4.3 Stablecoins

Return to Common Elements | **Provide Feedback**

Overview

Return to Top

Stablecoins is a category of cryptocurrencies attempting to control price volatility and achieve price stability by linking the value of the Coins offered by the cryptocurrency to an external asset.

- **Stablecoins** are cryptocurrencies that attempt to peg their market value to some external reference.
- **Stablecoins** may be pegged to a currency like the U.S. dollar or to a commodity's price, such as gold.
- **Stablecoins** achieve their price stability via collateralization (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives.

CB Insights defines four types of Stablecoins as depicted in Figure 1[1)].

Figure 1: CB Insights defines four classes of Stablecoins[2)]

CB Insights defines the four classes of Stablecoins as follows[3)]:

- **Fiat-Collateralized Stablecoins** are the most common type of Stablecoins that are collateralized, or backed, by a fiat currency and are generally backed at a 1:1 ratio, meaning 1 Stablecoin is equal to 1 unit of currency. So for each Stablecoin that exists, there is (theoretically) one real fiat currency being held in a bank account to back it up.
- **Commodity-Collateralized Stablecoins** are backed by other kinds of interchangeable assets. The most common commodity to be collateralized is gold. However, there are also Stablecoins backed by oil, real estate, and various precious metals. Holders of commodity-backed Stablecoins are essentially exposed to the value of a real-world asset.
- **Crypto-Collateralized Stablecoins** are Stablecoins backed by a “basket” of other cryptocurrencies. In theory, allowing crypto-backed Stablecoins to be more decentralized than their fiat-backed counterparts since everything is conducted using blockchain technology. To reduce price volatility risks, these Stablecoins are often over-collateralized to help absorb price fluctuations in the collateral.
- **Non-Collateralized Stablecoins** are not backed by anything tangible. An example is the US Dollar, which decades ago was backed by gold. However, the US Dollars are still perfectly stable because people believe in their value. Generally, these types of coins use an algorithmically governed approach to control the Stablecoin supply.

Global StableCoins (GSC)

Return to Top

The U.S. CBDC could be implemented using a Stablecoin.

As with many financial services available over the internet, the technological infrastructure underlying Stablecoins are not restricted to a geographic region. When a Stablecoins becomes popular to man End Users in multiple jurisdictions, it may become a Global StableCoin (GSC). A major confronting GSC are the numerous National laws and regulations in the various jurisdictions. For more details, see the following sections:

- U.S. National Privacy Considerations
- U.S. National Security Considerations
- International Considerations

GSCs are not without their vulnerabilities. These have been elaborated by The Financial Stability Board[4] in Table 1.

Table 1: Examples of vulnerabilities and related functions and activities in a Global StableCoin (GSC) arrangement (stylised presentation)[5]

Type of Vulnerability	**Main Determinants**	**Functions and Activities Primarily Concerned**
Financial exposures in the Global StableCoin (GSC) arrangement, giving rise to market, liquidity and credit risks.	1. Choice, composition, and management of the GSC reserve assets 2. Robustness of liquidity provision by GSC resellers/market makers 3. The ability of actors in the GSC arrangement to employ leverage	1. Governing the GSC arrangement 2. Issuing, creating, and destroying GSCs 3. Managing reserve assets 4. 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.	1. Reliability and resilience of the GSC's ledger and validation mechanism, including validator nodes 2. The capacity of the network to validate and process large volumes of transactions	1. Reliability of custodians/trustees 2. Governing the GSC arrangement 3. Operating the infrastructure 4. Validating transactions 5. 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	1. Effectiveness of governance in preventing fraud 2. Operational resilience 3. Clarity and robustness of claims that users have[6] 4. Robustness of liquidity provision by GSC resellers/market-makers	1. Governing the GSC arrangement 2. Storing of private keys providing access to GSCs 3. Exchanging, trading, reselling, and market-making of GSCs

The type of regulatory coverage of Stablecoin activities varies by jurisdiction.

> *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, and investor and consumer protection regulations, also apply to Stablecoin activities like issuance, exchanging, and trading of Stablecoin.* See the Table 2 on potential vulnerabilities arising from Stablecoin activities.[7)]

Table 2: Examples of vulnerabilities, regulatory tools, and international standards by activity of a Global StableCoin (GSC) arrangement[8)]

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 Global StableCoin (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 decentralized 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 government bodies of centralized 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 for 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 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. [9)] For GSC arrangements deemed to perform systemically important payment system functions or other FMI functions that are systemically important, the PFMI applies. On the basis of a preliminary analysis, some of the most relevant principles regarding these vulnerabilities would be those on a 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[10)] covering Cooperation in regulation (Principles 13 to 15), IOSCO's Multilateral MoU Concerning Consultation and Cooperation and the Exchange of Information,[11)]the Enhanced Multilateral MoU Concerning Consultation and Cooperation and the Exchange of Information,[12)] IOSCO's Principles on Cross-Border Supervisory Cooperation[13)] of May 2010, the cross-border regulatory cooperation aspect of the IOSCO 2015 Cross-Border Regulation Task Force Report[14)] and the work of the Follow-Up Group to address potential regulatory arbitrage).

Regulatory authorities and potential tools to address the vulnerabilities			
Activities	**Vulnerabilities**	**Authority/Tool**	**Relevant international standard**
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 applies. 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 Regulation of Exchange Traded Funds (2013)[15] 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),[16] IOSCO Principles for the Regulation of Exchange Traded Funds or IOSCO Policy Recommendations for MMFs (2012). [17] For GSC arrangements deemed to perform systemically important payment system functions or other FMI functions that are systemically important, the PFMI applies. 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.

Regulatory authorities and potential tools to address the vulnerabilities			
Activities	**Vulnerabilities**	**Authority/Tool**	**Relevant international standard**
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).[18)] For GSC arrangements deemed to perform systemically important payment system functions or other FMI functions that are systemically important, the PFMI applies. 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.
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 applies. On the basis of a preliminary analysis, some of the most relevant principles regarding these vulnerabilities would be those on a framework for the comprehensive management of risks and settlement. See Annex 4 on CPMI-IOSCO preliminary analysis.

Regulatory authorities and potential tools to address the vulnerabilities			
Activities	**Vulnerabilities**	**Authority/Tool**	**Relevant international standard**
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 applies. On the basis of a preliminary analysis, some of the most relevant principles regarding this vulnerability would be 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 a 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 perform systemically important payment system functions or other FMI functions that are systemically important, the PFMI applies. On the basis of a preliminary analysis, a relevant principle regarding these vulnerabilities would be an operational risk. See Annex 4 on CPMI-IOSCO preliminary analysis.
Exchanging, trading, reselling and market making of stablecoins	Withdrawal of liquidity provision by authorized resellers/market makers Disruption of a trading platform. Fraud, market manipulation, unauthorized transactions Cyber incident	Liquidity and other financial risk safeguards Settlement finality requirements Allocation of legal responsibility for unauthorized transactions Cyber security and other operational resiliency safeguards AML/CFT and sanctions controls	FATF Standards apply to all businesses carrying out trading/exchanging activity. The FATF Standards do not explicitly apply to peer-to-peer transactions without the use of a VASP or financial institution. 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 applies. See Annex 4 on CPMI-IOSCO preliminary analysis. Issues Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms (2020)[19], discussing IOSCO Principles[20], [21], [22] and associated IOSCO reports.

Stablecoin Theoretical User Scenario

Return to Top

> **Note:** The following Stablecoin Theoretical User Scenario is only provided for discussion purposes. Actual User Scenarios would be developed during systems analysis and modeled using a Model-Based Systems Engineering (MBSE) approach and address the problem is far more detail with a team of experts.

In the following example, the CBDC is modeled as Stablecoins, each account representing an End User. The End Users would actually "own" a wallet that contains account information, where Stablecoins are recorded as a balance that can be added to or subtracted from. For example, a retail purchase would deduct the amount of the purchase from the customer End User's account and add it to the Store's account.

Figure 2 represents a stylized use of a Stablecoin flow of a consumer (End User) buying a product from a retail store.

Figure 2:

- Table 3 represents the initial contents of a Stablecoins of an End User. Each Stablecoin balance in the wallet, such as the \$1,489.72 balance, is signed by the owner of the Stablecoin Wallet.
- Table 4 represents the initial contents of at Stablecoins Till at a store. Each Stablecoin, such as the $1,910.00 balance, is signed by the store that owns the Stablecoin Till.

Table 3: Example of the initial contents of an End User Stablecoin Wallet.

Account	Balance
98761234	$1,489.72
TOTAL	$1,489.72

Table 4: Example of the initial contents of a store's Stablecoin Till.

Account	Balance
456712349876	$1,910.00
TOTAL	$1,910.00

In this example, the End User's Stablecoin Wallet is used to purchase an item in a store that lists for \$488.78.

Table 5 provides a possible withdrawal from the End User's Stablecoin Wallet. If the withdrawal is accepted by the Stablecoin Wallet's owner, the Stablecoin ownership is changed to the stores.

Table 5: The Stablecoin from the wallet required to make the \$488.78 purchase.

Item	Quantity	Sum
8642-97531	1	$488.78
TOTAL		$488.78

> **Note:** there are many ways the \$488.78 could have been achieved using the Stablecoin Wallet provided in Table 3. This is one way. In an actual implementation, the contents of the composition

of cash could be modified by the End User as long as it summed to \$488.78, just as would occur in a real wallet.

- Table 6 represents the contents of the Stablecoin Wallet of the End User after the transaction.
- Table 7 represents the contents of the Stablecoin Till of the store after the transaction.

Table 6: Example of a Stablecoin Wallet and its contents for an End User after transaction.

Account	Balance
98761234	\$1,000.94
TOTAL	\$1,000.94

Table 7: Example of a Stablecoin Wallet and its contents for a store after transaction.

Account	Balance
456712349876	\$2,398.78
TOTAL	\$2,398.78

Examples

Return to Top

In this discussion, only the requirements were identified during the White Paper Analysis are considered. Table 8 represents the allocated of requirements germane to the Stablecoins.

Table 8: Example of mapping a subset of requirements identified during the White Paper Analysis conducted by the OMG's CBDC WG

Area	Desirements
Benefits	B0016, B0017, B0021
Policy and Considerations	P0008, P0015, P0016
Risks	R0010, R0022

Note: B = Benefit, **P** = Policy, **R** = Requirement, **D** = Design.

Discussion of Examples

Return to Top

Table 9: List of requirements (i.e., desirements) identified in the **White Paper** that require further research

Desirement No.	Desirement Text	Comment
B0016	**Provide Stablecoins that are:** **1. well-designed** **2. appropriately regulated**	Stablecoin is a specific solution
B0017	**Provide Stablecoins that are:** **1. faster** **2. more efficient** **3. more inclusive payment**	Stablecoin is a specific solution
B0021	**Maintain value by not using backing by an underlying asset**	**Conflict** with **B0017**

Desirement No.	Desirement Text	Comment
P0015	**The PWG report recommends that Congress act promptly to enact legislation that would ensure payment of stablecoins**	Stablecoin is a specific solution
P0016	**The PWG report recommends payment stablecoin arrangements are subject to a consistent and comprehensive federal regulatory framework**	Stablecoin is a specific solution
R0010	**CBDC has Risk of significant energy footprint similar to Cryptocurrencies**	This depends on the Consensus Algorithm used for the Stablecoin.
R0022	**Risk of stablecoins and other types of nonbank money shifting deposits away from banks even without a CBDC**	Stablecoin is a specific solution
B = Benefit Considerations		
P = Policy Considerations		
R = Risk Considerations		
D = Design Considerations		

1) 2) 3)
CB Insights, What Are Stablecoins?, 25 January 2022, Accessed: 20 March 2022, https://www.cbinsights.com/research/report/what-are-stablecoins/

4) 5) 7)
The Financial Stability Board, Regulation, Supervision, and Oversight of "Global Stablecoin" Arrangements Final Report and High-Level Recommendations, 13 October 2020, Accessed: 26 April 2022, https://www.fsb.org/wp-content/uploads/P131020-3.pdf

6)
Including whether or not users have a right to redeem at par in fiat.

8)
The Financial Stability Board, Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements Final Report and High-Level Recommendations, 13 October 2020, Accessed: 26 April 2022, https://www.fsb.org/wp-content/uploads/P131020-3.pdf

9)
Enhanced Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information (EMMoU), 2016, 2017, Accessed: 26 April 2022, https://www.iosco.org/about/?subsection=emmou

10) 21)
International Organization of Securities Commissions, Objectives and Principles of Securities Regulation, May 2017, Accessed: 26 April 2022, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD561.pdf

11) 22)
International Organization of Securities Commissions, Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information (MMoU), 2022, Accessed: 26 April 2022, https://www.iosco.org/about/?subsection=mmou

12)
International Organization of Securities Commissions, Enhanced Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information (EMMoU), 2016, 2017, Accessed: 26 April 2022, https://www.iosco.org/about/?subsection=emmou

13)
Technical Committee of the International Organization of Securities Commissions, Principles Regarding

Cross-Border, Supervisory Cooperation, Final Report, May 2010, Accessed 26 April 2022, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD322.pdf
14)

The Board of the International Organization of Securities Commissions, IOSCO Task Force on Cross-Border Regulation, Final Report, September 2015, Accessed: 26 April 2022, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD507.pdf
15)

Board of the International Organization of Securities Commissions, Principles for the Regulation of Exchange Traded Funds Final Report, June 2013, Accessed: 26 April 2022, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD414.pdf
16)

International Organization of Securities Commissions, IOSCO issues recommendations and good practices to improve liquidity risk management for investment funds, IOSCO/MR/02/2018, 1 February 2018, Accessed: 26 April 2022, https://www.iosco.org/news/pdf/IOSCONEWS486.pdf
17)

International Organization of Securities Commissions, IOSCO Consults on Money Market Fund Systemic Risk Analysis and Reform Options, OSCO/MR/07/2012, 27 April 2012, Accessed: 26 April 2022, https://www.iosco.org/news/pdf/IOSCONEWS232.pdf
18)

International Organization of Securities Commissions, IOSCO Publishes Recommendations Regarding the Protection of Client Assets, IOSCO/MR/03/2013, 8 February 2013, Accessed: 26 April 2022, https://www.iosco.org/news/pdf/IOSCONEWS265.pdf
19)

International Organization of Securities Commissions, IOSCO publishes key considerations for regulating crypto-asset trading platforms, IOSCO/MR/03/2020, 12 February 2020, Accessed: 26 April 2022, https://www.iosco.org/news/pdf/IOSCONEWS556.pdf
20)

Financail Stability Board, Objectives and Principles of Securities Regulation, 31 May 2017, Accessed: 26 April 2022, https://www.fsb.org/2017/05/cos_100601/