SIA Group
Views on the Report Global Stablecoins (GSC) - FSB Questionnaire
SIA Group is grateful to the Financial Stability Board for the opportunity to provide a contribution on the topic of Global Stable Coins Arrangements, an emerging phenomenon that can have a significant impact on international payment systems and on the financial industry as a whole. We agree on the importance of the topics and the setting of the Report and the objectives it sets itself.

The purpose of this document is to illustrate the answers provided SIA Group - in its quality of technological provider - in respect of the Questionnaire included in the FSB Consultative Document of the 14th April 2020, concerning the regulatory, supervisory and oversight challenges raised by "global stablecoin" agreements. The document also include a summary which synthetize the overall views of SIA Group with reference to the Questionnaire.

The summary (slide 2) focuses on the technological and infrastructural issues concerning GCS Arrangements, particularly dealing with the following topics:
- DLT permission model;
- Interoperability;
- Governance;
- Transactions audit;
- Cyber security.

Detailed answers to each question are reported in the continuation of the document (slide 3 to 17).
Executive summary

- DLT-based GSC would be better based on permissioned platforms whose features are better suited in order to provide security, reliability auditability and compliance to AML/ATF obligations.

- A DLT-based GSC Arrangement is likely to involve multiple technical infrastructures, hence a specific focus should be posed to interoperability issues, also in order to ensure the traceability of transactions among different jurisdictions.

- Where several entities are involved to perform the various functions and activities, Authorities should verify how the responsibility over the DLT platform operations are shared and regulated among the various entities. Authorities should have a clear understanding of corporate structure and decision-making chain related to the various functions and activities to prevent mismanagement at technical, operational and financial level.

- DLT-based GCS arrangement should include a role into the network with the right to audit the historical chain of transactions and enforce the rules underlying the network.

- DLT must be assessed from the perspective of cyber-security risks. International standards like ISO/IEC 27001 and COBIT 2019 framework as well as industry-specific guidelines like ECB "Cyber resilience oversight expectations for financial market infrastructures" could be used as a reference. A comprehensive analysis of the technological stack of the underlying technology of a GSC arrangements should address the following vulnerabilities: management of cryptography; performance limits and resource capacity; quality of the input data; communication protocol between nodes; consent protocol; immaturity of DLT and Smart Contracts. Such analysis should be extended to all the functional elements of the platform including digital wallets and custodian services.

- Regulatory oversight of the third parties should be ensured. GSCs are indeed completely new scenario from technical, operational, financial and regulatory point of view. Given such a novelty characteristics, even a consolidated Financial Institution could not have the capability to oversight the third parties involved in the arrangement. Regulator should thus exercise direct oversight over all the entities involved in the arrangement as long as a robust experience has been developed. Furthermore, in a more mature scenario, regulators should exercise direct oversight over third parties as it is currently done for critical service providers.

- A distinction between systemic and non-systemic GSC should also be considered in order to define more tight regulatory constraints for the former.
Characteristics of stablecoins

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

❑ Yes, we agree with the analysis of the characteristics of stablecoins that distinguish them from other crypto-assets. In particular, SIA agrees on the distinctive character of stablecoins which aims to reduce the fluctuation of its nominal value, which represents the main difference between stablecoins and other crypto-assets.

❑ In addition, we suggest to extend the definition of Stablecoin including: “mainly intended as a payment instrument or store of value. According to the specific regulatory framework in force in a given jurisdiction, Stablecoins can or can not be qualified as “funds” as defined, as an example, in EU Directive 2015/2366 (PSD2). According to the specific Arrangement, the issuer of a Stablecoin can or can not ensure the right to redemption of the coin into one or more fiat currencies”.

❑ Moreover, we suggest to integrate in the definition of Crypto Asset as follows:

"With the term Crypto Asset we refer to a unit of information that is:

• Electronically stored, typically over a distributed ledger;
• Not duplicable;
• Univocally associated to an address represented by an anonymous or pseudonymous owner;
• Exchangeable."
Are there stabilisation mechanisms other than the ones described, including emerging ones, that may have implications on the analysis of risks and vulnerabilities?

- The document addresses the stabilisation mechanism towards two generically accepted options: a “peg” to various financial assets, or an algorithm mechanism.

- In our opinion, there is the possibility to consider an additional stabilisation mechanism represented by integration of a flexible saving rate mechanism. The savings rate of a GSC is a specific extension of the stabilisation of its nominal value price, in addition to the stability fee represented by the reserve assets. The interest is variable, being adjusted from time to time by the governance of the GSC. If GSC’s market price is above its nominal value, interest is reduced. This action discourages GSC’s demand, causing GSC’s market price to adjust. The savings rate is a global parameter that must be frequently described to cope with short term changes in market conditions. On the other hand, raising interest is incentivizing holders to not spend their GSC, in order to stimulate GSC’s demand on the market and have a price growth effect.

- GSC arrangement can implement one or more mechanisms to encourage or discourage GSC holders in purchasing or exchanging coins by applying, for example, differentiated transaction fees and/or interests. Such a stabilisation mechanism could have negative effects on the whole system if a correct balance between the need of value stability and the need of smooth circulation of coins is not guaranteed.
Does the FSB properly identify the functions and activities of a stablecoin arrangement? Does the approach taken appropriately deal with the various degrees of decentralisation of stablecoin arrangements?

- Even though we agree on the analysis of the functions and activities identified by the FSB, we underline the following additional functions and activities:
  - Functions: interact with supervisory entities;
  - Activities: provide evidence of compliance-related fulfillment.
  In respect of the operational design elements, adequate tools and processes should be implemented to provide evidence to any relevant Authority in order to fulfill obligations required by applicable regulations.

- Regarding “transfer of coins” functions, SIA believes that a DLT-based GSC should be based on a permissioned structure, whose features are better suited in order to provide security, reliability and auditability.

- In a GSC scenario, it is possible that the arrangements will run on multiple technical infrastructure, since different jurisdictions are involved and therefore there cannot be a single infrastructure. In this sense, the capability for a GSC to be spendable, accessible and secured via interoperable technical facilities is a fundamental function of GSC.

- Furthermore, with reference to the governance framework, it’s important to note that the traceability of transactions among different jurisdictions and the aforementioned distinct technical infrastructure must be taken into account, and this has great impact on how KYC and AML procedures are implemented into a GSC arrangement scenario.

- It’s relevant to note that an higher degree of decentralisation has direct impact with the risks that holders must bear in lieu of a trusted party. For example, in a non-custodian model in which users holds and store their private keys, the effort related to securization and recovery of the private keys resides totally on the users.
What criteria or characteristics differentiate GSC arrangements from other stablecoin arrangements?

- In SIA opinion a stablecoin arrangement gets the status of GSC if:
  - an acceptance network enabling the use of GSC to buy products or services is active in multiple jurisdiction;
  - a distribution network that reduce the onboarding effort in multiple jurisdiction;
  - it is possible for the GSC holder to exchange the coin against multiple currencies (according to the various exchange rates);
  - for asset backed stablecoins, the basket of assets constituting the reserve includes assets denominated in several currencies.

- A GSC Arrangement that is meant to be globally accepted need to implement an audit process that will reduce to the maximum extent the possibility of a failover or unavailability of the underlying asset class.
Do you agree with the analysis of potential risks to financial stability arising from GSC arrangements? What other relevant risks should regulators consider?

- The **value of the stablecoin** does not lie in the place where it is deposited, but on the **economic strength of the issuer**. Indeed, even a stablecoin deposited with the central bank has no value if the issuer of the stablecoin goes bankrupt. From a general perspective, the risks would be then higher in a model were the issuer is a non-supervised private entity. On the contrary, the GSC **model with a financial institution or supervised entities as issuer** is the most suitable one to leverage the financial strength and stability of the offering institution.

- Within a GSC ecosystem the **roles of issuer of GSC should be carried out by a financial institution or by supervised entities that have implemented the KYC and AML/ATF procedures**. Moreover, it would be appropriate that such entities were subjects to a common set of general rules directly established by the FSB itself.

- The introduction of a **mechanism of interest increases risks** and partly distorts the function of a GSC which is to be above all a payment instrument, becoming more like an investment instrument.

- We point out that different potential risks arise according to some characteristics of the specific GSC, in particular if the arrangement provides guarantee of the possibility to exchange coins with currency. In case of a full asset-backed GSC with guarantee of redemption achieving substantial volume, the underlying reserve could amount to a relevant value, comparable to a primary sovereign wealth fund. Investment strategies of such a huge amount of funds could have destabilizing effects on selected market. The **risk posed by a lack of complete independence of the entity in charge of managing the reserve** should also be considered. On a micro-level, in cases where the conversion coin-currency is not guaranteed, the disruption of the arrangement could pose a substantial risk of complete loss of value for coin holders, mainly in EMDEs. A GSC arrangement achieving substantial volume could get such a relevant reserve under management that in case of failure or disruption an intervention from a State could be required (like bank bailout).
Do you agree with the analysis of potential risks to financial stability arising from GSC arrangements? What other relevant risks should regulators consider?

- The digital transformation, particularly the spread of disruptive technologies, makes the securitization of financial market infrastructures extremely difficult and requires continuous updating and adaptation to the stresses that emerge on global scale.

- DLT, like any emerging technology that finds direct or indirect application in support of financial services, must be assessed from the perspective of cyber-security risk, both for a single financial institution and for the wider and more interconnected infrastructure, as well as for bodies that monitor the stability and resiliency of the system.

- An impact can be associated with the risks, which indicates the possible loss in case of realization of the risk itself. The impact can be of a different nature (economic loss, impairment of reputation, loss of business, violation of regulations, etc.) and multiple impacts can occur as a consequence of the realization of a single event.

- With reference to the security objectives of a GSC Arrangement, the following technological risk classes have been identified:
  - loss of register availability and functions;
  - loss of ledger’s integrity;
  - loss of confidentiality of the information contained in the ledger;
  - repudiation of transactions;
  - impossibility to guarantee the uniqueness of the transactions;
  - loss of authenticity and veracity of transactions.
Do you agree with the analysis of the vulnerabilities arising from various stablecoin functions and activities? What, if any, amendments or alterations would you propose?

- We agree on the analysis of the vulnerabilities related to the proposed framework.

- In addition, underline that a comprehensive analysis of the technological stack of a GSC arrangement and the underlying technology should address also the following vulnerabilities:
  - vulnerability related to the management of cryptography;
  - vulnerability related to performance limits and resource capacity;
  - vulnerability related to the quality of the input data;
  - vulnerability related to the communication protocol between nodes;
  - vulnerability related to the consent protocol;
  - vulnerability related to the immaturity of DLT and Smart Contracts.
Do you have comments on the potential regulatory authorities and tools and international standards applicable to GSC activities presented in Annex 2?

- Regarding fair competition in financial markets, **GSC arrangements have the potential to promote market concentration** thus hampering fair competition and antitrust policies. Due to strong networks that spur their adoption, GSC arrangements can achieve market dominance in a significantly short period. In the event that GSC systems are built on **proprietary systems**, they’ll **prohibit entry or increase barriers to entry** to such systems. This may be for instance the case where enterprises that govern the stablecoin arrangements control the key channels that consumers and businesses use to access a range of services. Increased barriers of entry may adversely affect interest rates earned by stablecoin holders as GSCs that hold dominance can offer relatively low-interest rates. Conversely, with robust competition frameworks, GSCs will compete by providing better interest rate terms*.

- **Regulatory authorities** should thus deal with the different activities and functions involved in GSC arrangements ensuring an adequate competition framework at every level of the chain, by providing:
  - safeguards for granting consumers and businesses the right to join GSC ecosystems (e.g. interoperability protocols should be required);
  - effective controls and proportionate sanctions to prevent anticompetitive business practices (e.g. abuse of dominant position).

The adoption of an adequate competition framework will at once benefit digital transformation, while safeguarding stakeholders trust in the financial system, in such a way that **boost the mass-adoption** of stablecoins designed to reach global scale.

- A recommendation for every GCS arrangement is to include a role into the network that may have the right to audit the historical chain of transactions and enforce the rules underlying the network.

- Regarding the tools applicable to GSC activities, it should be appropriate to provide:
  - **procedures** available to reverse/recover invalid transactions also due to a bug in smart contracts code;
  - **insurance/surety** to deal with liquidity risks/solvency.

* On these issues see: https://medium.com/xinfin/stablecoins-legacy-finance-how-can-stablecoin-holders-earn-interest-from-legacy-finance-397ae7f9b7d2
In order to assess the issues of risks, vulnerability and threats, the following standards have to be considered:

- the ISO / IEC 27001 standard on "Information technology - Security techniques";
- the ISO / IEC 27001 standard on "Information technology - Security techniques"001 - "Information security management systems – Requirements" which defines "information security" as the safeguarding of confidentiality, integrity and availability of information itself.

The fundamental information of a DLT can ultimately be identified in the "ledger" and in the "transactions" contained therein.

Considering the above, the security objectives of a DLT-based infrastructure can be defined as the need to guarantee the following requirements:

- **availability** of the transactions and/or the ledger and, more generally, availability of the functions made available by the GSC arrangements;
- **integrity** of the transaction ledger and the information it contains, meaning the technical integrity of the data;
- **confidentiality** of the information contained in the transaction register (when requested at the business level);
- **non-repudiation** of transactions;
- **uniqueness** of transactions;
- **authenticity and truthfulness** of transactions, meaning the correspondence of transactions to actual reality.

Additionally, for GSC arrangements it would be also possible to use the COBIT framework for their identification and evaluation. Specifically, the COBIT 2019 framework provides 4 specific areas of objectives. As an example, these IT risks can be applied to Blockchain solutions:

- Delivery, Service and Support (DSS) addressing operations, service requests incidents, problems and process controls;
- Build, Acquire, Implement (BAI) assets, configurations, changes, capacities, solutions and requirements;
- Align, Plan and Organize (APO) service agreements relationships, suppliers, architecture, skills, HR and budget & control;
- Monitor, Evaluate and Assess (MEA) towards monitoring control systems, compliance to external requirements and assurance management.
Do you agree with the characterisation of cross-border issues arising from GSC arrangements?

- Even though we agree on the analysis concerning the cross-boarder issues strictly related to the matter of supervision, we also identify a number of aspects directly connected with the multi-jurisdictional operativity. In addition to the aspects analyzed by the Consultative Document, indeed, GSC arrangements also raise **matters concerning the disputes resolution**, due on one hand to the potential reach and adoption across multiple jurisdictions of GSCs, and on the other hand to the lack of territoriality of the online environment.

- Particularly, cross-border disputes raise a number of **specific issues**, including:
  - questions concerning the **jurisdiction**: in which country or countries can the claim be brought?
  - questions concerning the so called **“forum shopping”**: in which country would it be most advantageous for it to be brought?
  - questions concerning the **enforceability**: will a judgment be recognised in another country’s jurisdiction?

- Since the regulatory classification of SCs among different countries is extremely diverse, the issues inherent to all cross-boarder disputes could be harsher in respect of GSCs disputes. In this sense, the effective commitment of different countries towards **the implementation of FSB recommendations at local level** could represent a key factor to mitigate the territorial fragmentation in the context of GSC arrangements, so that it could also lower the risk of litigation.

- If stablecoins are seen as a form of privately issued money, the risk is on the issuer and the way that might be affected based for example on its jurisdiction (e.g. **Patriot Act**).
Are the proposed recommendations appropriate and proportionate with the risks? Do they promote financial stability, market integrity, and consumer protection without overly constraining beneficial financial and technological innovation?

- **Recommendation 1**: in a DLT-based GSC Arrangement, Authorities should have the possibility to perform audit actions over the ledger through a purpose-conceived technical tool (auditor node in a DLT architecture as described in BIS-CPMI “Distributed ledger technology in payment, clearing and settlement”, February 2017). In addition to identify the legal entities responsible for relevant activities, Authorities should also have the possibility to have a clear understanding of their corporate structure and decision-making chain.

- **Recommendation 2**: in addition to what explained, Authorities should adopt, and have at their disposal the tools and procedures allowing to an approach that ensure the correct balance between the oversight and control needs and the need to foster innovation and market efficiency.

- **Recommendation 3**: Authorities should consider the complexity posed by a GSC Arrangement where the various functions and activities can be performed by several entities, each of which located in a different jurisdiction, with a specific reference to how relationship among the various entities are managed from a legal point of view also considering the specific issues of cross-border disputes like:
  - questions concerning the jurisdiction;
  - questions concerning the so called “forum shopping”;
  - questions concerning the enforceability.

- **Recommendation 4**: in order to prevent risks to financial stability due to mismanagement of the reserve, Authorities should have the possibility to verify the strategies and decision-making mechanism regarding the investment of reserve assets and how any profit deriving from investment activities are managed. The full independence of decision makers should be assessed.
Are the proposed recommendations appropriate and proportionate with the risks? Do they promote financial stability, market integrity, and consumer protection without overly constraining beneficial financial and technological innovation?

- **Recommendation 5**: for arrangement that heavily rely on algorithms and smart contracts to perform core activities, Authorities should verify all the tools and procedures available to deal with invalid transactions also due to bugs in smart contracts and algorithms. Specific risk-mitigating strategies should be put in place.

- **Recommendation 6**: where the Arrangement involves several entities to perform the various functions and activities, Authorities should verify how liabilities about data management are shared and regulated among the various entities.

- **Recommendation 7**: Authorities should verify if and how obligations towards third parties are managed in case of resolution and how the holders of coins are. Moreover, authorities should be empowered to prescribe the set-up of insurances and/or sureties in order to mitigate risks in case of resolution.

- **Recommendation 8**: Authorities should verify that the information provided should include all the potential risks for GSC holders, in particular when the GSC Arrangement do not grant right to redemption in fiat currency. GSC users should be informed about the benchmark against which the value of the coin is evaluated to be considered “stable”.

- **Recommendation 9**: Authorities should verify that in order to exercise the right to redemption, the coin holder is not subject to misleading or unfair clauses.

- **Recommendation 10**: Authorities should verify that the GSC Arrangement provide clear and exhaustive information to all the concerned parties whenever the need to comply to new regulatory requirements involves a change in the operations of the GSC. In this case, the GSC Arrangement should ensure to any party the right to withdrawal without any impact on obligations, included the right to redemption where applicable.
Do you think that the recommendations would be appropriate for stablecoins predominately used for wholesale purposes and other types of crypto-assets?

- We consider the **recommendations appropriate for wholesale-oriented GSC** mainly intended to payment operations among financial institutions (e.g. the Utility Settlement Coin initiative).

- **Other Crypto-assets** (for example the so called Security Tokens, Utility Tokens and Tokenized Assets) **should be subject to a specific analysis** in order to identify the peculiar features and implications.
Are there additional recommendations that should be included or recommendations that should be removed?

- An impact analysis must be conducted toward two distinct areas such as the i) **integration** with current business and financial ecosystem and ii) **security standards** to be met.

<table>
<thead>
<tr>
<th>Technology</th>
<th>Governance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Integration with current ecosystem</strong></td>
<td></td>
</tr>
<tr>
<td>- Rules and standards to be developed in order to ensure full interoperability of different applications developed by various entities</td>
<td>- Asses the governance framework</td>
</tr>
<tr>
<td>- Integration with the Financial Legacy Systems in particular, integration with existing international payment infrastructure if any sort of settlement in fiat currency is required.</td>
<td>- Asses the regulatory model</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td></td>
</tr>
<tr>
<td>- Security implications of wallet and Key Custody management</td>
<td>- Identity management requirements</td>
</tr>
<tr>
<td>- Analysis of the underlying DLT protocol taking into account global capacity and operation model in a real-life scenario</td>
<td>- Anonymity / pseudonymity of transactions</td>
</tr>
</tbody>
</table>
Are there cost-benefit considerations that can and should be addressed at this stage?

- We highlight the need for a **reasonable balance between the complexity and pervasiveness of the control and surveillance actions**, which entail a significant commitment on both the Authorities and the entities participating in the GSC Agreement, and **the need to facilitate innovation in the global system of payments and promote financial inclusion** especially in EMDEs. Authorities should thus have at their disposal a **regulatory framework that is flexible enough** to be able to adjust the surveillance and control burdens according to the growth of the volumes reached by a certain GSC Agreement.

- At the same time, **regulatory oversight of the third parties should also be ensured**. GSCs are indeed completely new scenario from technical, operational, financial and regulatory point of view. Given such a novelty characteristics, even a consolidated Financial Institution could not have the capability to oversight the third parties involved in the arrangement. Regulator should thus exercise direct oversight over all the entities involved in the arrangement as long as a robust experience has been developed. Furthermore, in a more mature scenario, regulators should exercise direct oversight over third parties as it is currently done for critical service providers.

- In addition, a **distinction between systemic and non-systemic GSC** should also be considered in order to **define more tight regulatory constraints for the former**.