coinbase

To:
Otávio Ribeiro Damaso
Diretor de Regulação
Quadra 3, Bloco "B", 9° andar,
Edifício-Sede,
Brasília (DF)
70074- 900

January 2024

Re: Banco Central do Brasil's public consultation on regulating the virtual assets market (No. 97-2023)

Coinbase Global, Inc. (**Coinbase**) welcomes the opportunity to respond to the Central Bank of Brazil's consultation on regulating the market for the provision of virtual asset services in Brazil (**Consultation**).[1]

Coinbase started in 2012 with the idea that anyone, anywhere, should be able to send and receive Bitcoin easily and securely. Today, we are publicly listed in the US and provide a trusted and easy-to-use platform relied on by millions of verified users in over 100 countries around the world to access the broader crypto economy.

Coinbase is the platform of choice for many of the largest, most sophisticated participants in crypto markets, who demand high standards of compliance, risk management, and investor protection. The practices developed at Coinbase provide useful insights that inform our comments.

We are excited to follow the progress Brazil is making towards its mission to become a global virtual asset hub, and we appreciate the Government's openness to dialogue and the thoughtful and strategic approach it is taking to regulating the sector. We stand ready to support the Government as it develops a regulatory framework that delivers on its ambitions and puts Brazil on a strong competitive footing in the crypto economy.

Yours sincerely,

Faryar Shirzad
Chief Policy Officer

Fabio Plein
Country Director, Brazil

[1] For the purposes of this consultation response, Coinbase uses the term "virtual assets," consistent with the definition of the term in Law No. 14,478, to mean "digital representations of value that can be traded or transferred via electronic means and used for making payments or investments."

coinbase

Introduction

Blockchain technology is the backbone of a new financial architecture. While nascent, it is already bringing efficiency, transparency, and resiliency to the existing financial system.

Blockchain applications enable people to transfer value quickly and at lower cost because it eliminates the need for intermediaries. Stablecoins that put fiat currencies on digital rails will drive competition in the payments space. Decentralized finance, smart contracts, and related new technologies will drive further innovation and exponentially expand opportunities for the financial system. Yet, virtual assets are more than a financial innovation; they have the potential to transform every sector of the economy. Today's internet is dominated by a handful of companies that profit from monetizing their users' personal data. The next phase of the internet's development will be owned by builders and users and will be driven by tokens, creating a more decentralized and community-governed version of the internet.

Brazil is an emerging leader in financial technology as evidenced by its Pix payment system. We believe this is a critical and important first step to the adoption of a digitally native financial system. As a result, Coinbase has made a dedicated effort to expand its operations in Brazil, including integration with Pix. We are excited to do so because we believe a well-designed and implemented virtual asset regulatory framework will put Brazil at the forefront of the digital finance revolution. Delivering legal and regulatory certainty to the market through an appropriately tailored regulatory framework will position Brazil to be a global leader in digital asset technology.

Key principles for a regulatory framework

In this letter, we respond to the questions posed by the Central Bank of Brazil by discussing how virtual asset service providers (**VASPs**), including Coinbase, conduct their business. We also provide our views on how the Central Bank of Brazil should approach implementing a comprehensive regulatory scheme for virtual assets and VASPs. As an initial matter, we wish to highlight five concepts that inform our responses to the Central Bank of Brazil's questions below:

1. **Virtual asset custody rules should promote customer protection**

Responsible innovation must be coupled with customer protection. Customer protection requires customer rights to be well-defined under law, including when an exchange or other custodian becomes insolvent. The failure of FTX has understandably led many jurisdictions to focus attention on appropriate custody standards for virtual assets as part of virtual asset custody regimes.

At Coinbase, we believe that customer assets should be held on a fully reserved, 1:1 basis. Such assets should not be staked, pledged, rehypothecated, or otherwise used

except with the customer's express, informed consent. This should be an expectation of all registered custodians. Intermediaries should be required to disclose how assets are held and used, and the Central Bank of Brazil should have sufficient oversight powers to ensure intermediaries follow through with these disclosures.

It is also important that the Central Bank of Brazil help enshrine proper protections for customers in the event of a VASP's insolvency, including processes for the resolution of claims on the insolvent VASP in a timely and orderly manner. Brazil should require VASPs to track assets through robust recordkeeping, so that the assets can be returned to their rightful owners quickly should the need arise. Moreover, the Central Bank of Brazil should make clear that in the event of a VASP's insolvency, customers' assets should not be used to satisfy the claims of any other creditors on the VASP, and customers should otherwise be treated as having priority over other creditors of the relevant VASP.

The customer property protections in place at Traditional financial (**TradFi**) institutions, like securities brokerage firms, may provide a useful example to the Central Bank of Brazil's approach. Notably, the supervisory approach has been to allow these institutions to:

- Hold customer assets in omnibus customer accounts;
- Maintain some limited firm assets in the same customer account to support the operation of the market; and
- Rehypothecate customer funds with their clients' express permission.

We believe VASPs should be permitted to do the same. The Central Bank of Brazil should also support efforts by VASPs to create self-custody solutions that allow consumers to retain control over their virtual assets. Coinbase has developed wallets which rely on multiparty computation (**MPC**) and multi-sig configurations to provide additional security to consumers.[2] These technologies require both consumer approval and custodian approval to transfer a virtual asset. This gives the consumer control over its assets while providing a fallback mechanism in the event that the consumer's private keys are stolen or lost.

We believe that this type of innovative self-custody solution provides significant protections to consumers. We urge the Central Bank of Brazil to encourage their development and recognize that these types of solutions are different from traditional custody services. They are software products, not financial services. It would be inappropriate to apply custodial requirements applicable to typical financial custodians to providers of self-custody solutions.

We expand on these points below.

[2] For more information on MPC and Coinbase's efforts to provide simple and safe wallets, *see* Coinbase, Building user-focused web3 wallets at Coinbase, June 20, 2023.

2. Virtual asset custodians should be able to operate across jurisdictions

Virtual asset security is best served by a global infrastructure that requires coordinated action from geographically distributed actors to operate. Current security best practices include separating and storing private key materials across different locations, time zones, and business functions. Imposing requirements that would limit the ability of a custodian to follow best practices related to the physical location of key materials would diminish rather than strengthen their resiliency and security protections. Geographic separation of human capital and security infrastructure eliminates the ability to compromise the safeguarding of assets through a single point of failure and minimizes the potential damage of an isolated security breach within any single jurisdiction.

We believe that the Central Bank of Brazil should recognize the existence of these security risks and refrain from imposing physical localization requirements. Any requirement for specific human or technical resources to be exclusively located in a single jurisdiction would materially increase the vulnerabilities of a cyber-attack. Where Brazil is a host-country, it should rely to the extent possible on cooperation with a VASP's home-country regulators, in the interest of promoting consistently high standards of security for customer assets. Effective cooperation and oversight by both host-country and home-country authorities can alleviate the potential bankruptcy or fraud risks to a host-jurisdiction's citizens that could otherwise result from a decentralized model. As a result, we believe that international cooperation and a rejection of localization should go together.

3. Blockchain technology provides a unique defense against illicit finance

The unique characteristics of blockchain technology provide innovative opportunities to identify bad actors and keep the ecosystem safe. Blockchains record all transactions on a common, public ledger. VASPs, regulators and law enforcement can analyze transactions carried out on that blockchain – whether or not they took place on the VASP's own platform.

In contrast, transaction information in the traditional financial space is generally only available to each specific intermediary involved, making it difficult to stitch together the sources and uses of funds throughout a transaction lifecycle. For example, if a bank's client wants to deposit cash into an account, the bank must rely on information provided by the customer about the source of those funds. This can create blind spots for both financial institutions and their regulators. The blockchain fixes this problem by giving VASPs unprecedented access to an immutable public record that contains the full transaction history of an asset, and thus the ability for institutions and regulators to develop innovative solutions to stop illicit activity. These solutions are discussed further below.

Coinbase treats financial crimes compliance with the utmost priority. It is the largest group within Coinbase's Compliance team and incorporates all of the components and controls customers expect from a traditional financial institution – from policies and procedures, to training, to customer due diligence.

4. Disclosures empower customers to make informed decisions

A vibrant and well functioning virtual asset ecosystem requires that its participants have access to disclosures that enable them to make informed choices. For VASPs, this includes readily-accessible, easily-understandable information about their policies, procedures, and controls.

Centering VASP regulation around a disclosure framework that permits differentiated activity and customer treatment will be more efficient and effective than a regime that prescribes treatments or imposes restrictions. It is important for this emerging technology to permit continued innovation while also protecting customers. This will provide consumers with new types of services and products. Allowing different operating models in a way that ensures consumers are well informed about market participants' practices should be a focus of the Central Bank of Brazil.

5. Regulators should embrace cross-border cooperation

Virtual assets exist in code—they do not stop at a country's borders. Cooperation and information sharing among domestic authorities are therefore crucial to the development of international regulatory standards for virtual asset activities.

Responsible innovation across borders would benefit from consistent, globally coordinated regulatory requirements. We encourage the Central Bank of Brazil to prioritize the development of a passporting or equivalence regime for VASPs that are fully licensed and regulated in other jurisdictions to standards that are high enough to satisfy the Central Bank of Brazil.We believe that measures like these will encourage more consistent regulation and deeper, more vibrant markets for virtual assets internationally.

Theme 1 **Asset segregation and risk management**

1. **The proper segregation of clients' assets, understood as their available resources and the virtual assets they own segregated from the assets of the entity provider of virtual asset services, is one of the most critical issues in the field, especially in crisis scenarios. In your opinion, what are the most efficient mechanisms for the adequate operational and legal segregation of clients' assets from those of the assets of virtual asset service providers?**

We strongly support regulatory efforts to ensure that customer assets are secure and protected. We also are of the view that permitting VASPs to use a variety of methods and structures to securely hold and track customer assets will best advance the shared goal of protecting customer assets. This technology-agnostic approach supports and facilitates innovation rather than locking in current best practices that may ultimately be surpassed by better solutions.

Properly segregating customer assets

VASPs often record customer asset ownership in two places: in their internal ledgers and on-chain. Customer assets should be clearly identified on a VASP's internal ledger as separate and distinct from those belonging to the VASP, which are frequently held to facilitate customer activity as described below. A VASP's internal ledger should also be accurate and up-to-date at all times.

When ownership of customer assets is clearly identified on a VASP's internal ledger, the VASP can often obtain security and efficiency benefits by storing those customer assets in an omnibus on-chain wallet. While the customer assets in an omnibus wallet will belong to multiple customers, a VASP's internal ledger should still reflect each customer's ownership of the wallet's contents.

Allowing for a de minimis amount of VASP assets to be used to facilitate instant trading for customers

Notably, it may be beneficial for VASPs to hold a de minimis amount of their own assets in customer omnibus accounts to facilitate customer transaction order instructions. This is consistent with how many regulated TradFi entities operate today. For example, in the United States, CFTC-regulated futures commission merchants are required to add a de minimis amount of their own funds to customer omnibus accounts to ensure that they never use one customer's assets to pay for another's obligations. These funds are treated as if they belong to customers, meaning that they are subject to the same protections and use restrictions as customer funds, and would be treated as customer property in an insolvency. A similar practice employed in virtual asset trading allows Coinbase to pay customers' network or "gas" fees. It also allows trading platforms like Coinbase to

temporarily bridge the movement of customer assets between cold and hot storage for immediate order execution, without using one customer's assets to cover another customer's trading fees or requirements.

Many VASP trading platforms, like Coinbase, hold a large percentage of customer assets in cold storage. For customers who want to trade immediately, a trading platform can allow the customer to trade out of the trading platform's hot wallet using an asset pre-positioned there by the trading platform for such purpose. This means that the customer would not be impacted by the operational delay of moving assets out of cold storage. Instead, this operational delay is borne by the trading platform, as the asset in cold storage would be moved to the trading platform's own wallet to replace the asset used for trading in the hot wallet. Because the intermediary has control over both the cold and hot wallets, the intermediary would not bear any risk of loss during this process.

To preserve these benefits, we propose that Brazil permit as part of any asset segregation requirement for VASPs to hold de minimis house-originated assets in customer accounts solely for the purpose of facilitating user transactions.

Providing certainty over the ownership of customer assets held by VASPs

As is already the required practice for some regulators, these assets should be treated as belonging to customers for all relevant purposes, including in the event of an insolvency.[3]

Distributing custody functions across jurisdictions

As discussed in greater detail above, virtual asset security is best served by a global infrastructure that requires coordinated action from geographically distributed actors to operate. For that reason, we believe that the Central Bank of Brazil should refrain from imposing physical localization requirements that could materially increase the vulnerabilities of a cyber attack.

2. **Can the funds handed over by clients to virtual asset service providers that have not yet been allocated to any investment be subject to some protection, such as the requirements imposed on entities in the distribution segment, to mitigate risks arising from the eventual discontinuation of the institution? What safeguards can be adopted at an infra-legal level, in addition to the existence of specific accounts, to mitigate such risks?**

We strongly support efforts to protect and safeguard customer assets, including funds that have not yet been deployed. A VASP should be allowed to deposit customer funds at regulated financial institutions or invest customer funds in highly safe, liquid assets, such

[3] *See* NYDFS, Guidance on Custodial Structures for Customer Protection in the Event of Insolvency, at n.7,Jan. 23, 2023.

as money market funds. In doing so, a VASP should operate in a manner that allows the VASP to maximize the available protections for customer funds under Brazilian law. A VASP should also clearly disclose its practices to customers. Moreover, its terms and conditions and agreements with third parties should make clear that such funds belong to the customer, not the VASP. As well, a VASP should maintain clear, accurate, up-to-date records that identify how much funds are in each customer's account.

3. **According to diagnoses from international authorities, it is not uncommon for some virtual asset service providers to use, even partially, the virtual assets in their possession or control to guarantee their own operations or those of other companies in their conglomerate. What measures could mitigate the risks associated with such uses if similar permission were adopted in the regulatory framework?**

   Virtual asset custodians should not use customer assets for any purpose without customers' express, informed permission. To the extent that Brazilian law addresses these issues in the context of traditional finance, such as for securities lending transactions, we generally agree that it would be appropriate for similar requirements to apply for virtual assets as well.

4. **Regarding risk assessment, can a client's virtual asset be used as a warranty for other ongoing operations of the same client with the same virtual asset service provider? If so, what limitations should be applied?**

   Clients should be able to use their virtual assets to the same extent that they can use their TradFi assets. An important part of TradFi markets is the ability for a client to use its assets as collateral to secure its obligations with another market participant. Clients generally should not be restricted from doing the same with their virtual assets. However, as with traditional assets, VASPs accepting collateral should adopt appropriate risk management safeguards.

5. **Considering some of the existing mechanisms in the financial system's regulatory framework, should there be some protection for investors in the form of insurance or guarantee funds (such as the Credit Guarantee Fund – *Fundo Garantidor de Créditos* known as *FGC* in Portuguese) or the Credit Cooperative Guarantor Fund - *Fundo Garantidor do Cooperativismo de Crédito* known as FGCoop in Portuguese), with coverage up to specific amounts, with resources originating from the segment itself? What types of insurance can be associated with the segment's operations?**

   We do not believe it is appropriate to require VASPs to contribute to an insurance pool or guarantee fund. A mandatory insurance or guarantee fund could result in VASPs with thoughtful and comprehensive risk controls, like those described in response to Question 1, subsidizing the risks taken by less scrupulous businesses in a way that is inconsistent with the relative risk posed. For example, if the amount of the required contribution to the

insurance pool or guarantee fund is based on the size of the VASP, large, but safe, VASPs that attract customers based on the robustness of their customer protection systems, like Coinbase, would be penalized

Instead, we believe that if there is considerable demand for risk pooling arrangements, the market will respond. VASPs should be allowed to determine whether risk pooling is appropriate for their businesses. Customers who demand risk pooling arrangements could choose to use such VASPs of their own accord, thus allowing the market to choose. To the extent that VASPs wish to participate in risk pooling, they should have the chance to innovate and develop their own risk pooling solutions.

6. **Virtual asset custody services may be associated with a remuneration resulting from staking, which consists of validating transactions on the blockchain by providing virtual assets as a guarantee. However, this practice assumes some risks, including the loss of part or all of the virtual assets, such as penalties for errors in verifying transactions and records on the blockchain. Therefore, what measures could be adopted to protect the investor that authorizes the custodian of virtual assets to employ their resources as a guarantee for staking and to mitigate the operational risk involved, if this operation is eventually admitted in the Brazilian regulation?**

Staking plays a critical role in maintaining the veracity of distributed ledgers. Validators stake their tokens to participate in the block proposal and verification process. Their work keeps blockchain networks secure and accurate. As compensation for their efforts, validators may receive rewards. Staking services provide customers a convenient means to participate in the security of the distributed ledger.

We support efforts to protect customers who turn to staking service providers. We believe that private industry participants have already developed an effective set of principles for staking, and would encourage the Central Bank of Brazil to incorporate these principles into its approach.[4] In particular, these principles are that:

- **VASPs should communicate clearly to ensure that users have all the information necessary to make informed decisions** – VASPs should be clear about the services being provided and offer full and fair disclosure to their customers, including by using accurate terminology and offering a clear fee schedule;
- **Users should opt-in to staking and control how much of their virtual assets to stake** – Users should be required to affirmatively opt-in to staking arrangements and VASPs should always make clear that the customer remains the owner of the underlying staked assets and rewards; and
- **VASPs should have explicitly delineated authority and responsibilities** – VASPs should not manage or control liquidity for users and should not provide any guarantees on the amount of staking rewards that a user will earn.

[4] Proof of Stake Alliance, Staking Industry Principles — Proof of Stake Alliance.

7. **A concern of regulators and supervisors relates to the risks of making cross-border payments through virtual assets, considering possible attempts at regulatory arbitrage. What are the advantages and disadvantages of cross-border payments settled with virtual assets? How can virtual asset service providers inhibit attempts to cover up illegitimate transactions using such instruments?**

   As a preliminary comment, we strongly believe that cross-border payments settled with virtual assets should be encouraged, as they not only provide more efficient payment solutions but also foster a more decentralized, inclusive and democratic financial system.

   Moreover, we understand that establishing reasonable FX controls is important to mitigate the risks of illegitimate foreign exchange transactions. In such regard, we note the rules set forth under Circular 3,978 of January 23, 2020 and would consider it appropriate for application of these rules to be extended to also encompass VASPs.

8. **Virtual assets enable the creation and development of new and complex business models by virtual asset service providers as a means of payment or investment. About international capital, is there interest in using virtual assets in direct investment operations (for example, the payment of money abroad by a resident investor or in the country by a non-resident investor) and in external credit operations (e.g., foreign funding of virtual assets by residents)? What are the advantages and disadvantages?**

   Efforts to build and maintain virtual asset networks involve actors from all different countries, enabling users from across the world to participate in the growth of the crypto economy.

   We believe that Brazil should encourage investment by Brazilian residents in the burgeoning virtual asset sector being developed across the world. Global virtual asset developers have joined their partners in Brazil to bring the underbanked population into the digital economy. The Central Bank of Brazil should encourage Brazilian residents to be a part of, and invest in, these efforts. Otherwise, Brazil may not be well-represented in these global projects, and Brazilian developers will be unable to work with their peers to bring virtual asset products and services to Brazil.

9. **The regulations relating to foreign capital in the country do not expressly provide for virtual assets, which results in the application of the discipline aimed at a broad category of "intangible assets." Should any specific qualification be considered for virtual assets in the regulations on Brazilian capital abroad and foreign capital in the country? And in terms of treatment, what should be considered?**

   Coinbase's view is that virtual assets are native to the internet, which by nature is free and open to people all across the world, and that markets for virtual assets should be similarly free and open. To the extent this openness is inconsistent with existing regulations applicable to intangible assets, we believe that specific qualifications providing for different treatment of virtual assets would be appropriate.

10. **What measures can institutions adopt to ensure sufficient funds to meet the commitments of derivative contracts involving virtual assets, especially in adverse market conditions, such as stressful situations?**

    Coinbase has adopted, and we would encourage the broader adoption of, sophisticated risk parameters to measure the potential volatility and liquidity of positions, over the relevant time horizon of risk. Institutions' liquidity risk planning should also consider whether their derivative contracts are subject to auto-liquidation (in which case they might consider maintaining a collateral buffer with the derivative provider) versus a margin call window (in which case they should ensure liquidity on hand to timely meet a call). Coinbase's risk management practices also include the adoption of fail safes that are activated for situations of high volatility. More broadly, we believe that best practices for risk management that have been developed over time in the traditional financial system can, with some adaptation, apply just as effectively to risk exposures associated with virtual assets. Participants in virtual asset markets who adhere to these practices will be well-positioned to successfully navigate a wide range of market conditions, including periods of stress.

Theme 2 **Activities developed and virtual assets traded**

11. The Central Bank of Brazil is interested in knowing whether virtual assets service providers aim to request authorization for various activities, among those provided for in Law no. 14,478, of December 21, 2022, or whether they seek specific approval for a single activity. What would these activities be for particular authorization?

Coinbase intends to seek authorization to conduct a range of activities in Brazil, and we expect many other VASPs to do the same. We believe that it is reasonable and efficient for the Central Bank of Brazil to allow a VASP to participate in any of the activities listed in Law no. 14,478 upon receiving authorization to operate as a VASP in Brazil. Each of the activities provided for in Law no. 14,478 implicate similar risks and opportunities. The Central Bank of Brazil should be able to properly examine whether an applicant for VASP authorization can properly engage in each of the listed activities. It is unnecessary to require a VASP to seek re-authorization each time it wishes to engage in a different virtual asset service activity. Similarly, in order to facilitate customer activity on the VASP's platform, a VASP should be permitted to custody customer fiat directly as a result of the VASP authorization rather than having to obtain a separate Payment Institution license.

Additionally, Coinbase aims to deliver to its customers the deepest, most liquid, and efficient digital asset exchange in every geography it serves, including Brazil. To achieve this goal, Coinbase sources global liquidity, and operates a unified order book. At the same time, Coinbase is committed to providing all services in priority markets like Brazil through locally regulated subsidiaries.

To operate via its global, unified order book, every Coinbase customer digital asset trade in Brazil requires a foreign exchange transaction between BRL and USD. One of the models under which Coinbase could operate is using Coinbase's Brazilian subsidiary to facilitate foreign exchange transactions on behalf of its Brazilian customers under the "eFX" regulatory regime. The "eFX" regime requires Brazilians to actually purchase the applicable goods or services directly from an offshore merchant. Presumably, under the incoming digital asset regulations, this purchase would also need to be facilitated by an onshore regulated Brazilian subsidiary of Coinbase; but regardless, under the "eFX" regulatory regime, Brazilian customers would necessarily have to enter into a contractual arrangement with, and receive digital asset exchange services from, an offshore entity.

To enable Coinbase and other exchanges (most of whom also rely on global liquidity) to achieve this goal of delivering to Brazilians the deepest, most liquid, and efficient digital asset marketplace possible, we believe that the regulations to be issued should set forth licensing rules that enable local VASPs to service Brazilian customers as an intermediary, but also relying on foreign custodians and global liquidity. We believe that allowing local VASPs to act as regulated eFX providers would be the best solution for this purpose while still adhering to Brazilian foreign exchange rules and regulations, especially considering

that current eFX regulations already provide for specific codes for the purposes of intermediating foreign virtual asset trades.

It is important to stress that a licensing regime that has the flexibility to support global liquidity (such as the model proposed above) is pivotal, in our view, for the sustainable and successful development of the Brazilian market, since most if not all local and foreign players that operate in Brazil rely on global liquidity sourced from onshore and offshore market participants.

12. **Should the authorization to operate virtual asset service providers cover existing financial and payment institutions in the country, or should it be linked to a specific and exclusive type of institution to be authorized by the Central Bank of Brazil?**

As between these approaches, Coinbase does not have a strong preference, provided that the Central Bank of Brazil establishes a level playing field between existing institutions and new entrants into the market, and that the authorization process enables new entrants that successfully meet all applicable requirements to begin operating in Brazil without business disruption.

13. **What risk might the participation of a virtual asset services provider, as an entity authorized and regulated by the Central Bank of Brazil, represent in a financial market infrastructure?**

We believe that the regulation of VASPs will reduce the overall risk to Brazil's financial system. Currently, entities that seek to engage in virtual asset activity in Brazil are incentivized to do so either without the proper oversight or by offshoring. By providing a feasible, regulated path to conduct virtual asset activity in Brazil, the Central Bank of Brazil would greatly reduce these more risk-prone incentives.

In addition, as exemplified in the failure of Silicon Valley Bank in the United States, where a bank failure was the cause of volatility in virtual asset markets, contagion risks can flow from TradFi to virtual assets, not only the other way around. As a result, there is little reason to believe that the incorporation of regulated VASPs into the Brazilian financial system will have a destabilizing effect and doing so may instead reduce risk.

14. **It is recommended that virtual asset service providers establish criteria for selecting or choosing the virtual assets made available to their customers' operations. In this regard, which mandatory compliance requirements should be adopted concerning the virtual assets offered and their respective issuers?**

We strongly agree with the Central Bank of Brazil's view that VASPs should be required to establish criteria for the virtual assets they choose to list, but that the ultimate criteria should be the choice of the VASP itself. We believe that requiring certain listing criteria is an important requirement for centralized exchanges. Coinbase evaluates a variety of

listing criteria for new assets in its Asset Listing Process[5] led by its Digital Asset Support Group. Before making an asset available on its platform, Coinbase carefully considers the local regulatory context and thoroughly evaluates each asset, any associated platform or blockchain, the individuals developing or promoting the asset, and Coinbase's own ability to maintain safety and integrity of trading activity involving that asset on its platform.

The success of new protocols depends critically on their ability to reach a wide distribution of users, and if rules are imposed that make it difficult for users to use emerging protocols, then Brazil will be deterring innovation by encouraging developers to aim their efforts elsewhere. Instead, these ultimate determinations should be made by individual VASPs based on their understanding of the needs and financial interests of their clients, as well as their assessment of the risk associated with a given virtual asset.

15. What regulatory requirements are necessary to ensure safety in the custody of virtual assets, considering the differences between this activity and traditional custodians of financial assets and securities?

As we noted in response to Question 1, we believe that efforts to protect and safeguard customer assets and to ensure that VASPs are taking appropriate steps to do so is of paramount importance for a new regulatory regime. However, as we discussed above, we believe that the strength of protections for customer assets can in fact be undermined by the adoption of ill-fitting regulatory requirements, e.g. such as requirements to maintain physical infrastructure or other resources in a specific location or jurisdiction.

As another example, we believe that VASPs, unlike TradFi institutions, should be allowed to combine exchange and custodial functions in the same entity. This combination would create a more efficient process for the market and for individual customers. Today, Coinbase is able to provide both exchange and custodial services through an integrated global platform. Blockchain-based recordkeeping has both enabled this combination and made it more efficient than in the traditional financial system by removing the need for centralized settlement and clearance of market trading activity. Providing both exchange and custody services as part of an integrated business model serves the interest of customers, who gain the benefits of faster settlement and more liquidity. Having a separate local custodian would undermine the efficiency and potentially customer protection. Importantly, the combination of functions also does not lead to any conflicts of interest. If a customer wishes to use an unaffiliated trading platform, the customer can move the customer's virtual assets to the other trading platform. At no point is a user limited to using the exchange solutions provided by an affiliate of the customer's virtual asset custodian.

More broadly, we encourage the Central Bank of Brazil to engage in international cooperation, particularly with respect to issues surrounding custody where varying

[5] Coinbase, Asset Listing Process (2023)

standards would result in significant disruption to virtual assets activities. For example, the International Organization of Securities Commissions has made a number of thoughtful recommendations for how regulators around the world can effectively regulate virtual asset custody.[6] Their recommendations include:

- Prioritizing the safety of client assets in a technology agnostic manner, rather than mandating assets be held in "hot" or "cold" wallets;
- Requiring client assets be held in trust or be otherwise segregated from the VASP's proprietary assets;
- Requiring VASPs to provide full and clear disclosure of the structure and risks arising from custody;
- Requiring VASPs to maintain systems and policies to allow for reconciling client assets; and
- Requiring VASPs to adopt appropriate policies and systems to protect against the loss or theft of client assets.

We would encourage Brazil to adopt measures with these recommendations in mind.

[6] IOSCO, FR11/23 Policy Recommendations for Crypto and Digital Asset Markets (iosco.org), November 16, 2023, 33-38 .

Theme 3 Hiring essential services

16. **In cases where providers maintain custody of customers' virtual assets in custody services providers established abroad, what guarantees must be provided by the entity in the country to preserve clients' funds? What measures are appropriate to ensure access to customer assets and compliance with legal demands and other possible needs?**

    As we have discussed above, we support efforts to protect and safeguard customer assets, including when those assets are held by a third party. Customer assets should be subject to the same protections whether they are held by the VASP itself or by a third party. VASPs can accomplish this by incorporating custody requirements into their agreements with the custody service provider, which should include requirements on segregation and clear recordkeeping the same as if the asset were held by the VASP. Brazil should also cooperate with other jurisdictions and incorporate principles of substituted compliance as appropriate.

17. **Regarding item 16, what guarantees can be required from suppliers for other activities contracted from third parties established abroad, including technology services, to safeguard customers?**

    We support the adoption of similar safeguards for VASPs hiring third parties as already exist in TradFi. In practice, that would mean that VASPs can outsource activities, but they cannot outsource their responsibility to their customers to perform that activity. VASPs should ensure that they maintain service level agreements with any third-party service provider that require the service provider to perform the activity to the same degree as if it were performed by the VASP itself and also provide for a certain degree of control by the VASP.

18. **It is essential to adequately identify and qualify partners, collaborators, or correspondents for services of any kind. In this context, how can virtual asset service providers minimize the risks of hiring third-party services, including other service providers in the virtual asset market, such as intermediaries, custodians, and portfolio and liquidity providers? What rules could be imposed in the infralegal framework to deal with such hiring?**

    As we discussed in response to Question 17, we support the adoption of similar safeguards for VASPs as exist in TradFi. VASPs should be able to outsource to third parties in line with these safeguards. In particular, VASPs should engage in thorough vetting of service providers before entering into an agreement to outsource any services and should perform regular monitoring of their service providers to ensure that any requirements imposed by the VASP or Central Bank of Brazil are being met.

19. **Virtual asset service providers often turn to liquidity providers based in Brazil or abroad to enable their clients' operations. Given this, what specific controls and procedures can virtual asset service providers adopt to ensure that these liquidity providers comply with the regulations applicable to prevent money laundering and terrorist financing? Furthermore, what information should be requested, and what procedures can be strengthened to ensure compliance with international foreign exchange and capital markets regulations?**

    As mentioned in the response to Question 11, we believe that the Central Bank should encourage a virtual asset market that does not prevent or restrict access to global liquidity, and thus recommend the adoption of a licensing regime that is flexible enough to support said development while still adhering to Brazilian foreign exchange rules and regulations, which is the "eFX model" discussed in the referenced response.

    Also, as discussed above in response to Question 17, we believe that detailed service level agreements with third parties should be adopted to ensure that requirements (including anti-money laundering and terrorist financing rules) that apply to the VASP are also applied to the service provider. VASPs should review the service provider's policies in these areas for compatibility with any applicable requirements before entering into a service agreement. In addition, VASPs should engage in ongoing monitoring and testing of the service provider's compliance programs.

Theme 4 **Governance and conduct rules**

20. How are private keys stored in the workflow of virtual asset service providers? What should be and what can be the procedures for storing and managing private keys, including when they are partitioned and assigned to different parties? For each storage procedure, identify how the division of responsibilities between party holders would take place and the risks associated with these procedures. What procedures are - or could be - adopted for the constitution of liens and encumbrances or to carry out the judicial blocking of virtual assets?

Private keys allow a virtual asset custodian to sign transactions involving their customers' virtual assets, often for transactions initiated by customers using the custodian's user interface. As a result, virtual asset custodians often need to maintain the private keys associated with their customers' virtual assets. Custodians have available numerous options to maintain their customers' private keys in a safe manner. For instance, Coinbase stores many of its customers' private keys in cold storage facilities disconnected from the internet.[7]

Virtual asset custodians can take careful measures to safeguard private keys and reduce the risks of hacks. We encourage the Central Bank of Brazil to look to principles developed by other foreign bodies regarding the proper safekeeping of private keys. For example, the Monetary Authority of Singapore has helpfully outlined the following principles that VASPs should embody to ensure the safety of their customers' private keys:

- Ensure that critical system functions and procedures are carried out, or overseen, by multiple individuals ("never alone");
- Segregate duties and responsibilities involved in building out custodian solutions among different groups of employees ("segregation of duties"); and
- Monitor employees' access rights and limit each employee's access to that which is necessary to fulfill their duties ("least privilege").[8]

Customers who utilize third-party custodians may nonetheless suffer loss of their virtual assets. The compromise of customer-held credentials and resulting losses, in spite of protections offered to customers, are referred to as account takeovers. Most account takeovers are due to scams and are independent of safeguards employed by a VASP. Nonetheless, VASPs can offer online security features such as multi-factor authentication that can help mitigate account takeover risks.

Not all custody solutions are the same. Some VASPs offer customers virtual asset self-custody solutions, where the user is ultimately in control of their virtual assets. One

[7] What does Coinbase do with my digital assets?
[8] Monetary Authority of Singapore, Proposed Regulatory Measures for Digital Payment Token Services, October 26, 2022, P008 - 2022.

subset of self-custody solutions relies on technological advances like MPC and multi-sig configurations. These tools allow a VASP to split up a private key into multiple shards and distribute those shares to different entities. Each party holding a shard is required to sign a transaction. MPC and multi-sig configurations provide additional safeguards against theft. Even if the customer's share is stolen, the VASP's shard is also needed to sign any transactions involving the customer's virtual assets. Conversely, if the VASP is hacked, the customer can block any transactions involving their virtual assets by refusing to sign their shard.

21. What are the benchmarks for pricing virtual assets for trading on platforms and exchanges? How can regulation address provisions that mitigate the risks of capturing prices from different providers?

The quoted prices listed on the Coinbase trading platform are determined using a market order book maintained by Coinbase. The market order book tracks, in real-time, buy and sell orders submitted by Coinbase's customers for particular virtual assets.[9] Trading platforms should generally adopt similar practices to make sure that pricing for a particular virtual asset reflects the balance of supply and demand on the platform at any given time. This will enable effective arbitrage by market participants across trading platforms both within jurisdictions and globally, so that consumers benefit from price parity no matter where they are.

22. What mechanisms can be adopted to identify and curb attempts at market manipulation and fraudulent practices?

Market surveillance is an important means to prevent or detect abusive behaviors. VASPs can employ software that monitors and detects the trading activities of their customers and employees for potential market manipulation, fraud, behavioral patterns, and rule violations. The software and any alerts generated can be monitored by a team with regulatory, trading, and surveillance experience.

Notably, the market surveillance tools used by VASPs can be superior to those commonly used by securities exchanges. As one example, Coinbase's market surveillance system operates on a real-time basis, 24/7/365, as compared to the typical T+1 or T+2 monitoring lag common for such systems in TradFi markets. Because virtual assets settle instantly, VASPs need instant visibility into their markets, and every VASP should be performing market surveillance proactively. In addition, Coinbase's surveillance system uses machine learning techniques to add an additional layer of monitoring above manual tracking, enabling real-time, actionable insights.

[9] For more information on how Coinbase determines quoted prices, see the discussion of "Trading fees and spread" at Coinbase pricing and fee disclosures.

VASPs have also developed best practices to manage and address potentially abusive behaviors. These practices build on tools and learning from TradFi markets, with further enhancements specific to virtual asset markets. Coinbase has for years made public the principles and approaches that guide its market integrity and trade surveillance operations.[10] And as Coinbase continues to gain experience, it applies this knowledge to further its longstanding mission of leaning into compliance in virtual asset markets. Coinbase currently takes the following steps, among others, to safeguard its platform from abuse:

- Maintain insider trading policies that prevent those associated with Coinbase from trading virtual assets with non-public information, including based on changes to its list of supported virtual assets, with an enhanced policy for employees who have more insight and control over non-public information;
- Provide employees with a regularly updated list of restricted virtual assets to prevent any such insider trading;
- Mandate that all Coinbase employees and directors trade virtual assets that Coinbase supports only on its platform so we can proactively disable trading for certain assets and have full visibility into employee and director trading behavior to monitor for prohibited trading activities;
- Prohibit the use of trading algorithms by Coinbase employees;
- Prohibit wash trading, trade spoofing, trade layering, front-running, trade churning, and quote stuffing;
- Maintain an auction process for natural price discovery, matching bids and offers on the first day of a listing or for the restarting of trading; and
- Follow an escalation process for when we find instances of market manipulation that includes reporting to the appropriate regulatory authorities and taking steps to prevent further manipulation by a given customer, including by removing their access to its platform.

The Central Bank of Brazil can also play a role in preventing manipulation in virtual asset trading markets. Prohibitions on front-running, wash trading, momentum ignition strategies, spoofing, and other manipulative trading practices should be strongly considered by Brazil, to promote fair, orderly, and efficient virtual asset markets.

23. How does the settlement flow of asset purchase and sale transactions occur at virtual asset service providers and related partners? How does this flow differ from the financial assets and securities settlement processes?

When offering on-chain settlement, Coinbase combines order matching and custody, making its trading platform safer and more efficient. Customers can on-board their virtual assets to Coinbase, trade their virtual assets, and then move their virtual assets back to their personal or custodial wallets. Leveraging the 24/7 nature of the blockchain, all of

[10] Coinbase, How Coinbase thinks about market integrity and trade surveillance (Oct. 11, 2021).

these actions can take place within a matter of minutes. As a result, transactions are able to settle in real-time, meaning that there is little to no risk that a transaction fails to settle. This real-time settlement reduces inefficiencies and mitigates the potential harm that consumers may face as a result of delayed settlement.

Coinbase also provides off-chain settlement for virtual asset exchanges between Coinbase customers. Leveraging its combined custody and order matching functions, Coinbase allows two users to instantly exchange virtual assets without incurring transaction fees. Any virtual asset exchanged through Coinbase's off-chain settlement service remains in Coinbase's omnibus wallet, where Coinbase holds virtual assets for the benefit of its customers. Coinbase updates its ownership records to reflect the change in ownership of the exchanged virtual asset.[11]

Meanwhile, in TradFi markets, transactions can take days to settle. Various entities are responsible for carrying out different responsibilities. For instance, many securities markets rely on centralized securities depositories to act as recordkeepers of customers' securities holdings. Whenever a customer transacts through a securities broker or exchange, the broker or exchange must verify the customers' holdings with the centralized securities depository. The depository is then tasked with matching the order requests it receives from different brokerages and exchanges. Verification can take days and is often more difficult during times of heavy market volatility. As a result, settlement failures are more common in TradFi markets. Some centralized securities depositories make efforts to reduce counterparty risk, like requesting market participants to pledge collateral against settlement failure. These capital requirements, however, can inconvenience customers.[12]

24. Considering the volatility of asset prices and, in some cases, even of the fees for some types of transactions, what measures should virtual asset service providers adopt to guarantee clear information about the costs charged so that clients can make decisions that are in line with their interests, needs, and objectives? What regulatory requirements could ensure that the customer properly understands this information?

A virtual asset's price is affected by numerous factors, including market trends and material events that affect the virtual asset's native protocol. Coinbase provides customers with publicly available information for each of the virtual assets listed on the

[11] For an explanation of Coinbase's off-chain settlement services, *see* Coinbase, Off-chain Sending and Receiving.

[12] A notable example of this inefficiency in the United States is the GameStop episode in 2021, which highlighted the potential harm to consumers within the current regulatory system. A sharp spike in retail trading caused a dramatic increase in the volatility and trading volume of GameStop shares. As a result, some brokers needed to suspend trading because National Securities Clearing Corporation models required capital in excess of what was being held. Such an episode could have been averted with real-time settlement as currently practiced in virtual asset markets.

Coinbase trading platform.[13] We believe that providing customers with all readily available information allows them to make fully informed decisions. The Central Bank of Brazil should encourage VASPs to share information with customers where information regarding a virtual asset's development is readily available. However, in some instances, information regarding a virtual asset's native protocol or platform may not be fully available. For example, some virtual assets relate to fully decentralized projects where information regarding the projects is not made public. We do not believe Brazil should hold VASPs liable if pertinent information relating to certain virtual assets is not publicly available.

We also believe that VASPs should be transparent about the fees charged to customers. Consumer platforms that engage directly with customers and provide exchange services, or brokers that operate exclusively on a single, specialized platform on behalf of its customers, should clearly disclose their pricing models, including plain-language explanations of all fees charged. For example, prior to any transaction, Coinbase indicates to each customer the fees the customer will pay for a particular transaction. Coinbase also identifies the bid-ask spread that the customer may experience in the particular transaction. We believe that these open disclosures, along with Coinbase's explanation of its pricing and fees model, properly inform customers transacting on the Coinbase platform.[14]

While it may be proper for the Central Bank of Brazil to indicate the types of disclosures VASPs should make to customers regarding pricing and fees, Brazil should not prescribe the form of disclosure provided by VASPs. VASPs are subject to regulations from numerous worldwide entities, including those that relate to consumer disclosures, and should be allowed to use forms similar to those required by other jurisdictions. Creating additional disclosure forms could cause consumer confusion as residents of different countries will need to refer to different places to find their relevant disclosures.

25. Should a minimum percentage of assets held in cold wallets be defined? What is the technical basis for establishing this percentage?

We support the Central Bank of Brazil's goal of providing assurance to virtual asset market participants that their assets are protected, and we think that cold storage can help achieve this objective. However, we do not think that it is appropriate to impose on all custodians a requirement that a certain percentage of virtual assets be held in cold wallets. For example, during times of high demand, a virtual asset custodian subject to a cold storage requirement may need to pull virtual assets out of cold storage to meet

[13] For example, Coinbase provides customers interested in exchanging bitcoin with helpful resources discussing bitcoin. Coinbase helpfully links to a website established by Bitcoin.org to disseminate information on bitcoin development efforts and directs customers to the Bitcoin whitepaper. *See* Coinbase, *About Bitcoin*.

[14] For Coinbase's explanation of its pricing and fees model, *see* Coinbase Pricing and Fees Disclosure.

customers' withdrawal requests. However, virtual assets held in cold storage may have a lengthy withdrawal process. As a result, during heavy redemption periods, virtual assets custodians may not be able to quickly meet their customers' withdrawal requests.

Further, technologies other than cold storage may be equally appealing. For example, other wallet storage technologies, like Coinbase's MPC solutions discussed in response to Question 20, are also highly secure solutions for exchange use-cases and should be permitted. While historically Coinbase has held an overwhelming portion of its customers' virtual assets in cold storage, that was largely because the technology used to store virtual assets was still evolving and we believed it was the best security solution available at the time. We see areas of technological innovation maturing to a point where a suitable combination of wallet technologies can provide a high level of security while offering faster access to stored virtual assets, thereby better balancing the security versus availability trade-off.

We have had productive discussions with other governments regarding our wallet technologies and we would welcome the opportunity to have similar discussions with the Central Bank of Brazil. It would be desirable to have the flexibility to store virtual assets in a variety of wallet types based on business needs, as long as a comparable level of security can be guaranteed. Prescribing a strict percentage of virtual assets that must be held in cold storage will largely foreclose virtual asset custodians from responsibly adopting any technology outside of the traditional cold storage option.

26. Can virtual asset service providers provide liquidity to their client's operations, acting as counterparties in the transactions? What methods and limits should be adopted to curb the risks involved in these operations?

Virtual asset trading platforms that operate order matching engines depend on the participation of market makers, which provide liquidity to customers through a willingness to take either side of a transaction and earn a spread.

However, issues may arise when a virtual asset trading platform has an affiliate that acts as a counterparty to its customers' exchanges. The affiliate may have an unfair advantage when trading on the platform, especially if it has privileged access, lower latency, or other preferred terms. This conflict is exacerbated if the affiliate has access to confidential information, such as counterparty positions and orders, which may inappropriately inform trading and lead to the front running of customers. The risks of combining these activities are high and any market making arrangement tied to exchange order matching should be clearly disclosed and subject to a commensurate level of controls and oversight. In addition to implementing information barriers and independent governance, as noted below, trading platforms should be required to treat all market makers on the same terms irrespective of affiliation.

Mitigating potential conflicts of interest from combined functions begins with separate governance and management to help ensure that decisions are made independently. Well-constructed and understood information barriers can minimize opportunities for improper use of information. Clear articulation of the duties that employees have to customers can clarify whose interests need to be considered. Disclosure and the transparency of the blockchain can keep the market and regulators apprised of inter-company relationships. Simple to understand, written disclosures should help customers understand any potential conflicts of interest.

27. One of the most relevant issues about virtual assets is the characterization of control over these assets. In your opinion, what is the most appropriate way of defining control over virtual assets and how does this definition fit in with cases of key sharing?

We appreciate the Central Bank of Brazil's desire to ensure that custodians that safeguard virtual assets do so in a safe and responsible manner. To achieve this policy objective, we believe the Central Bank of Brazil should focus its regulation on entities that can move a customer's virtual assets without the customer's input. Therefore, any definition of "control" should relate to a person's ability to unilaterally transfer a virtual asset.

A standard virtual asset custodian often can move customer assets between accounts and may even be able to rehypothecate customer assets. We believe it would be prudent for the Central Bank of Brazil to craft a definition of "control" that prevents misuse or misbehavior by virtual asset custodians involving their customers' virtual assets.

However, we urge the Central Bank of Brazil to recognize that issues present with standard virtual asset custodians are not applicable to VASPs that provide MPC and multi-sig custody solutions (**MS Providers**), which are discussed in response to Question 20. An MS Provider's private key is necessary to effect a transaction. But it is not sufficient. Therefore, issues related to the misuse of customers' virtual assets are not present.

The Central Bank of Brazil should refrain from broadly defining "control" to capture MS Providers. Otherwise, Brazil may improperly subject MS Providers to requirements that should only apply to "true" digital financial asset custodians – i.e., entities that, like traditional custodians, have sole practical control over a customer's assets. These requirements, which are likely designed for financial intermediaries and custodians, are ill-suited for software developers like MS Providers.

28. **The provision of virtual asset services adequately and consistently presupposes a minimum organizational structure, which includes governance capable of guaranteeing adherence to current legislation and regulations, systems for processing and controlling operations, and information security. What would be the minimum organizational structure for adequate governance of virtual asset service providers? The fulfillment of conditions like these by organizations can be attested to by some certifications currently on the market. Considering the peculiarities of the segment, what certifications would be appropriate for a virtual asset service provider that wants to operate regularly and serve its clients well?**

We agree that VASPs should develop a governance structure that addresses their regulatory obligations. Such governance structures are required by many regulatory regimes. For example, consistent with the requirements of the New York State Department of Financial Services' BitLicense regulatory regime, Coinbase has implemented an anti-money laundering program, cybersecurity policy, and business continuity and disaster recovery plan. Coinbase has also developed governance procedures to ensure proper oversight of functions, reporting to leadership, and review of policies.

The BitLicense Regulations identify the key risks that all VASPs face. They require that each VASP develop written policies and procedures addressing the risks and appoint individuals to oversee certain risk management programs. We believe the Central Bank of Brazil should consider requiring similar broadly-applicable governance features.

The Central Bank of Brazil should be mindful that the risks faced by VASPs vary based on their specific lines of business. A VASP that provides custody solutions to customers faces different risks, and requires different capabilities, compared to a VASP that issues stablecoins. Therefore, any governance requirements put forward by Brazil should provide VASPs with flexibility to adapt the requirements to their line of business.

29. **It is essential that companies carry out a proper risk assessment to identify how their products and services could be used for illicit purposes, such as money laundering and unauthorized or unofficial transfers. In this context, what kinds of crimes can be committed through transactions with virtual assets? How can virtual asset service providers act to prevent this type of crime from occurring?**

As discussed in response to Question 7, illicit activity can be conducted through all forms of assets and mechanisms, most notably with cash and through TradFi institutions. While illicit activity can also be performed using virtual assets, as noted above, the rate of illicit activity conducted through virtual asset transactions is considerably lower than through TradFi.

The evidence demonstrates that illicit actors—ransomware groups, sanctioned entities, darknet markets, scammers, and other cybercriminals—seek out VASPs located in jurisdictions that do not enforce (or do not have) applicable anti-money laundering

requirements.[15] This is no mystery, as criminals prefer VASPs that require minimal (if any) know-your-customer (**KYC**) information, do not restrict their customers from exchanging funds with illicit counterparties, and do not file suspicious activity reports (**SARs**) with government authorities. In failing to implement anti-money laundering controls, noncompliant VASPs not only attract criminals; they also attract some law-abiding customers who may simply want to avoid the hassle of providing KYC information that compliant VASPs are required to collect. This gives noncompliant VASPs a competitive edge for engaging in improper behavior. The Central Bank of Brazil is uniquely positioned to use its authorities to ensure that all VASPs with ties to Brazil are held to the same standards and to rout out illicit finance risks posed by this arbitrage.

Nonetheless, companies like Coinbase have devoted significant resources to developing effective compliance programs. This includes traditional controls like collecting customer information, monitoring on-platform transactions, and filing SARs. For example, Coinbase complies with sanctions laws and regulations in the jurisdictions where it operates. Coinbase also has in place systems designed to capture and prevent attempts to conduct illicit activity on Coinbase's platform.

VASPs have also begun to deploy innovative technologies that leverage the public and transparent nature of the blockchain to combat illicit activity. Blockchains collect all transactions and record them on a common, public ledger. As discussed above, public ledgers mean VASPs can conduct sophisticated analyses to determine the risk of a specific transaction or asset – using tools and methods broadly referred to across the virtual asset ecosystem as know-your-transaction (**KYT**). A number of high quality blockchain analytics firms have developed in recent years to assist both VASPs and law enforcement in utilizing the abundant data available on public blockchains.

VASPs can combine KYT with traditional compliance tools to enhance their risk ratings of customers associated with those transactions. Whereas KYT is immediate, independent, and dynamic, traditional KYC information is the opposite. It is based on financial institutions collecting static data points about a customer at the time of account opening, such as identification documents, account statements, corporate records – and typically only occasionally refreshing those data points.

Further, VASPs have used KYT in their compliance programs by directly incorporating it into transaction monitoring tools so that a VASP can be alerted when a customer engages in risky transactions, as well as screening for sanctioned crypto addresses and identifying larger networks of addresses that are associated with the sanctioned addresses in order to prevent their customers from transacting with such addresses.

[15] For example, see Chainalysis, *The 2021 Crypto Crime Report*, 9, 13, 74 (Feb. 16, 2021), https://go.chainalysis.com/2021-Crypto-Crime-Report.html (highlighting that "[cybercriminals] rely on a surprisingly small group of service providers to liquidate their crypto assets," including "money services businesses with lax compliance programs").

Coinbase has leveraged the power of blockchain technology to build out a suite of scaled compliance solutions for governments, financial institutions, and other VASPs.[16] These tools allow entities to monitor transactions in real time and proactively prevent fraudulent activity. They also enable entities, including VASPs, to satisfy anti-money laundering requirements.

30. **The anti-money laundering regulations require the identification of final beneficiaries for legal entity clients. How are virtual asset service providers meeting this requirement? What tools or mechanisms are they using? How can these institutions ensure compliance with the Travel Rule by Recommendation 16 of the Financial Action Task Force/Global Financial Action Task Force (known as FATF/GAFI in Portuguese)?**

We appreciate the need to combat illicit finance activity using KYC and other procedures. Coinbase conducts a multi-step process to confirm the identity of its customers, using personal identification and customer-submitted information. When onboarding institutional customers, Coinbase requires these types of customers to include personal identification information for any of their material beneficial owners, and Coinbase uses independent sources to verify such information on a risk-sensitive basis.

We also recognize the role that the Travel Rule plays in combating illicit finance. For traditional financial institutions, Travel Rule compliance is relatively straightforward: they can easily identify their financial institution counterparties and include Travel Rule data with the underlying transmittal orders. But for VASPs, the blockchain alone does not identify when a counterparty is another VASP, and there is no way to include Travel Rule data in the transmittal order itself. Thus, applying the Travel Rule to crypto transactions raises complex technical challenges around accurately identifying other VASPs and securely transmitting highly sensitive Travel Rule data.

To address this issue, Coinbase has worked alongside a large group of VASPs over the last few years to pioneer the development of the Travel Rule Universal Solution Technology (**TRUST**) – a Travel Rule solution that allows VASPs to accurately identify their counterparties and securely exchange required data. We have invested significant legal, compliance, engineering, and other resources to build the TRUST solution, which VASPs around the world are already using to exchange information required under the Travel Rule.

TRUST's rapid growth since its launch in 2022 is a testament to the industry's commitment to solving complex compliance challenges. All VASPs who join TRUST undergo comprehensive evaluations to help ensure that their security protocols are equipped to prevent unapproved access to sensitive customer data shared by TRUST participants. Further, TRUST was designed so that no customer personally-identifying information is stored on a centralized database but is instead only shared directly

[16] *See* Coinbase, Scaled Compliance Solutions from Coinbase.

between counterparty VASPs via encrypted, peer-to-peer channels, reducing the risk of hacking or improper access. These and other features have been critical to TRUST's growth to become the world's leading Travel Rule solution.

31. **It is considered essential that companies are prepared to comply immediately, in the form of Law No. 13,810, of March 8, 2019, with the determinations of unavailability of assets provided for in resolutions of the United Nations Security Council (UN) or its sanctions committees. How should virtual asset service providers handle suspicious transactions? How should anti-money laundering and anti-terrorist financing (AML/CFT) monitoring be carried out?**

VASPs should implement AML/CFT monitoring by relying on the powerful new set of compliance tools that enhance the effectiveness of identifying and disrupting illicit finance. As noted in the response to Question 29, these tools (generally referred to as KYT) harness the public and transparent nature of the blockchain, allowing VASPs to track the flow of assets beyond what happens on their individual platforms, thus giving them a far deeper and richer understanding of the risks posed by specific transactions and customers. Blockchain data can then be combined with traditional compliance tools (e.g., gathering personal information when onboarding a customer) to enhance transaction monitoring and screening, customer risk ratings, SAR filings, and market integrity, all leading to more effective compliance.

Theme 5 **Cybersecurity**

32. Cybersecurity is one of the critical issues for the proper functioning of virtual asset service providers. What are the requirements for maintaining this security in the segment, and what factors mitigate cyber risk in the segment?

VASPs should have a framework in place for addressing cybersecurity risks. The framework should identify the protections the VASP takes to protect customers' virtual assets as well as the VASP's business continuity policies and procedures. VASPs should perform an operational business impact assessment annually that identifies critical business processes and support systems, and they should regularly test their systems for critical weaknesses.

Importantly, VASPs require customers to entrust them with certain information, including their private keys in some instances, in order for the VASPs to perform certain services. VASPs should ensure that they have adequate protections in place to protect their customers' sensitive information. Moreover, VASPs should be equipped to monitor for, and prevent, possible third-party takeover attempts involving their customers' accounts. Although not all instances of customer takeovers can be prevented, VASPs can take steps to further protect their customers' accounts.

Coinbase has implemented a number of tools to protect customer property and accounts, including:

- Automatically enrolling customers in two-step verification;
- Irreversibly hashing any passwords stored by customers in Coinbase's database;
- Monitoring third-party data breaches and darknet markets for threat indicators;
- Providing customers with the ability to lock their accounts; and
- Using machine learning models to evaluate customers' virtual asset transactions for potential fraudulent activity.

Theme 6 **Providing information and protecting customers**

33. The adequate provision of information to clients, concerning the risks of transactions with virtual assets, is one of the main points for the proper discipline of the virtual asset market. Therefore, what is the leading information to be provided to clients to guarantee an adequate level of information for clients and users?

We agree that virtual asset customers need to be properly informed about the risks involved in transacting in virtual assets. VASPs should educate their users through transparent and easy-to-understand disclosure statements. For example, a VASP could provide customers with a Virtual Asset Risk Statement that describes the risks of trading or acquiring virtual assets. The Virtual Asset Risk Statement could be provided to customers when they onboard onto a VASP's platform.

From experience with our customer base, we have found that risk warnings are best comprehended and internalized where they are fewer (between 2-3) and when they are highlighted in the logged-in experience just before a product or service is accessed for the first time. A lengthy Disclosure Statement shown to a user during onboarding has a risk of not being properly read and understood (or accurately remembered at the appropriate time).

We believe that the Central Bank of Brazil should coordinate with VASPs to determine whether industry guidance on assessments, education programmes and disclosures would be effective. Such practices can help ensure a consistent baseline level for all retail customers. But we also believe that VASPs should retain a degree of flexibility to implement their own customer assessments, education programmes and disclosures that are tailored to their particular set of virtual asset services.

34. If virtual asset service providers allow by electronic means trading, transfer, use as a means of payment or use as investment of digital instruments representing value, stabilization mechanisms in relation to a specific asset, to be carried out electronically or a basket of assets, policies and procedures must be implemented to ensure the suitability of the instrument to the profile of its clients. What elements are necessary to implement this policy?

Assessments of retail customers' knowledge of the risks of certain virtual asset services may be appropriate. However, we recommend that the Central Bank of Brazil ensure that the assessments are appropriately calibrated to avoid unnecessarily excluding retail customers from virtual asset services. Retail use of virtual assets in Brazil has increased in recent years. Any suitability requirements that exclude large swaths of retail customers will impede the growth of the virtual assets market in Brazil and prevent Brazilians from using virtual assets in their everyday lives.

Any suitability calibration should depend on the virtual asset service being used. For example, the risks of virtual asset custody offerings differ from those of virtual asset brokerage activity. A deficiency in a retail consumer's knowledge of virtual services should not disqualify the consumer's ability from ever using virtual services. Users should have an opportunity to retake the assessment.

Rather than apply harsh bans, we believe that Brazil should require VASPs to provide clear disclosures on the risks faced by virtual asset customers. We believe that risks can be managed with explicit acceptance of the risks of such transactions, clear risk disclosures, educational initiatives and knowledge assessments. Outright restrictions are not necessary.

35. **In the process of distributing, placing, and trading virtual assets, the provision of information on the instruments must be guaranteed through reliable documents made available to the client, which must be in clear, objective language and appropriate to their nature and complexity, to allow a broad understanding of the operating conditions, their mechanisms and the risks incurred. In this process, what information is needed to fulfill this guarantee unequivocally?**

As noted in response to Question 24, a virtual asset trading platform can provide its customers with any publicly available documents regarding the virtual assets listed on the trading platform. Often, the teams that are working to develop a virtual asset have put together an information repository that explains how the virtual asset is meant to function and to be used on-chain. Through these documents, they also discuss their plans to further develop the virtual asset, or its associated protocol or ecosystem. By linking to these documents, virtual asset trading platforms empower their customers to make informed trading decisions. However, a virtual asset trading platform should not be held liable for any misinformation contained in these materials, nor should a virtual asset trading platform be held liable if certain material information concerning a listed virtual asset is not made publicly available.

Theme 7 **Transition rules**

36. How should the transition rule provided for in Article 9 of Law 14,478 of 2022 be regulated? Should adjustment phases be established? Should the time and criteria for adaptation be segmented according to the risk and size of the providers? If so, what criteria should be considered when regulating the transition rule? Considering the minimum period of six months in the transition rule, what would be the ideal period for the Central Bank of Brazil to establish?

We commend Brazil's approach toward the implementation of the regulatory measures. Issuing guidelines as a first step will help ensure all input on this complex and important topic are appropriately addressed.

Given the complexity and importance of developing an effective, fit-for-purpose regulatory framework, we do not think locking in a specific transition period would be prudent. There will need to be a careful analysis that should not be rushed. This is particularly the case because the guidelines will likely require technology and operational builds, which take time to do correctly. As the Central Bank of Brazil has recognized, technological and operational issues can lead to the irretrievable loss of private keys, and so it is important that VASPs are provided the time to implement the guidelines correctly.

Coinbase and many other VASPs are also responding to several other consultations—both in other regions and at the international/supranational coordinating level. We believe it would be highly beneficial for the industry and the regulatory authorities to establish a globally harmonized regulatory framework that applies consistent standards across as many jurisdictions as possible. To that end, we hope that the Central Bank of Brazil, where possible, will consider global best practices that the industry associations and certain supranational mainstream finance organizations endeavor to develop at present. This will help promote consistent regulatory and operational standards, reduce the risk of regulatory arbitrage, and minimize unnecessary operational costs. This alignment should include not only substance, but timing.

37. What are the main difficulties you foresee regarding the transition leading to effective authorization by the Central Bank of Brazil, both for virtual service providers and for other entities that support them in the virtual asset segment?

As noted in response to Question 36, VASPs will need time to comply with any comprehensive regulatory scheme put forward by the Central Bank of Brazil. The regulations discussed by the Central Bank of Brazil span many topics, ranging from custody solutions to anti-money laundering controls. They implicate nearly every line of Coinbase's business. While Coinbase already has a robust compliance mechanism in place, it may need to adapt its current technological offerings and adjust its operations to ensure that it properly adheres to the particular features of Brazil's regulations. Coinbase

will likely also need to hire and train new personnel to help it carry out these new regulations.

Meanwhile, at the same time that Brazil is considering new regulations for VASPs, other jurisdictions are contemplating doing the same. Coinbase, and other VASPs, will have to address the regulations put forward by other jurisdictions, further complicating their ability to quickly and efficiently adjust to Brazil's new regulations. As a result, we encourage Brazil to work with VASPs, including Coinbase, as well as other jurisdictions to develop a harmonious global regulatory scheme.

Theme 8 General manifestations

38. Considering the complexity and length of the issues surrounding the virtual assets segment, what elements not addressed in this public consultation should the Central Bank of Brazil consider when regulating the virtual assets market?

We appreciate the Central Bank of Brazil's thoughtful questions and attention to the important issues raised in this consultation. We would be happy to further engage with the Central Bank of Brazil to address the questions raised in this consultation and look forward to working together in the future to continue Brazil's progress towards becoming a global virtual asset hub.