BLOCKCHAIN ASSOCIATION OF SINGAPORE'S RESPONSE TO FATF'S PUBLIC CONSULTATION ON FATF DRAFT GUIDANCE ON A RISK-BASED APPROACH TO VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS

Introduction to the Blockchain Association of Singapore

1. The Blockchain Association of Singapore **("BAS")** is an industry body whose mission is to be the leading industry organisation for the advocacy, collaboration, convergence, and fair use of blockchain and scalable technologies in Singapore, which has a vibrant blockchain community.

2. Our members include Virtual Asset Service Providers **("VASPs")** (cryptocurrency exchanges, digital asset exchanges, custodial providers, OTC platforms, most of which are regulated in Singapore under the Payment Services Act), blockchain-based enterprises, academia, RegTech providers and professional consultancy firms.

3. BAS' Regulatory and Compliance Sub-Committee had organised a Webinar on 1 Apr 2021 attracting 247 registrants, attended by around 214 participants from about 156 companies. This set of submissions crystallizes some of the comments received during the Webinar.

4. A panel of the Sub-Committee members, comprising former regulators and compliance thought leaders from the community, had led discussion of issues during the Webinar.

5. At the outset, we would like to reiterate that BAS is committed to ensure upholding of robust and risk-appropriate standards of Anti-Moneylaundering **("AML")** and Combating the Financing of Terrorism **("CFT")** for the blockchain industry and is generally supportive of greater clarity on international prescriptions for AML/CFT compliance. For instance, we have conducted various webinars for our members to promote AML/CFT compliance, including a session relating to FATF's Virtual Assets Red Flags Indicators of Money Laundering and Terrorist Financing (Sep 2020).

Inherent Risks and Mitigants on the Blockchain

6. Much has been said about the moneylaundering and terrorist financing risks of the virtual assets **("VAs")** – largely due to factors such as pseudonymity, the speed of transfers and the ability to transcend borders quickly.

7. To generate balance in the discourse, and for the purposes of a more accurate and nuanced appreciation of the risks of VAs, our view is that not enough has been articulated about the inherent mitigants on the blockchain, as an immutable and permanent record of transactions. Further, there is a growing plethora of RegTech

solutions which are able to provide asset tracing capabilities on the specific VA – which is not possible for fiat transactions. The appreciation of these mitigants would, in our view, result in a more effective and nuanced risk-based approach on VAs and VASPs.

8. We also note that some of FATF's further proposal would result in more onerous obligations compared to fiat transactions, or conventional financial services. We will elaborate on these in due course.

9. We now set out our feedback on the specific areas set out in the FATF Consultation Paper.

Q1: Clarity on the definition of VASP (paragraphs 47-79) on which businesses are undertaking VASP activities and subject to the FATF Standards. Does the 'expansive' approach to the definition of VASP require clarity?

10. We note that the FATF proposal is to deem the following activities conducted natural or legal persons as VASPs [1]:

i. *Exchange* between virtual assets and fiat currencies;
ii. *Exchange* between one or more forms of VAs;
iii. *Transfer* of virtual VAs;
iv. *Safekeeping and/or administration* of virtual assets or instruments enabling control over VAs; and
v. Participation in and provision of *financial services related to an issuer's offer and/or sale* of a virtual asset.

Initial Coin Offers

11. In relation to an ***Initial Coin Offers***, we note that the FATF's remarks in Box 3:

> For example, a person ***creates*** a digital asset that meets the definition of a VA. The person sells the VA to purchasers, even though the VA itself is to be delivered to the purchaser at a later date and the business uses the value received from the sale to develop the platform or ecosystem in which the VA eventually may be used. In this scenario, the person ***selling*** the VA is a VASP, as it provides ***financial services*** related to the issuance of the VA (limb (v) of the VASP definition) to customers. ***Any business*** which assists the person provides ***additional financial services*** related to the offer and/or sale of the

[1] Paragraph 47

VA, regardless of whether they are formally affiliated with the person, would also be a VASP under limb (v) of the VASP definition.

12. Our views are as follows:

- The term "creation" of a digital asset could technically include blockchain-based developers and companies. For clarity, we suggest clarifying that such companies providing technical support should not be treated as VASPs. It is not clear whether Paragraph 69 covers this.
- There could be other businesses which could be providing services to the ICO issuer – for instance, businesses which provide fiat FX conversion, or which providing lending services to a corporation. In some jurisdictions, these activities may not be regulated as financial services. Typically, it would be a stretch to deem such as being VASPs. We suggest FATF's clarification in this.
- We seek clarity on whether persons providing advisory-related services on VAs (e.g. advising on the investment prospects of VAs) would also be deemed to be VASPs.

Licensing and Regulatory Regime for VASPs

13. The FATF report stated [2]:

For instance, such a (licensing or regulatory regime for VASPS) could include ***greater focus on technological capacity*** in AML/CFT analysis.

14. We agree on the greater focus on technological capacity in AML/CFT analysis – and this is where we can tap on the inherent mitigants of VAs on the blockchain. Some appreciation of this mitigant would more pointedly deal with any ML/FT risks, rather than force-fitting VASP regulation into existing regulations, which may not less fit for purpose. Suggest FATF providing guidance that jurisdictions should have the flexibility to consider these mitigants inherent on VAs.

Cross-Border Transactions

15. The FATF Revised Guidelines [3] mentioned that:

[2] Paragraph 110
[3] Paragraph 112

> "Host jurisdictions may therefore require registration or licencing of VASPs **whose services can be accessed by or are made available to** people residing or living within their jurisdiction, or may require VASPs that have employees or management located in their jurisdiction "

16. Our view is that such an approach of requiring licensing in the event that a particular service ***can be access by or made available to*** residents of a country is overly restrictive and not in sync with the approach taken even for conventional financial services.

17. Currently, if a resident of Country ***A*** wishes to trade in securities listed on an exchange in Country ***B***, and does so through an online broker-dealer in Country ***B***, the online-broker does not necessarily need to be licensed in Country ***A***, even if its services can be accessed by residents in Country ***A***.

18. The key determinant for licensing should be the extent to which the broker dealer (or in our current example, the VASP) conducts active marketing or solicitation in Country ***A*** *or targeted at residents in Country A*. Most online broker-dealers do not, but perform what is commonly known as ***reverse solicitation***.

19. The same approach should be taken for VASPs. Where the VASP's service can merely be accessed by residents in the host jurisdiction, that alone should not be a determinant for licensing. Whether or not the VASP has marketed or solicited residents in the host country should be a key determinant to determine supervisory oversight by the host regulator.

P2P Transactions

Q2: What are the most effective ways to mitigate ML/TF risks relating to peer-to-peer transactions (i.e., VA transfers conducted without the use or involvement of a VASP or other obliged entity, such as VA transfers between two unhosted wallets) (see paragraphs 34-35 and 91-93)?

20. FATF's acknowledgement [4] that P2P transactions are not explicitly subjected to AML/CFT obligations under the FATF Recommendation as the FATF Recommendation places obligations on intermediaries between individual and financial system and not

[4] Paragraph 34

on individuals themselves with the approach taken similar like a physical fiat currency (cash) transactions is realistic and a sensible approach.

21. We would like to seek guidance on what sort of measures VASPs are expected to undertake to ascertain that their customers engage in P2P activities (other than obtaining a client declaration). This expectation could be unduly burdensome on VASPs.

22. That logic must also transcend the rest of the policy approach towards P2P transactions – that the bulk of these transactions are legitimate use of VAs, just as fiat currency is currently being used.

23. The risk mitigating measures proposed by FATF [5] especially in *denying* the licensing for VASPs that allows transactions to/from non-obliged entities (i.e. private unhosted wallet) is not only inappropriate but remains too restrictive and does not accurately reflect the reality of how a P2P transaction is conducted.

24. There is nothing inherently sinister in P2P transactions – inasmuch as most of the transactions in fiat currencies happen on a P2P basis.

25. Additionally, this will also serve to exclude a significant portion of the 'unbanked' from utilising VAs for their VA transactions, especially those which may be located in jurisdictions where the services of VASPs are less accessible/trust worthy. This will only result in further financial exclusion for these communities.

26. It should be emphasized that VAs are not deemed as a legal tender and any illicit actors would logically want to convert VAs into local fiat currencies. Accordingly, any P2P transactions may eventually involve a VASP on either side of a transaction, initiating fiat on and off-ramps. Any proposal to take severe actions to limit or mitigate the risk of P2P transactions such as denying of licensing should be rejected as it is both unnecessary and ineffective in combating any illicit financial activity involving crypto-transactions.

27. This is over and above the fact that there are no equivalent expectations or restrictions for conventional financial transactions handling fiat currency.

28. Any recommendation to implement VA equivalent of a Cash Transaction Reporting requirement as documented is similarly counterintuitive and adds to the vast

[5] Paragraphs 91-93

compliance cost and resources that VASPs undertakes, as ultimately any transfers of VAs would leave 'digital footprint' or traces of blockchain addresses which would eventually be tracked and monitored.

29. Nevertheless, even if such a VA equivalent of a Cash Transaction Reporting be proven necessary, sensible thresholds for the implementation of such reporting and public consultation should be introduced. Any thresholds that are deemed too low by the industry may result in stifling of transactions potentially resulting in more users relying on any anonymous tools such as mixers and tumblers in order to circumvent any supervision.

30. Clarity needs to be made as to what exactly constitutes as 'unhosted wallet' in order for industry to appreciate uniformly the nature of the risk that FATF is trying to mitigate. It could be understood as 'private individual wallet' OR 'wallet of an unlicensed VASPs' OR 'wallet belonging to an non-obliged entities'.

Licensing and Supervisory Regime

31. We agree with the FATF [6] that countries should have the flexibility to manage the influx of licensing applications when a new regime is introduced.

32. However, we suggest that FATF provides guidance that regulators also consider proactively anticipate the regulatory resources needed to deal with such a scenario of an influx of licensing application in order not to delay applications – as that would be preferable in ensuring that the VASP community in that jurisdiction are quickly up to the mark in terms of meeting AML/CFT prescriptions set in regulations.

Consideration for Licensing VASPs

33. We agree that VASPs must be subject to robust licensing criteria, such as robust AML/CFT requirements built into products and services, having a local presence, being fit and proper persons, and subject to financial resource requirements.

34. The FATF paper suggested "substantial management presence" [7] as a precondition of licence. In this day and age of digital financial services (not just peculiar to VASPs), it is not uncommon for businesses to operate more efficiently by focusing their management in a particular jurisdiction. Depending on the scale and complexity of

[6] Paragraph 117
[7] Paragraph 119

their business, they may then decide to allocate actual management presence in specific jurisdictions. We would suggest that individual jurisdictions should be allowed to decide whether or not "substantial management presence" should be a requirement as a precondition to licensing.

Risk Factors Relating to Virtual Assets

35. The FATF paper [8] had identified **certain elements** that VASPs should consider in **risk-assessing** VAs:

- Number and value of VA transfers;
- Price volatility;
- Market capitalization;
- **Number of jurisdictions** of users;
- **Market share in jurisdiction;**
- Extent to which VA is used for **cross-border payments; and**
- ML/TF risks associated with VAs **being swapped for fiat** and removed from traditional financial system.

36. The Webinar discussed these factors and largely feel that these may be overly-prescriptive. The current practice is that VASPs already conduct due diligence on VAs by ascertaining whether the tokens are securities or payments tokens, assess the underlying business of the token issuer, track record and strength of the management team, assess the token economics etc. These are already quite onerous requirements.

37. The correlation between some of these factors (e.g. volatility and market capitalization) to moneylaundering or terrorist financing risks may be a stretch.

38. We are not convinced that it would be practical to require a VASP to assess, for instance, market share in a particular jurisdiction (if that data is available, taking into account that VAs are often time accessible from multiple jurisdictions depending on who has control of the private key), the extent to which VAs are used for cross-border payments, or being swapped to fiat. Any new prescriptions should make sense from a cost-benefit analysis. Again, there is no equivalent measure for fiat transactions.

[8] Paragraph 36

Risk Factors Relating to VASPs

39. The FATF report has identified certain **risk factors** [9] relating to VASPs, namely:
    a. Number & type of VASPs in a jurisdiction & offering to consumers & amount of transactions;
    b. Sophistication of VASP's AML/CFT program - tools and persons;
    c. Size and type of customer base of VASPs, both within the VASP and whether there is aggregation across platforms;
    d. Nature and scope of VA account, product or service (e.g. **small value savings and storage account that enable financially-excluded customers**);
    e. Measures by VASPs to **risk manage** (e.g limits);
    f. Business model of VASPS, whether the business model introduces or worsens risks;
    g. Whether VASP operates online **or in person;**
    h. Potential ML/TF and sanctions risk associated with VASP's connections and link to the jurisdiction;
    i. Whether the VASP implements the **travel rule;**
    j. Transactions to and from **non-obliged entities** (unhosted wallets, apps) and transactions where a **P2P transaction** has occurred earlier;
    k. The specific types of VAs that the VASP intends to offer and unique features (e.g. AECs, embedded mixers or tumblers); and
    l. VASP's **interaction and management of smart contracts.**

40. We think it is fundamentally important for VASPs be assessed, and agree that it is important to assess the quality of a VASP's AML/CFT program and compliance framework. However, we have comments on specific risk factors.

41. We are, however, curious on the rationale why certain scope of services are highlighted (e.g. small savings and storage accounts that could help financial inclusion). Why is financial inclusion necessarily a bad thing? In developing jurisdictions where financial inclusion is still problem for significant proportions of the population, affording access to financial or payment services through technology must be embraced (of course, subject to the VASP meeting other regulatory requirements).

42. We are similarly curious why another key factor flagged is whether the VASP operates online, or in person. In conventional financial services, the default business model is one which is done in person. Surely, whether or not a platform decides to offer services online or in person is a business decision. Why should it matter whether a

[9] Paragraph 36

business offers a physical presence – which arguably also offers better accountability to customers in the event of disputes?

43. Yet another risk factor relates to transactions to and from **non-obliged entities** (unhosted wallets, apps) and transactions where a **P2P transaction** has occurred earlier. We repeat our submission that there is nothing inherently sinister about P2P transactions or transactions involving unhosted wallets – this is similarly the case for fiat transactions. This is quite apart from the practical difficulty in assessing the extent to which a VASP has been exposed to such transactions.

Definition of VAs

44. The FATF's Paper of VAs state that:

> "VAs must be digital, and must themselves be digitally traded or transferred and be capable of being used for payment or investment purposes. That is, they **cannot be merely digital representations** of fiat currencies, securities and **other financial assets** that are already covered elsewhere in the FATF Recommendations, **without an inherent ability themselves to be electronically traded or transferred** and the **possibility to be used for payment or investment purposes."**

45. We would like to seek clarification on whether Non Fungible Tokens **("NFTs")** that are digital representations of property, intellectual property or other rights (e.g. digital art, celebrities, jewellery, other collectibles) would be treated as VAs under the FATF's rubric.

Q3. Travel Rule & Counterparty VASP Due Diligence – Need for clarity

46. We acknowledge the necessity for due diligence on counterparty VASPs at the outset. However to suggest the conduct of due diligence based on the Wolfsberg Questionnaire before initiating a VA transfer, could be overlapping and a bridge too far. The FATF recommendation [10] indicating the potential scope and extent of due diligence required to be undertaken from VASPs presents an unprecedented challenge for the VASPs in the VAs space especially on the issue of conducting such thorough

[10] Paragraphs 261-265

due diligence at a large scale. It is overly-cumbersome for VASPs to undertake a due diligence exercise, assessing adequacy and sufficiency of the AML/CFT laws and regulations of the counterparty VASPs' jurisdictions, considering the VASP may not necessarily have local legal competence and expertise to undertake a meaningful exercise.

47. As VASPs will be required by their local supervising authorities under local laws to implement and be AML/CFT compliant and be subject to strong supervision and independent audits, it would be sufficient for counterparty VASP DD to rely on their valid license and representation that they have in place relevant AML/CFT monitoring controls to mitigate.

48. Also, we would like to clarify if the intention is for the due diligence to be done only in relation to the initial transfer, and that there is no need for such due diligence on the same counterparty for subsequent transfers.

Q4: Travel Rule v. Data Protection

49. In addition to guidance provided by FATF on Travel Rule obligations, we think it is imperative that FATF tackle with other competent authorities the need for strong privacy or data protection rules in some jurisdictions, as this impacts on the ability for a VASP to share customer information with counterparties in those jurisdictions.

50. Jurisdictions with strong privacy and confidentiality rules, such as EU General Data Protection Regulation 2016/679 ("GDPR") similarly restrict any reliance on the customer's consent when the consent is given under duress and is not freely given or can easily be revoked at any time or for any reason by the client.

51. The EU Court of Justice, further delivered a landmark decision in the case of ***Schrems II*** in 2020, which significantly lays out that in accordance to Article 49 of the GDPR, any transfer of personal data must be occasional or objectively necessary for the **performance of a contract**. Consequently, any data transfers cannot take place on a large scale and must not be in systematic fashion. Any cross-border transfer of personal data must be restricted to a specific situation and must meet the strict necessity test.

52. Due to this, VASP would be left in a dilemma, with or without a presence of a contract privately drafted by two VASPs, as the absence of Travel Rule being adopted into local

laws significantly negates a legal/lawful basis for VASP to comply with Travel Rule with the transmission of information to other VASPs, consent of the customers could potentially be revoked prohibiting VASPs from proceeding with the transmission of customer's information to other VASPs and the case of ***Schremes II*** which essentially prohibits VASPs from complying with Travel Rule as the Travel Rule requires transmission of customer information to other VASPs on a consistent, large scale and systematic fashion and does not meet the occasional or objectively necessary requirement laid out by the EU Court of Justice.

53. In this circumstance, the conflict between Travel Rule and data protection should be addressed by FATF and further guidance be given as to how VASP should continue to comply with Travel Rule despite the existence of strong privacy and data protection rules in place restricting the VASP from complying with the Travel Rule.

REGULATORY AND COMPLIANCE SUB-COMMITTEE
BLOCKCHAIN ASSOCIATION OF SINGAPORE