

Submission to ASIC's Consultation Paper 381 - INFO 225: Digital assets: Financial Products and Services - Block Inc.

Thank you for the opportunity to provide a submission to ASIC's [CP 381 Updates to INFO 225: Digital assets: Financial Products and Services](#). Block, Inc. is a financial services and digital payments company that provides payment and software solutions to merchants through our brand Square, and buy now pay later services through our brand Afterpay. In relation to digital assets, we offer a self-custody bitcoin wallet called [Bitkey](#). Our responses to the consultation questions are outlined below:

- ***Question 2. Are there any topics or guidance that were included that you think should not have been included? Please provide details.***

The proposed regulatory treatment for wallets under the definition of a non-cash payment facility is currently too broad and risks mischaracterising self-custody wallets. Namely, the guidance should clearly distinguish between custodial and non-custodial wallets for digital assets. With a non-custodial wallet, the end-user (e.g. customer) retains full control and direct ownership of the asset, maintaining autonomy over their funds without intermediary risk. The non-custodial wallet hardware and software is provided to a customer to self-manage their digital assets directly. This is distinctly different from 'custodial' wallets where an intermediary party holds the digital assets and can exert a degree of control over those assets.

Technical principles of self-hosted wallets for digital assets

Self-hosted wallets such as Bitkey are software and/or hardware tools that a customer can purchase to aid with self-management of the credentials needed to access and use their digital assets. Developers and providers of self-hosted wallets do not have control over or insight into what customers do with the assets that they have the credentials stored in their wallet. They cannot access, freeze, or control user funds, nor can they initiate or block transactions. They do not hold the underlying accounts for their customers, or other non-cash payment facilities that are identified and covered in RG 185.

The concept of a self-custody wallet is particularly relevant given the nature of how blockchain-enabled digital assets function. Digital assets (such as Bitcoin) cannot leave the blockchain on which they are issued. The blockchain is a public distributed ledger that tracks which assets are associated with which blockchain addresses (i.e. the owner of the asset). A transaction on a blockchain is an instruction to update the ledger to reflect that a given asset formerly assigned to one address should now be assigned to another. Assets therefore cannot be 'withdrawn' and transactions taken on a ledger are done directly, without a third party intermediary. Consequently, a direct transfer of a digital asset is analogous to a cash transfer that occurs peer-to-peer; the difference being that rather than physically changing hands the asset digitally changes hands on the blockchain ledger.¹

¹ Coincentre, [overview of self-custody wallets](#), 2024

To demonstrate ownership, users need to prove they own both parts of a key pair: the private key, and the public key. The public key generates an address that can be safely shared, allowing others to 'find' the owner of the address in question - it is equivalent to a phone number listed in a directory that people can be given to call (or indeed send an asset to). The private key (analogous to a credential or password) is all that is necessary to access and control assets assigned to a particular public address. These keys provide the essential link between an owner and the blockchain address containing their assets.

As is the case with physical currency, digital assets require the need for safe and secure holding and storage facilities. Importantly, a self-custody wallet does not contain the digital assets, but instead stores the private keys that allow access to digital assets attributed to their corresponding public blockchain address. In this way, a digital asset self-custodial wallet provides a more secure way for users to keep and manage their own private keys (as an alternative to writing down private keys either physically or digitally). Similar to password managers or physical safes; these self-hosted wallets do not see, handle, or direct user activities or exert control over the asset.

Comparison of self-custody and custodial wallets

In a custodial wallet solution, the digital assets are directly controlled by the third-party intermediary on behalf of a customer. The third party often pools collective customer funds into a blockchain address they directly control themselves. These are commonly omnibus accounts, and an internal ledger by the third-party determines how much of each digital asset the third-party is holding on behalf of which customer. In a custodial solution, the customer no longer holds or has access to the private keys and can no longer unilaterally access their digital asset on the blockchain. Instead, the customer has a relationship with an intermediary who has access to the digital assets on their behalf. Custodial providers can then execute transactions on behalf of customers (including the ability to withdraw assets to their own self-custody wallet).

This fundamental distinction highlights why self-custody solutions like Bitkey cannot be appropriately classified as payment facilities. Where custodial solutions actively intermediate transactions and control user funds - properly bringing them within the scope of payment facility regulation - self-custody solutions provide only the technical means for users to secure and access their own digital assets. This is more akin to a physical safe or secure storage device than a payment service.

Proposed Information Sheet relating to self-hosted wallets

ASIC's interpretation of the Corporations Act broadly defines a non-cash payment as '*performing monetary obligations by means other than fiat currencies*'. ASIC outlines that determining whether a facility is a non-cash facility will '*depend on the terms and features of the arrangement*'. While it is clear that some digital assets could be considered under this broad definition, it is also critical that *the method* of transmission is sufficiently considered when applying licensing requirements. Namely, self-custodial wallets should not be considered non-cash payment facilities even if the underlying asset is determined to be a financial product.

Non-cash payment facility regulations were designed for intermediated payment services. The purpose being to protect consumers from intermediary risk and operational failure. With self-hosted wallets, there is no intermediary risk as users control their own keys and self-custody wallet providers do not hold or control digital assets or have the ability to make payments. Instead, self-custody provides a data storage facility that enables a user to undertake a direct, 'peer to peer' transaction. The user retains control of their assets. The 'role' of the self-custody wallet company has ended, and it now falls on the user to manage, store, and use their assets. Therefore, the self-hosted wallet provider is not appropriately involved to be deemed a non-cash payment facility, because they neither '*make a payment*', or '*cause a payment to be made*' - this happens directly through the blockchain, or the digital peer to peer network.

Self-custody wallets provide a fundamentally different approach to custodial solutions, which generally can both 'make a payment' or 'cause a payment to be made'. This is a distinction acknowledged later in the guidance: when defining custodial services on page 19, ASIC notes that '*offering a 'self-custody' solution, or self-hosted wallet product, is unlikely to amount to providing a custodial and depository service*'. This logic should similarly apply when considering non-cash payment facilities due to the unique and separate features of a non-custodial wallet.

A tailored approach for self-custody wallets is also supported by [Regulatory Guidance 185](#) relating to customer 'uses' of a non-cash payment facility. 185.60 and 185.61 are indicative of the type of products intended to be licensed:

'(a) an instruction by a client to make a non-cash payment to a particular payee is a 'use' of the NCP facility by the client;

(b) for a cheque facility, the writing of a cheque to a particular payee is a 'use' of the facility by the client, while the arrangement giving the ability to write that cheque is the NCP facility;

(c) for a stored value facility, the NCP facility is the arrangement (which may include a physical device) that gives a person the ability to make non-cash payments to various payees from time to time, while presentation of the device to make a purchase is a 'use' of that facility; and

(d) for direct debits, the NCP facility is the arrangement between the client and a financial institution that gives the client the ability to make direct debit payments to various persons (payees) from time to time, while an order by the client to make a direct debit payment to a payee is a 'use' of the facility.

Specific examples of NCP facilities include cheque accounts, traveller's cheques, stored value cards, electronic cash, direct debit services, payroll cards, funds transfer services and electronic bill payment services.

A self-custody solution is unlike any of the arrangements listed above. In each, the user is relying on a third party to *'make a payment'* or *'cause a payment to be made'*, whether that be directly (such as for a stored valued facility) or indirectly (for a check facility). Because there is no third party control of the shared ledger or blockchain, it is not analogous to suggest self-custody wallets are doing either.

The distinction between self-custody and custodial wallets is also recognised in international standards. For example the Organisation for Economic Co-operation and Development's (OECD) Crypto-Asset Reporting Framework (CARF) exempts many obligations on self-hosted wallets, because they do not retain control and are not party to any covered transactions, which are instead at the behest of the user. Instead, they argue it is *'those Entities or individuals that as a business provide services effectuating Exchange Transactions in Relevant Crypto-Assets, for or on behalf of customers... are expected to have the best and most comprehensive access to the value of the Relevant Crypto-Assets and the Exchange Transactions carried out.... [and are] considered Reporting Crypto-Asset Service Providers'*.² A similar distinction would be appropriate when considering a non-cash payment facility.

Finally, compliance with [RG 185](#) on non-cash payment facilities is likely to be - in accordance with relief provisions (RG185.17) - *'disproportionately burdensome'*, and the *'likelihood and extent of potential consumer detriment minimal'*. This is because compliance would impose unwieldy, unworkable requirements on self-custody providers, requiring a fundamental and foundational redesign of products. Self-hosted wallet providers and developers, who as outlined do not have, and are not required to have the same type of customer relationships with users as traditional financial services providers, would be required to undertake a number of new regulatory obligations, including licensing requirements, conduct and disclosure obligations and the ePayments Code.

To implement these requirements, self-hosted wallet providers would be required to fundamentally change their product and their relationship with the customers. For example, they would have to build insight into transactions - in order to provide things such as transaction confirmations. Self-hosted wallet providers *are not party to* and have *no insight into* transactions; such obligations would be nothing less than a complete redesign of a product category.

Moreover, these requirements would create a misleading regulatory framework that suggests to consumers that self-custody wallets operate with the same intermediary oversight as traditional payment facilities. This characterisation could lead to confusion about the nature of self-custody and the role of wallet providers, potentially undermining the very benefits of self-custody solutions - namely, user sovereignty and direct control over digital assets without intermediary risk. This remains one of the core reasons customers choose self-custody wallets.

²<https://www.oecd.org/tax/exchange-of-tax-information/crypto-asset-reporting-framework-and-amendments-to-the-common-reporting-standard.pdf>

The regulatory framework should instead recognize that self-custody solutions like Bitkey have fundamental differences from intermediated financial services, offering users the tools they need to maintain direct control over their digital assets. This aligns with the broader principles of blockchain technology and decentralised finance, where reducing intermediary risk and enabling direct peer-to-peer transactions are core features.

By appropriately distinguishing between custodial and non-custodial solutions in the regulatory framework, ASIC can better protect consumers while fostering innovation in digital asset security and self-custody solutions. This approach would maintain robust oversight of genuine payment facilities while recognizing that self-custody wallets represent a fundamentally different category of product, one that empowers users with direct control and reduces rather than introduces intermediary risk.

- **Question 4. Do you have comments on any of the proposed worked examples? Please give details, including whether you consider the product discussed may/may not be a financial product.**
- **Question 5 Are there any additional examples you would like to see included? Please give details of the suggested example(s), and why you consider the digital asset discussed may/may not be a financial product.**
- **Question 6. For any of these examples, are there any unintended consequences? If so, what are these and what do you propose in response? *(Responses for questions 4, 5 and 6 below)***

As outlined in the response to Question 2, custodial and self-custody wallets are distinctly different and different regulation is appropriate. In this regard, worked example 13 should be amended to refer to custodial wallets specifically and exclude self-custody wallets. An additional self-custody wallet could also be included as a separate worked example if required from a future licensing regime.