

Question: 06. TBD Could a CBDC adversely affect the financial sector? How might a CBDC affect the financial sector differently from stablecoins or other nonbank money?

[Return to CBDC Benefits, Risks, and Policy Considerations](#)

Question

[Return to Top](#)

1. **Could a CBDC adversely affect the financial sector?**
2. **How might a CBDC affect the financial sector differently from Stablecoins or other nonbank money?**

Answer

[Return to Top](#)

Overview

[Return to Top](#)

To answer the question it is important to first define what is meant by [Financial Sector](#), [Financial Market](#) and [Clearinghouse](#)

The **Financial Sector** refers to businesses, firms, banks, and institutions providing financial services and supporting the economy and encompasses several industries such as banking and investment, consumer finance, mortgage, money markets, real estate, insurance, retail, etc. The adoption of a U.S. CBDC will not affect all of the Financial Service industries and it will not affect each one in the same way. In general terms, the **Financial Sector** is used as an indicator of the health of the economy because it generates revenue through interest rates, mortgages, loans, debt finance, and capital funds, consequently spurring economic growth meaning the weaker the Financial Sector, the weaker the economy. This is why the question is so important.



Figure 1: The Composition of the Financial Services

Sometimes, the Financial Sector is falsely equated to [Financial Markets](#) which is a broad term and includes various types of markets where companies requiring investment can borrow money at a low cost.

These financial markets are regulated by independent regulatory bodies with strict rules and regulations. They have stringent and mandatory reporting and compliance standards. Any violation by companies, investors, brokers, banks, financial institutions, or any other authorized bodies can lead to heavy penalties and, in extreme cases, cancellation of license.¹⁾

Figure 2 provides a graphical representation of the composition of the Financial Markets.



Figure 2: The Composition of the Financial Market

At the heart of the U.S. CBDC (Stablecoin) will be a [DIDO Platform](#) (i.e. [Ethereum](#), [Hyperledger](#), [Iota](#), [Hedera](#), etc.). Each DIDO Platform has its own [Consensus Mechanism](#) (i.e., [Proof-of-Work \(PoW\)](#), [Proof-of-Stake \(PoS\)](#), etc.). Within the U.S. CBDC, the [DIDO Platform Consensus](#) will act as a Clearinghouse for [Transactions](#) within the DIDO Platform (see Figure 3).



Figure 3: The relationship between a buyer, a seller and a Clearinghouse.

1. Could a CBDC adversely affect the financial sector?

[Return to Top](#)

Technically

[Return to Top](#)

Each of the **Financial Sector** components will respond differently to the use of a U.S. CBDC depending on how much they want to support the use of CBDC as an alternative to the approved Clearinghouse. The Financial Sectors normally using U.S. Dollars on both sides of a transaction could use something like the [ACH/CBDC network proposal](#) (see Figure 4. This should require a minimum of change in their current processes and require them to be able to hold U.S. Dollars and U.S. CBDC in the pertinent accounts. The main benefit of using a CBDC Network should be the increase in speed (almost real-time) for settlements since the U.S. CBDC will use an automated [Consensus Mechanism](#). However, in order to check for Privacy and Criminal Activity by enforcing the [National Privacy Concerns](#) and [National Security Concerns](#) as well as respecting [International Concerns](#), the Consensus process most likely needs to be extended to help enforce the existing laws and regulations. This extension could rely heavily on the use of [Artificial Intelligence \(AI\)](#) and [Intelligent Agents](#).



Figure 4: Theoretical Very Simplified Dual ACH-CBDC Network Concept.

For those **Financial Sector** components that use U.S. Dollar-to-Asset transactions, the appropriate Clearinghouses could also support U.S. CBDC-to-Asset the speed of the clearing may be faster since securing the U.S. CBDC would be near real-time.

For those **Financial Sector** components that do not use U.S. Dollar to Dollar transactions, the individual Clearinghouses need to address the problem individually

Reputation

[Return to Top](#)

Obviously, if there is a breach or hack in the U.S. CBDC, all the **Financial Sector** components would be affected. See the existing [Risks](#) identified in the **White Paper** and the response to [q11](#).

2. How might a CBDC affect the financial sector differently from Stablecoins or other nonbank money?

[Return to Top](#)

There is an entire section on Stablecoin. See section [30_stablecoins](#).

Currently, Stablecoins and nonbank money need to be converted to U.S. Dollars in order for the money to be used within the financial sector.

Organization	Acronym	About	Summary
Basel Committee on Banking Supervision	BCBS	The Basel Committee on Banking Supervision (BCBS) is the primary global standard-setter for the prudential regulation of banks and provides a forum for regular cooperation on banking supervisory matters. Its 45 members comprise central banks and bank supervisors from 28 jurisdictions.	

Organization	Acronym	About	Summary
Financial Action Task Force	FATF	The Financial Action Task Force (FATF) is the global money laundering and terrorist financing watchdog. The inter-governmental body sets international standards that aim to prevent these illegal activities and the harm they cause to society. As a policy-making body, the FATF works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas. With more than 200 countries and jurisdictions committed to implementing them. The FATF has developed the FATF Recommendations, or FATF Standards, which ensure a coordinated global response to prevent organized crime, corruption, and terrorism. They help authorities go after the money of criminals dealing with illegal drugs, human trafficking, and other crimes. The FATF also works to stop funding for weapons of mass destruction. The FATF reviews money laundering and terrorist financing techniques and continuously strengthens its standards to address new risks, such as the regulation of virtual assets, which have spread as cryptocurrencies gain popularity. The FATF monitors countries to ensure they implement the FATF Standards fully and effectively and holds countries to account that does not comply.https://www.fatf-gafi.org/about/	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”. 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. 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 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 the 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, so-called Stablecoins will either be considered to be virtual assets or traditional financial assets depending on their exact nature. A range of the entities involved in any so-called Stablecoins 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 Stablecoins, particularly the extent to which the functions of the so-called Stablecoins are centralized or decentralized, and what activities the entity undertakes. ²⁾

Organization	Acronym	About	Summary
Committee on Payments and Market Infrastructures	CPMI	The Committee on Payments and Market Infrastructures (CPMI) is an international standard-setter that promotes, monitors, and makes recommendations about the safety and efficiency of payment, clearing, settlement, and related arrangements, thereby supporting financial stability and the wider economy. The CPMI also serves as a forum for central bank cooperation in related oversight, policy, and operational matters, including the provision of central bank services. https://www.bis.org/cpmi/about/overview.htm	
International Organization of Securities Commissions	IOSCO		

Table 1: Examples of vulnerabilities and related functions and activities in a [StableCoin \(GSC\)](#) arrangement (stylised presentation)³⁾

Type of Vulnerability	Main Determinants	Functions and Activities Primarily Concerned
Financial exposures in the StableCoin (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 have⁴⁾ - 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

Table 2: Examples of vulnerabilities, regulatory tools, and international standards by activity of a Blobale

StableCoin (GSC) arrangement⁵⁾

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 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 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. ⁶⁾ 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 Principles⁷⁾ covering Cooperation in regulation (Principles 13 to 15), IOSCO's Multilateral MoU Concerning Consultation and Cooperation and the Exchange of Information,⁸⁾ the Enhanced Multilateral MoU Concerning Consultation and Cooperation and the Exchange of Information,⁹⁾ IOSCO's Principles on Cross-Border Supervisory Cooperation¹⁰⁾ of May 2010, the cross-border regulatory cooperation aspect of the IOSCO 2015 Cross-Border Regulation Task Force Report¹¹⁾ 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 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 Regulation of Exchange Traded Funds (2013) ¹²⁾ 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), ¹³⁾ IOSCO Principles for the Regulation of Exchange Traded Funds or IOSCO Policy Recommendations for MMFs (2012). ¹⁴⁾ 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.

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). ¹⁵⁾ 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.
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	
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.

Regulatory authorities and potential tools to address the vulnerabilities			
Activities	Vulnerabilities	Authority/Tool	Relevant international standard
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 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. Fraud, market manipulation, unauthorised transactions Cyber incident	Liquidity and other financial risk safeguards Settlement finality requirements Allocation of legal responsibility for unauthorised 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 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 apply. See Annex 4 on CPMI-IOSCO preliminary analysis. Issues Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms (2020) ¹⁶⁾ , discussing IOSCO Principles ¹⁷⁾ , ¹⁸⁾ , ¹⁹⁾ and associated IOSCO reports.

- 1)
Madhuri Thakur and Dheeraj Vaidya, What is the Financial Market?, Wall Street Mojo, Accessed: 25 April 2022, <https://www.wallstreetmojo.com/financial-market/>
- 2) 3) 5)
, ,
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>
- 4)
Including whether or not users have a right to redeem at par in fiat.
- 6)
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>
- 7) 18)
,
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>
- 8) 19)
,
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>

9)

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>

10)

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>

11)

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>

12)

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>

13)

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>

14)

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>

15)

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>

16)

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>

17)

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

From: <https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link: https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:20_comments:brp:q06:start&rev=1651037471

Last update: 2022/04/27 01:31

