BitGo

THE MARKET LEADER IN INSTITUTIONAL CRYPTOCURRENCY FINANCIAL SERVICES

BitGo's Responses to the Australian Treasury's "Token Mapping" Consultation Paper

2 March 2023

2443 Ash St. Palo Alto, CA. 94306 | www.bitgo.com

Background to BitGo

BitGo provides regulated custody, staking, financial services, and core infrastructure for investors and builders alike. As a global leader in crypto asset security, custody, and liquidity, BitGo provides the operational backbone for more than 1,500 institutional clients in over 52 countries – a list that includes many regulated entities, and governments, as well as the world's top cryptocurrency exchanges and platforms.

Founded in 2013, BitGo pioneered the first commercially ready multi-signature crypto asset wallets, and for the past decade has provided the most secure, compliant, and scalable crypto asset custody infrastructure solution in the market with a proven track record of processing over US$2 trillion in total transactions and 20% of all Bitcoin transactions as the custodian for Wrapped Bitcoin (wBTC).

BitGo is regulated in various jurisdictions and holds itself to high regulatory and compliance standards. In the USA, BitGo is regulated in South Dakota and New York, and registered with FinCEN. In Europe, BitGo holds regulatory licenses and registrations in Germany, Switzerland, Italy, Poland and Greece. BitGo is also awaiting regulatory approval for a license in Singapore.

BitGo has operated in Australia since 2017 and currently supports many of the country’s largest cryptocurrency exchanges, asset managers, traditional financial institutions and web3 startups to responsibly custody and safeguard their clients’ crypto assets. With our experience operating both in Australia and in many regulated global markets, we look forward to assisting the Government in its efforts to develop appropriate regulatory settings for the Australian crypto sector.

BitGo would be happy to meet with you to provide you with a further overview of what we do, and to share our thoughts on best practices and regulating the crypto asset industry.

Responses to Consultation Questions

Q8) In addition to the functional perimeter, the Corporations Act lists specific products that are financial products. The inclusion of specific financial products is intended to both: (i) provide guidance on the functional perimeter; (ii) add products that do not fall within the general financial functions.

a) Are there any kinds of intermediated crypto assets that ought to be specifically defined as financial products? Why?

b) Are there any kinds of crypto asset services that ought to be specifically defined as financial products? Why?

BitGo's Response

"Custodial wallets" for crypto assets should also be considered as financial products, and the provision of such custodial wallets should be made a regulated activity requiring licensing from the relevant Australian agency such as ASIC.

There are a variety of crypto asset wallets available, of which not all should be considered as "custodial wallets". A custodial wallet should only be one whereby the wallet provider has sole, unilateral control of, and can unilaterally transfer crypto assets out of the wallet without requiring any other co-approvers/co-signers.

For such "true" custodial wallets, the wallet provider holds/controls all the required quorum of private keys (or, in the case of multi-party computation ("MPC") wallets, the required number of "shares") to unilaterally effect transfers of crypto assets out of the custodial wallet. To illustrate, take the case of a three-key multisignature wallet that requires a minimum quorum of two of the wallet's associated private keys to approve any transfer of crypto assets out of the wallet; the wallet should only be considered as a "custodial wallet" if the wallet provider controls at least two of the three private keys.

Crypto asset wallets where the wallet provider either holds none of the private keys, or an insufficient number of private keys to unilaterally transfer crypto assets out of the wallet, should be considered as

non-custodial (or “self-custody”) wallets and should not be defined as a financial product. The provision of such non-custodial wallets should also not be considered a regulated financial activity. Examples of such non-custodial wallet services include:

- Firms which provide backup key storage services, in which a customer who owns a 2-of-3 multisignature wallet gives the firm just one of the three keys to hold as a backup in case the customer loses his other two keys.
- Firms which hold only one key of a 2-of-3 multisignature wallet so they can act as a trusted co-signer for a customer’s wallet, with the firm only co-signing a transaction if it has verified that the transaction looks legitimate and does not breach any wallet policies the customer has previously set (e.g. the wallet policy could set limits on the maximum amount and frequency of crypto assets that can be withdrawn from the wallet).

A corollary of only considering wallet providers which can unilaterally transfer crypto assets out of a wallet as providing custodial wallet services (and as actual custodians) is that firms which provide wallet solutions or wallet technology where they do not possess such unilateral control of the wallet should be prohibited from describing themselves as “crypto asset custodians” or say they are providing “custodial wallets”. Referring to themselves as such may cause their customers to mistakenly believe that their crypto assets are being fully safeguarded by a regulated firm, when in reality the firm would be neither safeguarding all the requisite private keys to the wallet nor be regulated as a true custodian.

In addition, the meaning of “custody” from first principles should imply custody or safekeeping of property in a legally segregated and bankruptcy remote construct, meaning that in the event of default of the custodial wallet provider, their assets would be safe from the creditors of the wallet provider. “Custody” is also usually accepted to mean legal segregation and bankruptcy protection of client assets, as opposed to just technological / cyber, operational safeguards to protect customers’ assets which may not possess true legal segregation and bankruptcy protection. As such, a firm which purports to be providing “custody” or “custodial wallet services” must be able to demonstrate that it is providing “true” custody.

Q9) Some regulatory frameworks in other jurisdictions have placed restrictions on the issuance of intermediated crypto assets to specific public crypto networks. What (if any) are appropriate measures for assessing the suitability of a specific public crypto network to host wrapped real world assets?

BitGo's Response

Though the consultation paper does not specifically seek comments with regard to wBTC mentioned in paragraph 82 of the paper, as the sole custodian for wBTC, BitGo would like to clarify that the details of the wBTC arrangements are publicly available, such as through the wBTC whitepaper which sets out the detailed processes how wBTC works. We would also like to to provide the following information on wBTC for your reference:

1. wBTC operates through a model of Merchants and Custodians:
    a. Merchants (such as crypto exchanges) are institutions that onboard to BitGo and go through an extensive KYC process
    b. The custodian (i.e. BitGo) serves the role of custodian for wBTC

2. There is a separation of responsibilities (and powers) between Merchants and Custodians to ensure that the Bitcoin is independently custodied by BitGo rather than by the Merchants.

3. Merchants (once KYC-ed) can MINT (create wBTC from BTC) or BURN (remove wBTC for BTC).

4. Custodians verify MINT and BURN requests are valid (by verifying the amounts, merchant, etc.)

5. This overall structure, means that wBTC and participants benefit in the following ways:

    a. The BTC that is used to MINT wBTC is held by the Custodian (BitGo) on behalf of the Merchant.
    b. If BitGo were to cease operations, its bankruptcy remote provisions would kick in and ensure that the Merchants get their BTC back.
    c. Simultaneously, because Merchant funds (e.g. BTC) are held in BitGo custodial accounts, funds are insured up to US250M (though insurance BitGo has procured) in the event of loss or theft of keys and/or insider theft / dishonest acts by BitGo

employees.

6. Proof of reserves: The WBTC website has a proof-of-reserve section that is live (updates as things happen). This proof of reserve works by taking in on-chain data for WBTC and reconciling them with BTC data from BitGo Trust's cold storage wallets (that are managed for Merchants). In addition, there is a third party oracle /proof of reserve developed by Chainlink that also maintains live data and audits.

Q11) Some jurisdictions have implemented regulatory frameworks that address the marketing and promotion of products within the crypto ecosystem (including network tokens and public smart contracts). Would a similar solution be suitable for Australia? If so, how might this be implemented?

BitGo's Response

"Reverse solicitation", whereby a customer in Australia proactively reaches out to an overseas firm on his own initiative to request for financial products, should be permitted for crypto assets deemed "financial products". Such reverse solicitation arrangements are often permitted in other jurisdictions without requiring a license. For instance, the UK has recently issued a consultation paper on a proposed regulatory framework for crypto assets, and the paper contemplates allowing reverse solicitation arrangements without needing a license in the UK.

In addition, as described in our response to Q8 above, where a crypto asset or activity involving crypto assets is not deemed as a financial product or regulated financial activity respectively, these should fall outside the financial regulatory perimeter and firms should be allowed to market and sell such products in Australia without requiring licensing or permission from the relevant financial regulator (i.e. ASIC).