BLOCKCHAIN SECURITISATION: AN AUSTRALIAN-COMPLIANT FRAMEWORK FOR ON-CHAIN RMBS

Author: Daniel Cheah

Contact: contact@danielcheah.com

Date: 21 October 2025

ABSTRACT

This paper proposes a legally and operationally compliant framework for issuing Australian Residential Mortgage-Backed Securities (RMBS) on-chain. Unlike many blockchain proposals focused on speed, this model prioritises compatibility with existing Australian legal, regulatory and trustee structures.

The framework demonstrates **tokenisation without new legislation**, aligning with the *Corporations Act*, *PPSA* and *Torrens Title* system. It defines a **dual-layer structure**: on-chain *Mortgage NFTs™* record beneficial interests, while off-chain deeds preserve legal enforceability. Smart contracts, oracles and regulated AUD-denominated stablecoins enable atomic Delivery-versus-Payment (DvP) settlement and real-time waterfall automation.

Recent US securitisation failures - *First Brands Group* and *Tricolor Auto Acceptance* (2025) - exposed weaknesses in collateral verification and cash-flow integrity. Public filings alleged double-pledged receivables and poor servicer controls, risks this model is designed to eliminate. Unique, verifiable mortgage tokens and automated *T+0 On-Ramping™* for cash segregation ensure transparent asset provenance and immediate SPV fund isolation.

The legal analysis confirms enforceable true sale, dual perfection under the *PPSA*, and AML/CTF compliance. The paper concludes that a permissioned, trustee-supervised blockchain can satisfy **APRA's APS 120 Securitisation Standard**, bridging conventional RMBS structures with emerging digital-asset capital markets.

JEL Classification: G21, G23, G28, K22, O33

Keywords: Blockchain, RMBS, Securitisation, Tokenisation, Stablecoin, Smart Contracts, PPSA, True Sale, Atomic Settlement, Treasury Reform, Digital Assets

Author Declaration

This paper represents **independent research** conducted by the author. The views and opinions expressed are solely those of the author and do not represent the views of any organisation, institution, or employer. No confidential or proprietary information has been used in the preparation of this work.

Disclaimer

This paper is provided for informational and research purposes only. It does not constitute legal, financial, or regulatory advice. Readers should obtain independent professional advice before acting on any concepts, structures, or interpretations described herein.

Proprietary Designations

The terms *Mortgage NFT™, Smart SPV™, T+0 On-Ramping™, Verifiable PDS™, Smart Servicer™* and *Waterfall Smart Contract™* are proprietary designations used to describe conceptual and technological components of the proposed framework.

These terms are presented to establish authorship and usage in this publication. They are not registered trademarks under Australian law at the time of writing.

Contents

1.0 Introduction: The Case for On-Chain RMBS in Australia

The Australian Residential Mortgage-Backed Securities (RMBS) market is a cornerstone of the nation's financial architecture. It provides a critical funding channel for both Authorised Deposit-taking Institutions (ADIs) and the vibrant non-bank lending sector, fostering competition and providing liquidity to the housing market. This market operates on a mature and robust legal framework, governed primarily by the *Corporations Act 2001 (Cth)* and overseen by regulators including the Australian Securities and Investments Commission (ASIC) and, for ADIs, the Australian Prudential Regulation Authority (APRA).

However, despite its sophistication, the traditional securitisation process remains a product of its time. It is an intermediary-heavy, document-intensive and sequential process characterised by data silos, manual reconciliation and defined settlement windows. These legacy features create inherent frictions, costs and data opacities that weigh on issuers, investors and regulators alike.

This paper proposes that Distributed Ledger Technology (DLT), or blockchain, offers a new infrastructure stack capable of fundamentally re-engineering the RMBS lifecycle. It argues that a "blockchain-native" RMBS is not a "DeFi" (Decentralised Finance) instrument operating outside the regulatory perimeter, but rather a *technology-enabled* financial product that can operate *within* it, offering profound gains in efficiency, transparency and compliance.

1.1 The Traditional RMBS Process: Identifying Australian Frictions

In a typical Australian RMBS deal, a pool of mortgage assets is sold by an originator into a bankruptcy-remote Special Purpose Vehicle (SPV), established as a trust. This trust then issues debt instruments (notes) in tranches to investors, with payments "passed through" from the mortgage holders.

While effective, this structure creates specific, well-understood frictions:

- **Data Opacity and Asymmetry:** Investors and regulators rely on static, backward-looking reports (e.g., monthly trustee reports) to assess the performance of the underlying collateral. There is no "golden source" of truth; data is held in disparate silos by the originator, the servicer and the trustee, requiring costly reconciliation.
- **Intermediary Frictions:** The lifecycle is coordinated by a chain of intermediaries (Originators, Trustees, Servicers, Custodians, Paying Agents). While each performs a vital role, their sequential coordination adds cost and time, particularly in cash-flow management and reporting.

- **Settlement Delays and Risk:** Primary issuance and secondary market trading of RMBS notes settle through traditional systems like *Austraclear*. These systems are highly effective but operate on defined timetables (e.g., T+2 settlement for secondary trades), which introduces counterparty risk and ties up capital. Cash movements rely on the Reserve Bank Information and Transfer System (RITS), which also operates on a defined schedule.

1.1.1 Structural Weaknesses in Conventional Securitisation

The conventional RMBS structure depends on multiple intermediaries and asynchronous data reconciliation. While robust in principle, this fragmentation introduces operational and informational risk—particularly in asset verification and cash-flow segregation.

Recent failures in the US consumer and auto ABS sectors underscore these weaknesses. The 2025 collapses of **First Brands Group** and **Tricolor Auto Acceptance** revealed how poor collateral tracking and opaque remittance processes can mask double-pledging and misreporting of receivables. Public filings and media reports alleged such irregularities, with resulting investor losses now under investigation.

Although the Australian prudential framework is stronger, the same structural vulnerabilities exist in data latency, manual reconciliation and commingled servicing accounts. The framework proposed in this paper directly addresses these exposures. Each loan is represented by a uniquely hashed **Mortgage NFT**™ (Section 2.2), ensuring a single, verifiable title across the securitisation chain. **Automated T+0 On-Ramping**™ (Section 5.3) enables immediate allocation of borrower payments to the SPV, removing commingling lag and creating a continuous audit trail for trustees and regulators.

1.2 The Blockchain Value Proposition: An Australian Regulatory Lens

The central thesis of this paper is that blockchain technology can be applied in a "technology-neutral" manner, a principle consistently articulated by Australian regulators. An on-chain RMBS note is not a new, unregulated asset class; it is the *same financial product* - a "debenture" or an "interest in a managed investment scheme" as defined by the *Corporations Act* - represented in a new, superior digital format.

- **ASIC's Position:** ASIC guidance (for example, *INFO 225*) confirms that if a token displays the characteristics of a financial product, it is regulated as one. Accordingly, an on-chain RMBS offering would require the issuer to hold an Australian Financial Services Licence (AFSL) and unless restricted to *wholesale clients* under section 761G of the Act, would be subject to the disclosure requirements of Chapters 6D or 7 (prospectus or Product Disclosure Statement).

- **RBA's Vision:** The Reserve Bank of Australia, together with ASIC and industry partners, is now actively testing tokenised settlement infrastructure through *Project Acacia*. These trials demonstrate that tokenised securities and digital settlement assets can operate within existing prudential and payments frameworks. By enabling atomic Delivery-versus-Payment (DvP) settlement, they remove counterparty risk and open the pathway to continuous markets.

Taken together, these regulatory positions confirm that blockchain-based RMBS structures sit **within** Australia's existing legal perimeter, not outside it. Within this framework, the value proposition becomes clear:

1. **Radical Transparency and Immutability:** A permissioned blockchain serves as a single, auditable ledger for the entire collateral pool, accessible in real time by issuers, investors, trustees and regulators. Static monthly reports are replaced by a live "golden source" of truth.

2. **Automation via Smart Contracts:** The trust "waterfall" - which defines payment priorities among noteholders, servicers and other parties - can be encoded into a smart contract. This automates cash-flow distributions, reduces operational risk, and mathematically enforces compliance with the governing documents.

3. **Atomic Settlement:** Representing both the RMBS note (the asset) and the settlement medium (for example, a regulated stablecoin or future wholesale CBDC) on-chain enables instantaneous Delivery-versus-Payment. This reduces settlement risk, frees collateral, and eliminates the traditional T + 2 window.

Blockchain therefore functions as a **compliance technology**, not a disruption to regulation. It strengthens transparency, auditability and settlement integrity — aligning perfectly with the regulatory direction already being tested through *Project Acacia* and related Australian initiatives.

1.3 Paper Objectives and Structure

This paper does not advocate for replacing the Australian regulatory framework. Instead, it seeks to provide a comprehensive framework for applying blockchain technology *within* it. The objective is to map the entire RMBS lifecycle, from origination and tokenisation to servicing and redemption, to an on-chain, Australian-compliant model.

The following sections will deconstruct each phase of the deal cycle, analysing the technical implementation (e.g., smart contracts, oracles), the legal "wrapper" required to ensure enforceability and the specific compliance checkpoints required by ASIC, APRA and AUSTRAC.

2.0 Phase 1: Origination and Asset Tokenisation

The axiom of any securitisation is that the quality of the output (the securities) is entirely dependent on the quality of the input (the underlying assets). For a blockchain-based RMBS, this principle is amplified. The entire system's automated efficiency and transparency rest on the creation of a legally sound, verifiable and digitally-native *mortgage asset* from the moment of origination.

This "origination and on-ramping" phase is arguably the most complex, as it must bridge Australia's established legal frameworks for identity, contracts and property law with the new infrastructure of a blockchain.

2.1 The "Digital Mortgage": From Paper to On-Chain Asset

A "digital mortgage" in this context is not merely a PDF scan of a loan agreement. It is a package of data and legal rights, cryptographically secured and bound together. This requires solving two primary challenges: borrower identity and the legal status of the loan contract itself.

2.1.1 Borrower Digital Identity (DID) and On-Chain KYC/AML

Before any loan can be originated, the borrower's identity must be verified. This is a non-negotiable requirement under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth)*, enforced by AUSTRAC.

- **Traditional Process:** A borrower provides 100 points of identification to an originator (e.g., a non-bank lender), who is a "reporting entity" under the Act. This information is stored in the originator's private database.
- **On-Chain Model:** A blockchain model can use the concept of a **Digital Identity (DID) or Verifiable Credential (VC)**.
    1. **Once-Only Verification:** The originator, as a trusted and regulated reporting entity, performs the KYC/AML check exactly as they do today.
    2. **On-Chain Attestation:** Upon successful verification, the originator "issues" a non-transferable token (sometimes called a "soul-bound token" or a Verifiable Credential) to the borrower's digital wallet.
    3. **Privacy-Preserving Proof:** This token does not contain the borrower's personal data (e.g., passport number or name). Instead, it acts as a cryptographic "pass" that attests: *"I, [Originator AFSL #XXXXX], certify that the holder of this wallet has successfully completed an AUSTRAC-compliant KYC/AML check on [Date]."*
    4. **Compliance:** This allows the borrower to interact with other on-chain applications (like the "Smart SPV" or servicers) and prove their verified

status without repeatedly resubmitting sensitive personal information, enhancing both efficiency and data privacy.

2.1.2 Smart Contracts as Loan Agreements (e-Mortgages)

Smart contracts can express and enforce financial logic with deterministic precision. In a securitisation context, the loan agreement terms, such as principal balance, interest rate and repayment schedule, can be mirrored by a smart contract. However, this digital contract serves only as an **execution layer**, not as the **legal source of obligation**.

Under Australian law, the enforceable loan agreement remains the governing legal instrument. The smart contract automates its economic performance but does not itself constitute a legally binding mortgage under the **National Credit Code** or state property law.

The **Electronic Transactions Act 1999 (Cth)** allows for electronic execution and data storage of loan contracts, but enforceability still depends on compliance with standard legal requirements: borrower consent, identity verification and registration of the underlying mortgage interest on the **Torrens Title Register**.

- **Financial Terms as Code:** While the full legal terms and consumer credit disclosures (under the *National Consumer Credit Protection Act 2009*) would remain in a legally binding (electronic) document, the core *financial logic* of the loan can be embedded in a smart contract. This includes:
    - Principal Amount
    - Interest Rate (fixed or a formula for variable)
    - Loan Term
    - Payment Schedule (e.g., P&I, 1st of the month)
- **Integration with PEXA:** The registration of the mortgage as a security interest over the property title is the critical off-chain link. This process, managed by the state Land Titles Offices via platforms like **Property Exchange Australia (PEXA)**, remains the source of truth for the legal charge over the real-world asset. The "digital mortgage" smart contract would hold a verifiable reference (e.g., a transaction hash or ID) to the successful PEXA settlement and registration of the charge, immutably linking the on-chain financial asset to the off-chain legal security.

2.2 Tokenisation of the Mortgage Asset

Once the borrower is verified and the digital loan agreement is executed and linked to the property title, the loan itself (the financial asset) can be represented on-chain.

For tokenised interests, perfection under the PPSA would continue via registration on the PPSR. Control of the Mortgage NFT (via private key) functions as operational evidence of possession but does not yet substitute for statutory control. Accordingly, the on-chain record should be viewed as an evidentiary supplement, not a replacement for PPSA perfection.

2.2.1 Representing a Unique Loan (Non-Fungible Token - NFT)

Each mortgage is unique. It has a specific borrower, property, interest rate and outstanding balance. It is a "non-fungible" asset. The most logical way to represent this on-chain is as a **Non-Fungible Token (NFT)** (e.g., using the ERC-721 standard or a more specific financial-asset standard).

1. **Minting:** The originator (the lender) "mints" a unique NFT for each mortgage it originates.
2. **Metadata:** This NFT's metadata acts as the digital "container" for the loan. It holds all the critical data points required for securitisation:
    - Property ID (e.g., a hashed version of the title reference)
    - Loan Type (e.g., Prime, Non-Conforming)
    - Origination Date
    - Original Principal
    - Current Balance (this will be a dynamic field)
    - Interest Rate and Type
    - LVR at Origination
    - Link to the Verifiable Credential of the borrower (proving KYC)

The originator now holds a portfolio of these "Mortgage NFTs," each one a digitally native, verifiable representation of a specific loan asset.

2.2.2 Legal Wrapper and True-Sale Mechanism

This is the most critical step for legal enforceability in an Australian court. The **NFT** itself is merely code; it must be legally and unambiguously bound to the originator's rights under the underlying **loan agreement** - the *chose in action* representing the borrower's repayment obligation.

This linkage is achieved through a robust legal **"wrapper"** such as a **Deed Poll** or **Token Deed** executed by the originator at the time of minting. This deed establishes the **true-sale** mechanism that transfers the beneficial interest in the mortgage asset from the originator to the securitisation trust.

The deed should state, in clear and enforceable terms, that:

- The originator is the legal and beneficial owner of the mortgage (as registered on title) and the associated rights to its cash flows.
- The originator irrevocably declares that the **beneficial interest** in this mortgage asset is held by and travels with the holder of the specific NFT identified by its unique on-chain token ID.
- This deed ensures that the subsequent on-chain transfer of the NFT—for example, from the originator's wallet to the SPV's wallet—functions as the **immutable settlement record and verifiable audit trail** of the legal transfer. The true sale itself is legally enacted by a conventional off-chain **Master Sale Agreement**, in which this deed is referenced.

The on-chain transfer therefore conveys the **beneficial interest** in the mortgage receivable, the *chose in action* representing payment rights, while **legal title** to the underlying real-property mortgage remains registered off-chain under the relevant state **Torrens Title** legislation.

Functionally, this structure achieves the same economic and legal outcome as a traditional sale of mortgages into an SPV or trust. The on-chain token operates as a *digital bearer of beneficial interest*, whereas the statutory land-title register maintained by the state **Land Titles Office** (e.g., via **PEXA**) continues to record the legal charge over the real-world asset.

2.3 The "Oracle Design Challenge": Static and Dynamic Loan Data

Blockchains are deterministic systems; they cannot independently access external, real-world data. They must be "told" this information by a trusted data source known as an **oracle**. For RMBS, oracles are essential for both establishing the initial, immutable facts about a loan at origination and for tracking its subsequent evolution. The "Mortgage NFT" metadata must capture both.

- **Static Origination Data:** Certain key data points are fixed at the time of loan origination and form the baseline for analysis. When the "Mortgage NFT" is minted (as per 2.2.1), these fields are populated with immutable origination characteristics. The oracle (often the originator or servicer verifying the data) plays a role in ensuring this initial data is correctly recorded on-chain:
    - Original Principal Amount
    - Origination Date
    - Loan Term
    - Interest Rate Type (Fixed/Variable)

    - Original LVR (Loan-to-Value Ratio)
    - Original DTI (Debt-to-Income Ratio, if available)
    - Property Postcode/Region (Anonymised)
    - Loan Type (e.g., Prime, Non-Conforming)
- **Dynamic Loan Data (Oracle-Updated):** Most loan characteristics evolve. The **servicer** typically acts as the primary oracle responsible for pushing validated, real-time updates from its off-chain systems to dedicated *dynamic* fields within the corresponding NFT's metadata. This ensures the on-chain representation mirrors the current state of the off-chain loan:
    - **Current Balance:** Updated regularly (e.g., daily or monthly) reflecting payments and accruals.
    - **Current Applicable Interest Rate:** For variable-rate loans, the servicer-oracle pushes the *new, specific interest rate* when the lender adjusts it off-chain.
    - **Current Loan Status:** Updates regarding payment status (e.g., 'Current', '30+', 'Hardship') are pushed by the servicer-oracle.
    - **Current LVR:** Calculated using the *Current Balance* and the latest property valuation pushed by a **Valuation Oracle** (e.g., AVM provider).
    - **Current DTI:** Updated if/when the servicer receives and verifies updated income information, reflecting the borrower's current capacity (within the anonymised context).
    - **Loan Modification Data:** If a loan's terms are significantly altered (e.g., rate switch, term extension), specific fields are updated by the servicer-oracle to reflect the new structure, while preserving the original static data.

The integrity and reliability of these oracle feeds for *both* initial static data validation *and* ongoing dynamic updates are paramount. Maintaining this accurate distinction between origination facts and the current loan status within the NFT metadata is crucial for investor analysis, reporting and the overall trustworthiness of the on-chain system.

Disclaimer: The specific static and dynamic data fields listed above are illustrative examples. The final, comprehensive set of data points required to be included in the "Mortgage NFT" metadata for any given transaction will ultimately be determined by the specific requirements of investors and rating agencies, ensuring the necessary level of transparency and detail for thorough credit and operational risk assessment.

3.0 Phase 2: Pooling, Structuring and the "Smart SPV"

With a verified, legally-bound pool of "Mortgage NFTs" created, the next phase involves aggregating these assets into a securitisation trust and structuring the liabilities (the notes) to be issued against them. In Australia, the RMBS Special Purpose Vehicle (SPV) is almost universally a **trust** established by a trust deed. The challenge is to create a "Smart SPV" that is both legally robust under Australian trust law and operationally efficient on-chain.

3.1 The On-Chain Special Purpose Vehicle (SPV)

A common misconception is that a "blockchain SPV" must be a Decentralised Autonomous Organisation (DAO). For a regulated financial product like an Australian RMBS, this model is currently unviable. A DAO often lacks a clear legal personality, creating ambiguity around who holds title to assets, who to sue and how to apply the *Corporations Act*. ASIC's guidance suggests most DAOs would likely be deemed partnerships or, more appropriately for this context, a **Managed Investment Scheme (MIS)** under Chapter 5C of the *Corporations Act*. This would require a "responsible entity" (RE) with an AFSL, a structure that is far more complex than the standard, passive securitisation trust.

The superior and compliant model is a **hybrid approach**:

1. **Legal Structure:** The SPV remains a **traditional Australian securitisation trust** (e.g., "XYZ RMBS Trust 2026-1"), established by a professional trustee company via a standard off-chain Master Trust Deed. This trust has a legal personality, an ABN and is the legal entity that faces regulators.

2. **Operational "Brain":** The **smart contracts** act as *automated systems* executing the trustee's delegated administrative functions under explicit authorisation in the Trust Deed. Legally, they perform as tools of execution rather than independent agents, ensuring all fiduciary authority remains with the trustee.

3. **Legal Enforceability and the "Dual-Layer" True Sale:**

   The **true sale** of mortgages from the originator to the SPV remains the legal and economic cornerstone of securitisation, ensuring that the underlying assets are isolated from the originator's insolvency.

   In the blockchain-enabled model proposed here, the on-chain transaction (the token transfer) is **not** legally sufficient on its own to achieve a true sale. Australian law still recognises the **off-chain legal documentation** as the governing instrument. The model therefore adopts a **dual-layer approach**, where the off-chain agreements create and govern the rights, while the on-chain activity records and enforces them with cryptographic certainty.

This hierarchy is preserved in three dimensions:

1. **Creation of Rights** - The *Token Deed* (introduced in Section 2.2.2) gives legal power to the on-chain *Mortgage NFT™*. The token by itself is mere code; the Token Deed is the declaration that the beneficial interest in the mortgage travels with the token. The true sale is legally enacted through a conventional **Master Sale Agreement** executed under Australian contract law.

2. **Governance of Logic** - The **Master Trust Deed** remains the paramount governing document. The *Waterfall Smart Contract™* simply performs the instructions embedded in that deed. The blockchain does not create new legal rights. Rather, it automates compliance with existing ones.

3. **Resolution of Conflict** - In the event of a dispute, Australian courts will uphold the written trust deed over any inconsistent code execution. “Code is law” has no standing under Australian jurisprudence. The Trust Deed always prevails.

   Accordingly, the on-chain transfer of *Mortgage NFTs™* from the originator’s wallet to the SPV’s wallet is **not the sale itself**. It functions as the immutable settlement record and verifiable audit trail of the legal transaction perfected off-chain. This explicit legal hierarchy (paper governing code) is essential not only for enforceability but also for satisfying rating-agency and prudential-compliance requirements (see Section 9).

3.2 Automated Pooling, Selection and Collateral Analysis

This hybrid structure, which combines a traditional legal trust with on-chain assets, enables powerful automation of due diligence, pooling and live portfolio analysis. This is achieved through a symbiotic relationship between a user-facing "Poolcut Application" and the underlying "Smart Contracts."

3.2.1 The On-Chain Poolcut Application

In a traditional deal, creating a "poolcut" is a manual, iterative process of filtering a static spreadsheet of loans. In the on-chain model, this is replaced by a dynamic, user-facing application.

- **Function:** This tool acts as an interface for the issuer, warehouse provider, or arranger. It queries the entire live pool of "Mortgage NFTs" (from Section 2.2) held in the originator's wallet.

- **User Input (Desired Pool):** The user inputs their desired **Eligibility Criteria (EC)** into the application. For example:

    - LVR <= 80.0%

    - Arrears Status == 'False'

    - Loan Type == 'Prime'
    - Geographic Concentration (NSW) <= 40.0%
- **Live Analysis and Output:** The application queries the on-chain "Mortgage NFT" metadata and instantly returns:
    1. **A "Live" Stratification Report:** A real-time "strat table" (as described in 3.2.3) of the selected pool, allowing the user to see the impact of their criteria instantly.
    2. **A Definitive List of Assets:** A list of every "Mortgage NFT" (by its unique token ID) that matches the criteria.

The user can now model various poolcuts in real-time against verifiable, live collateral data, rather than a month-old static file.

3.2.2 Smart Contract Eligibility Enforcement

Once the user has selected their final pool using the application, the "true sale" (from 3.1) is initiated. This is where the "gatekeeper" smart contract takes over.

This contract acts as the automated enforcer of the Eligibility Criteria. Before the SPV's wallet accepts any "Mortgage NFT" in the sale, the contract automatically performs a final check:

- It reads the metadata of the incoming NFTs.
- It checks them against the **Eligibility Criteria** defined in the Trust Deed (which mirror the criteria used in the Poolcut App).
    - if (NFT.metadata.LVR > 80.0) { reject }
    - if (NFT.metadata.LoanType != 'Prime') { reject }
    - if (NFT.metadata.InArrears == 'True') { reject }

This provides cryptographic proof that every single asset in the final pool met the required criteria at the exact moment of acquisition, eliminating any "human error" between the poolcut and the final settlement.

3.2.3 Real-Time Portfolio Stratification (The "Engine")

This "dashboard" smart contract is the engine that powers both the Poolcut Application and the SPV's ongoing reporting. Once the Mortgage NFTs are held in the SPV's wallet, this contract continuously reads the metadata of the entire pool.

This allows any permissioned party (investors, the trustee, the RBA) to see a **live, real-time stratification report** ("strat table") at any time. This replaces the static, month-old

PDF servicer report with a dynamic, verifiable "golden source of truth" for the pool's Weighted Average LVR (W.A. LVR), arrears status and geographic concentration.

3.3 Structuring: Smart Contracts for Tranching

With the asset side of the balance sheet secured, the SPV structures its liabilities (the RMBS notes). These notes are issued as **fungible security tokens** (e.g., compliant with a standard like ERC-20 or ERC-3643).

- **Defining Tranche Characteristics:** A "tranche" smart contract defines the specific rights of each token. These tokens are the *digital representation* of the "debentures" (as defined in the *Corporations Act*) issued by the trust.
  - **Token A1:** (Tranche_ID: 'A1', Type: 'Senior', Priority: 1, Coupon: 'BBSW + 1.20%')
  - **Token B:** (Tranche_ID: 'B', Type: 'Mezzanine', Priority: 2, Coupon: 'Fixed 8.50%')
  - **Token E:** (Tranche_ID: 'E', Type: 'Equity', Priority: 3, Coupon: 'Residual')
- **Automated Credit Enhancement:** The smart contract logic can also automate the management of credit enhancement mechanisms.
  - **Overcollateralisation (OC):** The system can verifiably prove the OC level 24/7. A smart contract can constantly check (Value of Mortgage NFTs) / (Value of Notes Issued) and automatically block any action (like an equity note payment) that would breach a covenant.
  - **Reserves:** The smart contract (in Phase 5) will be programmed to automatically trap excess spread into a separate "reserve" wallet, building credit support exactly as defined in the trust deed.

4.0 Phase 3: Issuance, Offering and Distribution

The transition from a structured pool to a live issuance is where the "public" nature of blockchain intersects with the "permissioned" world of Australian securities law. This phase involves not only the technical Security Token Offering (STO), fully regulated by ASIC, but also the critical commercial process of book-building and allocation.

4.1 The Security Token Offering (STO)

The tokens representing the RMBS tranches are unequivocally **financial products** under the *Corporations Act*. As such, their offer and distribution must comply with all relevant laws.

The "Verifiable Prospectus" (PDS): Unless the offer is made exclusively to "wholesale clients" / "sophisticated investors" (under s 761G of the Act), a retail offer would require a **Product Disclosure Statement (PDS)** or **prospectus** under Chapter 7 or 6D.

This new model allows for a *Verifiable PDS*™ transforming the document from a static, "trust-me" disclosure into a dynamic, "don't trust, just verify" instruction manual. While traditional in its description of risks, structure and parties, the Verifiable PDS would also prove its own claims by embedding the on-chain addresses of the "Smart SPV" itself.

For example, the PDS would state:

1. **Proof of Assets:** "The 1,000 'Mortgage NFTs' securing this issuance are held in the 'Smart SPV' at the following public blockchain address: [0x1a2b3c...SPV Wallet Address]. Investors can use any public blockchain explorer to independently confirm that exactly 1,000 of these assets are held in this wallet at this moment."
2. **Proof of Quality:** "The real-time characteristics of this pool (e.g., W.A. LVR, arrears status) are continuously calculated by the 'Dashboard Smart Contract' located at: [0x4d5e6f...Dashboard Contract Address]. Investors can query this contract's public functions to verify the pool's live statistics."

This approach fundamentally shifts the paradigm. It allows investors to perform their own real-time, asset-level due diligence *before* investing, rather than relying on a static, month-old "Cut-Off Date" report. It eliminates information asymmetry and builds trust by empowering the investor to cryptographically verify the issuer's claims.

Token Standards and Compliance: The RMBS security tokens must have compliance built-in. A standard like ERC-3643 is designed for this. It allows the issuer to embed rules *into the token itself*, such as:

- **Transfer Restrictions:** The token can only be held by wallets that have been "whitelisted."

- **Forced Transfers:** The trustee can be given the power to move tokens (e.g., to comply with a court order).
- **Data Integration:** The token can hold references to the off-chain PDS.

4.2 Primary Market Book-Building and Allocation

Before the final issuance and settlement, the Arranger and Joint Lead Managers ("JLM Group") must conduct the crucial **book-building process** to gauge investor demand, achieve price discovery and determine final allocations. While blockchain offers potential efficiencies, the confidential nature of this process presents unique challenges.

- **Indications of Interest (IOIs):** Investors need to communicate their non-binding interest (volume, price sensitivity). Given the need for confidentiality in institutional markets, a fully transparent on-chain bidding process is unlikely. The initial, most probable approaches are:
    - **Hybrid Model (Off-Chain IOIs):** Investors submit IOIs via traditional, confidential channels (secure platforms, email, Bloomberg) directly to the JLM Group. The JLM Group builds the book off-chain. The blockchain is then used primarily for the subsequent allocation execution and settlement phases. This leverages existing relationships and ensures bid confidentiality.
    - **Potential Future Model (On-Chain Confidential Bids):** More advanced systems could utilize privacy-preserving technologies like Zero-Knowledge Proofs (ZKPs). Investors could submit encrypted bids to a "Book Building Smart Contract," provably recording their submission time without revealing the bid details publicly. Only the Arranger / Issuer would hold the keys to decrypt the bids. This requires significant technical and potentially regulatory development.
- **Pricing and Allocation:** Once the book is closed, the JLM Group / Issuer determines the final issuance spread/price based on demand. Allocations are then decided. While smart contracts *could* automate simple allocation logic (e.g., pro-rata, time priority), the nuanced, relationship-based nature of institutional allocation suggests that JLM Group / Issuer discretion (performed off-chain) will likely remain central. The smart contract's role would be to *execute* these predetermined allocations efficiently and transparently during the settlement phase.

4.3 Primary Market Distribution and Settlement

This is where the most significant efficiencies are gained, following the book-build and allocation decisions.

- **Smart Contracts for Investor Whitelisting:** Before an investor can participate *or receive an allocation*, they must complete an off-chain KYC/AML check with the issuer (or a licensed intermediary). Once verified, their wallet address is added to the "whitelist" on the tranche smart contract. This ensures that only **known, compliant investors** can receive or hold the security tokens, satisfying the issuer's obligations.

- **Atomic Settlement (DvP):** The traditional **T+2** settlement process introduces both **principal** and **counterparty** risk, the possibility that one party delivers securities or funds while the other fails to perform. A blockchain-based **Security Token Offering (STO)** enables **atomic settlement**, where payment and delivery occur within a single, indivisible transaction. This eliminates principal and counterparty settlement risk while compressing the settlement window from T+2 to **T+0**.

  An **Issuance Contract**, triggered once allocations are finalised, functions as an on-chain escrow:

  1. **Investor Funding:** Allocated investors send their payment (e.g., AUD 100,000 in a regulated AUD-denominated stablecoin) to the contract.
  2. **Issuer Prefunding:** The issuer (SPV Trust) pre-funds the same contract with the corresponding AUD 100,000 of Token A1 units designated for that investor.
  3. **Instant Swap:** The contract executes an atomic swap and the investor receives the tokens *if and only if* the issuer simultaneously receives the funds.

  This instant **Delivery-versus-Payment (DvP)** mechanism eliminates settlement-sequence risk, reduces capital held in transit and aligns with the principles being tested by the **Reserve Bank of Australia's "Project Acacia."**

  While atomic settlement removes counterparty and principal risk, it does not eliminate **operational** or **oracle** risks (e.g., node failure, congestion, or data-feed error). These are mitigated through redundant nodes, **multi-signature controls** and off-chain supervisory protocols embedded within the Trust Deed.

4.4 Broadening Investor Access

This new infrastructure has the potential to democratise access to fixed-income assets.

- **Fractionalization:** A $100,000 note can be tokenised into 100,000 units of $1 each. This allows smaller wholesale investors to gain exposure and build diversified portfolios.

- **Global Reach:** An Australian-compliant STO can, in theory, be accessed by any "whitelisted" investor anywhere in the world, 24/7, reducing reliance on traditional global custodians and clearing houses.

5.0 Phase 4: Servicing and Administration

Once the RMBS is "live" and the notes are held by investors, the deal enters its long-term servicing phase. In a traditional deal, this is a monthly, batch-processed and often opaque procedure handled by the servicer and trustee. A blockchain model transforms this into a transparent, automated and real-time process, though it still requires careful integration with off-chain realities.

5.1 The Smart Servicer™ and Supporting Oracles: Automating Cash Flow Management

The "waterfall" (the set of rules in the trust deed dictating payment priorities) is ideally suited for automation via a smart contract. However, this automation relies on accurate, timely data feeds from trusted oracles for both loan-level performance and external market data.

- **Receiving Borrower Payments (Servicer Oracle):** This remains a key "oracle" integration primarily managed by the **Servicer**.
    1. Borrowers continue to pay their mortgages as normal (e.g., via BPAY) into a bank account held by the servicer.
    2. The servicer (acting as a trusted oracle) sends a regular (e.g., daily) cryptographic attestation to the SPV: "Received $X in P&I payments".
    3. The servicer then "on-ramps" this fiat by sending the equivalent amount in stablecoin into the SPV's designated "Payment" wallet. The cash flows from the pool are now on-chain.
- **Obtaining Benchmark Rates (Benchmark Rate Oracle):** For floating-rate tranches linked to external benchmarks (e.g., 1M BBSW), the Waterfall Contract requires an independent, reliable data feed. This necessitates a **separate, dedicated Benchmark Rate Oracle**.
    - This oracle, likely provided by a specialised financial data firm, is responsible solely for sourcing the official benchmark rate (e.g., 1M BBSW set on the relevant determination date) from the verified off-chain source.
    - It securely pushes this rate onto the blockchain just before the Waterfall Contract needs it for coupon calculations.
    - Using an independent oracle for market data ensures accuracy, timeliness and avoids potential conflicts of interest compared to relying solely on the servicer oracle.

- **Automated Waterfall Distribution:** On the scheduled payment date (e.g., the 15th of the month), the *Waterfall Smart Contract™* executes automatically. It pulls all funds from the "Payment" wallet and reads the latest benchmark rate from the Benchmark Rate Oracle (if needed). It then distributes funds in a single, auditable transaction, strictly according to the priority defined in the Trust Deed:

    1. send(trustee.fee, trustee.wallet)
    2. send(servicer.fee, servicer.wallet)
    3. calculate_and_send(tranche_A1.coupon, tranche_A1.contract) *(using BBSW from oracle)*
    4. calculate_and_send(tranche_B.coupon, tranche_B.contract) *(using fixed rate)*
    5. send(principal.to.tranche_A1)
    6. send(residual.to.tranche_E) Investors receive their P&I payments instantly, rather than waiting days for a paying agent.

5.2 Handling Delinquencies and Default

The "oracle" system is also crucial for managing credit events.

- **Real-Time Monitoring:** The servicer's off-chain systems track delinquencies. When a loan is 30 days past due, the servicer-oracle updates the metadata of that specific "Mortgage NFT" to In Arrears == 'True'.
- **Automated Triggers:** The "Dashboard Contract" (from 3.2.3) reads this change instantly. The pool's 30+ day delinquency percentage is recalculated in real-time. If this percentage crosses a trigger level defined in the trust deed (e.g., 5%), it can automatically trigger pre-programmed actions, such as redirecting all principal payments to the senior noteholders or trapping all excess spread.
- **Loss Allocation:** In a default scenario where the property is sold, the servicer handles the off-chain legal process. If there is a shortfall (loss), the servicer "reports" this loss to the "Mortgage NFT" via the oracle. The "Waterfall Contract" then automatically allocates this loss to the first-loss (Equity) tranche, permanently writing down its value, all in a fully transparent manner.

5.3 Managing Cash and Bank Accounts On-Chain: Mitigating Sweeping Risk via Automated T+0 On-Ramping

While blockchain centralises the execution of the waterfall, traditional bank accounts still interface with the on-chain environment. This integration offers opportunities to significantly mitigate long-standing risks such as **servicer commingling and sweeping delay** through automated near-real-time processes.

- **The Core Risk: Servicer Commingling and Sweeping Delay**
    - **Commingling:** When a servicer collects SPV-owned mortgage payments into its own general corporate bank account, those funds are mixed ('commingled') with the servicer's own operational funds.
    - **Sweeping Delay (T+x):** Transaction documents typically require the servicer to identify SPV funds and 'sweep' (transfer) them to a dedicated SPV bank account within a specified timeframe (e.g., T+1 or T+2 business days).
    - **The Risk:** During this T+x period, if the servicer becomes insolvent, the SPV's funds held in the commingled account are at risk. The SPV ranks as an unsecured creditor for those funds, potentially facing significant delays and losses in recovering them. The longer the T+x period, the greater the exposure.
- **The Blockchain-Enabled Solution: Automated T+0 On-Ramping**

  The goal is to use technology to **identify SPV funds upon receipt** and immediately move them into the SPV's secure on-chain environment which effectively reducing the T+x sweeping delay to near T+0 (intra-day or near real-time).

  This requires deep integration between the servicer's off-chain banking and servicing platforms and the on-chain digital-asset infrastructure.
- **Technical Components and Granular Process Flow:**
    - **Step 1: Unique Payment Identification:**
        - **Mechanism:** Every mortgage payment must have a unique identifier linking it to the specific loan and corresponding "Mortgage NFT". In Australia, this could involve unique BPAY references, Direct Debit mandate IDs, or other embedded payment strings.
        - **Database Linkage:** The servicer's core system maintains a real-time map between payment identifiers and Loan ID / "Mortgage NFT" Token ID.
    - **Step 2: Real-Time Bank Account Monitoring (Off-Chain Agent):**
        - **Mechanism:** An automated software agent ("listener bot") runs off-chain, hosted securely by the servicer.

        - **Connectivity:** Connects to the servicer's collection bank account(s) via secure APIs (Open Banking, Direct Bank APIs or NPP Webhooks).
        - **Function:** Continuously monitors incoming transactions for payments linked to SPV-designated "Mortgage NFTs".
    - **Step 3: Automated Identification and Trigger:**
        - **Mechanism:** Upon detecting a matching payment, the agent parses the details (amount, identifier, timestamp).
        - **Validation:** Confirms the expected amount and valid ID.
        - **Trigger:** Initiates the on-ramping workflow upon validation.
    - **Step 4: Automated Fiat-to-Digital Asset Conversion (On-Ramp API):**
        - **Mechanism:** The agent makes an automated API call to a regulated digital-asset service provider (e.g., a licensed stablecoin issuer).
        - **Instruction Example:** "Receive AUD [amount] from Servicer Account [XYZ]; Mint/Issue equivalent [AUD-denominated stablecoin]; Credit Servicer's On-Ramp Wallet [0xABC...]."
        - **Funding:** Requires near-instant fiat settlement (e.g., via NPP) between the servicer's bank and the provider, or a pre-funded servicer account.
        - **Security:** Controlled API keys, rate limits and transaction thresholds are essential.
    - **Step 5: Automated On-Chain Transfer to SPV Wallet:**
        - **Mechanism:** Once the stablecoin is credited to the servicer's on-ramp wallet, the agent immediately initiates an on-chain transfer.
        - **Instruction:** Sends the digital-asset amount to the SPV's designated "Payment" wallet address (e.g., 0xSPV...).
        - **Execution:** Pays the network transaction fee ("gas") and broadcasts the transaction to finality.
    - **Step 6: Simultaneous Oracle Update (Optional but Recommended):**
        - **Mechanism:** Concurrently, the agent can act as (or signal) the **Servicer Oracle**.
        - **Instruction:** Updates the relevant "Mortgage NFT's" metadata (e.g., flagging payment received, updating Current Balance) via a

separate transaction or included data, ensuring near real-time asset-level synchronisation.

  - **Step 7: Automated Reconciliation:**
    - **Mechanism:** Continuous verification that fiat received = fiat converted = digital asset transferred.
    - **Exception Handling:** Automated alerts and manual intervention workflows manage discrepancies, failures, or flagged transactions.

- **Gas Fee Management via Batching:** Processing each individual payment separately on-chain could incur significant cumulative "gas" fees. To manage this, **batching** is essential. Identified SPV funds received by the servicer are aggregated over a defined short period before a single on-chain transfer (Steps 4 & 5) is initiated. The optimal frequency involves a trade-off:
  - **Intra-day Batching:** Minimizes the commingling risk window (near T+0) but incurs slightly higher gas costs.
  - **End-of-Day Batching**: Minimizes gas costs (one transaction per day) but leaves funds commingled for longer (up to one business day).

  The chosen frequency depends on balancing risk mitigation against cost on the selected platform, subject to rating agency acceptance.

  Batching intervals should be codified in the Servicing Agreement to ensure operational predictability for auditors and rating agencies.

- **Benefits and Operational Requirements:**
  - **Benefits:**
    - Compresses the commingling/sweeping-risk window from days (T+x) to minutes or seconds (near T+0).
    - Increases transparency, traceability and auditability of every cash movement.
    - Strengthens investor confidence by isolating SPV funds on-chain rapidly.
  - **Requirements:**
    - Deep integration between the servicer's banking, core servicing system and digital asset infrastructure (APIs, wallets, blockchain nodes).

    - Use of a reliable, regulated and liquid on-chain digital asset (e.g., a well-backed AUD stablecoin or tokenised deposit).
    - Robust security, monitoring, reconciliation and exception handling for the entire automated workflow.
    - Validation and technical assessment by rating agencies to ensure the operational and cyber-resilience of the system.

- **Regulatory and Fiduciary Compliance Overlay:** Any entity performing fiat-to-token conversion or managing wallets on behalf of an SPV would likely qualify as a **designated service provider** under the **Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth)**.

  Accordingly, such entities must:

  - Register with **AUSTRAC**;
  - Maintain AML/CTF programs, KYC processes and ongoing transaction monitoring; and
  - Report suspicious matters, threshold transactions and international funds transfers.

  In addition, the SPV trustee retains **fiduciary responsibility** for oversight of these automated processes. Smart-contract or API-driven execution does not displace trustee accountability; it enhances auditability and control within the existing trust-law framework.

This granular, automated on-ramping process materially upgrades the management of servicer sweeping risk, replacing manual batch processes with near real-time, technology-driven settlement directly into the SPV's secure on-chain environment while remaining fully aligned with AML/CTF obligations and rating-agency standards.

5.4 Integrating Off-Chain Agreements (e.g., Swaps)

Securitisation structures often involve external agreements like interest rate swaps. These remain primarily off-chain legal contracts but require careful integration with the on-chain cash flow mechanics.

- **Governing Off-Chain Contract:** The swap agreement (e.g., ISDA Master Agreement) remains the **paramount legal document** defining terms, calculations and counterparty obligations. This is not replaced by blockchain.
- **On-Chain Payment Integration:**
  - **Swap Receipts:** Payments due *to* the SPV from the swap counterparty must be received (likely into a designated account) and then "on-ramped"

(e.g., as stablecoin) into the SPV's on-chain "Payment" wallet before the waterfall execution.

  - **Swap Payments:** The Waterfall Smart Contract is programmed to send payments *from* the SPV *to* the swap counterparty (e.g., in stablecoin to their designated wallet) at the appropriate priority level within the automated distribution.

- **Oracles for Swap Data:** Depending on complexity, an oracle might be needed to provide specific calculation inputs (beyond standard benchmark rates) required under the swap agreement to the Waterfall Contract.
- **Counterparty Risk Management (Off-Chain Driven):** Triggers related to the swap counterparty's rating downgrade (requiring collateral posting, replacement, termination) are defined and governed by the **off-chain ISDA agreement**. While an oracle could *signal* a downgrade on-chain, the enforcement of remedies remains an off-chain legal process managed by the Trustee according to the swap contract. The smart contract executes payment flows but does not autonomously enforce complex legal remedies from external contracts.

5.5 The Evolving Role of Trustees and Custodians

In this on-chain world, the roles of intermediaries do not disappear, but they evolve significantly.

- **Trustee:** The trustee (e.g., a firm like Perpetual or Equity Trustees) shifts from being a *processor* of information to a *supervisor* of the system. Their role is to audit the smart contracts *before* launch to ensure they perfectly match the Trust Deed. Post-launch, they act as the ultimate "administrator" with special permissions (e.g., the ability to pause the waterfall contract, authorise oracle changes, manage admin keys), protecting the interests of noteholders.
- **Custodian:** The role of the traditional custodian (e.g., Austraclear) for the notes themselves is diminished, as investors can self-custody their security tokens in their own digital wallets. However, a new class of **digital asset custodian** emerges for institutional investors who do not wish to manage their own keys, providing insured, regulated "wallet-as-a-service."

5.6 Regulatory Audit Interface

The blockchain architecture must produce artefacts that can be inspected and verified by regulators and rating agencies without requiring direct interaction with smart-contract code.

Each *Waterfall Smart Contract™* instance generates a deterministic event log of all transactions, distributions, and parameter changes. These events are exported in real-time to an **off-chain reporting API** that transforms the data into machine-readable formats (JSON, CSV, and XBRL). The feed aligns with APRA's Data Modernisation Program and can populate existing ARF 720.1/721 templates used for securitisation trust reporting.

The interface also provides an audit trail for external reviewers. Each data snapshot includes block-hash references and digital signatures, allowing an independent auditor or APRA examiner to reconcile every reported figure back to an immutable on-chain event.

This "regtech bridge" ensures that on-chain automation enhances, rather than bypasses, established oversight. The design objective is simple: regulators should be able to verify trust performance using their existing analytical tools - without ever touching a private key.

5.7 Trustee Node Governance

The on-chain architecture does not replace the fiduciary role of the trustee; it operationalises it. The trustee operates a **read-write validator node** within a permissioned ledger, retaining full oversight but delegating no discretionary authority to code.

All smart-contract upgrade or pause functions are administered through a **multi-signature ("multi-sig") governance wallet**, with keys distributed among the trustee, the originator and an independent auditor. Any contract amendment, bug-fix deployment or emergency intervention requires a two-of-three consensus.

Governance policies are codified in the **Master Trust Deed**, ensuring that fiduciary control under Australian trust law remains paramount. The node's operational responsibilities fall within **CPS 231 Outsourcing** and **CPS 234 Information Security**, requiring the trustee to maintain adequate due-diligence, cybersecurity, and business-continuity frameworks for its technical environment.

This structure achieves functional automation while preserving legal accountability — the core principle of a *Smart SPV™* rather than a trustless one.

6.0 Phase 5: Redemption and Maturity

The final phase of the RMBS lifecycle is the return of principal to investors and the orderly winding up of the trust. Blockchain and smart contracts ensure this process is as transparent and automated as the rest of the deal.

6.1 Automated Principal Repayment

- **6.1.1 Handling Prepayments and Pass-Through Logic:** As borrowers sell their homes or refinance, the servicer's off-chain system receives these principal prepayments. The servicer-oracle (from Phase 5) reports this to the "Waterfall Contract." The contract automatically identifies these funds as principal and, during the next payment distribution, "passes them through" to the noteholders according to the payment priority (e.g., sequential paydown of the Note A1 tokens). This is far more efficient than the traditional monthly batching process.

- **6.1.2 Smart Contracts for Final Maturity:** When the final loan in the pool is repaid, the Waterfall Contract receives the last payment from the servicer. It executes its final distribution, paying the last of the principal and interest to all noteholders. The on-chain "outstanding balance" of all security tokens is now zero.

6.2 Automated "Clean-Up Calls" and Optional Redemption

Most Australian RMBS trusts include a "Clean-Up Call" option, allowing the originator to repurchase the remaining mortgages when the pool amortises below (typically) 10% of its original balance.

- **On-Chain Monitoring:** A smart contract can constantly monitor the pool's balance: if (current.pool.balance < 0.10 * original.pool.balance) { trigger(call.option) = 'True' }

- **Exercising the Call:** This trigger makes the "Call Option" (which itself could be a token) exercisable. The originator (or call holder) can then send the full repurchase price (the outstanding balance of all notes) to the Waterfall Contract.

- **Final Payout:** The Waterfall Contract receives this large payment, automatically distributes the full principal and final coupon to all noteholders and simultaneously transfers the remaining "Mortgage NFTs" from the SPV wallet back to the originator's wallet.

6.3 Token "Burning" and Final Discharge of the Smart SPV

Once all noteholders have been paid in full and the outstanding principal of their tokens is zero, the liabilities of the trust are fully discharged.

- **Token "Burning":** To finalise the process, the security tokens are "burned" by being sent to a provably unrecoverable address (e.g., 0x000...). This creates an immutable, on-chain cryptographic record that the financial instrument no longer exists and its liabilities are extinguished.
- **Winding Up the Trust:** The on-chain SPV wallet now holds no "Mortgage NFTs" (assets) and has no corresponding security tokens in circulation (liabilities). The trust is an empty shell. The trustee can then perform the final off-chain legal steps to wind up the trust, with a perfect, auditable and immutable on-chain record of the entire deal from cradle to grave.

7.0 Key Framework Features: Transparency, Liquidity and Compliance

The "golden source" of truth established on the blockchain eliminates information asymmetry and creates the foundation for a truly liquid, compliant secondary market.

7.1 Radical Transparency: The Immutable Audit Trail

In the current Australian market, investors and regulators rely on static, backward-looking (monthly) PDF reports prepared by the servicer or trustee. A blockchain-native RMBS replaces this with a live, dynamic and non-discretionary reporting framework.

7.1.1 Real-Time, Asset-Level Reporting

Any permissioned party (e.g., an investor holding a Note A1 token, or a regulator like ASIC/RBA) can be given "read-access" to the SPV's on-chain data. They can query the pool 24/7 and see:

- The current W.A. LVR of the pool, based on the latest oracle-fed data.
- The precise number of "Mortgage NFTs" in 30+, 60+ and 90+ day arrears *at that exact moment*.
- The total outstanding principal balance of the pool, accurate to the last dollar.

This moves the market from a "Trust, then Verify" model to a "Don't Trust, Just Verify" model.

This level of asset-specific transparency, however, must be carefully balanced with borrower privacy obligations under the *Privacy Act 1988 (Cth)*. While on-chain data is anonymised (e.g., no borrower names), the combination of specific metadata fields like Property Postcode, Origination Date and Loan Type could create a **re-identification risk** for a specific loan.

Therefore, the "radical transparency" must be **permissioned**. A superior model would use a **'layered-access' data approach**:

1. **Public/Investor-Level Access:** This layer provides *aggregated* pool-level data only. This is the output of the "Dashboard Contract", showing the real-time W.A. LVR, total arrears percentages and geographic concentration by state, but not loan-by-loan data.
2. **Permissioned/Fiduciary-Level Access:** Only highly-trusted, permissioned parties (specifically the **Trustee** and **Regulators** like ASIC/RBA) are granted 'read-access' to the specific, loan-by-loan "Mortgage NFT" metadata.

3. **Data Obfuscation:** For any metadata that is made more broadly visible, sensitive fields like Property Postcode should be replaced with a less granular field (e.g., 'Statistical Area 4' or 'State') to further mitigate privacy risks while still providing useful data for credit analysis.

7.1.2 Verifiable Proof of Collateral

A primary risk in complex finance is the "double-pledging" or re-hypothecation of collateral. On-chain, this is impossible. Any party can cryptographically verify that the 1,000 "Mortgage NFTs" representing the collateral pool are sitting in the SPV's wallet and have not been moved, pledged, or otherwise encumbered.

7.1.3 Automated Regulatory Reporting (RegTech)

This has significant implications for compliance. Regulators like ASIC and the RBA could be given a dedicated "node" with read-only access. Instead of issuers manually compiling and submitting securitisation reporting data, the regulator could pull live, standardised data directly from the source, drastically reducing the compliance burden on issuers.

7.2 Secondary Market Liquidity

The Australian RMBS secondary market is notoriously illiquid, operating on an Over-The-Counter (OTC) basis with T+2 settlement via *Austraclear*. Tokenisation fundamentally rewires this market.

7.2.1 Trading Security Tokens: AMMs vs. Order Books

Regulated security tokens would trade on-chain via licensed platforms, which could take two forms:

- **Permissioned DEX (Order Book):** A familiar order book model, similar to the ASX, but running on-chain.
- Permissioned AMM (Liquidity Pool): An "Automated Market Maker" pool where investors can deposit their RMBS tokens (e.g., Note A1) and a stablecoin into a pool to provide constant liquidity for other traders.

Both models would be "permissioned," meaning only whitelisted, KYC-verified investors could interact with them.

7.2.2 Always Open 24/7/365 Markets and Instantaneous Settlement

These on-chain markets never close. An institutional investor in Sydney can sell a position to a "wholesale client" in another jurisdiction at any time, day or night. As discussed in Phase 3, the settlement is **atomic (DvP)**. The swap of tokens for stablecoins happens in a single transaction, eliminating the T+2 counterparty risk that exists in the *Austraclear* system.

7.2.3 Compliance in Secondary Trades

This is the most critical element. Compliance is not left to a back-office administrator; it is enforced by the token's smart contract.

- An investor attempts to sell their "Note B" token on the DEX.
- The "Note B" smart contract automatically checks: is(buyer.wallet) on (the 'whitelist')?
- If the buyer is not a verified wholesale client, the contract reverts the transaction. The trade simply cannot happen.

This automates compliance with Australia's wholesale investor regime (s 761G of the *Corporations Act*) at the protocol level.

7.3 Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF) and Digital Identity Integration

The on-chain RMBS framework operates entirely within the scope of Australia's existing AML/CTF regime and does not exempt any participant from its reporting obligations. All entities engaging in the origination, issuance, servicing or funding of securitised exposures remain **"reporting entities"** under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth)* and must comply with ongoing obligations to verify identity, report suspicious matters, and maintain transaction records.

The blockchain layer enhances, rather than replaces, the verification process. Each participating institution - originator, trustee, investor, warehouse funder and liquidity provider - interacts with the permissioned ledger through **verified digital identities** issued and attested by AUSTRAC-registered reporting entities. These digital credentials act as cryptographic attestations of KYC completion, rather than as anonymous blockchain addresses.

Identity attestations are anchored to the ledger using hash-based proofs. The underlying customer information remains off-chain within the secure systems of the originating reporting entity, ensuring compliance with the *Privacy Act 1988 (Cth)* and APRA's *CPS 234 Information Security* standard.

The on-chain record therefore functions as a **regtech evidence layer**: it confirms that AML and CTF checks were performed without disclosing personally identifiable data to other participants.

T+0 Settlement and AML Sequencing

Instantaneous or *T+0 On-Ramping™* settlement refers only to **post-KYC cleared funds**. Investor onboarding, subscription payments and beneficial interest allocations occur only once identity verification and source-of-funds checks have been completed through standard institutional onboarding channels. Once verified, each wallet address is whitelisted within the permissioned network, allowing atomic transfer of digital securities and payment tokens between KYC-cleared counterparties.

This sequencing preserves all AML/CTF controls while enabling near-instant settlement within the regulated perimeter.

The approach can be summarised as:

1. **Off-chain:** KYC/AML verification by reporting entity (originator, funder, or trustee).
2. **On-chain:** Attestation of verification status (hash proof + timestamp).
3. **Execution:** T+0 transfer and settlement between whitelisted, verified wallets.

This design ensures that the RMBS blockchain serves as an **audit-enhancing infrastructure**, not a parallel financial system. Every on-chain transaction remains traceable to a fully identified, institutionally verified counterparty.

Regulatory Alignment

This model aligns with:

- AUSTRAC's *Digital Identity Policy Principles (2022)* and *Reporting Entity Guidance Note 13 (Digital ID use in AML programs)*.
- APRA's *CPS 231 (Outsourcing)* and *CPS 234 (Information Security)* standards for data integrity.
- The *Corporations Act 2001* provisions on investor suitability and anti-fraud measures for managed investment products.

By retaining the existing AML/CTF control environment while automating the evidence trail, the framework transforms compliance from a static reporting exercise into a continuous assurance mechanism.

In this respect, it advances the supervisory objectives of both AUSTRAC and APRA: transparency, traceability, and accountability—executed at the speed of modern capital markets.

8.0 Key Challenges and Considerations

While the efficiency and transparency gains are compelling, transitioning the multi-trillion dollar Australian RMBS market to a new infrastructure is fraught with significant challenges. These hurdles are not merely technical but deeply legal, regulatory and commercial.

8.1 Legal and Regulatory Uncertainty

Australian regulators, including ASIC, maintain a "technology-neutral" stance: a financial product is regulated as such, regardless of its underlying technology. However, the *application* of legacy law to this new model creates critical ambiguities.

8.1.1 Enforceability of Smart Contracts

A smart contract is "self-executing" code, whereas a traditional trust deed is a legal document subject to court interpretation. The central challenge arises if there is a bug in the code. "Code is law" is not a valid legal defence in Australia. The legal framework must be explicit: the **off-chain legal trust deed is the paramount source of truth** and the smart contract is merely a **tool** for its execution.

A clear legal mechanism is needed for pausing, amending, or overriding a faulty smart contract, which must be legally vested with the trustee. This legal supremacy must be backed by a robust technical implementation. The smart contracts (particularly the "Waterfall Contract") should be built with explicit, audited 'administrator' functions, such as:

- A pause() function to immediately halt all distributions in an emergency (e.g., a detected oracle failure or exploit).
- An upgrade() function to replace the contract's logic with a new, audited version to correct a bug or comply with a court order.

Critically, these administrative functions should not be controlled by a single private key. They should be controlled by a **multi-signature ("multi-sig") wallet**. The off-chain Trust Deed would legally define the key-holding structure, designating the **Trustee as the primary and decisive keyholder**, reflecting their fiduciary duty. Other parties, such as the servicer or a dedicated security auditor, could be assigned secondary keys. This multi-sig mechanism ensures that no single party (not even the Trustee) can act unilaterally, providing a secure, auditable and legally-grounded 'kill switch' and 'upgrade path' that is governed by the trust's legal documents.

8.1.2 Trustee Liability

This new model places an enormous and novel burden on the trustee. They must now supervise not just cash flows, but the integrity of the smart contract code itself. This raises new questions of liability. Are trustees liable for losses from a code exploit in an audited smart contract? This will require a new class of professional indemnity insurance and a new industry standard for "trustee-grade" smart contract audits.

8.1.3 PPSA Perfection for Tokenised Assets

The **Personal Property Securities Act 2009 (Cth)** (PPSA) is the bedrock of securitisation, governing how security interests are *perfected,* that is, made enforceable against third parties and given priority in insolvency.

The Act, however, was never designed for **digital assets**. It remains unclear how a lender or warehouse provider perfects a security interest over a "Mortgage NFT" or "Note Token." Does perfection occur through *control* (analogous to an ADI account), or does it require *registration* on the **Personal Property Securities Register (PPSR)**?

As of **October 2025**, the **Treasury's PPSA Review** is ongoing and is considering whether tokenised financial instruments and digital assets require new collateral classes or specific perfection mechanisms. Clear statutory guidance will be essential before such instruments can function as mainstream collateral in structured-finance transactions.

Interim Best Practice: The "Belt and Braces" Model

Pending reform, the most conservative and legally robust approach for a lender (e.g., a warehouse provider) is to adopt a **dual-layer perfection strategy** to ensure enforceability:

- **Perfection by Registration (PPSR):** The lender should register a security interest on the PPSR.

  The "Mortgage NFT" or "Note Token" would likely be classified as a **general intangible** under the current PPSA framework.

  The collateral description must be precise - referencing:

    - the asset's unique on-chain identifier (token ID and contract address); and
    - the off-chain **Token Deed** or equivalent legal wrapper that gives the token its substantive legal character.

- **Perfection by Control:** Concurrently, the lender should demonstrate *control* by holding or supervising custody of the tokenised asset within a digital wallet that it controls directly or through a secure **multi-signature arrangement**. In practice, "control" equates to the **cryptographic ability to transfer or restrict transfer** of the asset, analogous to the concept of control for ADI accounts under existing PPSA regulations.

This **dual-layer approach** provides the strongest possible claim in an insolvency scenario, offering redundancy across both statutory and operational dimensions.

Long-Term Policy Direction

Over the longer term, Australia's legal framework should evolve to **explicitly recognise tokenised assets as a new form of "financial property."** Under such a regime, **perfection by control** - defined as the cryptographic power to transfer the digital asset - could be deemed sufficient under prospective reforms aligning with emerging international models. This direction is reinforced by APRA's concurrent prudential-data-modernisation program, which explicitly anticipates digital-native asset evidencing.

This reform would align Australia with emerging international approaches (such as Singapore's and the EU's proposed digital-asset collateral regimes) and remove the operational friction of PPSR registration for digitally native assets used in securitisation structures.

8.2 Technical Challenges

8.2.1 Public vs. Permissioned Blockchains

A public, "permissionless" blockchain like Ethereum offers immense transparency but suffers from high/volatile transaction fees ("gas") and slower throughput, making it unviable for institutional RMBS. Permissioned or consortium-governed distributed-ledger platforms such as Hyperledger Fabric or R3 Corda which deliver speed, privacy and cost predictability by limiting validators to approved institutions. While this structure reintroduces elements of central governance, a multi-institution consortium model can preserve decentralisation of trust without full public exposure.

8.2.2 Operational Dependence on Oracles

The system is only as good as its data inputs. The entire automated waterfall and reporting system (Phases 5 & 6) is completely dependent on trusted "oracles" (e.g., the servicer, a valuation provider) to push accurate off-chain data (payments, arrears, property values) on-chain. This does not remove counterparty risk; it *concentrates* it on the oracle. A compromised or faulty oracle could cause catastrophic failures in the automated logic.

8.2.3 Private Key Security and Custody Risk

While this framework diminishes traditional custody risk via CSDs, it introduces a new, highly concentrated operational risk: **private key security**. The entire system's integrity rests on the secure generation, storage and management of the cryptographic private keys associated with critical wallets:

- The SPV's Asset Wallet: This wallet holds all 1,000+ "Mortgage NFTs". If its private key is compromised, a malicious actor could steal the entire collateral pool in a single transaction.

- The Trustee's Admin Keys: These keys control the multi-sig wallet with the power to pause or upgrade the core smart contracts. If these keys are lost, stolen, or mismanaged, the Trustee's ability to perform its fiduciary duty is nullified.

This necessitates a new institutional-grade standard for "digital asset custody," likely involving regulated, insured, third-party custodians who use multi-party computation (MPC) or hardware security modules (HSMs). Rating agencies will conduct deep due diligence on these custody arrangements, as they represent one of the most critical new points of failure in the on-chain model.

8.2.4 Lack of a Scaled, Regulated AUD Settlement Asset

This remains one of the most significant practical hurdles to implementing the framework at scale. While atomic settlement (DvP) is a key benefit, it requires a high-integrity, liquid and regulatorily sound on-chain version of the Australian Dollar.

8.2.4.1 Why AUD is Crucial

Using a native **AUD digital settlement asset** (like a regulated AUD stablecoin, a future wholesale CBDC, or tokenised bank deposits) is practically essential. Australian mortgages generate AUD cash flows, borrowers pay in AUD and Australian RMBS investors require returns in AUD. Introducing non-AUD stablecoins (e.g., USDC) would create significant **FX risk and basis risk** unless complex, costly and operationally burdensome hedging mechanisms were integrated throughout the entire lifecycle (on-ramping, waterfall distribution, secondary trading). This complexity would negate many efficiency gains and likely deter Australia's primarily AUD-focused institutional investors. Regulatory alignment also points strongly towards AUD settlement, as evidenced by the RBA's focus in Project Acacia.

8.2.4.2 Current AUD Stablecoin Landscape

The market is nascent but developing. Major banks like **ANZ (A$DC)** and **NAB (AUDN)** have launched their own AUD stablecoins, pegged 1:1 to the AUD and backed by reserves. These have been successfully used in pilots for specific institutional use cases like carbon credit trading, remittances and repo transactions. However, as of late 2025, neither A$DC nor AUDN (nor any other private AUD stablecoin) has achieved the **scale, widespread market adoption, or established infrastructure** necessary to reliably handle the *billions* of dollars in daily settlement flows typical of the primary and secondary RMBS market. They remain largely within pilot phases or closed ecosystems.

8.2.4.3 Stablecoin Regulation

The Australian Government is in the process of establishing a dedicated regulatory framework for **payment stablecoins** under the **Payment Systems (Regulation) Act 1998 (Cth)**. Treasury's consultation paper *"Regulating Digital Assets and Stablecoins"* closed in **August 2025**, with draft legislation expected in **Q1 2026**.

The framework is expected to introduce requirements for reserve backing, segregation of client funds, operational resilience and licensing of stablecoin issuers under the **Australian Financial Services Licence (AFSL)** regime. Once enacted, this would enable the development of **fully regulated AUD stablecoins** suitable for use as settlement assets in institutional markets such as securitisation.

8.2.4.4 RBA's Role (Project Acacia)

The RBA's ongoing **Project Acacia** is directly exploring and testing various digital AUD settlement solutions, including wholesale CBDC, tokenised deposits and stablecoins, specifically for tokenised asset markets. Its findings (expected early 2026) will be crucial in determining the viable paths forward for institutional digital AUD settlement.

8.2.4.5 Near-Term Reality

Until a scalable, regulated digital AUD rail is established (whether via licensed stablecoins, wCBDC, or tokenised deposits), on-chain RMBS transactions requiring settlement will likely retain an off-chain fiat leg (e.g., using NPP or RITS), reintroducing some settlement risk and delays and limiting the full benefits of atomic DvP.

8.2.5 Implications for Foreign Currency (FX) Tranches and Cross-Currency Swaps

8.2.5.1 Standard Practice

Australian RMBS deals sometimes include tranches denominated in foreign currencies (e.g., USD, EUR) to attract international investors. Often, these structures incorporate **cross-currency swaps** to hedge the FX risk between the AUD assets and the FX liabilities. The SPV typically receives AUD from the underlying assets, pays AUD to the swap counterparty and receives the required FX amount (e.g., USD) from the swap counterparty to pay the FX tranche investors.

8.2.5.2 Governing Off-Chain Contracts

Both the FX tranche notes and the associated cross-currency swap agreement (e.g., ISDA Master Agreement) remain traditional, **off-chain legal documents**.

8.2.5.3 On-Chain Integration Options

a) **Option 1 (FX Stablecoin Settlement):** If settling the FX tranche directly with an FX stablecoin (e.g., USDC), the process involves:
   - The Waterfall Smart Contract calculates the AUD due to the swap counterparty.
   - The contract pays the swap counterparty in AUD stablecoin (to their designated wallet).

    - The swap counterparty (off-chain or via their own on-chain mechanism) delivers the required FX stablecoin amount (e.g., USDC) into the SPV's designated FX stablecoin wallet.
    - The Waterfall Contract then distributes this FX stablecoin to the FX tranche investors' wallets.
    - This requires managing multiple stablecoin types and relies on the swap counterparty's timely on-chain FX stablecoin delivery.

b) **Option 2 (Off-Chain FX Settlement - More Likely Near-Term):** This integrates the swap payment *before* final off-chain FX conversion:
    - The Waterfall Smart Contract calculates the AUD due *to* the swap counterparty.
    - The contract sends this AUD amount (in AUD stablecoin) to the swap counterparty's designated wallet.
    - Simultaneously (or as per the swap agreement timing), the swap counterparty makes the required FX payment (e.g., USD) **off-chain** to the Trustee or Paying Agent responsible for the FX tranche.
    - An **FX Rate Oracle**, providing reliable, real-time FX rates, might still be needed by the smart contract or Trustee for reporting, valuation, or potentially verifying the *expected* AUD equivalent flowing through the swap.
    - The Paying Agent then makes the final payment to the investors in their required currency (e.g., USD via SWIFT) through traditional channels.

8.2.5.4 Counterparty Risk Management

As with interest rate swaps, triggers related to the cross-currency swap counterparty's rating downgrade (requiring collateral, replacement, termination) are defined and governed by the **off-chain ISDA agreement**. The Trustee manages the enforcement of these remedies off-chain, potentially informed by on-chain oracle data regarding downgrades.

8.3 Interoperability and Adoption

- **Bridging Legacy Systems:** A blockchain solution cannot exist in a vacuum. It must integrate with Australia's existing, entrenched financial infrastructure: **PEXA** for property title, the **RITS/NPP** for fiat payments and the servicers' internal loan management systems. These integrations are complex and costly.

- **Market Acceptance:** The Australian securitisation market is mature and conservative. Issuers, investors (especially superannuation funds) and rating agencies (S&P, Moody's) must be convinced of the model's robustness. Rating agencies, in particular, will need to develop new frameworks to assess the *operational risk* of smart contracts and oracles.

- **Industry Standards:** The **Australian Securitisation Forum (ASF)** will need to play a pivotal role in developing industry standards for data, token formats and smart contract logic to prevent a fragmented market of walled-garden solutions.

9.0 Blockchain Platform Selection: Managing Costs and Scalability

A fundamental structural decision for any blockchain-based securitisation is the choice of the underlying DLT platform. This choice significantly impacts transaction costs (particularly "gas" fees), scalability, security, governance and regulatory perception, directly influencing the economic viability discussed in Section 13.0.

9.1 Understanding "Gas" Fees

Many blockchain networks, especially public permissionless ones like Ethereum mainnet, require users to pay a transaction fee, commonly known as "gas". This fee compensates network validators for the computational resources used to process and secure transactions. Gas fees can be volatile, fluctuating based on network congestion. For a high-volume process like RMBS servicing, involving potentially thousands of daily payment acknowledgements or frequent oracle updates, unpredictable or high cumulative gas fees on certain platforms could render the on-chain model uneconomical.

9.2 Platform Options and Cost Implications

The primary structural approach to managing these costs involves selecting an appropriate platform:

- **Public Layer 1 Blockchains (e.g., Ethereum Mainnet):** Generally unsuitable for the high-frequency, low-value transactions typical of RMBS servicing due to potentially high and volatile gas fees. While offering maximum decentralisation, the cost unpredictability poses significant operational risk.
- **Permissioned/Private Blockchains (e.g., Hyperledger Fabric, R3 Corda, Provenance.io):** These enterprise-focused platforms are strongly preferred for institutional use cases like securitisation. They offer several advantages:
    - **Controlled Cost Structures:** Transaction fees ("gas") are often minimal, fixed, predictable, or managed via consortium funding rather than market-based auctions. This allows for reliable cost forecasting.
    - **Scalability and Throughput:** Typically designed for higher transaction volumes than public Layer 1s.
    - **Privacy and Governance:** Allow control over who can participate, validate transactions and view data, aligning better with regulatory and commercial requirements.

- **Layer 2 Scaling Solutions (e.g., Polygon PoS, Arbitrum, Optimism):** These operate on top of public blockchains (like Ethereum) to provide significantly lower transaction fees and faster processing. They achieve this by processing transactions off-chain or in batches before settling them more efficiently on the main Layer 1. Layer 2s represent a potential compromise, offering lower costs than Layer 1 while retaining some interoperability with the broader public blockchain ecosystem, though they introduce their own technical complexities and potential centralisation points.
- **"Zero Gas Fee" Blockchains:** Some public networks advertise very low or zero fees, but these models require careful scrutiny regarding their security assumptions, degree of decentralisation and long-term economic sustainability, which may not meet the robustness requirements for critical financial infrastructure.

9.3 Optimisation Strategies

Regardless of the platform, minimizing on-chain transaction volume remains crucial:

- **Batching:** As detailed in Section 5.3, aggregating multiple off-chain events (like payment receipts) into single, periodic on-chain transactions is the primary method for reducing overall transaction count and associated costs.
- **Efficient Smart Contract Design:** Optimizing code to minimize computational complexity directly reduces the resources (and thus cost) required for execution.

9.4 Confidentiality and Competitive Concerns

Beyond technical and cost factors, the *governance and ownership* of the chosen blockchain platform raise strategic considerations, particularly if leveraging platforms developed by potential competitors.

- **Using Competitor Infrastructure:** Platforms like Provenance.io, developed by Figure Technologies, offer a purpose-built, proven infrastructure. However, an Australian issuer using such a platform must consider the implications of operating core infrastructure owned or heavily influenced by another market participant (and potential competitor).
- **Data Privacy and Confidentiality:** While blockchain transactions can be cryptographically secured and permissioned layers can restrict data access, concerns may arise regarding:
    - **Metadata Visibility:** Even if transaction contents are private, the pattern, volume and timing of transactions (metadata) on a shared ledger could potentially reveal strategic business information to the platform operator or other participants.

    - **Platform Operator Access:** Understanding the level of access the platform owner/operator (e.g., Figure in the case of Provenance) retains to the underlying infrastructure and potentially aggregated, anonymised data is crucial.
    - **Future Strategy Alignment:** Reliance on a competitor's platform introduces dependency risk. Future platform upgrades, changes in fee structures, or shifts in the owner's strategic direction could impact the issuer's operations.
- **Mitigation:** These concerns might favour the use of:
    - **Neutral Consortia Chains:** Platforms governed by a consortium of industry participants rather than a single dominant entity.
    - **In-House or Private Deployments:** For maximum control, though potentially at higher cost and complexity.
    - **Strong Legal and Governance Frameworks:** Clear contractual agreements defining data access rights, privacy obligations and operational service levels with the platform provider.

The choice of platform therefore involves not just technical suitability but also a careful assessment of the competitive landscape and the long-term strategic implications of infrastructure dependencies.

10.0 Analysis against Prudential Standard APS 120

For any Australian Authorised Deposit-taking Institution (ADI), compliance with **Prudential Standard APS 120 Securitisation** (APS 120) is non-negotiable. The standard applies broadly to **all roles an ADI may undertake** in a securitisation, including acting as an **originator**, an **investor** in the RMBS notes, or a **funder** providing warehouse facilities, liquidity or credit enhancements. It governs how ADIs manage these "securitisation exposures" and their associated capital requirements.

A common misconception is that a blockchain-based structure would be incompatible with these prudential rules. However, the "dual-layer" hybrid model proposed in this paper is specifically designed to comply with APS 120 by maintaining the **economic substance** and **legal separateness** of a traditional deal, while using blockchain as a superior execution and reporting layer.

The 2023 revision of APS 120, para 25(b), explicitly recognises that “beneficial interests may be evidenced or recorded in digital or electronic form.” This recognition provides clear regulatory latitude for tokenised structures in which the beneficial interests in an SPV’s assets are represented by digitally recorded instruments - such as the ‘Mortgage NFTs’ and security tokens described in this paper - without altering their legal substance.

Accordingly, the proposed on-chain RMBS framework is consistent with APS 120’s core requirements that (i) the SPV hold legal title to the securitised exposures and (ii) investors hold clearly defined, enforceable beneficial interests in those exposures. The blockchain layer functions purely as the evidentiary and operational medium through which those interests are recorded and administered, fully preserving the economic and legal separateness that APS 120 mandates.

The framework's compliance is best analysed against the core principles of APS 120 (with the following sections focusing on the originator role, which presents the most complex compliance hurdles):

10.1 Legal Isolation and "True Sale" (Para 17)

- **APS 120 Requirement:** An originating ADI must obtain a legal opinion confirming the securitised assets are "legally isolated... beyond the reach of the ADI and its creditors". This is the "true sale" test.
- **Framework Compliance:** This is the central tenet of the paper's "dual-layer" model. The true sale is *not* effected by the on-chain token transfer. Instead, it is legally perfected by the traditional, off-chain **Master Sale Agreement** and the **Token Deed**, which irrevocably binds the beneficial interest to the "Mortgage NFT". The on-chain transfer is the *immutable record and technical settlement* of this off-

chain legal sale. This structure is explicitly designed to satisfy the legal opinion requirement for legal isolation.

10.2 Prohibition on Implicit Support (Paras 13, 69)

- **APS 120 Requirement:** An ADI must *not* provide "implicit support" to a securitisation beyond its explicit, documented contractual obligations. Its undertakings must be "fixed as to time and amount".
- **Framework Compliance:** The proposed framework arguably provides a *stronger* guard against implicit support than traditional structures.
    - **Automated Enforcement:** The "Waterfall Smart Contract" is a non-discretionary, self-executing agent. It *cannot* be influenced by the ADI to make discretionary payments to support a tranche or cover unexpected losses. It will only execute the exact logic of the Trust Deed.
    - **Trustee Control:** The paper's model vests critical administrative functions (like pause() or upgrade()) in a multi-sig wallet controlled by the **Trustee**, not the ADI-originator. This prevents the ADI from using a contract "bug" or upgrade as a vehicle for providing implicit support.

10.3 Capital Relief vs. Funding-Only (Attachments A & B)

- **APS 120 Requirement:** An originating ADI must designate the deal at inception. To achieve **regulatory capital relief**, it must demonstrate "significant credit risk transfer" (SCRT). Unlike US or EU rules that *mandate* 5% risk retention ("skin in the game"), APS 120's logic is the opposite: to get capital relief, the ADI must *transfer* the risk, not retain it. The standard imposes a *ceiling* on retention, stating an ADI *cannot* hold more than 20% of the non-senior securities.
- **Framework Compliance:** The blockchain framework is agnostic and supports both designations, while making compliance fully auditable.
    - **Enabling Capital Relief (Att. A):** The STO process allows the ADI to sell 100% of all non-senior tranches (e.g., the "Token E" equity tranche) to whitelisted third-party investors. This is the most effective way to prove SCRT. The public, immutable ledger provides a perfect audit trail to APRA, proving the ADI is no longer exposed to the first loss.
    - **Enabling Funding-Only (Att. B):** Alternatively, if the ADI *chooses* to keep its "skin in the game" by retaining the "Token E" tranche, this retention is transparent on-chain. This would clearly fail the SCRT test, correctly defaulting the deal to "funding-only" status, which requires the ADI to keep the assets on its balance sheet for capital purposes.

10.4 Separation and Control (Paras 16, 19, Att. D)

- **APS 120 Requirement:** The ADI must not control the SPV, act as trustee, or "maintain effective or indirect control" over the transferred assets.
- **Framework Compliance:**
    - **SPV Structure:** The paper's "Smart SPV" is legally a traditional Australian trust with an independent, professional trustee, satisfying the requirement that the ADI not be the trustee.
    - **Servicer Role:** The ADI's role as servicer and oracle-provider could be seen as "effective control". However, footnote 9 of APS 120 explicitly states that servicing *does not* constitute control, provided it complies with Attachment D.
    - **Attachment D Compliance:** The paper's framework aligns with Attachment D. The "Waterfall Contract" is programmed to pay servicer fees at high priority, ensuring they are not "subordinate, deferred or waived". The servicer-oracle is simply a *reporter of facts* (payments received), not a discretionary *manager* of the assets.

10.5 Analysis of Specific Facilities (Liquidity, Swaps and Reserves)

The blockchain framework not only supports compliance for the core "true sale" but also enhances the auditable implementation of specific facilities, such as liquidity lines and swaps, which are strictly governed by APS 120.

10.5.1 Liquidity and Servicer Cash Advances (Attachment D, paras 2 & 3)

- **APS 120 Requirement:** APRA places strict conditions on liquidity facilities. Crucially, draws must be subject to an asset quality test (i.e., not be used to cover non-performing assets) and the facility's repayment must *not* be subordinated to investors. Servicer cash advances must rank "the most senior to all other claims".
- **Framework Compliance:** The proposed blockchain model enforces these rules deterministically.
    - **Automated Asset Quality Test:** The "Waterfall Smart Contract" can be programmed to *only* allow a draw on the liquidity facility if the servicer-oracle's data shows the pool's arrears are *below* the non-performing threshold. This automates the asset quality test.
    - **Enforced Seniority:** The repayment of these facilities is not left to interpretation. It is coded into the "Waterfall Smart Contract's" logic at the highest priority, ensuring auditable compliance with the non-subordination and seniority rules.

10.5.2 Swap (Derivatives) Contracts (Para 30, Att. D paras 5 & 6)

- **APS 120 Requirement:** APRA has three primary concerns with swaps provided by an ADI:
    1. **Implicit Support (Att. D, para 5):** A basis swap provided by an originating ADI must be on "arm's-length" terms. Critically, if it is not, it must be "constructed with sufficient margin such that the ADI is not expected to be a net payer over the life of the transaction". This is the primary test to ensure the swap is not a hidden subsidy.
    2. **Payment Priority (Att. D, para 6):** Swap payments from the SPV must *not* be subordinated to any investor interests.
    3. **Capital Treatment (Para 30):** If an ADI holds a swap with a positive mark-to-market (gain), this must be deducted from its Common Equity Tier 1 (CET1) capital, as it represents unrealised future income.
- **Framework Compliance:** The blockchain model provides deterministic, auditable solutions for all three requirements.
    - **Enforcing Priority:** As noted in Section 5.4, the "Waterfall Smart Contract" is programmed to pay the swap counterparty at the appropriate *senior* priority level, ensuring auditable compliance with Attachment D, para 6.
    - **Enforcing the "No Net Payer" Test:** This is where the framework provides its greatest value. Proving an ADI is "not expected to be a net payer" is traditionally a difficult, model-based assessment done at inception. The on-chain model transforms this from a static "expectation" to a *dynamic, verifiable fact*.
        - The "Benchmark Rate Oracle" provides a live, trusted feed for the benchmark (e.g., BBSW).
        - The "Servicer Oracle" provides a live, trusted feed of the actual weighted average interest payments being collected from the pool.
        - By feeding these two live data points into the "Dashboard Contract", the swap's real-time mark-to-market (MTM) can be calculated and displayed 24/7. This gives the ADI, APRA and rating agencies an *ongoing, auditable proof* that the swap is not providing implicit support.
    - **Verifiable Capital Treatment:** This same real-time, verifiable MTM calculation provides the precise, auditable amount required for the ADI's CET1 deduction under Paragraph 30, replacing periodic, opaque estimates with a live, "golden source" value.

10.5.3 Reserves and Spread Accounts (Para 29)

- **APS 120 Requirement:** Paragraph 29 requires an ADI to deduct from CET1 any funds *it provides* to establish a reserve account.
- **Framework Compliance:** The "Reserves" mechanism proposed in this paper is distinct and more efficient. It is an *on-chain wallet* funded automatically by the "Waterfall Smart Contract" trapping *deal-generated excess spread*. Because these are not ADI-provided funds, the CET1 deduction under paragraph 29 would not apply. The smart contract automates this trapping mechanism, providing full transparency over the reserve's funding and balance.

By prioritising the supremacy of the off-chain legal "paper" and using smart contracts as automated, auditable *agents* of the independent trustee, this framework can meet the prudential requirements of APS 120 for any role an ADI undertakes.

11.0 Investor Risk Retention ("Skin in the Game")

A primary commercial demand from investors globally, particularly following the 2008 Global Financial Crisis (GFC), is *risk retention*. Investors now commonly require originators to maintain "skin in the game" to ensure interests are aligned and to mitigate the "originate-to-distribute-and-forget" risk. This has led to international regulatory standards, such as those in the US and EU, typically mandating a minimum 5% risk retention. While these specific regulations do not apply directly in Australia, the methods for achieving retention are globally understood and often demanded by investors as a commercial prerequisite for participation. The blockchain framework provides transparent, verifiable mechanisms to manage and prove this alignment, regardless of the originator's specific retention strategy.

11.1 Standard Risk Retention Methods

The commonly accepted methods for demonstrating "skin in the game," recognised internationally, include:

- **Vertical Slice:** The originator retains a percentage (typically 5%) of *each and every tranche* issued by the SPV. This means the originator shares pro-rata in the performance of all parts of the capital structure.
- **Horizontal Slice (First Loss):** The originator retains the most junior tranche (the equity tranche), representing the first 5% (or more) of potential losses in the pool. This is the most common method as it concentrates the originator's exposure.
- **Representative Sample (On-Balance Sheet):** The originator retains a randomly selected pool of assets *outside* the securitisation SPV, equivalent to 5% of the securitised pool. These assets must be representative of the overall quality of the securitised assets.

11.2 On-Chain Verification of Retention Methods

The blockchain framework allows for cryptographic proof of adherence to these retention methods:

- **Vertical Slice:** The originator would mint 5% of the tokens for *every* tranche (Token A1, Token B, Token E, etc.) and hold them in its publicly declared wallet. Investors can verify the originator holds a slice across the entire capital stack.
- **Horizontal Slice:** The originator would mint the "Token E" (equity) tranche and hold 100% of it in its wallet. This is the simplest to verify on-chain.
- **Representative Sample:** This is more complex to prove on-chain as the retention occurs off-chain. However, the originator could mint "Mortgage NFTs" for the retained pool and hold them in a separate, publicly declared "Retention Wallet".

While not part of the SPV, the existence and characteristics of these retained assets would be transparently verifiable by investors using the same on-chain tools (like the "Dashboard Contract") used to analyse the main pool.

11.3 "Covenant by Code": The Future of Risk Retention

The framework's ultimate advantage is turning a retention promise into a cryptographic fact. By holding the required tokens (whether vertical or horizontal slices) in a publicly verifiable wallet, or potentially even time-locking them via a smart contract, the originator offers investors mathematically enforced proof of its ongoing "skin in the game". This transparency acts as a powerful deterrent; any attempt by the originator to transfer or sell these "locked" tokens in breach of their retention covenants would be immediately and immutably visible on the public ledger.

12.0 The Rating Agency Perspective: A New Risk Framework

For an on-chain RMBS to be viable, it must be rated by agencies like S&P, Moody's and Fitch. These agencies will apply their existing securitisation methodologies but will introduce a new, rigorous framework to assess the unique technology and operational risks of a DLT-based structure.

Their analysis will likely bifurcate into two main components:

1. **Traditional Risk Analysis (The "What"):** Assessing the credit, legal and structural risks.
2. **Technology and Operational Risk Analysis (The "How"):** Assessing the risks of the new on-chain infrastructure.

12.1 Traditional Credit and Legal Risk Analysis

In this area, the rating agencies' analysis will be largely unchanged and the on-chain model provides significant benefits.

12.1.1 Credit Risk of Collateral: The agencies will continue to analyse the credit quality of the underlying "Mortgage NFTs" (the loans) just as they do today, assessing LVRs, borrower seasoning and credit scores.

12.1.2 Legal and Structural Integrity: This is where the paper's "dual-layer" hybrid model is essential. The agencies will need legal opinions confirming:

- The **"true sale"** is legally perfected and enforceable in an Australian originator's insolvency.
- The **off-chain Trust Deed** is the paramount governing document, with the smart contract acting only as its "agent".
- The **Trustee's power** to override or pause the smart contract in a dispute or bug scenario is legally unambiguous.

12.1.3 Cash Flow and Waterfall Analysis: Agencies will model the cash flow waterfall to ensure the structure can withstand various stress scenarios (defaults, prepayments). The on-chain model *helps* this, as the "Waterfall Contract" is a piece of auditable code, not a complex legal clause open to interpretation. They can mathematically verify the payment logic.

12.2 New Technology and Operational Risk Analysis

This is the critical new hurdle. The agencies will conduct deep due diligence on the technology itself, treating it as a new form of operational risk. Their key areas of focus will be:

12.2.1 Smart Contract Risk

- **Code Integrity:** Agencies will demand multiple, independent, "institutional-grade" audits of all smart contracts (especially the "Waterfall Contract").
- **Vulnerability:** They will assess the risk of a "hack" or exploit that could drain funds or freeze the waterfall.
- **"Admin Key" Risk:** They will analyse who has the power (e.g., the trustee, the issuer) to pause or upgrade the contract and what controls are around those "admin keys." **Crucially, administrative control must reside solely with the Trustee**, reflecting their fiduciary duty, not with operational parties like the servicer.

12.2.2 Oracle Risk

- The agencies will identify the oracles (e.g., the servicer, the AVM provider) as **critical single points of failure**.
- They will assess the security, reliability and accuracy of the data being pushed on-chain. *What happens if the servicer's oracle is compromised and reports millions in non-existent payments?*
- They will require redundant or pre-approved backup mechanisms for critical data feeds.

12.2.3 Blockchain Infrastructure Risk

- **Platform Choice:** They will assess the risk of the underlying blockchain (e.g., Ethereum vs. a permissioned ledger). A private, permissioned chain will likely be preferred for its stability, low costs and controlled access.
- **Resilience and Uptime:** They will need to be satisfied that the network is resilient to outages and cannot be halted by a single party.

12.2.4 Counterparty Risk and Operational Resilience

The roles of the **servicer** (as oracle) and **trustee** (as smart contract supervisor) become *more* critical, not less.

12.2.4.1 Standby Servicer Capability (Critical)

The traditional requirement for a standby servicer remains, but its role evolves significantly. The standby servicer must not only be capable of taking over all traditional off-chain servicing duties (payment collection, borrower interaction, default management) but must also possess the **technical capability and operational readiness** to seamlessly step into the role of the **oracle**. This requires:

- Proven infrastructure to connect to the deal's specific blockchain.
- Robust, audited processes for providing accurate data feeds (payments, arrears, etc.) to the smart contracts.
- Pre-tested procedures for activation, likely requiring formal authorisation from the Trustee.
- **Crucially, the standby servicer will *not* hold administrative keys** to the smart contracts. Their permissions will be strictly limited to providing oracle data, with the Trustee retaining ultimate control over the contract's operation. This necessitates a new level of technical due diligence by rating agencies on the standby servicer's "on-chain savvy."

12.2.4.2 Trustee Technical Oversight

The agencies will assess the trustee's technical capability to actually perform its new supervisory role. *Does the trustee have the expertise and systems to monitor oracle performance, identify a stuck contract and securely manage the administrative keys?*

12.2.4.3 Real-World Application

S&P Global Ratings is actively building this capability. In May 2025, it announced a Proof-of-Concept with Metrika to build a "comprehensive, real-time risk framework" for tokenised assets, creating over **100 Key Risk Indicators (KRIs)**. In October 2025, it began publishing its **"Stablecoin Stability Assessments"** on-chain via Chainlink, demonstrating a live framework for assessing a key counterparty risk (the settlement asset).

13.0 Micro-Economic Viability: Oracle Costs vs. Efficiency Gains

The introduction of blockchain infrastructure, particularly the reliance on multiple, specialised oracles (Servicer, Valuation, Benchmark Rate, potentially FX Rate and Rating Agency), inevitably introduces **new operational costs** to the SPV structure. Oracles are essential services that incur expenses, including potential service subscription fees, per-call data fees, network transaction (gas) costs for putting data on-chain and the infrastructure costs if an entity (like the servicer) operates its own oracle function.

However, the fundamental premise and business case for adopting an on-chain RMBS model is that these new technology-related costs are expected to be **significantly offset and likely outweighed, by substantial cost savings and efficiency gains** realised elsewhere in the traditional securitisation value chain. Key areas where savings are anticipated include:

- **Reduced Intermediary Fees:** Automation via smart contracts can diminish or eliminate the need for certain traditional roles, particularly:
    - **Paying Agents:** The automated waterfall largely removes the need for manual calculation and distribution, saving associated fees.
    - **Trustee Administration:** While the trustee's supervisory role evolves, the automation of cash flow calculations and reporting reduces their administrative burden, potentially lowering ongoing fees.
    - **Custody:** Reduced reliance on traditional CSDs like Austraclear for note holding and transfers can decrease custody and settlement costs.
- **Operational Efficiency Gains:**
    - **Reconciliation:** Establishing a "golden source of truth" on the blockchain eliminates costly manual reconciliation between the servicer, trustee and other parties.
    - **Reporting:** Automated, real-time access to verifiable pool data can dramatically reduce the effort and cost associated with compiling and distributing periodic investor and regulatory reports.
    - **Servicing Automation:** Smart contracts automate waterfall distributions, trigger events based on oracle data and manage reserves, reducing manual processing by the servicer/trustee.
- **Capital Efficiency and Liquidity:**

    - **Faster Settlement:** Atomic (T+0) settlement eliminates the capital tied up during traditional T+2 settlement windows and reduces counterparty risk exposure, potentially lowering funding costs.
    - **Enhanced Liquidity:** Increased transparency, fractionalization and the potential for 24/7 secondary trading could improve market liquidity, potentially leading to tighter pricing spreads for investors and issuers.
- **Audit and Compliance:** The immutable and transparent nature of the blockchain ledger can streamline audit processes and enhance the efficiency of regulatory compliance and reporting.

Ultimately, the economic viability of the blockchain RMBS model hinges on demonstrating that the aggregate savings from automation, disintermediation and increased efficiency surpass the new costs associated with blockchain infrastructure, smart contract deployment/auditing and ongoing oracle services. The successful implementation by entities like Figure Technologies suggests this economic balance is achievable.

While oracle and automation costs define micro-level efficiency, the broader economic impact on capital velocity and operational transparency is addressed in the following section.

14.0 Macro-Economic and Operational Impact

Traditional securitisation structures are administratively efficient but technologically dated. Settlement lags, reconciliation cycles, and fragmented data flows create measurable frictions that increase both issuance costs and systemic latency. The proposed on-chain RMBS model preserves the legal and prudential architecture of APS 120 while eliminating redundant intermediaries and manual processes.

The table below presents an **illustrative comparison** between a conventional RMBS transaction and the blockchain-enabled framework described in this paper. Figures are indicative only and based on observed market practices, published trustee reports, and estimated cost savings from automation and reduced reconciliation requirements.

Metric	Conventional RMBS Model	On-Chain RMBS Framework	Indicative Improvement
Settlement latency	T+2 days (via Austraclear or manual fund transfer)	T+0 (atomic settlement via *T+0 On-Ramping™*)	> 99% faster
Servicer reconciliation cost	~A$150k p.a. per deal	<A$20k p.a. (automated ledger-level reconciliation)	~ (85)%
Trustee report production time	20–30 days post-cut-off	Instantaneous via *Regulatory Audit Interface*	Near-real-time
Data accuracy	Manual aggregation from multiple systems	Single on-chain event log	Error rate → 0%
Operational risk events (e.g., mis-posting, double-pledge)	Moderate (human entry risk)	Cryptographically impossible (hash-verified assets)	Eliminated
Rating-agency verification cycle	2–3 weeks	Automated evidence feed	~80% time
Issuance cost per trust	~A$600k – A$900k (all-in)	~ AUD $350k – $500k (after automation)	~40 – 50%

Interpretation

These gains stem primarily from three effects:

1. **Process Compression** - Atomic settlement and shared data eliminate the need for end-of-day batching, reducing liquidity drag and improving warehouse-to-capital-market velocity.

2. **Automation of Verification -** Trustee and servicer reconciliations become deterministic events derived from the same immutable ledger, collapsing audit cycles.

3. **Reduction in Intermediary Overhead** - Legal and fiduciary layers remain intact, but administrative intermediaries (data custodians, reconciliation teams) are materially reduced.

From a prudential perspective, faster and more accurate settlement reduces the likelihood of operational and liquidity risk events under **CPS 220 (Risk Management)** and **CPS 234 (Information Security)**.

For issuers, the reduction in time-to-market and ongoing reporting cost enhances capital efficiency.

For investors, it yields real-time transparency and verifiable collateral performance.

While further empirical validation through live pilots is required, the indicative data support the hypothesis that blockchain-native securitisation achieves **functional compliance at lower operational cost** - precisely the type of productivity improvement envisaged by APRA's digital-transformation agenda.

15.0 Case Studies and Market Precedents

While no public, on-chain RMBS has been issued in Australia, several local and international projects provide a clear proof-of-concept that this model is now a market reality.

- **Australian Precedents (DLT Bonds and RBA Projects):** The RBA alongside major banks (including CBA, ANZ and NAB) has been a pioneer in this space. Its early experiments with DLT-based bond issuance ("Kangaroo Bonds") and the ongoing **Project Acacia** are critical. Project Acacia, which involves 24 use cases from industry, is directly testing tokenised asset settlement. Its findings, expected in early 2026, will be foundational for establishing the "digital cash" and settlement infrastructure required for a viable on-chain RMBS market.
- **Global Precedent (Figure Technologies, US):** Figure is the definitive global leader, having moved from proof-of-concept to a live, rated market. In October 2025, Figure announced it had received a 'AAA' rating from S&P Global Ratings for a securitisation. This landmark event represents the first major rating agency to apply its full credit and operational risk framework to a blockchain-native securitisation.
    - **What they've proven:** Figure has demonstrated the entire lifecycle, from digital origination (of HELOCs) to on-chain securitisation, servicing and trading **using its own native blockchain, Provenance.io**. They have *proven* that this model can meet the rigorous standards of a 'AAA' rating, successfully mitigating the operational, legal and smart contract risks outlined in Section 12.0.
    - **Relevance for Australia:** Figure proves that a vertically integrated "originate-to-distribute" model on-chain is not theoretical. It is reportedly a multi-billion dollar business model with AAA-rated securitisations.
- **Global Precedent (Provenance.io, US):** The Provenance blockchain itself, **developed by Figure Technologies** , is purpose-built for financial services. It has processed billions in loan transactions.
    - **What it proves:** It demonstrates a viable **public, permissioned and purpose-built** blockchain designed specifically for regulated financial assets. It has its own utility token (HASH) and a mechanism for on-chain, compliant settlement. While public at its base layer, financial applications built upon it incorporate necessary access controls.
    - **Relevance for Australia:** This provides a model for a purpose-built financial services ledger, as opposed to adapting a general-purpose

blockchain like Ethereum. However, its ownership by a potential competitor raises considerations (see Section 9.0).

- **European Precedent (MQube, UK)**

  In October 2025, the UK fintech MQube, through its lending arm MPowered, announced it had tokenised £1.3 billion (US$1.73 billion) of its residential mortgage debt on an Ethereum-compatible blockchain. This transaction represents the first major-scale tokenisation of residential mortgage assets by a European lender.

  Relevance for Australia: The MQube initiative validates the core premise of this paper that large, established mortgage portfolios can be represented on-chain within a robust, regulated financial market (the UK).

  Complements the Figure Model: While Figure Technologies has proven the vertically integrated "originate-to-distribute" model, MQube's move demonstrates the value for existing lenders in tokenising their balance sheet assets to achieve data integrity, auditability and prepare for a future on-chain securitisation market.

16.0 Conclusion: The Future of Securitised Credit in Australia

The traditional Australian RMBS process is not broken, but it is a product of a pre-digital age. It functions through a series of intermediaries, data silos and batch processes that add cost, time and opacity. The framework outlined in this paper is one of an Australian-compliant, on-chain securitisation and is not a radical "crypto" proposal. It is the logical and evolutionary next step for financial market infrastructure.

- **A Summary of Benefits:** By creating a single, verifiable "golden source of truth," a blockchain-native RMBS delivers **efficiency** (automating the cash-flow waterfall and eliminating T+2 settlement), **transparency** (providing investors and regulators with real-time, asset-level data) and **liquidity** (enabling 24/7 secondary markets with fractionalised assets).
- **An Australian Roadmap:** The path to adoption in Australia is now becoming clear:
    1. **Legal Clarity:** The Government must finalise PPSA reforms to address digital assets.
    2. **Settlement Infrastructure:** The RBA's work on Project Acacia must mature into a live wholesale settlement asset (a CBDC or regulated private stablecoin).
    3. **Industry Standards:** The ASF, in collaboration with industry, must define the standards for data and smart contracts to ensure interoperability.
    4. **Pilot Transactions:** The market must move from proofs-of-concept to the first live, rated and publicly-issued on-chain RMBS.

The framework demonstrates that regulatory alignment and technological innovation are not opposing forces. A blockchain-native RMBS can preserve every legal safeguard of Australia’s prudential architecture while correcting the operational inefficiencies that have long constrained transparency and settlement speed.

The next phase is empirical: limited pilot transactions under existing law, co-supervised by trustees, originators and APRA-regulated ADIs. Such pilots would test atomic settlement, waterfall automation and data-feed integrity without requiring new legislation. Demonstrating that the system functions safely within APS 120 would move the debate from theory to implementation - a shift the global securitisation market is already beginning to make.

A detailed mapping of the proposed framework against Prudential Standard APS 120 (2023) is provided in Annex A.

Annex A — APS 120 (2023) Compliance Mapping

Purpose:
This annex maps the requirements of Prudential Standard APS 120 - Securitisation (January 2023) to the corresponding mechanisms within the proposed on-chain RMBS framework. It demonstrates functional equivalence between the prudential objectives of APS 120 and the digital implementation described in the paper. All clause numbers below refer to the 2023 revision of APS 120.

APS 120 Reference	Regulatory Requirement (summary)	Blockchain RMBS Framework Implementation	Commentary
¶ 17 – True-sale and legal isolation	Securitised exposures must be legally isolated from the ADI and held by an SPV in a completed, enforceable true-sale.	Legal title transferred to SPV under conventional Sale & Assignment Deed. Digital Mortgage NFTs™ represent beneficial interests - control and audit trail enforced on-chain.	Token layer evidences beneficial interest but does not alter legal conveyance. True-sale remains under contract law, satisfying ¶ 17.
¶ 25(b) – Evidencing beneficial interests	Beneficial interests may be evidenced or recorded in digital or electronic form.	Mortgage NFTs™ constitute digital records of beneficial interests maintained on a permissioned ledger.	Clause directly supports this implementation. Digital recording is compliant with ¶ 25(b).
¶ 26 – SPV independence	The SPV must be bankruptcy-remote and not under effective control of the originator.	Smart SPV™ structure preserves trust law separation. Governance implemented through trustee-controlled node and multi-sig upgrade policy.	Maintains legal separateness - automation does not confer control. Complies with ¶ 26 (a–c).
¶ 37 – Servicer and cash-flow management	Servicer must maintain accurate, timely cash-flow reporting and segregation of funds.	T+0 On-Ramping™ and Smart Servicer™ automate fund segregation and	Improves compliance by eliminating manual lag - aligns with ¶ 37 and CPS 234 (Information Security).

		reporting via on-chain settlement.	
¶ 46 – Liquidity and funding facilities	Liquidity or redraw facilities must be at arm's length and documented.	Liquidity providers integrate through stablecoin escrow contracts governed by identical facility documentation mirrored on-chain.	Digital escrow records meet disclosure and arm's-length requirements - no prudential deviation.
¶ 63–70 – Reporting and transparency	Trustees must provide timely, accurate reporting to investors and APRA.	Regulatory Audit Interface exports on-chain events to JSON/XBRL feeds mapped to ARF 720.1/721 templates.	Enables continuous disclosure - materially enhances transparency beyond current manual standards.
¶ 74 – Servicer and trustee responsibilities	Trustee must ensure ongoing compliance - servicer must provide verifiable data.	Trustee Node Governance (multi-sig control) and immutable data trail.	Ensures auditability and preserves fiduciary oversight.
¶ 82 – Operational risk and data integrity	Originators must ensure systems maintain data accuracy, security and recoverability.	Permissioned ledger under CPS 234-aligned controls - redundant nodes and hash-based verification.	Satisfies ¶ 82 through immutable, cryptographically verifiable records.
¶ 92 – Regulatory access	APRA must be able to obtain timely access to data and records.	Read-only API gateway and auditor node for regulatory viewing.	Immediate compliance - enhances APRA's supervisory reach.
¶ 103 – Disclosure and investor communication	Investors must receive timely, consistent information on pool performance.	Verifiable PDS™ provides dynamic, authenticated disclosure and investor dashboards.	Surpasses baseline disclosure obligations under Corporations Act s. 1013D.

Interpretation Notes

- The mapping asserts functional equivalence, not statutory substitution. All existing legal and prudential obligations remain intact.
- The on-chain elements are evidentiary and operational mechanisms designed to improve accuracy and timeliness of compliance.

- The model assumes continuing oversight by APRA, ASIC and the trustee under the existing licensing and reporting regimes.

Conclusion of Annex A

This mapping shows that the blockchain-native RMBS structure can satisfy the substance and intent of APS 120 (2023) without legislative amendment. Where uncertainty remains (e.g. PPSA control or digital perfection), the implementation is designed to be legally parallel rather than substitutive, ensuring compliance through both conventional documentation and digital verification.

GLOSSARY OF TERMS

AUSTRALIAN REGULATORY AND LEGAL TERMS

ADI (Authorised Deposit-taking Institution): A financial institution authorised by APRA to take deposits from the public, including banks, building societies and credit unions.

AFSL (Australian Financial Services Licence): A licence issued by ASIC required to provide financial services or products to Australian clients.

AML/CTF (Anti-Money Laundering and Counter-Terrorism Financing): Regulatory framework under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) requiring financial institutions to verify customer identities and report suspicious transactions.

APRA (Australian Prudential Regulation Authority): Australia's prudential regulator supervising banks, insurance companies and superannuation funds.

ASIC (Australian Securities and Investments Commission): Australia's corporate, markets and financial services regulator responsible for enforcing company and financial services law.

AUSTRAC (Australian Transaction Reports and Analysis Centre): Australia's financial intelligence agency responsible for regulating entities under AML/CTF legislation.

Austraclear: ASX's settlement system for debt securities, enabling book-entry transfer and settlement of fixed income securities.

Corporations Act 2001 (Cth): Primary legislation governing companies and financial services in Australia, including rules for managed investment schemes, fundraising and market conduct.

Electronic Transactions Act 1999 (Cth): Commonwealth legislation providing legal recognition for electronic communications and transactions, enabling digital signatures and contracts.

INFO 225: ASIC Information Sheet 225 titled "Crypto-assets," providing guidance on how existing financial services laws apply to crypto-assets and initial coin offerings.

KYC (Know Your Customer): Processes used by financial institutions to verify customer identities, assess risk profiles and comply with AML/CTF regulations.

NPP (New Payments Platform): Australia's fast payments infrastructure enabling real-time, data-rich payments between participating financial institutions.

PEXA (Property Exchange Australia): Australia's national electronic property exchange system enabling digital conveyancing and settlement.

PPSA (Personal Property Securities Act 2009): Commonwealth legislation establishing a national regime for security interests in personal property, including a centralized register (PPSR).

PPSR (Personal Property Securities Register): National register where security interests in personal property must be registered to achieve perfection and priority.

Reporting Entity: An organisation required to comply with AML/CTF obligations under AUSTRAC regulation, including customer identification and transaction reporting.

RITS (Reserve Bank Information and Transfer System): The RBA's high-value payments settlement system used for interbank settlements in Australia.

Section 761G: Provision of the Corporations Act 2001 (Cth) defining "wholesale client," a classification determining disclosure and conduct obligations.

Torrens Title: Australia's land registration system (originating in South Australia) where ownership is established through registration rather than historical chain of title.

Trustee: Entity holding legal title to assets on behalf of beneficiaries, with fiduciary duties to act in beneficiaries' interests. In RMBS, the trustee administers the securitisation trust.

Wholesale Client: Under s 761G of the Corporations Act, sophisticated investors (such as institutional investors) exempt from certain disclosure and conduct requirements.

SECURITISATION TERMS

Arrears: Overdue loan payments where borrowers have failed to make scheduled payments by the due date.

Call Option: Right (but not obligation) for the issuer or servicer to repurchase or redeem securities before scheduled maturity, often triggered when outstanding balance falls below a threshold ("clean-up call").

Collateral: Assets pledged as security for debt obligations; in RMBS, the underlying mortgage loans serve as collateral for issued securities.

Counterparty Risk: Risk that a party to a transaction will fail to fulfill their contractual obligations, potentially causing financial loss to other parties.

Credit Enhancement: Structural features designed to improve the credit quality of securities, including subordination, overcollateralisation, reserve accounts and third-party guarantees.

Debenture: Under Australian law, a document evidencing debt or acknowledging indebtedness, commonly used to describe debt securities.

Delinquency: Status of a loan when borrower payments are overdue but not yet in default; typically measured in days past due (30+, 60+, 90+ days).

DvP (Delivery-versus-Payment): Settlement mechanism ensuring simultaneous exchange of securities and payment, eliminating settlement risk.

Managed Investment Scheme: Under Chapter 5C of the Corporations Act, a scheme where investors contribute money or assets, which are pooled or used in a common enterprise to generate financial benefits.

Originator: Financial institution (bank or non-bank lender) that initially creates and funds mortgage loans before selling them to a securitisation vehicle.

Paying Agent: Entity responsible for distributing payments from the securitisation trust to noteholders according to the payment waterfall.

Perfection: Legal process of establishing priority for a security interest, typically through registration (PPSR) or control, protecting the creditor's interest against third parties and in insolvency.

Poolcut: Selection and aggregation of individual mortgage loans into a defined pool that will back a securitisation transaction.

Prospectus: Disclosure document required under Chapter 6D of the Corporations Act for offers of securities to retail investors, containing detailed information about the investment.

RMBS (Residential Mortgage-Backed Securities): Debt securities backed by a pool of residential mortgage loans, with cash flows passed through to investors.

Securitisation: Process of pooling assets (such as mortgages) and issuing securities backed by those assets, transferring credit risk from originator to investors.

Servicer: Entity responsible for collecting borrower payments, managing borrower relationships and handling defaults on behalf of the securitisation trust.

SPV (Special Purpose Vehicle): Bankruptcy-remote legal entity established to hold securitised assets and issue securities, isolating assets from originator's insolvency risk.

Stratification: Analysis breaking down a loan pool by various characteristics (LTV ratios, geographic distribution, loan sizes) to assess risk profile and portfolio quality.

Subordination: Credit enhancement mechanism where junior tranches absorb losses before senior tranches, providing protection to senior investors.

T+2 Settlement: Settlement convention where trades settle two business days after the transaction date, standard for many securities markets.

Tranche: A specific class or tier of securities within a securitisation structure, typically differentiated by risk, return and payment priority (e.g., Class A, Class B).

True Sale: Legal mechanism ensuring assets sold to the SPV are legally isolated from the originator's bankruptcy estate, essential for achieving bankruptcy remoteness.

Waterfall: Priority structure governing the distribution of cash flows from the collateral pool to different parties (senior noteholders, junior noteholders, servicer, equity).

Weighted Average Life (WAL): Average time until principal is repaid, weighted by principal amounts, providing a measure of expected security duration.

BLOCKCHAIN AND DIGITAL ASSET TERMS

Atomic Settlement: A transaction where all components either complete successfully together or none complete at all, ensuring consistency (e.g., simultaneous asset and payment transfer in DvP).

Blockchain: Distributed ledger technology where transactions are recorded in blocks cryptographically linked in a chronological chain, providing transparency and immutability.

CBDC (Central Bank Digital Currency): Digital form of fiat currency issued and controlled by a central bank (such as the RBA), potentially used for wholesale or retail payments.

Custodian: Entity providing secure storage of digital assets, managing private keys on behalf of investors, often with institutional-grade security controls.

DeFi (Decentralised Finance): Financial services and applications built on blockchain technology, typically operating without traditional intermediaries through smart contracts.

DID (Decentralised Identifier): Self-sovereign digital identity standard enabling verifiable, cryptographic identity without centralized identity providers.

DLT (Distributed Ledger Technology): Broader category encompassing blockchain and other distributed database technologies where data is replicated across multiple nodes.

ERC-20: Ethereum token standard for fungible tokens, where each token is identical and interchangeable, commonly used for cryptocurrencies and utility tokens.

ERC-721: Ethereum token standard for non-fungible tokens (NFTs), where each token is unique and represents distinct assets or rights.

ERC-3643 (T-REX Standard): Ethereum token standard designed for regulated securities, incorporating built-in compliance rules, identity verification and transfer restrictions.

Gas Fees: Transaction costs on blockchain networks (especially Ethereum) paid to validators for processing and recording transactions on the ledger.

Hash: Cryptographic function converting input data into a fixed-size string, used for verifying data integrity and linking blocks in a blockchain.

HSM (Hardware Security Module): Physical computing device providing secure cryptographic key generation, storage and management, protecting against unauthorised access.

Immutability: Property of blockchain where recorded transactions cannot be altered or deleted, providing a permanent, tamper-evident record.

Multi-Signature (Multi-Sig): Security mechanism requiring multiple private keys to authorise a transaction, distributing control and reducing single-point-of-failure risks.

NFT (Non-Fungible Token): Unique digital asset on a blockchain representing ownership or rights to a specific item, distinct from fungible tokens where units are interchangeable.

Node: Individual computer participating in a blockchain network, maintaining a copy of the ledger and validating transactions.

Oracle: Trusted data provider that inputs off-chain information (e.g., prices, events, payment data) onto the blockchain, enabling smart contracts to respond to real-world conditions.

Permissioned Blockchain: Blockchain network where participation (reading, writing, validating) is restricted to authorised entities, providing control over access and governance.

Permissionless Blockchain: Public blockchain where anyone can participate as a user or validator without requiring authorisation (e.g., Bitcoin, Ethereum mainnet).

Private Key: Secret cryptographic key providing control over blockchain addresses and enabling transaction authorisation; must be kept secure to prevent asset theft.

Project Acacia: RBA-led research initiative exploring tokenised asset settlement using various forms of digital money, conducted with the Digital Finance Cooperative Research Centre (DFCRC) and industry participants.

Smart Contract: Self-executing code deployed on a blockchain that automatically enforces agreement terms when predefined conditions are met, without requiring intermediary intervention.

Soul-Bound Token: Non-transferable token permanently linked to a specific wallet address, used for identity credentials or reputation that cannot be sold or transferred.

Stablecoin: Cryptocurrency designed to maintain stable value relative to a reference asset (typically fiat currency like AUD or USD), often backed by reserves or algorithms.

Stablecoin Stability Assessment (SSA): S&P Global Ratings framework assessing stablecoin reserve quality, governance and de-pegging risk, with scores available on-chain via oracles.

STO (Security Token Offering): Offering of tokenised securities on blockchain infrastructure, subject to securities regulation (as opposed to unregulated utility token offerings).

T+0 Settlement: Same-day settlement where transactions are completed on the trade date itself, enabled by blockchain's atomic settlement capabilities.

Token: Digital unit of value or rights represented on a blockchain, which may be fungible (like currency) or non-fungible (like unique assets).

Tokenisation: Process of representing real-world assets or rights as digital tokens on a blockchain, enabling programmable ownership and transfer.

Upgrade Function: Administrative capability in a smart contract allowing authorised parties (typically trustees) to modify contract logic, essential for correcting bugs or adapting to changed circumstances.

Verifiable Credential (VC): Cryptographically secure digital credential that proves claims about an identity (e.g., KYC compliance) without revealing underlying personal information.

Wallet: Software or hardware interface for managing private keys and interacting with blockchain networks, enabling users to send, receive and store digital assets.

RATING AGENCY AND RISK TERMS

AAA Rating: Highest credit rating indicating extremely strong capacity to meet financial commitments, with minimal credit risk.

APS 120: APRA Prudential Standard 120 on Securitisation, setting out requirements for ADI originators engaging in securitisation transactions.

CPS 234: APRA Prudential Standard 234 on Information Security, requiring entities to maintain information security capabilities commensurate with threats.

KRI (Key Risk Indicator): Quantitative metric used to monitor and assess risk levels in financial structures or operations.

Operational Risk: Risk of loss from inadequate or failed internal processes, systems, human errors, or external events, particularly relevant for technology-dependent systems.

Rating Agency: Independent organisation assessing credit risk of debt securities and issuers, providing ratings used by investors for risk assessment (e.g., S&P Global Ratings, Moody's, Fitch).

S&P Global Ratings: Major international credit rating agency providing credit ratings, research and risk analysis for securities and issuers.

TECHNICAL AND PROCESS TERMS

API (Application Programming Interface): Specification allowing different software systems to communicate and exchange data, essential for integrating blockchain with legacy systems.

Batching: Grouping multiple transactions together for processing as a single operation, reducing per-transaction costs and improving efficiency.

On-Ramping: Process of converting fiat currency to digital assets or bringing traditional assets onto blockchain infrastructure.

RegTech (Regulatory Technology): Technology solutions automating regulatory compliance, reporting and monitoring functions.

Reconciliation: Process of comparing and matching data from different sources to ensure consistency and identify discrepancies, traditionally manual but automated in blockchain systems.

ORGANISATIONAL TERMS

ASF (Australian Securitisation Forum): Peak industry body representing participants in Australia's securitisation market, developing standards and advocating for the industry.

Chainlink: Decentralised oracle network providing reliable off-chain data to smart contracts, widely used in blockchain financial applications.

DFCRC (Digital Finance Cooperative Research Centre): Australian research organisation collaborating with RBA on Project Acacia and other digital finance initiatives.

Ethereum: Leading public blockchain platform supporting smart contracts and decentralised applications, with extensive developer community and tools.

Figure Technologies: US financial technology company pioneering blockchain-based loan origination and securitisation, operating on the Provenance blockchain.

Hyperledger Fabric: Open-source permissioned blockchain framework designed for enterprise use, offering modularity, privacy and performance.

Metrika: Analytics firm partnering with S&P Global Ratings to develop risk frameworks for multi-chain digital assets.

Provenance Blockchain: Purpose-built blockchain platform for financial services developed by Figure Technologies, supporting loan transactions and securitisation.

R3 Corda: Enterprise distributed ledger platform designed specifically for financial services, emphasizing privacy and regulatory compliance.

RBA (Reserve Bank of Australia): Australia's central bank responsible for monetary policy, financial system stability and payments system oversight.

BIBLIOGRAPHY

LEGISLATION (COMMONWEALTH OF AUSTRALIA)

Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth).

Corporations Act 2001 (Cth). Specifically: Chapter 5C (Managed Investment Schemes), Chapter 6D (Fundraising) and Chapter 7 (Financial Services and Markets).

Electronic Transactions Act 1999 (Cth).

National Consumer Credit Protection Act 2009 (Cth).

Personal Property Securities Act 2009 (Cth).

REGULATORY GUIDANCE AND PUBLICATIONS (AUSTRALIA)

Australian Prudential Regulation Authority (APRA). Prudential Standard APS 120 Securitisation. APRA.

Australian Prudential Regulation Authority (APRA). Prudential Standard CPS 234 Information Security. APRA.

Australian Securities and Investments Commission (ASIC). Information Sheet 225 (INFO 225): Crypto-assets. ASIC.

Australian Securities and Investments Commission (ASIC). Speeches and Reports on Distributed Ledger Technology (DLT) and Tokenisation. ASIC.

Australian Transaction Reports and Analysis Centre (AUSTRAC). Guidance on the Regulation of Digital Currency Exchange Providers and KYC/AML Obligations for Reporting Entities. AUSTRAC.

Reserve Bank of Australia (RBA). Publications and Media Releases Related to Project Acacia (jointly with the Digital Finance Cooperative Research Centre - DFCRC). RBA.

Reserve Bank of Australia (RBA). Speeches and Bulletins on the Tokenisation of Assets, Central Bank Digital Currencies (CBDC) and the Future of Payments Infrastructure. RBA.

INDUSTRY BODIES AND MARKET INFRASTRUCTURE

Australian Securitisation Forum (ASF). Industry Guidance, Market Reports and Submissions to Treasury on Regulatory Reform and Market Practices. ASF.

ASX Limited. Austraclear System: Official Documentation on Settlement Procedures for Debt Securities. ASX.

Property Exchange Australia (PEXA). Documentation on Electronic Conveyancing and Property Settlement Process. PEXA.

INTERNATIONAL REGULATORY AND INDUSTRY DEVELOPMENTS

European Union. Markets in Crypto-Assets Regulation (MiCA). Official Journal of the European Union.

Monetary Authority of Singapore (MAS). Guidelines on Digital Asset Collateral Regimes. MAS.

United States Securities and Exchange Commission (SEC). Securities Act of 1933 Registration Statements and Public Filings. SEC.

RATING AGENCY RESEARCH AND METHODOLOGIES

S&P Global Ratings. (2023). Stablecoin Stability Assessments Framework (Launched December 2023). S&P Global Ratings.

S&P Global Ratings. (2025, May 14). Press Release: Metrika and S&P Global Ratings Conclude Proof-of-Concept for Multi-Chain Digital Asset Risk Framework. S&P Global Ratings.

S&P Global Ratings. (2025, October 14). Press Release: S&P Global Ratings and Chainlink Collaboration Brings S&P's Stablecoin Stability Assessments On-Chain. S&P Global Ratings.

S&P Global Ratings. Asset Isolation and Special-Purpose Entity Methodology. S&P Global Ratings.

S&P Global Ratings. Counterparty Risk Framework Methodology and Assumptions. S&P Global Ratings.

S&P Global Ratings. Structured Finance Methodology. S&P Global Ratings.

INTERNATIONAL CASE STUDIES AND COMPANY MATERIALS

Figure Technologies, Inc. Public Filings: S-1 Registration Statement. U.S. Securities and Exchange Commission.

Figure Technologies, Inc. White Papers: Blockchain-Based HELOC Origination and Securitisation Model. Figure Technologies.

Figure Technologies, Inc. (2025, October 20). Press Release/Company Announcement: S&P Global Ratings AAA Rating on Securitisation. Figure Technologies.

Provenance Blockchain Foundation. Provenance Blockchain: Technical Whitepaper. Provenance.io.

Provenance Blockchain Foundation. Documentation on Public, Permissioned Blockchain and Financial Asset Protocols. Provenance.io.

Thompsett, L. (2025, October 13). *MQube Tokenises £1.3bn Mortgage Debt in European First*. FinTech Magazine. https://fintechmagazine.com/news/mqube-tokenises-1-3bn-mortgage-debt-in-european-first

BLOCKCHAIN TECHNICAL STANDARDS

Ethereum Community. EIP-20: Token Standard (ERC-20 Fungible Token Standard). Ethereum Foundation. https://eips.ethereum.org/EIPS/eip-20

Ethereum Community. EIP-721: Non-Fungible Token Standard (ERC-721). Ethereum Foundation. https://eips.ethereum.org/EIPS/eip-721

Ethereum Community. EIP-3643: T-REX - Token for Regulated EXchanges Standard. Ethereum Foundation. https://eips.ethereum.org/EIPS/eip-3643

Note: Token standard designed for regulated financial assets, extending ERC-20 with embedded compliance and identity-verification capabilities for permissioned token issuance, management and transfer under regulatory constraints.

BLOCKCHAIN PLATFORMS AND INFRASTRUCTURE

Chainlink Labs. Chainlink: Decentralised Oracle Network Documentation. Chainlink.

Hyperledger Foundation. Hyperledger Fabric: Enterprise Blockchain Framework Documentation. Linux Foundation.

R3. Corda: Distributed Ledger Platform for Financial Services Documentation. R3.

ACADEMIC AND RESEARCH PUBLICATIONS

Digital Finance Cooperative Research Centre (DFCRC). Research Publications on Tokenisation and Digital Asset Settlement. DFCRC.

Treasury of the Commonwealth of Australia. Personal Property Securities Act Review: Consultation Papers on Digital Assets and Collateral Reform. Treasury.

SUPPLEMENTARY REFERENCES

Australian Taxation Office (ATO). Guidance on Taxation Treatment of Digital Assets and Cryptocurrencies. ATO.

International Organization of Securities Commissions (IOSCO). Policy Recommendations for Crypto and Digital Asset Markets. IOSCO.

World Economic Forum. White Papers on Blockchain Technology in Financial Services. WEF.

NOTE ON CITATIONS

This bibliography includes references to regulatory guidance, industry standards, company materials and technical specifications current as of October 2025. Given the rapidly evolving nature of blockchain technology and digital asset regulation, readers are encouraged to consult the most recent versions of regulatory publications and technical standards.

Where specific press releases or announcements are cited with dates, these represent publicly available information as of the paper's publication date. Readers seeking to verify specific claims should refer to official sources including ASIC's website (asic.gov.au), the RBA's website (rba.gov.au), APRA's website (apra.gov.au) and company investor relations pages.

For legislation and case law, readers should consult official government legal databases such as the Federal Register of Legislation (legislation.gov.au) to access the most current consolidated versions of Acts and Regulations.