PiperAlderman

Senate Economics Legislation Committee review of
Corporations Amendment (Digital Assets Framework) Bill 2025

Digital Assets Framework

Introduction

Piper Alderman welcomes the opportunity to provide this submission to the Senate Economics Legislation Committee's review of the *Corporations Amendment (Digital Assets Framework) Bill 2025* (the **Bill**) and provide input towards shaping the scope of the Bill. One of Australia's oldest law firms with a national reach, Piper Alderman also operates one of the largest specialist teams in Australia focused on blockchain and digital assets. We have deep technical and legal experience in the fintech and digital asset space, having served Australian and global clients at the forefront of innovation in the digital economy. Over the past decade, we have been deeply engaged in key Government consultations concerning regulatory approaches to digital assets.

We advise start-ups, digital currency exchanges, financial institutions and investors, analyse innovative products and services, act in controversies, advise on taxation and assist in restructuring matters.

The principal author of this submission is Steven Pettigrove, a Partner in the Financial Services and Fintech team at Piper Alderman and Head of the Blockchain Group. Steven is ranked a Band 2 Fintech lawyer in Australia by the prestigious Chambers & Partners and is co-author of Australia's first blockchain textbook "Law of Code: Blockchain and Digital Assets in Australia" published by Lexis Nexis.

The views within represent the authors' views and should not be taken as being representative of the views of the other partners of Piper Alderman.

We take a politically neutral position when considering policy, underpinned by a belief in the economic and social benefits of technology and innovation, and a focus on what regulation means at a practical level for both businesses and their customers and users.

We welcome the review of the Bill and the provision of further guidance and shaping of the legislation as it applies to digital assets. In reviewing the Bill, it is important that policymakers take into account the Government's stated objectives of supporting innovation, competition and productivity. Policymakers should also have regard to the unique features and risks of blockchain technology and digital asset markets, as well as international developments that will inevitably influence Australia and the way Australians engage with digital assets. Doing so is essential to protecting consumers and ensuring that Australia and Australians can participate meaningfully in, and benefit from, the emerging digital economy.

We thank the Senate Economics Legislation Committee for the opportunity to contribute to this review and trust that our feedback, alongside submissions from other stakeholders, will assist in fostering innovation, strengthening regulatory effectiveness, and ensuring the Bill appropriately accommodates digital asset-related offerings.

Steven Pettigrove

Partner and Head of Blockchain Group

Katrina Sharman

Special Counsel

With thanks to Tahlia Kelly and Sophie Nguyen

Executive Summary

We support the Government's objective of extending regulatory oversight to custodial digital asset intermediaries in order to enhance consumer protection and market integrity, while continuing to encourage the development of digital asset infrastructure and markets.

This submission focuses on a limited number of foundational issues that arise from the Bill's reliance on certain threshold concepts, particularly *possession* and *control*, to determine the scope of the proposed regulatory regime. In our view, aspects of the current drafting risk extending the regulatory perimeter beyond its intended target by capturing non-custodial software providers and infrastructure participants who are not typically understood as financial intermediaries, and lack unilateral practical ability to deal with customer assets.

Drawing on the technical architecture of modern digital asset systems, including non-custodial wallets, cross-chain bridges and Layer 2 networks, this submission identifies four discrete issues where targeted clarification would materially improve the operation of the Bill. The proposed amendments are intended to be high-impact and low-complexity, preserving the Bill's core objectives while reducing the risk of unintended regulatory outcomes.

This submission is intended to support further consultation and refinement of the Bill and does not seek to propose a comprehensive alternative framework.

Regulatory Precision and Technological Context

Effective regulation of digital asset markets depends on accurately identifying where control, risk and responsibility genuinely reside. Non-custodial wallets and decentralised infrastructure are designed to reduce reliance on trusted intermediaries through cryptographic and architectural constraints, rather than discretionary control over user assets.

Financial services regulation, including Australian Financial Services License (**AFSL**) obligations and client asset rules, are premised on the existence of an intermediary that exercises practical control over client assets and provides discretionary services to clients. These assumptions do not hold in the context of software development, open-source protocols, non-custodial software or the maintenance of public digital infrastructure, where participants, including software developers, may design, deploy or upgrade code but lack the technical ability to unilaterally initiate transactions or appropriate user assets.

If the Bill does not sufficiently reflect these distinctions, there is a risk that obligations will be imposed on participants who are not capable of complying with the legislation or causing the harms the regime is intended to address. Accordingly, precision at the definitional level is critical to ensuring that the regulatory framework targets activities that present real consumer or systemic risk, while continuing to permit and encourage software development and security-enhancing technologies.

Possession and Control as Threshold Concepts

The Bill relies on the concepts of *possession* and *control* as key gatekeeping mechanisms. In decentralised and non-custodial contexts, however, these concepts do not always align with traditional notions of custody. Participants may perform technical, verification or administrative functions without having the ability to unilaterally initiate or complete transactions. If such distinctions are not clearly reflected in the drafting, the framework risks capturing participants beyond recognised cryptocurrency exchange and custodians and types of conduct which has heretofore fallen outside the financial service licensing framework.

The financial services licensing and compliance regime as currently framed is not well adapted for this purpose. For example, the imposition of asset-holding and settlement standards are not well suited to infrastructure providers or non-custodial wallet software where the software provider does not offer custody services or receive and perform client instructions.

The regulation of digital asset infrastructure (e.g. decentralised finance) is an emerging area as set out in section 8 below, which requires further detailed study to ensure that Australian regulations align with international approaches and do not discourage the development of emerging technologies in Australia.

In any event, the legislature should be careful to avoid measures which may inadvertently discourage the development and implementation of verification and security controls in software applications and infrastructure.

Issue 1: Possession, Control and Multi-Party Computation (MPC): ***Relevant provisions: s 761GB(2) & Section 86***

The Bill provides that a person may be taken to control a digital token where they can transfer the token or exclude others from transferring it, including where that control is exercised jointly. While section 86 includes a limited exclusion for joint possession, concerns remain regarding arrangements involving "negative control" where a party does not have the ability to use or move assets themselves, but their cooperation is required for a transaction to proceed.

In a common 2-of-2 MPC wallet configuration, a user initiates transactions using their key, while a second key performs a verification function and is technically incapable of initiating transactions independently. Although the second key is required to complete a transaction, its holder cannot unilaterally use, move or consume the digital asset.

These arrangements are widely adopted as a security measure to reduce single points of failure and mitigate fraud risk. These measures are designed to detect high risk or malicious transactions, thereby providing more security to the software user (i.e. a second key is not applied if there is a suspicion of a malicious transaction or scam). Treating verification or security measures as constituting possession or control risks disincentivising the use of MPC architectures and encouraging less secure single-signature designs. At the same time, these arrangements do not present the same consumer risks as intermediary custody arrangements.

As currently drafted, Section 83(3)(b) only excludes from the definition of possession arrangements where at least one party can unilaterally transfer electronic records. Accordingly, third party verification or security arrangements may be caught by the definition.

Recommendation: Amend s 86(3) to provide that a person does not jointly possess a digital token where they lack the technical ability to unilaterally initiate a transaction or transfer of the token, regardless of whether their cooperation is required to complete a transaction initiated by another party.

Drafting suggestion: Amend s 86(3)(b) to read: "*(b) the person does not have the ability to unilaterally transfer the digital token.*"

Issue 2: Upgradeable blockchain infrastructure*: Relevant provisions: ss 761GC and 761GD*

The definition of a *Digital Asset Platform* (DAP) and *Tokenised Custody Platform* (TCP) may capture certain forms of blockchain infrastructure, such as layer 2 blockchains or upgradeable cross-chain bridge infrastructure. In these models, assets are typically held or transferred by smart contracts rather than by a legal person. Developers may retain administrative or governance powers, such as

the ability to pause or upgrade contracts, for security and maintenance purposes.

While there may be a developer of the smart contracts, there is no “operator” in the custodial sense. The asset are “held’ by the smart contract code, not by a legal person. These powers do not confer unilateral discretion to deal with user assets for the developer’s own benefit. Upgrades are often subject to time delays and they exist to pause bridge activity or patch a critical bug if it is discovered, potentially protecting users from a devasting hack.

Treating upgrade or pause powers as indicative of custody risks subjecting non-custodial infrastructure providers to AFSL obligations that are not practically capable of compliance. For example, the developer has no ability to segregate or hold assets locked on-chain under future asset holding standards. Moreover, it is unclear how a software developer can practically provide disclosure or comply with design and distribution obligations in circumstances where a user can interact with bridge infrastructure on-chain without the need to access any website interface.

Upgradeability should be viewed as a security feature and/or software maintenance and not a custodial business model. The imposition of these measures may discourage the inclusion of security features that are critical to incident response and vulnerability management.

Recommendations:

- Modify ss 761GC and 761GD to clarify that holding administrative, governance or security powers over smart contract code does not, of itself, constitute operating a DAF or TCP where those powers do not confer unilateral discretion to deal with user assets; or
- Introduce targeted safe harbours for blockchain infrastructure or upgradeable bridge infrastructure where specified risk-mitigating features are present (such as upgrade timelocks, separation of upgrade and pause powers, or hard-coded rate limits). This would remove concerns over ‘factual control’ and give users and the community time to consider and audit the proposed upgrade before it is implemented; or
- Consider a fit for purpose infrastructure-focused registration regime for non-custodial bridge infrastructure, directed to security, audit and governance standards rather than custodial financial service obligations which are poorly adapted to software development services.

Drafting suggestion: Insert as s 761GC(5) and s 761GD(4):

"A person is not an operator of a facility merely because they hold administrative keys or governance rights capable of updating or pausing the software code that holds the underlying assets, provided they do not have the unilateral discretion to deal with the assets for their own benefit."

Issue 3: Public Infrastructure and the “Critical Participant” test: *Relevant provision: s 9E(2)(c)*

The Bill exempts *Public Digital Token Infrastructure* from regulation, but removes that exemption where the infrastructure depends on a participant whose role is critical to transmitting, processing or recording transactions.

This formulation does not distinguish between *liveness* (the ability to process transactions) and *integrity* (the ability to compromise or misappropriate assets). For example, some layer 2 blockchain networks rely on a single sequencer to order transactions. While the sequencer may affect liveness if it goes offline, it cannot unilaterally move or misuse user

assets, which remain cryptographically secured on the underlying layer 1 blockchain.

Without clarification, the Bill risks treating control over how transactions are processed as control over assets themselves, even where the infrastructure cannot access or move those assets.

Recommendation: Clarify that the public infrastructure exemption is only displaced where a participant has unilateral power to alter ownership or transfer digital tokens without the owner's authority, and not merely because the participant plays a critical role in transaction processing. Alternatively, consideration should be given to an additional exemption for digital asset infrastructure providers.

Drafting suggestion: Amend s 9E(2)(c) to read: *"(c) no participant has the unilateral ability to alter electronic records or transfer digital tokens."*

Issue 4: Concept of mixed assets in TCPs; Section 9(md)(iv)

To qualify as a regulated TCP, rather than a Managed Investment Scheme (MIS), the Bill requires that "all underlying assets must belong to the same class of asset" (s 9(md)(iv)). Clarification is required to ensure this requirement operates at the level of individual tokens, rather than the platform or facility as a whole. That is, an operator can still qualify for the exemption if they tokenise multiple asset types, although a single token can only be created for each underlying asset.

This position applies both to TCP operators and potentially non-custodial infrastructure (e.g. bridges) to the extent that it is captured by the DAF and TCP regimes (see our comments above). In practice, bridges may simultaneously hold multiple asset types (for example, ETH, stablecoins and NFTs). A platform-level interpretation does not engage the MIS exclusion and should be clarified.

Recommendation: Clarify that the "same class of asset" requirement applies to the underlying asset backing a particular class or type of token, rather than to the platform or facility as a whole.

Drafting suggestion: Amend s 9(md)(iv) to read: "*(iv) in respect of each class of digital token issued, the underlying assets backing that token must belong to the same class of asset.*"

International Comparison

A comprehensive comparative analysis of international regulatory frameworks for non-custodial software providers and blockchain infrastructure participants is beyond the scope of this submission. However, as a general observation, the Bill does not appear to adequately accommodate for these activities when compared with other key jurisdictions such as the European Union and the United Kingdom with the result that those jurisdictions may offer greater regulatory certainty and more attractive policy settings for digital assets investment and software development activities.[1]

[1] Regulation (EU) 2023/1114 on Markets in Crypto-Assets [2023] OJ L 150/52 (MiCA) recital 22 excludes services provided 'in a fully decentralised manner, without intermediaries'; art 142 mandates a Commission report on DeFi regulation. The UK FCA has indicated that 'truly decentralised' DeFi will fall outside the UK's regime, though DeFi 'where there is a clear controlling person' remains regulated. Financial Conduct Authority (UK), Consultation Paper CP25/40: Regulating Cryptoasset Activities (Consultation Paper, 2025) [7.2] and [7.4].

As drafted, the Bill may apply to non-custodial software providers and blockchain infrastructure participants, including multi-signature wallets, bridges and Layer 2 networks, in circumstances where participants lack unilateral control over user assets and which could impose licensing and compliance obligations which are poorly adapted to these activities. This approach appears to depart from emerging international practice, which generally excludes non-custodial software providers and blockchain infrastructure from custodial regulation by reference to whether a participant has independent practical ability to deal with customer assets.

Clarifying that the blockchain infrastructure exemption applies unless a participant has unilateral authority to alter ownership or transfer digital tokens, supported by targeted amendments and appropriate safe harbours, would better align the Bill with international approaches directed towards enabling permissionless innovation.[2]

Conclusion

The Bill should be refined to ensure that regulatory obligations apply to intermediaries with unilateral practical ability to deal with customer assets and to expose customers to loss through discretionary actions. Applying custodial financial services obligations to non-custodial wallets or software infrastructure risks discouraging security-enhancing practices and increasing, rather than reducing, consumer risk. As outlined in this submission, this risk is particularly acute where technical participation or operational criticality is treated as equivalent to custodial control.

The targeted clarifications proposed in this submission would better align the Bill with its stated policy objectives while supporting technological innovation and safety. In doing so, they would also bring the Bill into closer alignment with emerging international approaches that focus custodial regulation on centralised intermediaries, while seeking to exclude or appropriately treat non-custodial infrastructure and software-based models.

[2] In the US, CFTC Chairman Selig has stated the agency 'will explore ways … to encourage innovation in software development', including assessing innovation exemptions and establishing 'clear and unambiguous safe harbors for software developers': Michael S Selig, 'The Next Phase of Project Crypto: Unleashing Innovation for the New Frontier of Finance' (Speech, CFTC-SEC Event on Harmonisation, 29 January 2026).

piperalderman.com.au

Adelaide | Brisbane | Melbourne | Perth | Sydney