To:
Financial Stability Board
fsb@fsb.org

From:
The Badger Technology Company Limited ("Bitso")
Unit 1.02 World Trade Center
6 Bayside Road
Gibraltar
GX11 1AA

FSB | Public Consultations | Answers

To avoid unnecessary repetition, this document will address only questions **3**, **4**, **6**, **7, 9** and **10**. We believe that by answering these questions we could properly emphasize our point of view and opinion on the important matters under discussion by the Financial Stability Board.

These brief answers to the Public Consultation are provided as reference information only for Financial Stability Board exclusively use, reflects information available as of the date hereof or as of such other date indicated herein and is subject to change. None of Bitso, subsidiaries, affiliates, employees and/or contractors (i) makes (or shall be deemed to have made) any representation, warranty or guarantee as to the accuracy, completeness, utility or relevance of any information contained herein; (ii) has (or shall be deemed to have) any obligation to update any information contained herein; or (iii) shall be responsible or liable (or be deemed to be responsible or liable) for any kind of accuracy, utility, completeness or relevance of, or any interpretations of or conclusions drawn from, any information contained herein. Accordingly, any person or entity (i) shall assume full responsibility for the use of any information contained herein; and (ii) shall not be entitled to rely, and shall be deemed not to have relied, on any information contained herein.

Please contact Bitso for further questions and information at legal-regulatory@bitso.com.

Question 3. Is the distinction between GSC and other types of crypto-assets sufficiently clear or should the FSB adopt a more granular categorization of crypto-assets (if so, please explain)?

Yes, additional categorization should be adopted to distinct crypto-assets used as means of payment, as financial instruments or to access certain services/products. Therefore, crypto-assets are not necessarily riskier *per se* as these assets have different functions and degrees of decentralization and should be treated accordingly. Fundamentally, the regulation without a clear taxonomy may create blockers for the full potential of the crypto economy.

For this reason, it is advisable to note that market infrastructure (e.g., custody, trading, settlement) has direct impacts on the functions and utilization of any asset. While the regulation of crypto participants (e.g., crypto issuers and providers) is recommended on some level (e.g., KYC/AML, customer protection and prudential requirements), it is also important to measure the impacts it will have on some functions performed by the crypto-assets, such as means of payment. Basically, one cannot fully use a means of payment with too much entry costs, meaning an asset used as a means of payment cannot be regulated as a security or derivative. Therefore, as different functions have different risks, it is recommended to observe the asset's actual use/functions before regulating it.

Question 4. Do the CA Recommendations and the GSC Recommendations each address the relevant regulatory gaps and challenges that warrant multinational responses?

Blockchain-based technology is borderless, cross-jurisdictional. They exist regardless of territorial jurisdictions. CA Recommendations should elaborate on how global crypto providers could address different regulatory formats, as it is not efficient to serve different countries with different rules. In other words, given the global reach of crypto services, how to create effective international collaboration?

In general terms, CA Recommendations do advocate for a regulatory methodology that prevents conflict of regulations and avoids double regulatory requirements, but as the new crypto legislations are being enacted now a clear action plan should be created in order to avoid over-regulation of the crypto economy. As each jurisdiction will try to impose its own rules, an effective collaboration based on clear principles should be implemented as soon as possible.

Question 6. Does the report accurately characterize the functions and activities within the crypto ecosystem that pose or may pose financial stability risk? What, if any, functions, or activities are missing or should be assessed differently?

One comment regarding Decentralized Finance ("DeFi") protocols is important. DeFi protocols are creatures of coding and, in their essence, do not have a normal legal format nor a legal constitutive act. In fact, by design, DeFi protocols cannot have a legal wrapper because they are decentralized nodes based in several jurisdictions.

That said, DeFi protocols are essentially secure and transparent. First, the blockchain technology does not have a central hardware or management body, eliminating the possibility of platform scams as the user can control the private keys of assets (or trust a third party to hold the private key on their behalf). Second, blockchain is transparent because the code is open-source and every trade (on a public chain) is visible to third parties. Therefore, it is important to understand what exactly one wants to regulate in the DeFi ecosphere.

According to the CA Recommendations,

> *"Regulators and supervisors need to look past the labels and marketing around a product or service, and consider the facts and circumstances of each case to establish ways to*

> *<u>identify who exercises effective control on the protocol or provides access to the protocol,</u> and to make them accountable under existing or future regulation"*

DeFi protocols are considered to be "ownerless" entities due to the decentralization mechanisms. All decisions are voted by the nodes and no effective control is actually possible, so the regulation of DeFi protocols is very unlikely to happen. Therefore, it lacks some clarity on what exactly the authorities will regulate. Nonetheless, it is true that regulatory measures can be taken towards more certain regarding DeFi, such as creating procedures for crypto providers as gatekeepers of DeFi protocols, ensuring that they run the proper KYC/AML and other anti-money laundering mechanisms. In other words, one cannot actually regulate DeFi, but for sure one can ensure some level of risk mitigation, especially through crypto providers.

Finally, DeFi environment has been extremely heterogeneous, not only for financial services. According to Yao[1], there were 7,200 types of tradable digital assets as of October 2020, with a total market value of USD 330 billion, which illustrate the importance of this market. Also worth mentioning that many fields, not related to payments, lending, custody or derivatives, use DeFi ecosphere, such as market infrastructure, insurance, prediction markets and KYC & identity. These activities show the versatility of DeFi protocols and should be taken into consideration by the Financial Stability Board.

Question 7. Do you agree with the analysis of activity patterns and the associated potential risks?

Not entirely. "Same activity, same risk, same regulation" may not be totally appropriate as a governing principle for crypto assets and services. Crypto providers may have the same or similar service/activity than traditional finance, but the risks are different considering the technology used and the decentralization inherent to the crypto economy. As well known, public blockchains are *distributed ledger technologies* with transparency and traceability capabilities, so the public authorities may leverage and ensure to have full visibility on the transactions made in the blockchain. Also, smart contracts are automatically executed, curtailing any type of human intervention that could generate a financial exposure.

As for "off-chain" crypto providers that do not have the inherent public transparency, there are methods of ensuring more transparency towards the custody of assets. Crypto providers should follow general privacy rules, but that does not mean that they use privacy enhancing mechanisms. Therefore, crypto providers can (and should) be able to provide reliable information regarding the client's assets. The crypto services providers, as the holders of client's private keys, have access to all the transactional information which can easily be made available for the public authorities when requested.

That is the reason why the crypto industry would benefit if the CA Recommendations gave more details on the following sentence: "*many crypto-asset service providers (e.g., trading platforms,*

---

[1] YAO, Qian. **Blockchain-based new financial infrastructures.** Singapore: Springer, p. 163.

lending platforms and custodians) do not disclose sufficient information to understand their financial conditions and risk profiles". As many crypto providers are already regulated by several jurisdictions, these regulated providers already have disclosure obligations with the relevant authorities. Therefore, would it be important to specify to whom the suggested disclosure would apply (regulators and/or customers).

Question 9. Do you agree with the differentiated requirements on crypto-asset issuers and service providers in the proposed recommendations on risk management, data management and Disclosure?

Although the risk differentiation (Annex 1) is clear, it is not clear the differentiated requirements on crypto-asset issuers and providers. CA Recommendations treat them instinctively as "crypto-asset market participants" and the differentiation should be more clearly defined.

We also consider that the use of prudential rules for risk by the regulators should be avoided or not be a common practice since it hinders innovation and new product delivery by prohibiting certain products or business models under the pretense of establishing a “healthy” separation between crypto and the financial system. It also generates regulatory gaps between jurisdictions by allowing the regulators to use vague and overbroad prohibitions and disregard the “same activity, same risk, same regulation” principle. Regulation must be clear, concise, functional and strive for the transparency of the crypto market.

Question 10. Should there be a more granular differentiation within the recommendations between different types of intermediaries or service providers considering the risks they pose? If so, please explain.

The use of existing regulatory, supervisory and oversight for crypto providers and issuers should be the exemption, not the general rule. As the new technology opens the possibility for new and disruptive products, it is hard to answer the question if the activity is covered in the existing framework. We also need to consider that there are many providers that aggregate different type of crypto products and services. That said, there are two answers for this question.

If **yes**, the authority must address the issue on how to allow it formally and there are two possibilities: clarify application (authorization/license required) or supplementary guidance. If **not,** the authority may include in the existing framework, which means revise the legal framework to include crypto services or new bespoke framework, defining new regulatory perimeter and requirements.

The problem is one cannot frame equally products based on different technologies without running the risk of creating real blockers for new services and products. Fundamentally, blockchain and crypto are enablers and infrastructure tools to build more financial alternatives that can coexist with traditional finance.

Therefore, the industry should think on how to propose future-proof regulations at the same time as addressing prudential and KYC/AML concerns. Specifically for crypto providers, the recommendation is that a middle ground between the *authorization* and *licensing* approaches are desirable, ensuring the compliance with the AML/CFT rules, prudential legislation (e.g., segregation of funds) and entry requirements, but guaranteeing that the regulated company has the flexibility to launch new products without the need to request additional authorizations. This approach can be described as ‘flexible licensing’.

***