based model records the amount of coins associated with each account, and transfers occur through adjusting the amount of coins in accounts.

Annex 2: Examples of vulnerabilities, regulatory tools, and international standards by activity of a GSC arrangement

		Regulatory authorities and potential tools to address the vulnerabilities	
Activities	**Vulnerabilities**	**Authority/tool**	**Relevant international standard**
Establishing rules governing the stablecoin arrangement	Fraud or conflict of interest of those governing the GSC arrangement Lack of contractual arrangements among the entities of the GSC arrangement Difficulties to tackle the uncertainty for users due to an unclear definition of roles and responsibilities within the GSC arrangement Inadequate governance framework Lack of clear central body to hold accountable	Ability to regulate and supervise the GSC arrangement in a holistic manner, e.g. through cooperation among authorities (akin to comprehensive consolidated supervision) Ability to require a GSC arrangement to be governed in a manner that facilitates effective regulation and supervision, including by prohibiting fully decentralised systems Governance, internal control and risk management requirements applicable at the level of the entire GSC arrangement Power to wind down or resolve a GSC arrangement Governance requirements requiring a solid legal basis Cyber security and other operational resiliency safeguards AML/CFT and sanctions controls	The revised FATF Standards apply. Based on known models, developers and governance bodies of centralised GSCs will, in general, have AML/CFT obligations as a financial institution (e.g., as a business involved in the 'issuing and managing means of payment') or a VASP (e.g. as a business involved in the 'participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset'). They can then be held accountable for the implementation of AML/CFT controls across the arrangement and taking steps to mitigate ML/TF risks (e.g. in the design of the so-called stablecoin).This could include, for example, limiting the scope of customers' ability to transact anonymously using the so-called stablecoin and/or by ensuring that AML/CFT obligations of AML/CFT-obliged intermediaries within the arrangement are fulfilled. For GSC arrangements set up entirely by banks, the Basel Framework and associated principles for supervision and colleges would provide a basis for overseeing the setup.

	For GSC arrangements deemed to perform systemically important payment system functions or other FMI functions that are systemically important, the PFMI apply. On the basis of a preliminary analysis, some of the most relevant principles regarding these vulnerabilities would be those on legal basis, governance and comprehensive management of risks. Responsibility E would provide a strong basis for cooperation among relevant authorities. See Annex 4 on CPMI-IOSCO preliminary analysis. For GSC arrangements where the token or the reserve qualifies as a security, relevant IOSCO Principles and Standards that cover governance arrangements would apply, depending on the structure. These would include relevant cooperation agreements (IOSCO Principles[37] covering Cooperation in regulation (Principles 13 to 15), IOSCO's Multilateral MoU Concerning Consultation and Cooperation and the Exchange of Information,[38] the Enhanced Multilateral MoU Concerning Consultation and Cooperation and the Exchange of Information,[39] IOSCO's Principles on Cross-Border Supervisory

37 https://www.iosco.org/library/pubdocs/pdf/IOSCOPD561.pdf

38 https://www.iosco.org/about/?subsection=mmou

39 https://www.iosco.org/about/?subsection=emmou

			Cooperation[40] of May 2010, the cross-border regulatory cooperation aspect of the IOSCO 2015 Cross-Border Regulation Task Force Report[41] and the work of the Follow-Up Group to address potential regulatory arbitrage).
Issuing, creating and destroying stablecoins	Inability to meet redemptions in stressed conditions For algorithmic arrangements, errors in the issuance or redemption algorithm that impact value	Adequate liquidity (risk) management Liquidity risk management tools (e.g. redemption gates) Certain own funds/liquidity requirements Cyber security and other operational resiliency safeguards AML/CFT and sanctions controls	FATF standards apply to firms "issuing and managing means of payment" or to those who provide "participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset". For GSC arrangements involving banks, the prudential risks and operational resilience vulnerabilities would be subject to the Basel Framework and *Principles for the sound management of operational risk*. For GSC arrangements deemed to perform systemically important payment system functions or other FMI functions that are systemically important, the PFMI apply. On the basis of a preliminary analysis, some of the most relevant principles regarding these vulnerabilities would be those related to frameworks for comprehensive risk management and settlement. See Annex 4 on CPMI-IOSCO preliminary analysis. Depending on the creation/redemption processes, the IOSCO Principles for the

40 https://www.iosco.org/library/pubdocs/pdf/IOSCOPD322.pdf

41 https://www.iosco.org/library/pubdocs/pdf/IOSCOPD507.pdf

			Regulation of Exchange Traded Funds (2013)[42] could be relevant.
Managing reserve assets	A sharp fall in price and/or liquidity of reserve asset(s) Change in reserve allocation across reserve assets Lack of transparency in the composition of reserve Fraud or mismanagement of the reserve Investment in illiquid assets Significant increase in the price volatility of the reserve assets that cannot be or is not readily managed	Portfolio diversification rules and issuer limits rules Liquidity and other financial risk safeguards Liquidity risk management tools (e.g. redemption gates) Requirements on disclosure of the composition of the assets Disclosure of investment policies Cyber security and other operational resiliency safeguards AML/CFT and sanctions controls	FATF standards apply to those who provide "safekeeping and administration of cash and liquid securities on behalf of other persons", or "safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets". For GSC arrangements involving banks, the prudential risks and operational resilience vulnerabilities would be subject to the Basel *Framework and Principles for the sound management of operational risk*. Depending on its structure, the reserve may engage IOSCO Liquidity Risk Management Recommendations (2018),[43] IOSCO *Principles for the Regulation of Exchange Traded Funds* or IOSCO *Policy Recommendations for MMFs* (2012).[44]

42 IOSCO (2013), *Principles for the Regulation of Exchange Traded Funds*, June

43 https://www.iosco.org/news/pdf/IOSCONEWS486.pdf.

44 http://www.iosco.org/library/pubdocs/pdf/IOSCOPD392.pdf.

			For GSC arrangements deemed to perform systemically important payment system functions or other FMI functions that are systemically important, the PFMI apply. On the basis of a preliminary analysis, some of the most relevant principles regarding these vulnerabilities would be those on custody and investment risks and transparency. See Annex 4 on CPMI-IOSCO preliminary analysis.
Providing custody/trust for reserve assets	Custodian failure, cross-border resolution, fraud Liquidity Lack of legal clarity regarding rights to reserve assets, particularly where legal regimes of different jurisdictions are implicated	Segregation requirements/rights for reserve assets Liquidity and other financial risk safeguards Cyber security and other operational resiliency safeguards AML/CFT and sanctions controls	FATF standards apply to those who provide "safekeeping and administration of cash and liquid securities on behalf of other persons" or "safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets". For GSC arrangements involving banks, the prudential risks and operational resilience vulnerabilities would be subject to the Basel Framework and *Principles for the sound management of operational risk*. IOSCO *Recommendations Regarding the Protection of Client Assets* (2013).[45] For GSC arrangements deemed to perform systemically important payment system functions or other FMI functions that are systemically important, the PFMI apply. On the basis of a preliminary analysis, some of the most relevant principles regarding these vulnerabilities would be those on custody and

45 *Recommendations Regarding the Protection of Client Assets Consultation Report* and Final Report.

			investment risks and transparency. See Annex 4 on CPMI-IOSCO preliminary analysis.
Operating the infrastructure	Disruption to the mechanism that links the value of the stablecoin and the value of its reserves, for example a cyber incident Uncertainty on the revocability of the payments GSC ledger compromised due to design flaw, operational (e.g. cyber) incident	Liquidity and other financial risk safeguards Requirements on payments finality Cyber security and other operational resiliency safeguards AML/CFT and sanctions controls	FATF Standards apply to GSC infrastructure if it satisfies the definition of a financial institution or a virtual asset service provider provided in the FATF glossary. For GSC arrangements involving banks, the prudential risks and operational resilience vulnerabilities would be subject to the Basel Framework and *Principles for the sound management of operational risk*. For GSC arrangements deemed to perform systemically important payment system functions or other FMI functions that are systemically important, the PFMI apply. On the basis of a preliminary analysis, some of the most relevant principles regarding these vulnerabilities would be those on framework for the comprehensive management of risks and settlement. See Annex 4 on CPMI-IOSCO preliminary analysis.
Validating transactions	GSC ledger compromised due to failure of multiple validator nodes	Cyber security and other operational resiliency safeguards AML/CFT and sanctions controls	Depending on the functions they perform, the validator nodes that validate the underlying distributed ledger technology may be VASPs or financial institutions. For GSC arrangements involving banks, the prudential risks and operational resilience vulnerabilities would be subject to the Basel Framework and *Principles for the sound management of operational risk*.

			For GSC arrangements deemed to perform systemically important payment system functions or other FMI functions that are systemically important, the PFMI apply. On the basis of a preliminary analysis, some of the most relevant principles regarding this vulnerability would be that on operational risk and settlement. See Annex 4 on CPMI-IOSCO preliminary analysis.
Storing the private keys providing access to stablecoins (wallets)	Disruption of a wallet, for example theft of coins from digital wallet or operational (e.g. cyber) incident. Direct loss, including by consumers	Liquidity and other financial risk safeguards Cyber security and other operational resiliency safeguards AML/CFT and sanctions controls	FATF Standards apply to all businesses providing custodial wallet services. The FATF Standards do not place explicit obligations on unhosted wallets. For GSC arrangements involving banks, the prudential risks and operational resilience vulnerabilities would be subject to the Basel Framework and *Principles for the sound management of operational risk*. For GSC arrangements deemed to be perform systemically important payment system functions or other FMI functions that are systemically important, the PFMI apply. On the basis of a preliminary analysis, a relevant principle regarding these vulnerabilities would be that on operational risk. See Annex 4 on CPMI-IOSCO preliminary analysis.
Exchanging, trading, reselling and market making of stablecoins	Withdrawal of liquidity provision by authorised resellers/market makers Disruption of a trading platform.	Liquidity and other financial risk safeguards Settlement finality requirements Allocation of legal responsibility for unauthorised transactions	FATF Standards apply to all businesses carrying out trading/exchanging activity. The FATF Standards do not explicitly apply to peer-to-peer transactions without use of a VASP or financial institution.

	Fraud, market manipulation, unauthorised transactions Cyber incident	Cyber security and other operational resiliency safeguards AML/CFT and sanctions controls	For GSC arrangements involving banks, the prudential risks and operational resilience vulnerabilities would be subject to the Basel Framework and *Principles for the sound management of operational risk*. For GSC arrangements deemed to perform systemically important payment system functions or other FMI functions that are systemically important, the PFMI apply. See Annex 4 on CPMI-IOSCO preliminary analysis. *Issues Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms* (2020)[46], discussing IOSCO Principles[47] 13, 14, 15, 33, 34, 35, 36, 37, 29, 30, 31, 32, 38 and associated IOSCO reports.

46 IOSCO (2020), *Issues, Risks and Regulatory Considerations*, February

47 IOSCO (2017), *Objectives and Principles of Securities Regulation*, May

Annex 3: Summary of stocktake responses

This annex presents findings from the FSB survey on regulatory and supervisory approaches to so-called “stablecoins” (hereinafter “SCs”). All FSB members as well as the members of its Regional Consultative Groups (RCGs) were invited to participate in the survey.

A total of 51 jurisdictions completed the survey, including 25 FSB jurisdictions and 26 RCG jurisdictions. All questions have not necessarily been answered by jurisdictions, i.e. the sum of responses in tables and graphs may be fluctuant and less than the total number of responses received.

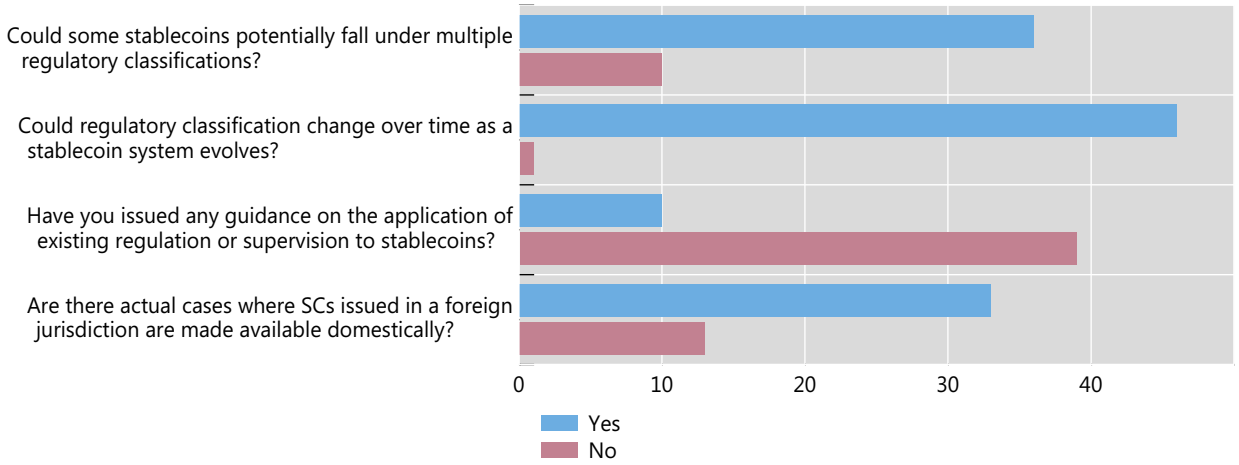
Current regulatory approaches

The majority of jurisdictions do not currently have SCs issued domestically. SCs are available in 31 jurisdictions, mostly cross-border. The majority of those jurisdictions, including several AE, do not currently have regulatory or supervisory regimes that are specific to SCs per se. However, regulatory and supervisory approaches in many of those jurisdictions do apply in whole or part to SCs.

Graph 1 summarises responses concerning the current regulation of SCs. Most respondents note that SCs could be classified under more than one regulatory category, and that the classification could change as the nature and use of the SC evolves. Many respondents are of the view that the existing regulatory and supervisory framework may not be adequate to address the risks emanating from SCs, and that there may be a need to adjust existing regulatory frameworks.

Regarding cross-sectoral issues, most jurisdictions are of the view that existing cooperation mechanisms between sectoral authorities enable them to address the need for cooperation and coordination, possibly with some adaptations (e.g. through Memoranda of Understanding (MoU)).

Stablecoins-Aspects of current regulation **Graph 1**



Source: FSB

Regulatory classifications

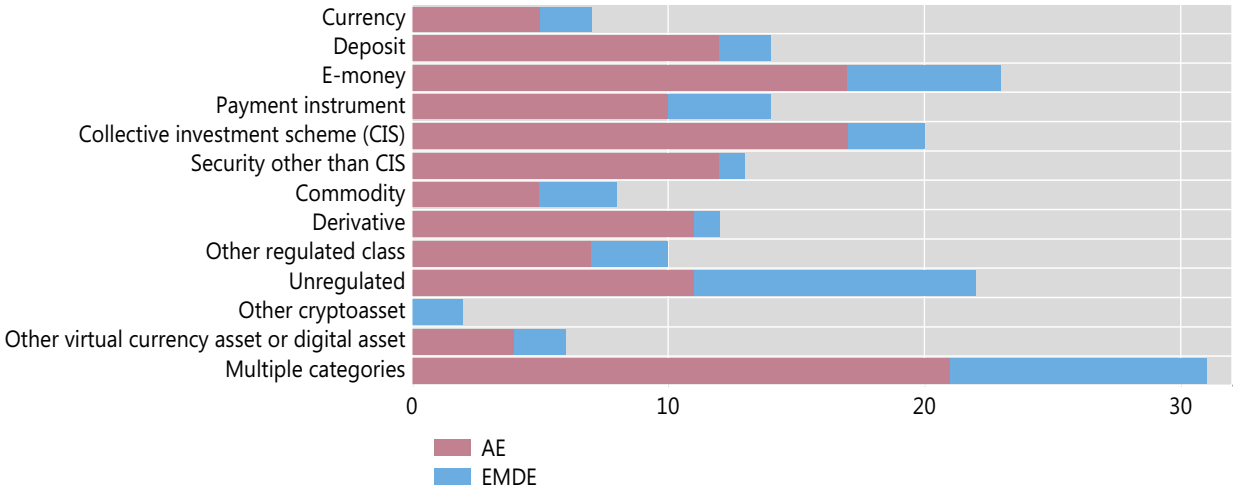
Thirty-seven jurisdictions provided some information about how they *might* classify SCs. Jurisdictions in AEs were more likely to have a classification scheme in place.

Graph 2 shows current and prospective classifications. SCs are most frequently classified as e-money, a collective investment scheme (CIS) in the AEs, followed by deposits, security other than CIS and as derivative. For EMDEs, the most common classifications used were e-money and payment instrument.

Thirty one jurisdictions indicated that SCs could fall under multiple classifications. Jurisdictions that classified SCs as e-money were likely to also classify them as either deposit or as a payment system. Four out of five jurisdictions that classified a SC as a CIS (16 out of 20) also classified it as another security, including security other than CIS, derivative, or commodity. One jurisdiction mentioned that depending on the details, a SC could exhibit bond-like features.

A few respondents indicated that under their current legal framework, it is not possible to classify SC as falling under multiple regulatory classifications. As such, certain activities may not be regulated/captured depending on which regulatory classification the SC ecosystem would fall under. Table 1 also shows that the most prominent regulation types considered by respondents are AML/CFT, cyber/technology risk, safety/soundness, and data privacy.

Current and prospective classification of SCs **Graph 2**



Total number of responses: 40 including 22 from advanced economies (AEs), and 18 from emerging market and developing economies (EMDEs)

Source: FSB

Regulation by activity

Table 1 shows applicable regulation by activity within a SC ecosystem. Issuing/redeeming SCs; managing SC reserve assets; providing custody for SC reference assets; trading/exchanging SCs (including reselling to retail users) and storing SCs (wallets) are the functions that are most frequently covered by regulation, in particular provisions with respect to AML/CFT. Regulatory coverage is lowest with respect to governance and the operation of infrastructure arrangements for SCs.

One respondent noted that certain activities could be easily operated remotely and shift location quickly (e.g. mastermind, issuance of SC, reserve management) and thus would be more likely to be prone to regulatory arbitrage than those activities that tend to have domestically-focused functions (e.g. trading, storing, custody of SCs).

Table 1: Classification of SCs into activities and applicable regulations[48]

	AML/CFT	FMI/ payments	Competition	Investor protection	Consumer protection	Market conduct /integrity	Cyber /technology risk regulation	Safety and soundness	Data privacy	Other
Governing/controlling the SC arrangement (“mastermind”)	17	16	17	11	11	11	15	18	19	5
Operating the infrastructure of the SC arrangement (e.g. payment or settlement system)	18	20	16	7	11	11	17	20	21	3
Issuing/redeeming SCs	33	16	16	12	17	12	18	18	21	3
Managing SC reserve assets	23	9	15	15	12	10	18	22	17	3
Providing custody for SC reference assets	21	11	13	17	13	10	21	21	17	6
Trading/exchanging SCs (including reselling to retail users)	35	8	13	19	16	20	25	22	21	6
Storing keys to access SCs (wallets)	32	12	12	14	16	9	22	17	20	5
Undertaking other type of activity (please specify)	4	2	2	1	3	2	4	2	4	1

[48] The number in each cell indicate the number of responses received for a given activity and regulation type, e.g. 33 jurisdictions indicated that AML-CFT regulations exist and would apply to issuing/redeeming of stablecoins.

Cross-border regulation and supervision of SCs

Most jurisdictions have some power with respect to SCs arrangements operating in a cross-border context,[49] whether it be SC activities provided out of a foreign jurisdiction available to a jurisdiction's domestic customers (Graph 3), or a SC arrangements operating domestically offering services cross-border outside of the country (Graph 4).

An authority's regulatory/supervisory reach also depends on whether the SC could be classified under an existing regulatory framework. Most jurisdictions' authorities would have the same power with respect to SCs issued overseas but being available to users domestically, so long as the SC can be classified under the domestic regulatory framework. Jurisdictions in AE generally indicate having more powers both domestically and abroad.

A majority of respondents feel that international cooperation would be very or somewhat important in regulating and supervising SC activity (Graph 5), supporting cooperative oversight and cross-border information sharing (e.g. through the application of international standards such as the PFMI,[50] existing regulatory regimes in geographies[51] or cooperation mechanisms between authorities[52]), or even considering the establishment of a cross-border coordination mechanism or cooperation network.[53] Considerations concerning cross-border cooperation seem to be at an earlier stage in EMDEs.

With regards to data on SCs that authorities are able to collect and exchange, including across borders, this would highly depend on the actual classification and regulation of the SC or SC arrangement. If a given entity performing an activity of a SC arrangement is regulated, generally broad powers are available to authorities to collect data, e.g. on payment transactions, exposures of financial institutions to SCs, investor and trading data (depending on the licensing regime considered). In those cases, data sharing is generally covered by existing cooperation mechanisms in place with foreign authorities. Challenges arise where entities fall outside of the regulatory perimeter.

---

49 Several so-called "stablecoins" have been mentioned as being available cross-border, with Tether being the leading one. A non-exhaustive list also includes DAO, DAI, TrueUSD, USDPax, PAXGold, Everex, SGDR, 1SG, SDS, USDC, USDS, EURX, JPYX, GBPX, AUDX, NZDX, CNYX, RUBX, CHFX, CADX, GLDX, SLVX.

50 More precisely, Responsibility E.

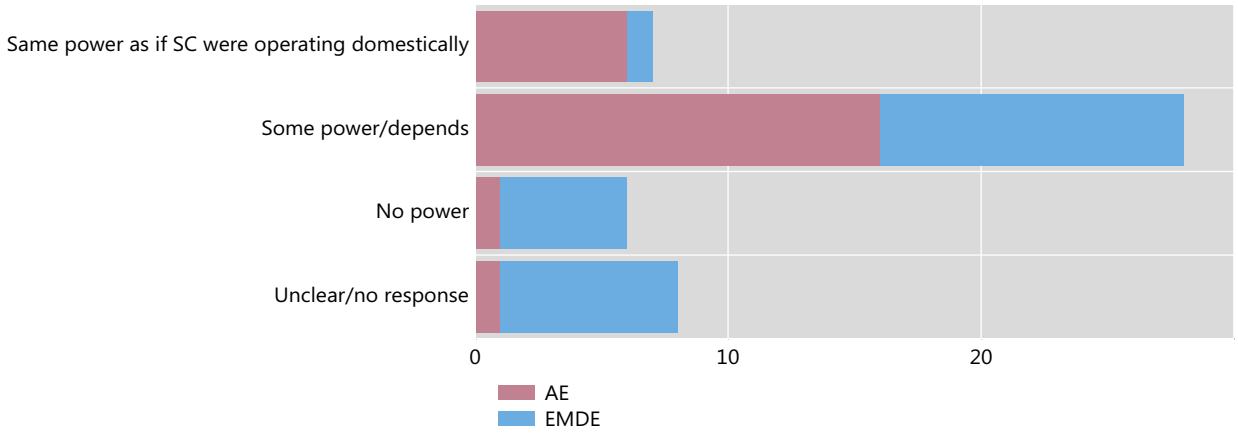
51 For example, in Europe, under the passporting rules for licensed entities, and through the supervisory and regulatory cooperation mechanisms in place within the European Supervisory Authorities (EBA, ESMA and EIOPA).

52 Through existing or extended MoUs and similar bilateral/multilateral agreements between authorities (e.g. as offered by SSBs such as IOSCO).

53 The existing arrangement for SWIFT has been mentioned.

Power that authorities have with respect to SC activities operating out of a foreign jurisdiction available domestically (incoming)

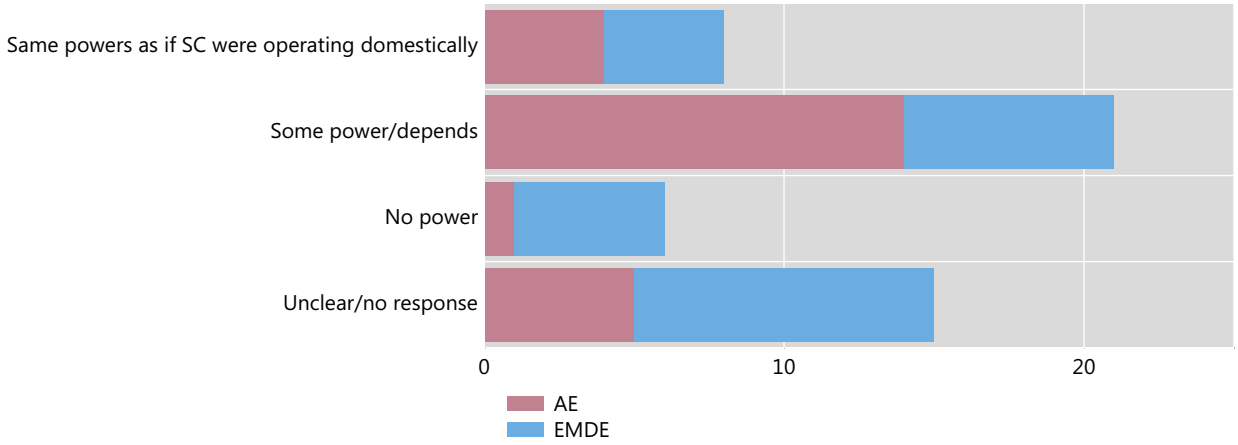
Graph 3



Source: FSB

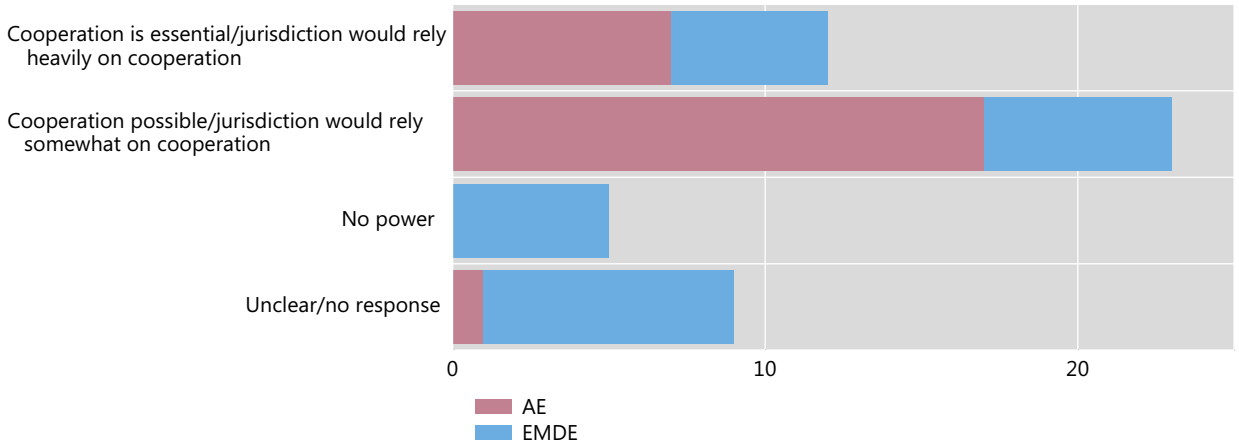
Power that authorities have with respect to domestic SC activities operating overseas (outgoing)

Graph 4



Source: FSB

Extent to which a jurisdiction would rely on cross-border cooperation to regulate or supervise SC activity **Graph 5**



Source: FSB

Potential evolution of regulation

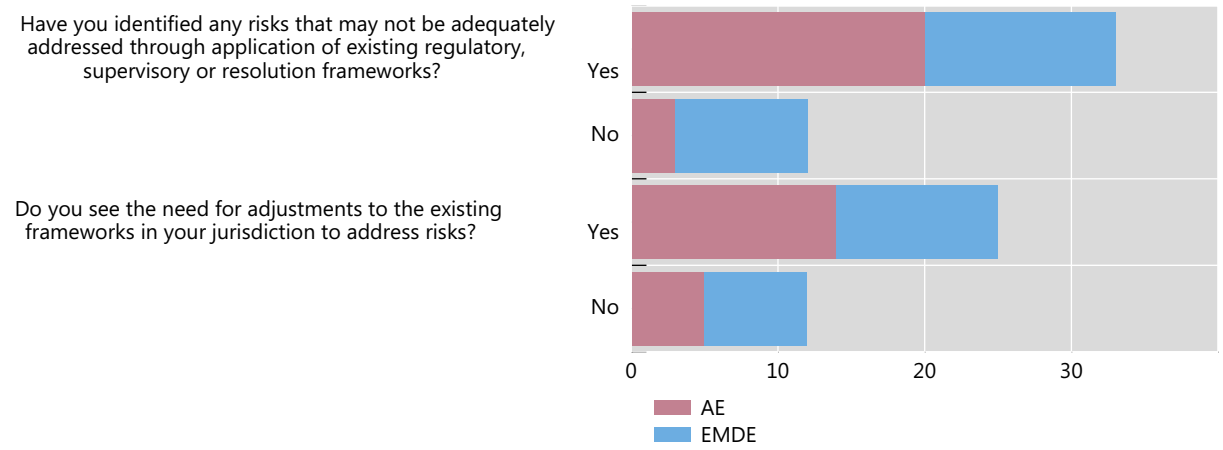
Graph 6 summarises responses concerning the potential evolution of regulation of SCs. Changes in the structure of the SC (change in the composition of the reserve, i.e. assets, stabilisation mechanism), the rights associated to it (existence of changes in the claim on the reserve assets), and the actual use of the SC (e.g. becoming a payment means, used for credit, a change in scale of the adoption) could trigger a re-evaluation of its regulatory classification. Some jurisdictions noted that a change in the regulatory environment could influence existing classifications.

Regarding risks that may not be adequately addressed, respondents noted that cross-border and cross-sectoral issues would need to be considered carefully. Most jurisdictions stressed that risks related to financial stability, monetary policy, monetary sovereignty, currency substitution, consumer and investor protection, AML/CFT, data privacy and specific operational risks linked to the underlying technology (DLT/Blockchain) used by SCs would need to be assessed further. The decentralised nature of SCs systems has been underlined by some as a complexity factor. Finally, risks of regulatory arbitrage and the risk of not capturing key activities within the regulatory ambit have also been raised. Respondents also pointed to more general risks with GSCs, which could become a substitute to currencies (especially for EMDEs, where also large and volatile capital flows could become manifest through exchange rates), retail deposits or safe assets, exacerbate bank runs, and disintermediate more traditional financial institutions. Some respondents are confident that, if a GSC system were considered a payment system, existing frameworks (e.g. PFMI) would apply and cover risks adequately.

Most respondents indicated that adjustments to existing regulatory frameworks may be needed in the future. A few respondents indicated their intention to take legislative action, either to address missing parts in their regulatory regimes (e.g. trading/exchanging, storing SCs), or to adopt a comprehensive framework (e.g. in the EU, with a potential new legislation for a common EU approach to crypto-assets, including SCs).

Stablecoins: potential evolution of regulation

Graph 6



Source: FSB

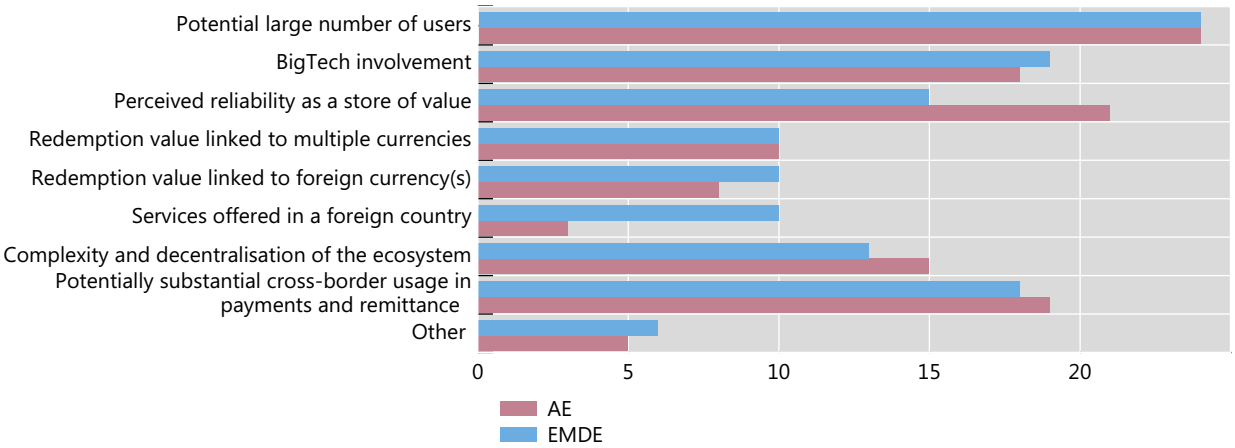
Policy development and considerations for the FSB

Graph 7 shows that jurisdictions from both AEs and EMDEs considered the potential large number of users, the involvement of BigTechs, the potential cross-border usage of a GSC for payments or remittances, and the ability for a GSC to become a store of value to be the main features of a GSC that would distinguish it from other SCs and could pose a greater risk to financial stability and regulatory objectives pursued by authorities.

Jurisdictions in the AEs tended to be more concerned by a GSC's perceived reliability as a store of value and the complex and decentralised nature of a GSC's ecosystem. On the other hand, EMDE jurisdictions expressed greater concern about a GSC being linked to foreign currency, whether it be the service provided or redemption value of a GSC being linked to foreign currency.

Features of a GSC that would distinguish it from other SCs

Graph 7



Source: FSB

Annex 4: Details from standard-setting bodies on work underway

BCBS

The Committee's work on crypto-assets comprises three broad elements:

1. vigilant monitoring of market and regulatory developments related to crypto-assets, and an assessment of the impact of such developments on the banking system;

2. the quantification of banks' direct and indirect exposures to crypto-assets and related services through periodic data-collection exercises; and

3. an assessment of the appropriate prudential treatment for banks' crypto-asset exposures, and the extent to which this treatment should vary based on different types of crypto-assets.

In March 2019, the Committee published a newsletter on the risks associated with crypto-assets. The Committee noted that the continued growth of crypto-assets has the potential to raise financial stability concerns and increase risks faced by banks, and that many types of crypto-assets do not reliably provide the standard economic functions of money issued or backed by a government or public authority and are unsafe to rely on as a medium of exchange or store of value. The newsletter outlined a set of minimum supervisory expectations for banks that are authorised, and decide, to acquire crypto-assets and/or provide related services.

The Committee published a discussion paper in December 2019 to seek the views of stakeholders on a range of issues related to the prudential regulatory treatment of crypto-assets, including:

1. the features and risk characteristics of crypto-assets that should inform the design of a prudential treatment for banks' crypto-asset exposures; and

2. general principles and considerations to guide the design of a prudential treatment of banks' exposures to crypto-assets, including an illustrative example of potential capital and liquidity requirements for exposures to high-risk crypto-assets.

The Committee is also assessing the supervisory and bank implications of GSCs, including the role of banks acting as intermediaries, custodians, or providers of other services, and with respect to liquidity risk, operational risk, and AML/CFT risk.

FATF

In July 2020, the FATF further expanded on these findings in its report to the G20 on so-called stablecoins. The FATF has found that so-called stablecoins share many of the same potential ML/TF risks as some virtual assets, in virtue of their potential for anonymity, global reach and layering of illicit funds. Depending on how they are designed, they may allow anonymous peer-to-peer transactions via unhosted wallets. These features present ML/TF vulnerabilities, which are heightened if there is mass-adoption. When reviewing current and potential projects, so-called stablecoins appear better placed to achieve mass-adoption than many virtual assets, if they do in fact remain stable in value, are easier to use and are under sponsorship of large firms that seek to integrate them into mass telecommunication platforms.

In line with its previous statements, the FATF found that the revised FATF Standards clearly apply to so-called stablecoins. Under the revised FATF Standards, a so-called stablecoin will either be considered to be a virtual asset or a traditional financial asset depending on its exact nature. A range of the entities involved in any so-called stablecoin arrangement will have AML/CFT obligations under the revised FATF Standards. Which entities will have AML/CFT obligations will depend on the design of the so-called stablecoin, particularly the extent to which the functions of the so-called stablecoin are centralised or decentralised, and what activities the entity undertakes.

Importantly, central developers and governance bodies of so-called stablecoins will have AML/CFT obligations under the revised FATF Standards, where they are carrying out the activities of a financial institution or VASP, in addition to the AML/CFT obligations of other entities with AML/CFT obligations, e.g. wallet providers. The central governance bodies of so-called stablecoins are in a unique position to undertake ML/TF risk mitigation, as they determine the functions of the so-called stablecoin, who can access the arrangement and whether AML/CFT preventive measures are built into the arrangement. For example, they could ensure that the access to the transfer system is only possible through AML/CFT-compliant regulated VASPs. Not all so-called stablecoins may have a readily identified central body however.

Based on current known models, the FATF consider that so-called stablecoins with potential for mass-adoption will be centralised to some extent, with an identifiable central developer or governance body. The FATF considers that these developers and governance bodies will be, in general, financial institutions (e.g., as a business involved in the ‘issuing and managing means of payment’) or a VASP (e.g., as a business involved in the ‘participation in and provision of financial services related to an issuer’s offer and/or sale of a virtual asset’) under the revised FATF Standards. This is an important control to mitigate the ML/TF risks posed by such so-called stablecoins. Furthermore, there will be a range of other entities with AML/CFT obligations even in a centralised arrangement, including customer-facing exchanges and transfer services and custodial wallet providers.

While decentralised so-called stablecoins without such an identifiable central body, prima facie, may carry greater ML/TF risks due to their diffuse operation, the FATF considers that their potential for mass-adoption is lower than centralised arrangements and, therefore, their associated ML/TF risks are smaller (although still present). However, even in a decentralised structure, there could also be a range of entities with AML/CFT obligations, including customer-facing exchanges and transfer services and custodial wallet providers. Importantly, there are functions that may mean an entity has AML/CFT obligations prior to the launch of a decentralised

so-called stablecoin, as the process necessary to bring a product to launch is unlikely to be able to be fully decentralised.

The FATF considers that the preventive measures required of intermediaries under the revised FATF Standards have worked to mitigate the ML/TF risks posed by so-called stablecoins currently in existence. Accordingly, the FATF does not consider that the revised FATF Standards need amendment at this point in time. Nonetheless, the FATF recognises that this is a rapidly evolving area that must be closely monitored and that jurisdictions must be effectively implementing the revised Standards.

In particular, it is important that ML/TF risks of so-called stablecoins, particularly those with potential for mass-adoption and increased anonymity, are analysed in an ongoing and forward-looking manner and are mitigated before such arrangements are launched. As so-called stablecoins could quickly become available globally, with their functions decentralised across multiple jurisdictions, international co-operation between jurisdictions is critical to ensure ML/TF risks are appropriately addressed.

The FATF has also identified potential risks which may require further action, including; so-called stablecoins located in jurisdictions with weak or non-existent AML/CFT frameworks (which would not properly implement AML/CFT preventive measures) and so-called stablecoins with decentralised governance structures (which may not include an intermediary that could apply AML/CFT measures) and anonymous peer-to-peer transactions via unhosted wallets (which would not be conducted through a regulated intermediary).

In addition to working collaboratively with the FSB and other global standard-setting bodies, the FATF agreed to undertake four actions:

(i) The FATF calls on all jurisdictions to implement the revised FATF Standards on virtual assets and VASPS as a matter of priority.

(ii) The FATF will review the implementation and impact of the revised Standards by June 2021 consider whether further updates are necessary. This will include monitoring the risks posed by virtual assets, the virtual asset market, and proposals for arrangements with potential for mass-adoption that may facilitate anonymous peer-to-peer transactions.

(iii) The FATF will provide guidance for jurisdictions on so-called stablecoins and virtual assets, as part of a broader update of its Guidance. This will set out in more detail how AML/CFT controls apply to so-called stablecoins, including the tools available to jurisdictions to address the ML/TF risks posed by anonymous peer-to-peer transactions via unhosted wallets.

(iv) The FATF will enhance the international framework for VASP supervisors to co-operate and share information and strengthen their capabilities, in order to develop a global network of supervisors to oversee these activities.

CPMI-IOSCO Preliminary analysis of the application of the PFMI to stablecoin arrangements

Key points

CPMI-IOSCO have undertaken a preliminary analysis of the applicability of the Principles for Financial Market Infrastructure (PFMI)[54] to stablecoin arrangements.

The PFMI are designed to apply to all systemically important Financial Market Infrastructures (FMI). The PFMI are based on a functional approach and allow for a wide range of organisational forms, institutional designs, and arrangements.

Stablecoin arrangements can be designed to cover a range of functions and those functions will determine the standards that will be applied. Some stablecoin arrangements will be designed to settle payments via a transfer mechanism, providing a core function that meets the definition of a payments system, as defined in Annex D of the PFMI.[55] However, other stablecoin arrangements may perform a variety of different FMI functions. Some of these arrangements may be systemically important, having the potential to trigger or transmit systemic disruption. **Where stablecoin arrangements perform systemically important payment system functions or other FMI functions that are systemically important (hereafter "systemically important stablecoin arrangements"), the PFMI apply to such arrangements.**

To the extent that systemically important stablecoin arrangements perform additional functions not covered by the PFMI, they will be subject to relevant standards for those functions in addition to the PFMI. These standards may have interdependencies. For example: the PFMI (Principle 9) state that systemically important FMIs should use a settlement asset with little or no credit or liquidity risk, and where commercial bank money is used this relies on the Basel standards for commercial banks.[56] Further work may be needed to explore and lay out clearly the interdependencies of the PFMI with other international standards, including how each addresses the risks associated with a systemically important stablecoin arrangement's stabilisation activities.

---

54 PFMI are available on the CPMI and IOSCO websites: www.bis.org/cpmi/publ/d101a.pdf and www.iosco.org/library/pubdocs/pdf/IOSCOPD377-PFMI.pdf.

55 Annex D of the PFMI states: "A payment system is a set of instruments, procedures, and rules for the transfer of funds between or among participants; the system includes the participants and the entity operating the arrangement." (Paragraph 1.10 of the PFMI).

56 Principle 9 (Money settlements) is applicable to systemically important payment systems, securities settlement systems and CCPs.

Regulatory or supervisory principles around consumer and investor protection, data privacy, Anti-money laundering (AML) and market integrity are also likely to be crucial elements of the overall regulatory framework that would apply to a systemically important stablecoin arrangement. Cross border regulatory cooperation will be important given the potential for regulatory arbitrage.

The PFMI are technology neutral. It may be challenging for some systemically important stablecoin arrangements to comply with the high standards of the PFMI, particularly for those systemically important stablecoin arrangements that are partially or highly decentralised. Nevertheless, systemically important stablecoin arrangements will need to adapt to meet them.

Some clarification or interpretation may help explain how systemically important stablecoin arrangements may comply with the PFMI, but such clarification or interpretation would not change the underlying principles that apply to a systemically important FMI. Such clarification or interpretation would seek to explain how the PFMI apply to organisations providing novel but systemically important FMI functions and to help such organisations understand what observing the PFMI, at minimum, will require of their design choices. CPMI-IOSCO are carrying out further work to explore the need for such clarification or interpretation.

1. Introduction

The Principles for Financial Market Infrastructures (PFMI) are designed to apply to all systemically important Financial Market Infrastructures (FMI).[57] FMIs facilitate the clearing, settlement and recording of monetary or other financial transactions, such as payment, securities, and derivatives contracts. They play an essential role in the global financial system and the broader economy. If not properly managed, FMIs can be sources of financial shocks, such as liquidity dislocations and credit losses, or a major channel through which these shocks can be transmitted across domestic and international financial markets. Responsibility E of the PFMI provides the framework for cooperation among central banks, market regulators, and other authorities for promoting the safety and efficiency of systemically important FMIs.

This note describes CPMI-IOSCO's preliminary analysis of how the PFMI[58] are relevant and applicable to systemically important stablecoin arrangements. Stablecoin arrangements can be complex, consisting of multiple entities, possibly located in several jurisdictions and possibly performing a mix of different FMI functions. Ultimately, how the PFMI are applied to a particular systemically important stablecoin arrangement would depend on the arrangement's specific design, characteristics, and features, which would have to be addressed on a case-by-case basis.

Preliminary analysis suggests that the PFMI provide relevant international standards for authorities to take into account in (1) considering regulatory approaches that may be appropriate

---

57 The PFMI define an FMI in a broad sense as a "multilateral system among participating institutions, including the operator of the system, used for the purposes of clearing, settling or recording payments, securities, derivatives, or other financial transactions". In particular, the PFMI apply to systemically important payment systems (SIPS), central counterparties (CCPs), central securities depositories (CSDs), securities settlement systems (SSSs), and trade repositories (TRs).

58 The PFMI are made up of 24 principles that apply to one or more types of systemically important FMIs. Furthermore, five Responsibilities apply to authorities supervising or overseeing such FMIs. In particular Responsibility E addresses cooperation among central banks, market regulators, and other authorities. Annex F applies to critical service providers of FMIs.

for systemically important stablecoin arrangements, (2) promoting their safety and efficiency, and (3) cooperating in fulfilling their respective functions. While no need for an amendment of the PFMI is identified at this point in time, it is noted that proposed and prospective systemically important stablecoin arrangements may encounter challenges in meeting some of the relevant PFMI standards.

Certain functions of stablecoin arrangements may involve the application of other regulatory/supervisory frameworks in addition to the PFMI. Moreover, related work is already in progress in regulatory fora other than CPMI-IOSCO.[59] Thus, for systemically important stablecoin arrangements, observing the PFMI for their payment system function will be necessary, but might not be sufficient for the overall arrangement.

CPMI-IOSCO envisage conducting additional work to analyse how particular aspects of the PFMI may be applied to systemically important stablecoin arrangements. If this further analysis reveals any gaps or the need for clarifications, they would need to be addressed, but this will not amount to a derogation or disapplication of the underlying principle. CPMI-IOSCO will coordinate with other international bodies to share perspectives and avoid duplication of work.

2. Rationale for PFMI application to stablecoin arrangements

The PFMI are expected to be applied to systemically important FMIs. The PFMI are based on a functional approach[60] and allow for a wide range of organisational forms, institutional designs, and arrangements of payment processes. The key features of stablecoin arrangements may, to a large extent, be comparable to those of payment systems, as defined in Annex D of the PFMI.[61] In particular, most stablecoin arrangements appear to be inherently designed, at a minimum, to settle payments via a transfer mechanism, where "money settlement"[62] occurs, e.g. when a "token" transfer is recorded on the arrangement's "ledger".[63] In such an arrangement, the core activity of stablecoin arrangements may be a payment system function.

A stablecoin arrangement is also designed to enhance confidence in the value of the issued "tokens". Therefore, often "tokens" purportedly are "backed" by funds, such as central bank

---

59 A stablecoin arrangement, or particular parts thereof, may be classified as a different type of regulated entity (i.e. not only as a payment system) or a different type of regulated activity. Other regulatory/supervisory frameworks include IOSCO frameworks on Money Market Funds, Protection of Client Assets, and Crypto-Asset Trading Platforms, among others.

60 The PFMI emphasise the service provided, not the design choice: "FMIs can differ significantly in organisation, function, and design. FMIs can be legally organised in a variety of forms, […] may be owned and operated by a central bank or by the private sector, […] may also operate as for-profit or not-for-profit entities, […] can be subject to different licensing and regulatory schemes within and across jurisdictions. […] There can be significant variation in design among FMIs with the same function." Paragraph 1.9 of the PFMI.

61 "A payment system is a set of instruments, procedures, and rules for the transfer of funds between or among participants; the system includes the participants and the entity operating the arrangement." Paragraph 1.10 and Annex D of the PFMI.

62 Principle 9 (Money Settlements) is directly applicable to this key function, since it covers the situation when "an FMI conducts money settlements on its own books".

63 See Graph A.1 in Annex A of the G7 Working Group on Stablecoins, (2019), *Investigating the impact of global stablecoins*, October. Graph A.1 provides a functional view of the stablecoin ecosystem along three functions: Issues and stability mechanism, Transfer mechanism, User interface.

deposits, commercial bank deposits, and/or other assets such as securities.[64] This is one means by which a stablecoin arrangement may provide a stabilisation function.

Some stablecoin arrangements may also have a user interface function (interfaces may differ across stablecoin arrangements) that provides access points for users, e.g. wallets.

More broadly, some stablecoin arrangements may also be designed to provide services ancillary to typical payment system services (e.g. some Delivery versus Payment (DVP) or CSD/SSS type services) and may thus be of a "hybrid" FMI nature.

Given that some stablecoin arrangements are designed to be used as means of payment, CPMI-IOSCO believe that, for purposes of this preliminary consideration of the application of the PFMI, the existence of functions within a stablecoin arrangement not directly linked to payments does not weigh against using payment systems as an appropriate proxy for categorising stablecoin arrangements.

For the purpose of assessing the application of the PFMI to stablecoin arrangements, three high-level forms of stablecoin arrangements have been considered. These forms attempt to capture different potential approaches to the governance of the arrangement as a whole, the design of the "ledger" itself, and the unit of account the settlement asset represents. The three forms are:

1. Centralised stablecoin arrangements that aim to fix the price of the token to a particular fiat currency, have a central governance for all functions of these arrangements, and use a private and permissioned distributed ledger.

2. Partially-distributed stablecoin arrangements that have their own unit of account, the value of which is derived from a pool or basket of assets and do not necessarily have a fixed exchange rate to a fiat currency. There is a central governance entity for the issue, stabilisation and transfer mechanism, and the arrangement is based on a private permissioned distributed ledger. However, the user interface is usually provided by independent third party entities.

3. Highly-distributed stablecoin arrangements65 that have their own unit of account, the value of which is derived from a pool or basket of assets and does not necessarily have a fixed exchange rate to a fiat currency. A central entity may govern the issue and stabilisation mechanism. The transfer function is performed on a public un-permissioned distributed ledger meaning that no responsible entity can be identified. The user interface is provided by independent third party entities.

---

64 Principle 16 (Custody and investment risks) is directly applicable to this key aspect of a stablecoin arrangement, since it addresses the need for an FMI to "safeguard its own and its participants' assets" and to address the credit, market, and liquidity risks associated with the custody and investment of these assets.

65 Such arrangements seem to be theoretical at this stage.

3. Systemic importance of stablecoin arrangements

As noted above, the PFMI are expected to be applied to systemically important FMIs, and they provide guidance for relevant authorities to assess the systemic importance of payment systems.[66] Relevant authorities have also usually developed a set of qualitative and quantitative factors to assess whether an FMI is systemically important in their own jurisdictions which could inform the assessment of the systemic importance of a stablecoin arrangement for the purpose of PFMI application. Several authorities may be relevant for the purposes of assessing the systemic importance of a stablecoin arrangement due to the number of functions a stablecoin arrangement may carry out and the number of jurisdictions in which it may operate. Additional considerations could help in capturing specificities of stablecoin arrangements including oversight implications of different levels of decentralisation.

4. Stablecoin arrangements and the application of PFMI principles

Proposed and prospective developers of stablecoin arrangements may face challenges in meeting some of the PFMI standards and may need to consider potential design changes in order to ensure that the PFMI are observed.

Based on a preliminary analysis, the most relevant principles for systemically important stablecoin arrangements would appear to be Principles 1-5, 7- 9, 11-12, 15-23, and Annex F, given that stablecoin arrangements may perform functions that cut across a variety of FMI classifications. Preliminary analysis suggests that all of these may be of general application to any systemically important stablecoin arrangement. However, there are some principles which may be more challenging for systemically important stablecoin arrangements to meet either due to the uncertainty around what PFMI observance would look like in practice for any stablecoin arrangement or because of certain design choices associated with partially and highly-distributed stablecoin arrangements. The more decentralised the arrangements are, the higher the challenges may be.

CPMI-IOSCO's preliminary analysis suggests that systemically important stablecoin arrangements would face varying degrees of difficulty in observing the principles. While this is likely to create challenges primarily for the entities themselves, it could also pose challenges for authorities when it comes to their consideration of a stablecoin arrangement's consistency with the PFMI.

As an initial matter, for most of the principles, CPMI-IOSCO preliminarily note that observance would be challenging for both partially distributed and highly distributed stablecoin arrangements. Further, CPMI-IOSCO have identified several principles that likely would be challenging to observe for all types of stablecoin arrangements. For these particular principles, the precise application or interpretation may not always be straightforward.

---

66 The PFMI state that "…*a payment system is systemically important if it has the potential to trigger or transmit systemic disruptions; this includes, among other things, systems that are the sole payment system in a country or the principal system in terms of the aggregate value of payments; systems that mainly handle time-critical, high-value payments; and systems that settle payments used to effect settlement in other systemically important FMIs."* Paragraph 1.20 of the PFMI.

For example, Principle 1 states that "*an FMI should have a well-founded, clear, transparent, and enforceable legal basis for each material aspect of its activities in all relevant jurisdictions*". Because the legal qualification of stablecoins often is uncertain, stablecoin arrangements may face challenges in establishing the required (domestic and cross border) sound legal underpinnings. Moreover, protections under existing legislation, including payments law, settlement finality provisions and conflict of laws regimes in local jurisdictions, were not written with stablecoin arrangements in mind, and in some jurisdictions may not necessarily extend to such arrangements, leading to possible legal uncertainties in the absence of guidance. These challenges are expected to be even greater for partially-distributed or highly-distributed stablecoin arrangements as it may require a heterogeneous set of distributed entities (operating, for example, the transfer mechanism or parts of the user interface) potentially being located in multiple jurisdictions to function according to a common and unified set of rules consistent with Principle 1.

Further, Principle 9 states that "an FMI should conduct its money settlements in central bank money *where practical and available. If central bank money is not used, an FMI should minimise and strictly control the credit and liquidity risk arising from the use of commercial bank money.*" Stablecoin arrangements will still be expected to strictly minimise and control the credit and liquidity risk arising from their chosen settlement asset, including when a stablecoin arrangement provides settlement on its own books. However, the characterisation of the settlement asset in stablecoin arrangements (e.g. as commercial bank money or not) may not always be straightforward. Further consideration would also be useful to clarify how the PFMI address stablecoin arrangements when a settlement asset carries risk in addition to credit and liquidity risk (i.e. market risk).

Table 1 summarises the preliminary analysis (subject to change and ongoing CPMI-IOSCO review) on the application of the most relevant principles and Annex F to three high-level cases of stablecoin arrangements.

Stablecoin arrangements and the application of the PFMI – Preliminary analysis subject to change and review **Table 1**

	Centralised stablecoin arrangement	Partially distributed stablecoin arrangements	Highly distributed stablecoin arrangements
Principles			
1 Legal basis	Applicable but challenging to observe	Applicable but challenging to observe	Applicable but challenging to observe
2 Governance	Applicable	Applicable but challenging to observe	Applicable but challenging to observe
3 Framework for comprehensive management of risks	Applicable	Applicable but challenging to observe	Applicable but challenging to observe
4 Credit risks	Applicable	Applicable but challenging to observe	Applicable but challenging to observe
5 Collateral	Applicable	Applicable	Applicable
7 Liquidity risks	Applicable	Applicable	Applicable but challenging to observe
8 Settlement finality	Applicable	Applicable but challenging to observe	Applicable but challenging to observe
9 Money settlements	Applicable but challenging to observe	Applicable but challenging to observe	Applicable but challenging to observe

11 CSD	Applicable (to the extent that the arrangements are designed for asset settlements) but challenging to observe	Applicable (to the extent that the arrangements are designed for asset settlements) but challenging to observe	Applicable (to the extent that the arrangements are designed for asset settlements) but challenging to observe
12 Exchange-of-value settlement systems	Applicable (to the extent that the arrangements are designed for to Payment versus Payment (PVP) or DVP settlements) but challenging to observe	Applicable (to the extent that the arrangements are designed for to PVP or DVP settlements) but challenging to observe	Applicable (to the extent that the arrangements are designed for to PVP or DVP settlements) but challenging to observe
15 General business risk	Applicable	Applicable	Applicable
16 Custody	Applicable	Applicable but challenging to observe	Applicable but challenging to observe
17 Operational risk	Applicable	Applicable but challenging to observe	Applicable but challenging to observe
18 Access and participation requirements	Applicable but challenging to observe	Applicable but challenging to observe	Applicable but challenging to observe
19 Tiered participation arrangements	Applicable but challenging to observe	Applicable but challenging to observe	Applicable but challenging to observe
20 Links	Applicable but challenging to observe[67]	Applicable but challenging to observe	Applicable but challenging to observe
21 Efficiency	Applicable	Applicable	Applicable
22 Communication procedures and standards	Applicable	Applicable	Applicable but challenging to observe
23 Transparency	Applicable	Applicable but challenging to observe	Applicable but challenging to observe
Annex F	Applicable	Applicable but challenging to observe	Applicable but challenging to observe

Table 1 is intended to provide a high-level summary of the issues that CPMI-IOSCO have identified to date based on its preliminary analysis. CPMI-IOSCO do not intend for this summary table to constitute guidance or legal advice on which developers of stablecoin arrangements should rely when considering potential design choices. Going forward, CPMI-IOSCO are analysing further how particular systemically important stablecoin arrangements may comply with the PFMI. Some clarification or interpretation may help explain how systemically important stablecoin arrangements may comply with the PFMI, but such clarification or interpretation would not change the underlying principles that apply to a systemically important FMI. Such clarification or interpretation would seek to explain how the PFMI apply to organisations providing novel but systemically important FMI functions and to help such organisations understand what observing the PFMI, at minimum, will require of their design choices.

5. Application of Responsibility E to stablecoin arrangements

The PFMI Responsibilities are also applicable to authorities responsible for stablecoin arrangements. In particular, Responsibility E provides that “central banks, market regulators, and other relevant authorities should cooperate with each other, both domestically and

[67] To the extent that entities within stablecoin arrangements interact with other FMIs.

internationally, as appropriate, in promoting the safety and efficiency of FMIs." Responsibility E, together with its Key Considerations, provides a strong basis for cooperation among relevant authorities for the regulation, supervision and oversight of systemically important stablecoin arrangements.

As a stablecoin arrangement may have other features and provide services in addition to those of a payment system, and the services may be provided on a cross-border basis, a wider range of authorities may have an interest or responsibility vis-a-vis the stablecoin arrangement than only payment system supervisors and oversight authorities. In addition, partially distributed or highly distributed stablecoin arrangements may pose additional challenges. Therefore, it is important to identify and engage the potentially broader set of relevant authorities. Hence the range of authorities that should cooperate could be wider. CPMI-IOSCO are analysing further whether additional considerations would be helpful to achieve appropriate cooperation among relevant authorities.

IOSCO

On 23 March 2020, IOSCO published a report on *Global Stablecoin Initiatives*.[68] The report includes a discussion, at a high level, of how some of the relevant IOSCO Principles, Standards, Recommendations and Guidance (IOSCO Standards) could apply to GSC proposals. For purposes of the discussion on IOSCO Standards, the report used a hypothetical case study of a stablecoin that could act as a global currency and potential financial infrastructure used for domestic and cross-border payments, which uses a reserve fund and intermediaries to seek a stable price vis a vis a basket of low volatility currencies. The report's discussion of how this hypothetical case study could interact with the remits of securities regulators could apply to other GSC proposals, depending on their specific design and their legal and regulatory characteristics and features. The report does not provide an account of how any particular jurisdiction's domestic regulation might apply to GSC proposals.

The majority of IOSCO's report explores the potential application of IOSCO Standards to the "back-end" of a hypothetical GSC, including the management and structuring of the reserve fund; the creation and redemption of coins; coin arbitrage; and potential secondary market trading of the coin. The report also contains a preliminary analysis of the CPMI-IOSCO *Principles for Financial Market Infrastructures*.

Policy Recommendations for Money Market Funds (2012)[69]

Stablecoin arrangements that use a reserve fund to keep the secondary market price in line with the value of the referenced basket or assets in the reserve may have features that resemble a collective investment scheme, a securitised product, or other type of security. Certain characteristics of these reserve funds may be similar to money market funds, particularly with respect to portfolio construction, and market intermediaries may be considered to be acquiring a debt instrument. On this basis, Recommendations 1, 3, 9, 13 and 14 of the *IOSCO Policy Recommendations for MMFs (2012)* may be the most relevant.

Recommendations Regarding the Protection of Client Assets (2013)[70]

In a stablecoin arrangement, a reserve fund or the rights of the authorised participants (APs) with respect to the reserve fund, might be considered a security (e.g. an MMF, other collective investment scheme, or other security). Any third-party participants in GSC proposals involving such securities need to assess whether they are also providing regulated activities, including safeguarding activities. Intermediaries and other firms (such as investment firms, custodians, banks, payment services, e-money or trust companies) that hold or control client assets as part of their regulated business need to follow specific rules designed to protect client assets.

---

68 IOSCO (2020), *Global Stablecoin Initiatives*, March

69 http://www.iosco.org/library/pubdocs/pdf/IOSCOPD392.pdf.

70 *Recommendations Regarding the Protection of Client Assets Consultation Report* and Final Report.

Principles for the Regulation of Exchange Traded Funds (2013)[71]

Certain features of a reserve fund may exhibit similar characteristics to exchange traded funds (ETFs) and other exchange traded products (ETPs). For example, a stablecoin arrangement may use intermediaries acting similarly to APs to effect transactions of fiat currency and the coin, facilitating redemptions and providing liquidity to coin holders. The role of the APs includes establishing the demand for a coin and distributing the coin received through third party platforms to customers. This could be akin to the role of APs that purchase and redeem ETF shares, and distribute ETF shares to the public. IOSCO's *Principles for the Regulation of Exchange Traded Funds* (2013) make a number of observations on the role of APs and set out nine principles that regulators could consider for ETFs.

Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms (2020)[72]

Coin distribution could occur through APs that directly interact with the reserve fund (to mint or burn the coin) and such APs may use crypto-asset trading platforms (CTPs) to buy and sell the coin. As such, CTPs could be the main secondary market where users buy and sell coins. Where a securities regulatory authority has determined that a crypto-asset or an activity involving a crypto-asset falls within its jurisdiction, the basic principles or objectives of securities regulation should apply. The 2020 report describes some of the issues and risks associated with the trading of crypto-assets on CTPs. It describes key considerations and provides toolkits that are intended to assist regulatory authorities who may be evaluating CTPs within the context of their regulatory frameworks. CTPs may need to be regulated as trading venues and meet relevant domestic requirements and international standards.

Principles for Financial Benchmarks (2013)[73]

If any stablecoin pricing, or the value of any assets that are linked to the stablecoin, is used in the future to price or be the basis for the price of certain financial instruments, including those traded on a regulated venue (such as a fund or derivatives), there is the possibility the stablecoin or the value of the linked assets could become a benchmark. In turn, depending on the jurisdiction, the administrator of the benchmark might be carrying out regulated activity and need to be authorised. The principles outlined in this work are useful as a starting point to understand the areas of risk and key mitigants to address inherent risks in calculating and publishing prices.

Principles for the Regulation and Supervision of Commodity Derivatives Markets[74]

IOSCO's work on derivatives products may be relevant in two distinct ways. First, a coin itself could potentially be regarded as a derivative, deriving its value from an underlying basket of financial assets (i.e. a reserve fund). Secondly, future derivatives products could be introduced that would use the coin as the underlying asset from which they derive their value.

---

71 IOSCO (2013), *Principles for the Regulation of Exchange Traded Funds*, June.

72 IOSCO (2020), *Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms*, February

73 IOSCO (2013), *Principles for Financial Benchmarks*, July

74 IOSCO (2011), *Principles for the Regulation and Supervision of Commodity Derivatives Markets*, September

The following three IOSCO principles on commodity derivatives are potentially relevant: 1) economic utility (contracts should meet the risk management needs of potential users and promote price discovery of the underlying commodity); 2) transparency (information concerning a physical commodity derivatives contract's terms and conditions, as well as other relevant information concerning delivery and pricing, should be readily available to authorities and market participants; and 3) review of evolving practices (authorities should have, or contribute to, a process to review the perimeter of regulation to ensure that they have the power to address evolving trading practices that might result in a disorderly market).

Cooperation and information exchange

Given the cross-border nature of global stablecoins, it will be important that markets regulators and other financial supervisors cooperate amongst themselves to reduce the risk of regulatory arbitrage through fragmentation. These regulatory cooperation tools, both with other securities regulators and with banking and payments regulators, can strengthen the ability of authorities to protect their domestic investors and ensure stablecoin market transparency.

In this context, the IOSCO *Principles covering Cooperation in Regulation* could be important when assessing global stablecoin arrangements, by encouraging a broad range of cross-border cooperation and information sharing. The relevant principles are:

- **IOSCO Principle 13** – The Regulator should have authority to share both public and non-public information with domestic and foreign counterparts.
- **IOSCO Principle 14** – Regulators should establish information sharing mechanisms that set out when and how they will share both public and non-public information with their domestic and foreign counterparts.
- **IOSCO Principle 15** – The regulatory system should allow for assistance to be provided to foreign regulators who need to make inquiries in the discharge of their functions and exercise of their powers.

Enforcement Cooperation

IOSCO's *Multilateral MoU Concerning Consultation and Cooperation and the Exchange of Information* (MMoU) and the *Enhanced Multilateral MoU Concerning Consultation and Cooperation and the Exchange of Information* (EMMoU) will be relevant and may facilitate exchange of relevant information amongst members with respect to enforcement.

The MMoU, developed based on the Principles 13, 14 and 15 above, assists the signatories to the MMoU to exchange confidential information (including banking records, data, documents, metadata, recordings, and images, among others) to help them enforce their laws and regulations. Currently, there are 124 authorities that are signatories to the MMoU, both from developed and developing jurisdictions. IOSCO's MMoU Screening Group assesses and determines whether the prospective signatory fully complies with the standards of cooperation. Only applicants that fully comply with the standards of cooperation are admitted as signatories. IOSCO's MMoU Monitoring Group, monitors jurisdictions' adherence to the MMoU.

The IOSCO Enhanced MMoU (EMMoU) covers new areas, including subscriber records held or maintained by internet service providers, and other electronic communication providers, who are located within the jurisdiction of the requested authority, that identify subscribers (name and address), payment details, length of service, type of service utilised, network addresses, and session times/dates and durations.

Supervisory Cooperation

Due to their inherently cross-border nature, global stablecoins are also likely to create the need for cooperation in the area of supervision. Supervisory cooperation will therefore be essential to enable cooperation and coordination between regulatory authorities. In that context, IOSCO's *Principles on Cross-Border Supervisory Cooperation* published in 2010 can assist securities regulators in determining the form of cooperation best suited to the regulatory task at hand and by outlining the critical issues that regulators should agree upon outside of enforcement matters. These Principles remain valid in the context of stablecoins as they can assist financial regulators in identifying common concerns.

One tool – for example – that is discussed within the Report is the use of supervisory colleges. In the securities area, IOSCO published a *Report on Supervisory Colleges for Credit Rating Agencies* in 2013,[75] noting the challenges that the dispersion of internationally active CRAs present for domestic supervisors and promoting the use of colleges for these internationally active CRAs. Global stablecoins may similarly have global reach and raise novel risk issues; and can benefit from the supervisory cooperation applied to CRAs as indicated in IOSCO's Report.

However, to achieve effective cross-border oversight, information sharing is also an important condition of any cooperation agreement. Many jurisdictions have therefore used the sample annotated MoU developed by IOSCO in designing their bilateral supervisory arrangements. These types of agreements may also need to be explored for stablecoins as part of a wider supervisory cooperation strategy.

Deepening supervisory cooperation was identified as a key area to explore further by IOSCO and its Members in its *Report on Market Fragmentation and Cross-Border Regulation*.[76] IOSCO will therefore investigate ways to encourage supervisory cooperation, beginning with a review, as appropriate, of the 2010 *Principles for Supervisory Cooperation* and a review of the use of supervisory colleges to identify good practices in the establishment and conduct of existing and future colleges. Where appropriate, IOSCO will also identify practical issues which could be raised or usefully addressed through colleges and potential ways to increase their use. This work may provide further insights for the supervision of stablecoins.

Finally, IOSCO's 2015 *Report on Cross-Border Regulation* provides authorities with a toolkit of cross-border regulatory options and considerations. This toolkit has been used by authorities in other financial sectors and may assist regulators in developing, implementing and evaluating cross-border approaches with regards to stablecoins too in the future.[77]

---

75 IOSCO (2013), *Supervisory Colleges for Credit Rating Agencies,* July.

76 IOSCO (2019), *Market Fragmentation & Cross-border Regulation*, June.

77 IOSCO Task Force on Cross-Border Regulation Final Report.

Annex 5: Potential elements that could be used to determine whether a stablecoin qualifies as a GSC

A stablecoin's global systemic importance could be measured in terms of the impact that a stablecoin arrangement's financial or operational disruptions, or failure, can have on the global financial system and wider economy.

Given that a stablecoin may be used as a means of payment or store of value, and could be used in multiple jurisdictions, the criteria to be considered in determining whether a stablecoin qualifies as a GSC should take into account the potential uses in multiple jurisdictions.

The potential elements set out below that could be used to determine whether a stablecoin qualifies as a GSCs build on the criteria that are often considered in determining the need for or degree of regulation, supervision, and oversight of FMIs (PFMI, 2012), and global systemically important banks (BCBS, 2013). They include factors that could contribute to proliferation and considerations for authorities to determine whether a stablecoin has the potential to expand reach and adoption across multiple jurisdictions and has the potential to achieve substantial volume. Such potential elements are:

(i) Number and type of stablecoin users

(ii) Number and value of transactions

(iii) Size of reserve assets

(iv) Value of stablecoins in circulation

(v) Market share in cross-border use in payments and remittances;

(vi) Number of jurisdictions with stablecoin users

(vii) Market share in payments in each jurisdiction

(viii) Redemption linked to a foreign currency or multiple currencies

(ix) Interconnectedness with financial institutions

(x) Integration with digital services or platforms (e.g. social networks, messaging applications)

(xi) Available alternatives to using the GSC as a means of payment at short notice

(xii) Business, structural and operational complexity