From Promise to Protocol: The Evolution of Financial Regulation in the Age of Protocol-enforced Finance

Chris Adamek, Jazz Osvald, Josh Gonzalez[1]

Protocol-enforced Finance exposes a structural tension in modern financial regulation. Contemporary financial services law is designed to regulate the conduct of identifiable persons and institutions that make financial promises, and to achieve policy objectives through licensing, disclosure, supervision, and enforcement against accountable actors. In contrast, Protocol-enforced Finance enables economically significant financial functions to be performed by deterministic smart contracts on public blockchain infrastructure, such that transactions are executed and settled according to protocol rules without an intermediary able to intervene, reverse transactions, whether or not coerced or legally compelled to do so. This paper argues that, while Australia's post-Wallis Inquiry framework is functionally framed and technology-neutral in form, it remains anthropocentric in operation and therefore struggles to apply where there is no responsible operator, custodian, or service provider. It distinguishes genuine Protocol-enforced Finance as neutral infrastructure from "on-chain finance" – systems that retain meaningful control points and remain amenable to orthodox regulation – and maps the frictions that arise when financial services law concepts are applied to decentralised protocols. The paper concludes by outlining a research and policy agenda for system-based oversight, protocol-level assurance mechanisms, and the use of public blockchain transparency to support market integrity objectives.

This paper was submitted for presentation by Chris Adamek at the 28th Melbourne Money and Finance Conference, 9–10 February 2026.

[1] The authors are from the Digital Policy and Corporations Division, the Australian Treasury. The views in this article are those of the authors and not necessarily those of the Australian Treasury.

1. Introduction

Financial regulation is predicated on an anthropocentric model of finance: it assumes identifiable persons and institutions stand behind financial products and services, make enforceable promises, and can be held accountable.[2] Modern regimes reflect this by managing agency problems and information asymmetries through licensing, disclosure and conduct obligations imposed on responsible actors—entities whose behaviour can be shaped ex ante through supervision and ex post through enforcement.

Following several years of policy development and consultations by Australian Treasury to modernise Australia's regulatory settings for digital assets, the *Corporations Amendment (Digital Assets Framework) Bill 2025* (**Bill**) was introduced to Australian Parliament. The Bill rests on three policy premises: (i) digital assets are—or are not—subject to the financial services laws in the same way as other assets; (ii) most economically significant activity involving digital assets is carried out by intermediary service providers; and (iii) the risks, harms and regulatory uncertainty associated with those services can be mitigated by integrating them into existing regulatory machinery, with minor tailored amendments.[3] The Bill creates two new types of regulated financial product, digital asset platforms and tokenised custody platforms, and extends licensing, conduct and disclosure obligations to platform operators. Like the existing financial services laws it adopts, the framework is anthropocentric.

However, a core policy question remains: what protections (if any) should apply when two economic counterparties can transact on public blockchains without an intermediary? This is not theoretical. Australian courts have had to assess the nature of financial functions performed by software on public blockchains in place of intermediaries,[4] and ASIC has issued guidance on "products without issuers", using the bitcoin token (BTC) to illustrate the regulatory consequences of the absence of an issuing counterparty.[5]

Decentralised finance (**DeFi**) broadly refers to financial activities undertaken by a person using blockchains and smart contracts (programs executed on a blockchain). . However, the focus of this paper is not DeFi generally. Rather the focus is a subset of DeFi that we refer to as "Protocol-enforced Finance". While Protocol-enforced Finance can include some forms of activity commonly described as DeFi, the term is used here to refer specifically to a person using public blockchains to facilitate complex, multi-party financial transactions, where smart contracts (programs executed on a blockchain) facilitate an economic relationship between two or more persons without an intermediary, agent or promise.

Protocol-enforced Finance should also be distinguished from "on-chain finance", where intermediary businesses use blockchains and smart contracts to deliver financial services (for

---

[2] "*The purposes of financial regulations are to ensure at least that financial promises are understood and, in their more intense form, that they are met*" – Stanley Wallis, Financial System Inquiry Discussion Paper (Discussion Paper, Australian Government Publishing Service, 1996), Chapter 4.

[3] Explanatory Memorandum to the *Corporations Amendment (Digital Asset Framework) Bill 2025*.

[4] *Australian Securities and Investments Commission (ASIC) v Web3 Ventures Pty Ltd* (2024) 172 ACSR 327.

[5] Australian Securities and Investments Commission, Digital Assets: Financial Products and Services (Information Sheet No 225, October 2025) [Example 4].

example, on private blockchains, or via smart contracts on public blockchains with administrative control mechanisms).[6]

This paper argues that Protocol-enforced Finance runs into a structural limitation in Australia's functionally framed but operationally anthropocentric financial services regime. Even where the law conceptually applies to the economic function performed by a smart contract, the absence of an accountable intermediary can frustrate both ex ante regulation (licensing and supervision) and ex post accountability (liability and enforcement). Recognising this gap is a necessary predicate to evaluating policy responses.

1.1. Smart contracts as protocol-enforced rules

The term "smart contract" predates public blockchains and originally referred to the prospect of replacing aspects of legal and business performance with computer protocols.[7] However, in practice, early "smart contract" concepts still required a trusted person to maintain and operate the protocol. Public blockchains changed that by enabling transactions between unknown parties to be validated and settled on a shared ledger without a central clearing house.[8] In this setting, trust arises from distributed verification combined with incentive-aligned participation that coordinates individuals around a single transaction history (known in computer science as "permissionless consensus").[9] Along with basic transfers, the first public blockchain protocol, Bitcoin, supported limited "proto–smart contract" functionality, allowing parties to embed simple, protocol enforced spending conditions in transactions.[10]

> *Example 1 - Protocol-enforced transfer constraint (Bitcoin timelock)*
>
> Alice pays Bob in BTC using an output (i.e. token) that cannot be spent (i.e. transferred) until a specified time T (a block height or timestamp). Prior to T, any attempt to spend the output will be rejected by network nodes as invalid. The timelock is therefore enforced by the protocol itself. Even if a court ordered Bob to transfer early and somehow compelled all miners in the network to process the transaction, the network would not recognise the transaction before T (absent a change to the Bitcoin protocol itself).

However, the Bitcoin protocol's original scripting model was designed to be intentionally narrow to enforce simple conditions on the transfer of individual outputs. Early attempts to use the protocol for transacting and settling traditional financial instruments (e.g. shares, bonds, fiat

[6] Katrin Schuler, Ann Sofie Cloots and Fabian Schär, 'On DeFi and On-Chain CeFi: How (Not) to Regulate Decentralized Finance' (2024) 10(2) Journal of Financial Regulation 213.

[7] In computer-science, a 'protocol' is "*a sequence of messages between at least two computers. At a higher level of abstraction, a protocol consists of algorithms communicating via messages. These programs act as proxies, or agents, for human users, who communicate their preferences via users interfaces*". See Nick Szabo, 'Formalizing and Securing Relationships on Public Networks' (1997) 2(9) First Monday.

[8] Aaron Wright and Primavera De Filippi, 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia' [2015].

[9] Eric Budish, 'Trust at Scale: The Economic Limits of Cryptocurrencies and Blockchains' (2025) 140(1) The Quarterly Journal of Economics 1.

[10] Bitcoin Project, 'Bitcoin Developer Guides: Transactions' <https://developer.bitcoin.org/devguide/transactions.html>.

currency) therefore relied on "overlay" schemes that embedded token metadata in BTC transactions and used off-chain software to interpret the meaning of that metadata.[11]

> *Example 2 – Off-chain token semantics (a stablecoin on Bitcoin)*
>
> Alice buys 100 "StableDollars" from StableCo in exchange for a promise that each StableDollar will be redeemable for US$1 from StableCo on demand. StableCo represents StableDollars using an overlay scheme that tags certain BTC transactions (and their outputs) with metadata recognised by overlay-aware wallets or indexers. When Alice "sends" 10 StableDollars to Bob, her wallet broadcasts an ordinary BTC transaction transferring the relevant tagged outputs, plus whatever metadata the overlay scheme requires. Bitcoin's consensus rules validate only the BTC transfer (signatures, scripts, and non-double-spending); they do not validate StableDollar balances or enforce redemption or transfer restrictions. The stablecoin's semantics therefore depend on off-chain interpretation and StableCo's legal promise, rather than on protocol-level execution.[12]

The Ethereum protocol was designed to overcome the limits of the Bitcoin protocol by using a blockchain with an embedded general-purpose execution environment.[13] By allowing third parties to publish executable code to the shared ledger—and by recording that code's execution and resulting state changes on the same ledger – the Ethereum protocol was able to enforce arbitrarily complex, multi-step conditional logic through consensus of those that validated the state changes made on the ledger.

> *Example 3 – On-chain token semantics (a stablecoin on Ethereum)*
>
> Alice buys 100 "StableDollars" from StableCo in exchange for a promise that each StableDollar will be redeemable for US$1 from StableCo on demand. This time, StableCo represents StableDollars using a modified version of the ERC-20 token smart contract (the industry standard protocol for creating digital tokens). When Alice transfers 10 StableDollars to Bob, the transfer succeeds only if it satisfies the token contract's rules. For example, its rules might restrict transfers to or from specified addresses, pause transfers under defined conditions, or route certain transactions through a designated function for compliance or recovery. These rules are enforced by the protocol.

These examples illustrate a key defining feature of modern "smart contracts", which is that they are not "contracts" in a legal sense at all. Rather, they are executable and "practically

---

[11] For example, "Coloured coins" were a family of overlay techniques used in the 2012–2015 era that tried to represent non-bitcoin assets (shares, vouchers, property claims, IOUs, etc.) using the Bitcoin protocol by attaching extra meaning ("colour") to particular satoshis/outputs. See Meni Rosenfeld, *Overview of Colored Coins* (White Paper, 4 December 2012).

[12] The original version of the stablecoin Tether (USDT) used the Bitcoin protocol in a similar way. (See *Tether Limited, Tether: Fiat Currencies on the Bitcoin Blockchain* (White Paper, Tether Limited, 16 April 2015)).

[13] Vitalik Buterin, '*Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*' (December 2014).

immutable"[14] instructions in the form of computer code.[15] The ledger updates only when proposed state changes satisfy the relevant validation rules, including any conditions encoded in the relevant smart contract. The result is a hard constraint. In each of the examples above, parties could be coerced or incentivised to do what is within their own control (for example, disclose keys, sign a transaction, or refrain from interacting). However, no outside actor – whether a court, a regulator, a counterparty, or a would-be bribing intermediary – can cause the network to treat a non-compliant transaction as valid.[16] This rule-bounded determinism is the core property that makes smart-contract-based financial activity conceptually distinct from intermediary-based finance, which instead relies on legal promises and legal enforcement.

1.2. Protocol-enforced Finance defined: financial functions without intermediaries

In this paper, Protocol-enforced Finance is defined as activity undertaken through smart contract protocols that perform financial functions in the absence of promises, intermediaries, and agents.[17] In this context, smart contracts are used mainly to facilitate the atomic settlement of assets or the holding of assets as collateral. In both cases, the assets are subject to the smart contract's rules and change hands only if predefined conditions are met.[18] By varying these preconditions, various financial primitives can be created.

However, not all financial functions can be replicated by smart contracts. There is a general constraint in that deterministic protocols can enforce only what they can control. A smart contract cannot compel a *person* to do anything. Uncollateralised lending illustrates this limitation. While smart contracts can be used as tools to facilitate unsecured lending arrangements (e.g. to disburse funds, receive repayments, and flag defaults), they cannot deliver enforceable recourse on default because they cannot reach into the real world to enforce a claim against a borrower.[19]

Protocol-enforced Finance nonetheless exists for a range of financial functions in which protocol enforcement is feasible.[20] The following examples illustrate two such primitives – one that can operate without external data, and one that depends on an external price feed – showing how complex functions can be performed deterministically by code.

---

[14] "*Once data is loaded into a shared ledger, it requires extensive computational resources or massive collusion among nodes to modify it unnoticed by others, hence rendering it practically immutable. There is no difference whether the change is intentional or accidental, malicious or benign*." - International Telecommunication Union, Recommendation ITU-T F.751.0: Requirements for Distributed Ledger Systems (Recommendation No ITU-T F.751.0, International Telecommunication Union, 13 August 2020).

[15] Fabian Schär, '*DeFi's Promise and Pitfalls*' (2022) 59(3) Finance & Development 33.

[16] Primavera De Filippi, Chris Wray and Giovanni Sileno, '*Smart Contracts*' (2021) 10(2) Internet Policy Review 1.

[17] This is an intentionally narrow definition that is used to distinguish the kind of protocols (which some refer to as "true DeFi") that are the focus of this paper from the use of smart contracts as tools for a business to provide financial services (which is sometimes labelled "DeFi"). The threshold (i.e. absence of promises, intermediaries and agents) targets arrangements that arguably fall outside the *intended* scope of financial regulation (for example, the Wallis Inquiry concluded that financial regulation targets the performance of intermediaries, agents, and financial markets in meeting the underlying promises contained within financial contracts).

[18] Fabian Schär, '*DeFi's Promise and Pitfalls*' (2022) 59(3) Finance & Development 33.

[19] Chainlink, '*Onchain Private Lending: The Future of Institutional Credit*' (21 January 2026).

[20] The Court in *Australian Securities and Investments Commission (ASIC) v Web3 Ventures Pty Ltd* (2024) 172 ACSR 327 found that "*Smart contracts can be programmed such that this* [collateralised lending] *transaction happens automatically and anonymously. Smart contracts facilitate the loan, payment of interest and any repayment without the need for a centralised intermediary, like a bank, or without the parties needing to know and trust one another....*".

Example 4 – Automated market maker protocol (AMM)

An AMM allows digital assets to be exchanged atomically without an intermediary. A common design maintains reserves of TokenX and TokenY in an AMM's smart contract and uses the formula $x \cdot y = k$ to price the assets. x and y represent the quantities of TokenX and TokenY, and k is the resultant constant value. Each time TokenX and TokenY are swapped through the AMM, the ratio between x and y changes, which changes the price of each token.

For example, Bob deposits equal value of TokenX and TokenY into the AMM smart contract, which now holds reserves x and y. The AMM issues Bob liquidity-provider (**LP**) tokens representing his claim on the pool. Alice wants to acquire TokenY using TokenX. She transfers n TokenX to the AMM, it calculates how much TokenY to provide by enforcing the AMM's pricing rule ($x \cdot y = k$, after fees), then atomically: (i) debits Alice's TokenX; (ii) credits Alice with m TokenY; and (iii) updates the AMM's reserves. The shift in the ratio of x and y also changes the amount of TokenX and TokenY that Bob can withdraw upon redeeming his LP token with the AMM.

No exchange operator matches orders or controls settlement; pricing, clearing, and settlement occur as deterministic state changes are enforced by the protocol.[21]

Some Protocol-enforced Finance primitives require external inputs. A common dependency is an "oracle", which supplies on-chain protocols with data not native to the blockchain (for example, a reference price). Oracle reliance can create points of fragility and potential control (as they reintroduce "people in the loop"),[22] but it does not necessarily reintroduce a traditional financial intermediary who can discretionarily execute, unwind, or refuse transactions. The protocol still executes deterministically. The dependency just affects the integrity of the inputs used to execute that transaction.

Example 5 – Perpetual futures protocol

Alice wants long exposure to Tesla shares (TSLA) without buying the shares. She deposits USDC collateral into a perpetual futures smart contract and opens a TSLA-PERP long equivalent to 1 TSLA; Bob deposits collateral and opens an offsetting short. The protocol continuously marks both positions to a TSLA/USD reference price supplied by an on-chain oracle feed,[23] and updates each account's unrealised profit and loss accordingly.

The protocol enforces initial and maintenance margin: if Alice's collateral becomes insufficient (margin falls below the maintenance requirement), her position becomes eligible for liquidation and the protocol can deterministically close it (and

[21] See for example, Hayden Adams, Noah Zinsmeister and Dan Robinson, *Uniswap v2 Core* (White Paper, Uniswap, March 2020).

[22] Katrin Schuler, Ann Sofie Cloots and Fabian Schär, '*On DeFi and On-Chain CeFi: How (Not) to Regulate Decentralized Finance*' (2024) 10(2) Journal of Financial Regulation 213.

[23] See for example the TSLA/USD data feed available from the Chainlink Oracle, Chainlink Foundation.

apply the protocol's liquidation fee/penalty) without needing Bob's cooperation or any exchange operator.

To keep the TSLA-PERP price anchored to the reference, the protocol applies a periodic funding payment: when the perp trades above the oracle/index price, longs pay shorts; when below, shorts pay longs. Net longs are economically matched by net shorts, but settlement and risk management occur via deterministic state changes enforced by code rather than through bilateral contractual promises between traders.[24]

Taken together, these examples illustrate Protocol-enforced Finance's distinctive feature: blockchains can execute smart contract logic deterministically in a way that creates *economic counterparty* relationships among users who need not know one another, without necessarily creating *contractual counterparty* relationships between them or an intermediary who can intervene ex post. This is how Protocol-enforced Finance can reproduce complex financial functions while simultaneously eroding the person-based "access points" on which traditional financial regulation depends.

2. Why Protocol-enforced Finance matters: scale, assets, and system relevance

While Protocol-enforced Finance uses smart contracts, the mere use of smart contracts to perform financial functions does not itself amount to Protocol-enforced Finance. Regulated financial service providers may deploy smart contracts for standardisation, interoperability, and operational efficiency without removing the responsible promisor or operator. Example 3 above illustrates this distinction: a typical stablecoin is governed by a smart contract for transfer and accounting functionality, but the economic "product" remains the issuer's legally enforceable redemption promise.

However, all digital tokens (including those used for stablecoins and other tokenised "real-world assets") can be used within Protocol-enforced Finance protocols, assuming they were created using the relevant token standard (e.g. the ERC20 standard for the Ethereum protocol). This matters because Protocol-enforced Finance, in principle, is not simply a new venue for trading cryptocurrencies. If widely adopted and used for economically significant assets, Protocol-enforced Finance could lead to a "*highly interoperable financial system with unprecedented transparency, equal access rights, and little need for custodians, central clearing houses, or escrow services*".[25] The same design features that could make this vision attractive to some (i.e. open access, composability, and rule-bounded execution) also place pressure on regulatory approaches built around supervising intermediaries.

[24] This example broadly describes the mechanisms used for perpetual futures trading platforms. For example, see dYdX Trading Inc., 'Perpetual Contracts: V3 dYdX Documentation'.

[25] Fabian Schär, '*Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets*' (2021) 103(2) Federal Reserve Bank of St. Louis Review 153.

2.1. Chapter 7's anthropocentric 'hooks' and where they fail

Chapter 7 of the *Corporations Act 2001* (Cth) (**Act**) regulates, among other things, financial products, financial service providers and financial market infrastructure in Australia. However, its operational architecture is less "object-based" (products/infrastructure) and more anthropocentric (person-centred).[26] It defines "financial products" functionally by reference to the economic function of an arrangement,[27] but regulates those products indirectly by attaching permissions, prohibitions and ongoing duties to identifiable legal actors associated with it.

This architecture presupposes a responsible subject at each stage of the regulatory cycle. Entry controls (Australian financial services, clearing and settlement and market licensing) assume the existence of an entity that can apply for authorisation and be held to ongoing conditions.[28] Conduct and disclosure rules[29] assume someone is there to generate mandated communications, supervise representatives, manage conflicts, and maintain compliance systems – obligations that are intelligible only where there is an addressee to be held legally accountable. Enforcement likewise assumes contraventions can be attributed to a person and met with sanctions that deter misconduct and enable remediation. Much of the law that underpins banking, financial services and financial markets, whether common law or equity, is also anthropocentric. For example, the formation of a contract and the creation of a trust requires that the counterparty or trustee, respectively, is a person (whether a natural person, a corporation or some other kind of legal person).

Protocol-enforced Finance destabilises those assumptions. Where a protocol is deployed to a public blockchain as practically immutable code that can be used by parties to facilitate an economic relationship without an intermediary, many conventional regulatory "access points" are attenuated or absent. The protocol users take on a variety of risks due to their use of the protocol, but the protocol has no operator to license, no compliance system to audit, no dispute resolution system to deal with faults like coding bugs. There may be no contractual relationship to enforce, no fiduciary duties to rely on, and no entity capable of being compelled to suspend the protocol, alter its terms (if any), or compensate users. Even where there are identifiable contributors – developers, governance participants, or website interface providers – those actors may not occupy the kind of control position that Chapter 7 ordinarily treats as the basis for responsibility.[30]

The result is not simply an enforcement gap, but a structural mismatch between: (i) a framework designed to regulate issuers and operators (i.e. persons who are liable for the terms and obligations of a product); and (ii) a mode of financial activity in which the relevant functions are performed by deterministic code and distributed validation. Regulation cannot simply extend existing frameworks. For example, the mismatch can be shown by three stress-tests. Each takes

---

[26] Explanatory Memorandum, *Financial Services Reform Bill 2001* (Cth), [4.24], [6.31], [6.88].

[27] *Corporations Act 2001* (Cth) s763A; Explanatory Memorandum, Financial Services Reform Bill 2001 (Cth), [6.40].

[28] *Corporations Act 2001* (Cth) ss791A, 820A and 911A.

[29] *Corporations Act 2001* (Cth) s912A, Pt 7.7, Pt 7.9.

[30] The *Corporations Amendment (Digital Assets Framework) Bill 2025* (introduced to the Australian Parliament on 26 November 2025) proposes to amend the Corporations Act 2001 to introduce a variety of exclusions, exemptions, and carve-outs the effect of which is intended to ensure that Protocol-enforced Finance (referred to as decentralised applications and protocols in the Explanatory Memorandum to the Bill) which are not controlled by any person are not regulated under Chapter 7, and that any actors are not treated as if they control those protocols where they do not exercise such control. See paragraphs [1.41] – [1.77], [1.78] – [1.106] and [1.331] – [1.370] of the Explanatory Memorandum to the *Corporations Amendment (Digital Assets Framework) Bill 2025*.

a familiar Chapter 7 hook ("provider", "custodian", "market operator") and asks what, exactly, the regime is meant to *bite on* when the relevant function is performed by protocol logic rather than by an accountable intermediary:

(a) **"Providing" a financial service**. Chapter 7 confers protections and imposes duties by reference to the person who "provides" the service or issues the product. That framing assumes an actor who can be licensed, supervised, directed and sanctioned. In many Protocol-enforced Finance configurations, however, users interact directly with a smart contract (often via an interface that may be separable from the contract itself), and execution occurs deterministically once transaction conditions are satisfied. The difficult question is not merely semantic ("who is the provider?") but functional: who has the ongoing capacity to comply with conduct, disclosure, dispute resolution and remediation obligations that the regime presupposes? Where no actor occupies that position, responsibility can only be re-routed to partial proxies (developers, governance participants, interface hosts, infrastructure services) whose relationship to execution and control may be too attenuated to make the duties workable.

(b) **Custodian**. Custody regulation assumes a person who has possession or control of assets on behalf of another and can therefore be compelled to segregate, reconcile, freeze, return and remediate. In Protocol-enforced Finance, assets are frequently "locked" by protocol logic and released only when pre-coded conditions are met. That can be functionally custodial from the user's perspective while being legally and practically non-custodial in the traditional sense. If no person can unilaterally access, freeze or return the assets, there may be no custodian capable of performing the core obligations that justify the regime.[31] The regulatory choice then becomes stark: either treat peripheral actors as if they were custodians (risking duties they cannot discharge), or accept that user protection must be pursued through different levers (for example, protocol-level assurance about how custody-like functions operate and what failure modes exist).

(c) **Operating a financial market**. Market licensing obligations assume an operator who sets and enforces rules, controls access, monitors trading, intervenes when integrity is threatened, and can be compelled to maintain fair, orderly and transparent markets. Protocol-based trading venues — particularly automated market makers — produce economically intelligible outcomes without the institutional features those concepts presuppose (order priority, cancellations, auction procedures, best execution norms, and discretionary interventions). Treating protocol logic as a "market operator" therefore risks a category error: the market function exists, but the governance and control structure that Chapter 7 relies on to make the obligations meaningful may not.

In each case, Chapter 7 regulates a function by attaching obligations to a person who can be compelled to take action. In a Protocol-enforced Finance setting, classifying protocol logic as a "financial product", "financial service" or "financial market" does not, by itself, reduce risk or generate protections for users. These labels do not create an entity that can prepare disclosure, implement controls, freeze transactions, return assets, rectify misconduct, compensate loss, or respond to regulator directions. The designation therefore risks being purely nominal (i.e. it

[31] This is the policy basis underpinning the regulation of digital asset platforms and tokenised custody platforms under the *Corporations Amendment (Digital Assets Framework) Bill 2025*. See the Explanatory Memorandum to the Bill for further information.

identifies conduct that, in theory, falls within the perimeter, but it does not supply a regulated addressee through whom the regime can do work).

Put differently, Chapter 7 mitigates risk by changing the incentives and behaviour of regulated persons. Where there is no person capable of compliance, the regime cannot operate in its ordinary way. The law either fails to attach coherently (because there is no provider or operator to whom duties can be assigned), or it attaches only by extending liability to peripheral actors – developers, interface providers, validators, or infrastructure providers – who may not control protocol execution and therefore cannot practically discharge the obligations. In that scenario, regulation becomes an indirect prohibition rather than a workable risk management framework.

3. Conclusion

Australia's post-Wallis Inquiry framework is functional and largely technology-neutral. Its focus on the nature of financial functions being performed (rather than the form of those functions) was intended to future-proof the framework, ensuring that new delivery mechanisms (from electronic banking in the 1990s to internet platforms in the 2000s) would still fall within the regulatory perimeter if the underlying financial activity was the same.[32] Protocol-enforced Finance exposes the limits of that design choice. Where financial functions are performed by deterministic smart contracts on public infrastructure without an intermediary, the law's usual regulatory "hooks" weaken.

This does not mean that all Protocol-enforced Finance activity labelled "DeFi" sits beyond regulation. Many systems retain meaningful control points (for example, upgrade rights or privileged functions). Those arrangements remain amenable, and least in part, to orthodox regulation because responsibility can be attached to actors who can materially influence outcomes. However, much of the contemporary legal and policy debate has concentrated on identifying "regulatory hooks" along centralisation vectors – where a responsible person can plausibly be identified.[33] That emphasis is partly pragmatic, given many self-labelled "DeFi" protocols "*…have a hidden centralized authority and are decentralized in name only*".[34] However, the direction of travel is not one-way. Deutsche Bank and Northern Trust note that applying DeFi (which would include Protocol-enforced Finance) "*to institutional use cases*" is "*being met with great interest*", and define 'institutional DeFi' to include both the institutional "*adoption and adaptation*" of DeFi structures and "*institutional participation*" through existing DeFi applications.[35] Consistent with that trajectory, the Financial Stability Board also explicitly anticipates institutional participation in DeFi, noting that monitoring and closing data gaps can help institutional participants assess the associated risks.[36]

The policy implications of Protocol-enforced Finance being used for serious financial-system purposes – and its incongruity with existing legal categories – are that effective regulation is likely

---

[32] Financial System Inquiry (Australia) and Stanley Wallis, Financial System Inquiry Discussion Paper (Discussion Paper, Australian Government Publishing Service, 1996), Chapter 4.

[33] See for example: Ilya Kokorin, '*The Decentralisation Defence*' (2025) 57 Computer Law & Security Review.

[34] International Organization of Securities Commissions, Decentralized Finance Report (Report No OR01/2022, International Organization of Securities Commissions, March 2022).

[35] Dan J Sleep and Boon-Hiong Chan, *The Road to Institutional DeFi: How Decentralised Finance (DeFi) Can Be Used for Regulated Financial Activities* (White Paper, Deutsche Bank Corporate Bank and Northern Trust, June 2024).

[36] Financial Stability Board, *The Financial Stability Risks of Decentralised Finance* (Report, Financial Stability Board, 16 February 2023).

to require a shift in regulatory theory as well as in regulatory technique. For Australia, this points to a research and policy agenda centred on: (i) identifying where effective control and concentration sit across the protocol stack (including governance, admin keys, validators, oracles, and interfaces) and assessing how dependency risks can be appropriately mitigated;[37] (ii) protocol-level assurance mechanisms – such as code certification, lifecycle-based auditing, and graduated risk labelling and disclosure – that can operate where entity-based licensing is impracticable;[38] (iii) protocol-embedded compliance options;[39] and (iv) using the distinctive observability of public blockchains to support real-time monitoring, market-integrity oversight, and targeted intervention via distribution choke points.

An orthodoxy built around promises, intermediaries and agency is now being stress-tested by a reality of protocols-based finance. Recognising where the traditional model fails – and where it still bites – is a necessary predicate to designing safeguards that remain credible as finance becomes increasingly programmable.

[37] Katrin Schuler, Ann Sofie Cloots and Fabian Schär, '*On DeFi and On-Chain CeFi: How (Not) to Regulate Decentralized Finance'* (2024) 10(2) Journal of Financial Regulation 213.

[38] See for example, Olivier Fliche, Julien Uri and Mathieu Vileyn, "*Decentralised" or "Disintermediated" Finance: What Regulatory Response?* (Discussion paper, Autorité de contrôle prudentiel et de résolution (ACPR), Fintech-Innovation Hub, April 2023).

[39] See for example, Raphael Auer, *Embedded Supervision: How to Build Regulation into Decentralised Finance* (BIS Working Papers No 811, Bank for International Settlements, 16 September 2019); Bermuda Monetary Authority, *Call for Proposal — Embedded Supervision in the Context of Decentralised Finance* (Consultation Paper, Bermuda Monetary Authority, 3 February 2025).