15 July 2020

To: Financial Stability Board

Email: fsb@fsb.org

RESPONSE TO THE CONSULTATIVE DOCUMENT – ADDRESSING THE REGULATORY, SUPERVISORY AND OVERSIGHT CHALLENGES RAISED BY "GLOBAL STABLECOIN" ARRANGEMENTS

Dear Sir/Madame

First, I hope this finds you all well and safe in these current circumstances.

I would like to thank you for the opportunity to participate in the discussion on Stablecoin developments and provide my feedback on the Consultative Document '**Addressing the regulatory, supervisory and oversight challenges raised by "global Stablecoin" arrangements'** from 14 April this year.

In my professional experience, I have worked with various materials from the Financial Stability Board - notably, relating to Risk Appetite Framework, Risk Culture, Recovery and Resolution Planning, Bail-In, TLAC, FinTech, etc. – and would like to comment on a few brief observations which I feel strongly about based on my area of practice and previous projects, specifically around:

- Governance of Stablecoin arrangements,
- Internal validation/verification, and
- Internal audit.

Hope my comments make sense and support your ongoing work on regulatory developments of Stablecoin arrangements.

Feel free to contact me if you have any queries.

Regards,

Pavel Burkov, PhD
pburkov@gmail.com
+44(0)7714153539

Summary of responses

1. Do you agree with the analysis of the characteristics of stablecoins that distinguish them from other crypto-assets?

Yes, in principle I agree with the definition and analysis of Stablecoin characteristics and it does reflect current understanding across the industry and other researchers. Additionally, I can mention a couple of points that may be worth reflecting for a more complete landscape of digital assets/currencies:

a) *Synthetic CBDC as a form of Stablecoin arrangement.* There is ongoing research around Central Bank Digital Currencies ('CBDC') and, specifically, "synthetic CBDC" which can be seen as an extension to Stablecoin arrangements. In a broader context, these arrangements include Stablecoin providers with access to central banks' reserves, i.e., "*central bank could require stablecoin providers to back coins with central bank reserves*" [Adrian, T, and T Mancini-Griffoli (2019), "The rise of digital currency", IMF Fintech Note 19/01].

b) *Dependencies between CBDC and Stablecoin developments.* Developments of Stablecoins and CBDCs are simultaneously progressing from the public and private sectors. In some way, the emergence of CBDCs initiatives by monetary authorities' was in response to the rapid development of private Stablecoin initiatives since 2019. Hence, there may be a dynamic link between Stablecoin and CBDC, both evolving in direct competition with each other that may trigger additional risks, vulnerabilities to the financial system.
The Consultative Document does not specifically mention CBDCs and potential influence on Stablecoins initiatives, only broadly referring to "*issues related to central bank digital currencies are also outside the scope of the analysis*". Understandably, the purpose of the document is focused on Stablecoins. Although, both instruments are interlinked and recent CBDC developments certainly drive the evolution of Stablecoin arrangements and their characteristics (incl. proposals for global/cross-border CBDC and potential 'synthetic hegemonic currency').

5. Do you agree with the analysis of potential risks to financial stability arising from GSC arrangements? What other relevant risks should regulators consider?

In general, the distinction between "Potential risks to financial stability" and "Vulnerabilities arising from the functions and activities" is a reasonable construct to facilitate further analysis. Indeed, the boundary and delineation between "risk outcomes" and "vulnerabilities" may be subject to individual interpretation with potential overlaps and further granularity.

The observations below may provide additional context to GSC holistic analysis and specific concerns:

a) *Assumptions about exclusion of wider monetary issues.* The assumption that monetary issues are taken outside of the scope of the Consultative Document may be challenged, i.e. "*Wider issues such as monetary policy, monetary sovereignty, currency substitution, data privacy, competition, and taxation issues are beyond scope*". Stablecoins can impact monetary stability (especially, for EMDC economies and in case of widely used GSCs) and may represent a significant risk to the global financial system. Therefore, excluding this topic from the analysis undermines the purpose of holistic approach and provided a partial view for discussion on supervisory, regulatory and oversight challenges.

b) *Additional emerging channels of risks to financial stability* associated with Stablecoin arrangements which were not clearly referenced in the Consultative Document (although, can be mapped to existing 'risk channel' or considered as separate items):

- ***Impact on monetary policy*** – as above, although monetary policy and issues are taken out of the scope of the Consultative Document, the importance of Stablecoin arrangements for national/international monetary policies is deemed to be quite substantial and, in my view, should be included in the full picture.

- ***Dependency on new players, specifically BigTech companies*** –financial regulations around BigTech companies and their involvement in Stablecoin and other financial services is still a relatively new topic for research and regulatory coverage. From my individual's perspective, it is growing in importance and even more so with the introduction of private Stablecoin arrangements by these companies. Financial services are a supplement to the core business models of such players and their approach to financial products may be different from incumbent financial institutions that may lead to financial stability risks, especially through the extensive global reach of such companies and mix with other activities.

- ***Reliance on smart contracts and algos embedded into blockchains/GSCs*** – together with the acceleration of Stablecoins, CBDC, crypto-assets, DLT, and other innovative payment solutions, there may be a greater reliance on automated features of programmable money and embedded functionality within Stablecoin ledgers that will operate quite independently and subject to inherent glitches in the code. Furthermore, for algorithmic-based stabilisation mechanism, there will be greater reliance on automated functionality and logic to maintain price stability.

- ***Forks* -** potential use case would be a creation of a separate fork of a well-established and widely accepted GSC arrangement which may bring substantial damage to the financial system and lead to substantial loss of confidence and trust of entire Stablecoin ecosystem. Due to materiality, this may be considered as a separate risk channel in addition to 'operational disruption' of payment processing.

- ***Fraud schemes and illegal activities*** – existing examples and history of some ICOs have indicated that various Coin arrangements can be set-up with fraudulent and malicious purposes (incl. Ponzi schemes). Regulators have been flagging a number of risks and concerns about customer protection and the use of new digital currencies for illegal activities as well.

6. Do you agree with the analysis of the vulnerabilities arising from various stablecoin functions and activities (see Annex 2)? What, if any, amendments or alterations would you propose?

Analysis of GSC vulnerabilities was reflected in the following sections of the Consultative Document:

- Section 2.2. Vulnerabilities arising from the functions and activities of a GSC arrangement
- Section 2.2. Table 2: Examples of vulnerabilities and related functions and activities in a GSC arrangement and (stylised presentation)
- Annex 2: Examples of vulnerabilities, regulatory tools, and international standards by activity of a GSC arrangement

Conceptually, the overall logic makes sense and it was possible to follow across the different sections. In terms of specific amendments and alterations, I would like to highlight the following additional considerations:

a) *Consistency and clarification of "governance"-related vulnerabilities and mappings per functions/activities.* Looking specifically into the 'governance' component, there is some ambiguity within the document whether this is considered as one of the key functions of GSC arrangement or a more peripheral topic. It is reflected in "**Table 1: Functions and activities in a stablecoin arrangement**" (p. 10) and in **Annex 2** (p. 34). However, it is not clearly defined as a function within GSC arrangements in section "**1.2. Combination of multiple functions and activities"**. From the current industry perspective, governance of Stablecoin arrangements (especially in more decentralized projects) is clearly a challenging area and may need to be reflected accordingly in the Consultative Document.

Furthermore, all three high-level vulnerabilities were mapped to 'Governance' function (as per Table 2 on p. 14). Yet, specific reference to 'governance' is only explicitly mentioned in the description of the second vulnerability ("*…fragilities in the governance, operation and design of the GSC arrangement's infrastructure…*" – on p.13) and as a determinant in the third vulnerability ("*Effectiveness of governance in preventing fraud*" – p. 14). Nevertheless, this is also provided in a slightly different context from examples of vulnerabilities in Annex 2 relating to "*Establishing rules governing the stablecoin arrangement*" (p. 34) (ref. Appendix 1 below).

There is also a minor discrepancy that there is only a single activity mentioned "Establishing rules governing the Stablecoin arrangement" relating to "Governance of GSC arrangement" function (as per Table 1, p. 10). From experience, governance-related control frameworks should also refer to activities aimed at 'following the rules and mechanisms to enforce governance arrangements'.

b) *High level of aggregation in Vulnerabilities definitions and bundling of specific risk features.* There were some inconsistencies in terminology and details included across three sections of the Consultative Document and may need to be brought in sync in order to avoid misinterpretation of different mappings and definitions (based on my personal experience of working with other FSB material and document as a benchmark). Overall, the 3-4 top-level vulnerabilities are formulated at a very aggregated level bringing together various distinct components that are bundled together (e.g., risk types, descriptive risk exampled).

Potentially, additional components in the overall construct of 'risk outcomes' and 'vulnerabilities' may include:

- Risk-type taxonomy structure (starting from Risk Types, 'Top-Down' view) and

- Inventory of descriptive risks (based on specific use-cases, 'Bottom-Up' view).

From my perspective, such a combined view (ref. Appendix 2 below) will be more advanced and reflective of current Risk identification and management practices. This can also act as a toolkit for bringing together risk-type control frameworks and diverse universe of specific risk cases/examples. Ultimately, this will better align with professional practices of risk and control practitioners, especially in case of such an innovative, broad, and evolving topic.

11. Are there additional recommendations that should be included or recommendations that should be removed?

With regards to the Recommendations provided in the Consultative Document, I would like to suggest some additional context and clarification about greater alignment with 3Lines of Defense model and, specifically, about the roles of Internal Validation/Verification function and Internal Audit to promote more robust control environment and oversight within the Stablecoin arrangements internally. These may apply to the following recommendations:

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

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

Indeed, there is a clear reference made to Risk Management of GSCs as well as external audit requirements over valuation of reserve holdings (as with financial audits – on a periodic/annual basis with a time delay). Given the potential complexity of GSC arrangements and reliance on robust internal processes for day-to-day management, these two recommendations may be further expanded to bring into the picture specific references to:

- ***Internal verification and validation***, incl. attestations over internal processes based on expected principles/guidelines (may need to be developed), and
- ***Internal audit*** requirements to provide independent assurance over these areas and relevant attestations.

Presumably, these elements are already implicit in Risk Management and External audit requirements mentioned in the Recommendations. Nevertheless, based on my experience, I can say that if there is an explicit reference made to "Internal Validation" and "Internal Audit" expectations, the overall control environment and dedicated focus on day-to-day operations are usually much higher than in those cases when only implicit references exist. This is based on my experience of BCBS239 (requirements for 'internal validation'), AMA (requirements for 'internal validations of processes, data, methodologies'), Models (requirements for 'model validation'), Algo/Electronic trading (requirements for 'internal validation'), ICAAP (requirements for 'internal review'), etc.

I have also participated in a number of audits relating to complex subject matter and arrangements where no specific references to validation/internal audit existed. Although, these areas were still included in the scope of Risk Management Frameworks (i.e., through dedicated 2nd Line of Defense functions) and Internal Audit (by default, as 3rd LoD function) – this was usually in a much broader and indirect manner. Subsequently, the level of specificity and assurance provided was different and less compatible between different teams and organisations. That said, a generic approach also has its benefits as it provides an opportunity for a more robust coverage without a clear indication of a minimum level of standards, but this would be primarily driven by be-spoke relationships and individual interpretations of regulatory expectations and personal view on professional judgement.

Furthermore, having more clearly defined scope and practices of "internal validation" and "internal audit" roles may have a positive effect on the overall quality of the Risk Management Framework of GSC. It can also increase the reliance of external audit firms on internal assurance activities and, subsequently, reduce external audit fees of GSC arrangements.

As a suggestion, even making general references to "internal validation" to be performed by Risk Management/Compliance functions and independent assurance by "internal audit" will raise the bar for control environment requirements and, subsequently, level of trust in GSC arrangements from a third party and user perspective. It will also demonstrate greater adherence to the 3LoD concept which may be easier to follow through direct reference to a well-recognised 3LoD control framework concept.

APPENDIX 1 - References to ‘Governance’ in Vulnerabilities descriptions

Section 2.2. Vulnerabilities arising from the unctions and activities of a GSC arrangement	**Table 2: Examples of vulnerabilities and related functions and activities in a GSC arrangement (stylised presentation)**	**Annex 2: Examples of vulnerabilities, regulatory tools, and international standards by activity of a GSC arrangement**
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	**Financial exposures in the GSC arrangement, giving rise to market, liquidity and credit risks** Determinants: ▪ 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	**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
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.	**Weaknesses in the GSC infrastructure, giving rise to operational risk (including cyber risks) and risk of loss of data.** Determinants: ▪ 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	
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.	**Vulnerabilities in those parts of the GSC arrangement on which users rely to store, exchange and trade GSCs, including operational or fraud risk** Determinants: ▪ Effectiveness of governance in preventing fraud ▪ Operational resilience ▪ Clarity about the nature of claims that users have ▪ Robustness of liquidity provision by GSC resellers/market makers	

APPENDIX 2 – Risks/Vulnerabilities hierarchy

Table 2: Examples of vulnerabilities and related functions and activities in a GSC arrangement (stylised presentation)		**From Annex 2 – Vulnerabilities per processes** (and process to vulnerabilities mapping as per Table 2)
Core vulnerability/ weaknesses	Risk Types (Taxonomy – based)	Examples of descriptive risks
▪ Financial exposures in the GSC arrangement	▪ Market Risk ▪ Liquidity Risk ▪ Credit risk	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 Managing reserve assets ▪ Inability to meet redemptions in stressed conditions ▪ For algorithmic arrangements, errors in the issuance or redemption algorithm that impact value ▪ A sharp fall in price and/or liquidity of reserve asset(s) ▪ Change in reserve allocation across reserve asset ▪ 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 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
▪ Weaknesses in the GSC infrastructure	▪ Operational Risk ▪ Cyber Risk ▪ Loss of Data	Validating Transactions ▪ GSC ledger compromised due to failure of multiple validator nodes 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 Providing custody/trust services 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
▪ Vulnerabilities in those parts of the GSC arrangement on which users rely to store, exchange and trade GSCs	▪ Operational Risk ▪ Fraud risk	Storing the private keys providing access to stablecoins (wallet) ▪ Disruption of a wallet, for example theft of coins from digital wallet or operational (e.g. cyber) incident. ▪ Direct loss, including by consumers 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
▪ + Weaknesses in governance framework/ setting up and adherence to Stablecoin rules*	▪ Operational Risk ▪ Fraud	Governance of SGC arrangement/ 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

* Additional vulnerability added to reflect inherent weaknesses in Stablecoin governance