Macropod Global AUDM Stablecoin

Whitepaper

ISSUED BY CATENA DIGITAL PTY LTD

28 OCTOBER 2025

Table of Contents

Executive Summary ***2***

1. Blockchain & Stablecoin ***4***

2. Regulation ***6***

2.1 Financial Services **6**

2.2 Non-Cash Payment Facility **7**

2.3 Reserves **7**

2.4 Financial Transactions **8**

2.5 Reporting **9**

3. Technology ***10***

3.1 Private Key Management **10**

3.2 Token Standards **11**

3.2.1 Smart Contract Auditing 12

3.2.2 Customised Smart Contract 14

3.3 Controls **15**

3.3.1 Off-chain controls 16

3.3.2 On-chain controls 17

3.3.3 Role-Based Access Controls 17

3.3.4 Risk Controls 18

3.3.5 Fiat Payments 19

4. Final Word ***20***

Bibliography ***22***

Executive Summary

Catena Digital Pty Ltd, trading as Macropod Global (**Macropod**) is the owner and operator of the Macropod Platform and issuer of a stablecoin pegged to the Australian dollar (**AUD**) operating on blockchain technology (**AUDM Stablecoin**). Macropod is an Australian Financial Services License (**AFSL**) holder with AUSTRAC registration and operates within Australia's regulatory framework, providing institutional-grade digital payment solutions that bridge traditional banking systems with blockchain infrastructure.

Macropod addresses the critical market need for regionally compliant, fiat-pegged stablecoins in Australia. Unlike volatile cryptocurrencies, AUDM stablecoin is pegged 1:1 to the Australian dollar through reserves held in segregated trust accounts at regulated Australian banks. Macropod serves both retail and institutional customers seeking efficient, transparent, and compliant digital payment solutions that manage currency risk exposure.

Operating under an AFSL (No. 566313), Macropod meets ASIC's stringent regulatory requirements including capital adequacy, risk management, and operational controls. Macropod's AUSTRAC registration requires Macropod to comply with Australia's AML/CTF framework, including customer due diligence, transaction monitoring, and suspicious activity reporting. This regulatory foundation provides the necessary trust and confidence for institutional adoption while maintaining transparency and auditability.

AUDM Stablecoin is deployed on the Ethereum blockchain using enterprise-grade smart contracts built on audited OpenZeppelin standards. The Macropod Platform employs Multi-Party Computation (**MPC**) for secure private key management, eliminating single points of failure while enabling threshold signing for administrative operations. Role-Based Access Controls (**RBAC**) segregate operational duties across business functions, ensuring no single entity controls multiple critical operations.

The Macropod Platform incorporates institutional-grade compliance features including access controls, transaction monitoring, and recovery mechanisms. AUDM Stablecoin smart contracts include "DenyList" functionality for sanction compliance, token recovery capabilities for AML/CTF requirements, and pause/unpause functions for emergency risk control. Operations are subject to

maker/checker processes requiring multi-factor authentication and biometric verification.

Macropod integrates with Australia's New Payments Platform (**NPP**) for seamless fiat on-ramp and off-ramp capabilities, supporting traditional banking methods. Macropod maintains at-call deposits as reserves, ensuring sufficient liquidity for stablecoin redemptions.

As digital assets mature, Macropod's regulated approach means it is positioned to capture growing demand for stable, compliant digital payment solutions in Australia. Macropod's multi-chain deployment strategy, starting with Ethereum and expanding to other **Ethereum Virtual Machine (EVM**) compatible chains, ensures broad accessibility while maintaining consistent regulatory compliance and security standards.

Macropod represents a strategic investment in Australia's digital financial infrastructure, combining regulatory compliance, technical innovation, and a market opportunity to create a sustainable platform for the future of digital payments.

1. Blockchain & Stablecoin

Blockchain is a decentralised digital ledger that records transactions across a network of computers, ensuring that data are secure, transparent, and tamper-proof. Individual transactions are grouped into a block and, once verified, the new block is linked to the previous block. This chain of blocks - the blockchain - makes it nearly impossible to alter past records without changing subsequent blocks. All network participants must reach consensus on the newest block before it is added to the chain.

Gas is the fee required to execute operations on blockchain networks, representing the computational work performed by the network to validate and process transactions. Gas fees are paid in the blockchain's native cryptocurrency.

Stablecoins are a class of digital asset token. Unlike cryptocurrencies, stablecoins are intended to maintain a stable value relative to a reference asset, typically a fiat currency such as **AUD**. A stablecoin issuer controls the supply of tokens and stabilises the value through the exchange of the reserve asset for new tokens. Cryptocurrencies like Bitcoin[1] and Ethereum[2] experience high price volatility. Whist stablecoins operate on the same blockchain technology as cryptocurrencies, stablecoins are issued in exchange for the reference asset and seek to maintain a stable value relative to that reference asset. Stablecoins, therefore, offer the same fast, borderless transactions and programmable money capabilities as cryptocurrencies without the price uncertainty. A stablecoin provides fiat monetary value on a blockchain. For stablecoin operations, gas fees ensure secure and efficient processing while maintaining the network's decentralised consensus mechanism.

Smart contracts are self-executing computer programs that automatically enforce the rules governing token creation, destruction, and transfer without requiring intermediaries. Smart contracts contain the business logic for **minting** (creating new tokens), **redeeming** (burning tokens) and **transferring** (moving token balances between wallets), and are the foundational infrastructure for stablecoins. The stablecoin issuer deploys the stablecoin smart contract on a blockchain using a private key and paying gas fees, in the form of the native token of that blockchain. Ethereum is a blockchain that implements smart contract technology and is the blockchain of choice for most stablecoins. Other blockchains with smart contract capabilities include Redbelly Network and Solana.

A **private key** is a secret cryptographic code that provides control of a blockchain wallet address. The wallet securely stores digital asset balances like cryptocurrencies or stablecoins and controls access to smart contracts deployed by that wallet address. The process of submitting a transaction to a blockchain, with the associated private key, is called **signing**.

Users with a wallet address on the blockchain purchase a stablecoin by paying the reference asset — typically fiat currency — to the stablecoin issuer. In response the stablecoin issuer instructs the smart contract to mint a new token directly into the user's blockchain wallet. Minting a new token increases both the total supply of stablecoins and reference asset reserves. Conversely, when users redeem a stablecoin, the smart contract burns the token and the corresponding reference asset is paid to the user, reducing the total stablecoin supply and reference asset reserves.

This mint and redeem mechanism ensures the stablecoin maintains its 1:1 peg to the reference asset while providing transparency and trust through immutable, auditable code executed on the blockchain. The issuer provides a two-way exchange between the stablecoin and reference asset and holds the reference asset, or equivalent, in reserve in order to balance the supply and value. The mechanism functions to achieve price stability.

Users of stablecoins can make a payment by transferring the tokens to other users. User-to-user transfers are controlled by the stablecoin smart contract, which is the self-executing program through which payments are made.

> **Macropod is a stablecoin issuer operating in Australia. Macropod issues AUDM Stablecoin, an Australian dollar-pegged stablecoin on blockchain networks. The reference asset for AUDM Stablecoin is AUD. The AUD received by Macropod is held on trust for holders of AUDM Stablecoin and is segregated from the other assets of Macropod.**

2. Regulation

The issuance of stablecoins on-chain combined with the holding of reference asset reserves, firmly places an issuer within the scope of laws governing financial services.

2.1 Financial Services

Australian law governs the provision of financial services through a regulatory framework designed to ensure the integrity, stability, and fairness of the financial system[3]. The primary regulatory authority is the Australian Securities and Investments Commission (**ASIC**), which exercises powers granted under the *Corporations Act 2001 (Cth)* (**Corporations Act**)[4] to administer and enforce financial services laws. ASIC has responsibility for licensing financial service providers, monitoring compliance with legal obligations, and enforcing laws to protect consumers and maintain market confidence.

Under the Corporations Act any person — including individuals or companies — who carries on a financial services business in Australia must hold an **Australian Financial Services Licence (AFSL)**, unless an exemption applies[5].

Licensing requirements are primarily set out in section 912A of the Corporations Act and explained in ASIC's Regulatory Guides (e.g. RG 104 Licensing: Meeting the general obligations and RG 166 Licensing: Financial requirements). Licensing requirements help ensure that financial services are offered by qualified and reputable entities, which in turn protects the interests of consumers and promotes a robust financial system.

Licensing obligations include demonstrating competence, adequate financial and human resources, and adequate risk and compliance controls.

A **Responsible Manager** is a key individual nominated by an AFSL applicant or licensee to demonstrate to ASIC the organisation's competence. ASIC assesses whether a Responsible Manager has the necessary knowledge, skills, and experience to provide financial services efficiently, honestly, and fairly. Responsible Managers must have direct responsibility for significant day-to-day decisions related to service delivery and compliance under ASIC Regulatory Guide 105[6].

Macropod holds an Australian Financial Services Licence issued by ASIC and has appointed two executives of Macropod as Responsible Managers[7].

2.2 Non-Cash Payment Facility

A Non-Cash Payment Facility is a facility through which, or through the acquisition of which, non-cash payments are made[8]. A non-cash payment is any payment that does not involve cash, such as electronic payments, and a facility is an arrangement such as a legal contract. A Non-Cash Payment Facility is regulated as a financial product. Organisations offering Non-Cash Payment Facilities provide a financial service.

In Australia, fiat-backed, non-yield stablecoins are considered by ASIC to be a Non-Cash Payment Facility and therefore a financial product. The issuer is responsible under the legal contract for minting stablecoins and ensuring that stablecoins can be redeemed for an equivalent value in fiat currency. The minting and redemption processes are subject to regulatory obligations, including license conditions and compliance with capital requirements. The regulatory obligations reinforce the integrity and security of the payment system.

Macropod, which mints and redeems stablecoins in exchange for fiat currency, is authorised under an AFSL to issue a Non-Cash Payment Facility. The AFSL number is 566313 [7].

2.3 Reserves

To maintain sufficient reserves to meet stablecoin redemptions, a stablecoin issuer must hold in reserve the reference asset, or equivalent. Stablecoin issuers must also hold additional capital. The capital requirements are a licence requirement for issuers of Non-Cash Payment Facilities.

Reserves function solely to support the redemption of stablecoins and are segregated from the issuer's operating capital. Regular audits and transparency reports verify that the reserves backing the stablecoin are sufficient and properly managed in compliance with Australian financial regulations.

Macropod issues an AUD-linked stablecoin (AUDM Stablecoin) and holds AUD, or cash equivalent assets, as reserves in Australia. This is designed to offer 'at call' liquidity suitable for the immediate redemption of all AUDM

Stablecoins issued. All reserves and supporting capital are held with highly rated and regulated Authorised Deposit-Taking Institutions operating in Australia (i.e., banks). Macropod's reserves are maintained in a trust on behalf of the holders of the AUDM Stablecoin, which provides legal protection of the reserves and therefore the redemption process, from Macropod's liabilities.

2.4 Financial Transactions

Australian Transaction Reports and Analysis Centre (**AUSTRAC**) is Australia's primary financial intelligence unit and anti-money laundering and counter-terrorism financing (**AML/CTF**) regulator. Australian organisations involved in financial transactions - **designated services** - are subject to regulatory oversight to combat financial crimes.

Providers of designated services are deemed **reporting entities**. AUSTRAC monitors compliance with the AML/CTF Act[9] by businesses that provide designated services. The AML/CTF Act establishes a regulatory regime designed to protect the Australian financial system from exploitation by money launderers, terrorists and other threats.

The AML/CTF Act establishes customer due diligence requirements. Designated service providers must have robust customer identification and verification procedures that enable them to establish and maintain accurate information about their customers' identities, beneficial ownership structures, and the intended nature of their business relationships.

The AML/CTF Act also requires reporting entities to implement enhanced due diligence measures for high-risk customers, including politically exposed persons, customers from high-risk jurisdictions, and customers engaged in high-risk activities. These enhanced due diligence measures may include additional verification requirements, more frequent monitoring of customer relationships, and enhanced scrutiny of customer transactions.

The AML/CTF Act imposes transaction monitoring and reporting requirements on reporting entities, mandating the implementation of systems for the purpose of detecting and reporting suspicious transactions and activities.

Macropod offers the exchange of AUD for digital asset tokens, which is a designated service under the AML/CTF Act. Macropod is registered with

AUSTRAC (DCE100887005-001) and has provided AUSTRAC with detailed information about its organisation, business operations, ownership structure, and compliance capabilities. AUSTRAC registration requirements include ongoing obligations to report changes in business operations, ownership structures, and compliance arrangements.

2.5 Reporting

Designated service providers are required to file Suspicious Matter Reports with AUSTRAC when they have reasonable grounds to suspect that a transaction or attempted transaction involves proceeds of crime, is related to terrorist financing, or constitutes money laundering.

Macropod uses on-chain analysis of AUDM Stablecoin transactions to generate Suspicious Matter Reports for reporting to AUSTRAC.

3. Technology

Regulatory obligations require AFS licensees to operate efficiently, honestly, and fairly[10,11]. An AFS licensee's risk management systems must be supported by technology that is fit for purpose, scalable to business operations, and integrated with compliance and reporting systems[11]. Risk management expectations specific to responsible entities can be found in ASIC **Regulatory Guide 259** which includes guidance on implementing technology systems. ASIC stipulates that cybersecurity is an AFSL obligation, and requirements include strong password protection and access controls, incident response and business continuity plans, and regular reassessment of cyber risks and controls. ASIC recommends following the **Australian Cyber Security Centre**'s 'Essential Eight' mitigation strategies[12]. All AFS licensees must ensure that sensitive consumer information is protected. Protection measures include secure data storage and transmission, policies for data access and breach response, and minimisation of the risk of consumer harm from data misuse or loss.

3.1 Private Key Management

AFS licensees must protect private keys to stop unauthorised access to digital assets or smart contracts and provide a secure and reliable service for stablecoin users. An AFS licensee operating on a blockchain must ensure that private keys are managed such that they are secure from both internal and external threats.

Multi-Party Computation is one approach to private key management[13]. While traditional key management systems rely on a single private key stored in either a hardware security module or hot wallet, Multi-Party Computation distributes the private key across multiple parties or devices, which ensures no single entity possesses the complete key. Multi-Party Computation, therefore, eliminates single points of failure while maintaining security and functionality, reducing the risk of threats.

Multi-Party Computation enables **threshold signing**, where transactions are executed only when the predetermined number of parties — the threshold — collaborate to sign. Threshold signing allows digital asset transactions to be signed in a single round, vastly increasing transaction speed while maintaining enterprise grade security.

Macropod uses Multi-Party Computation to manage private keys controlling wallets and access to smart contracts, providing robust security and operational efficiency. Macropod also employs threshold signing to perform administration functions (e.g. smart contract deployment). Threshold signing is performed by Responsible Managers and satisfies regulatory obligations for key operations.

3.2 Token Standards

The **ERC-20**[14] token standard interface was designed to maximise compatibility between tokens, including stablecoins, using the Ethereum blockchain. The standard defines six mandatory functions to ensure all ERC-20 tokens can interact seamlessly with wallets, exchanges, and decentralised applications:

1. *totalSupply()* - querying total token circulation
2. *balanceOf(address)* - checking account balance
3. *transfer(address, amount)* - direct transfer to wallet - addresses the "**through which non-cash payments are made**" in Section 2.2
4. *transferFrom(address from, address to, uint256 amount)* - delegated transfer to wallet - also addresses the "**through which non-cash payments are made**" in Section 2.2
5. *approve(address spender, amount)* - authorising third-party spending limits
6. *allowance(address owner, address spender)* - querying approved spending amounts

The ERC-20 standard is augmented with ERC-2771[15], which implements gasless transactions. Both standards have been implemented using open source libraries and are widely used to deploy stablecoin smart contracts.

Macropod has issued AUDM stablecoin as an ERC-20 token on the Ethereum and Redbelly Network[16] blockchains, and also uses ERC-2771 contracts to manage transfers.

3.2.1 Smart Contract Auditing

OpenZeppelin

Even when leveraging standard smart contract libraries, independent security auditing is crucial to ensure robustness. **OpenZeppelin** – an open-source framework for secure blockchain development – provides a comprehensive suite of audited, community-vetted smart contract components[16]. OpenZeppelin's library implements widely used Ethereum standards (e.g. ERC-20 for fungible tokens) with a focus on security and best practices. Its codebase is known for high quality, being clean, modular, and following industry best practices according to independent audits.

OpenZeppelin upgradeable smart contract

Technical Explanation: OpenZeppelin supports an upgradeable contract architecture through the **Universal Upgradeable Proxy Standard (UUPS)**, defined in Ethereum's ERC-1822 proposal. This proxy pattern separates a token's **storage (state)** from its **implementation (logic)**. In practice, the token is deployed via a proxy contract that holds all permanent data, while delegate-calling an implementation contract that contains the functional logic. This design maintains state and user data integrity across upgrades. It allows deploying new logic – for example, to patch a security issue or add features – without disrupting or migrating existing token balances and user addresses. Authorization checks (e.g. only an owner or governance contract can upgrade) are built-in to the upgrade framework to ensure only trusted parties initiate upgrades. The UUPS proxy pattern is minimal and gas-efficient, and it conforms to the standardized proxy storage scheme (ERC-1967) to avoid storage collisions. In summary, using OpenZeppelin's upgradeable contracts enables future improvements to the token contract while **minimising disruption** to users.

What this means: OpenZeppelin has created smart contract architecture that splits a token into two parts: one part stores all the user information — like wallet balances — and the other part contains the operating instructions. If a token issuer needs to fix bugs or add new features, they can replace the instruction part, while keeping user data secure and unchanged. Only authorised parties can implement these upgrades. This allows token issuers to improve their products over time, without disrupting users.

OpenZeppelin – audit trail

Technical explanation: OpenZeppelin-based smart contracts incorporate **audit trail features** via comprehensive event logs emitted for every critical operation. Key administrative actions such as ownership transfers, role grants, token movements, and access control decisions trigger events (e.g. OwnershipTransferred, RoleGranted, Transfer, Approval) that are recorded on the blockchain ledger. These events form an immutable, timestamped log of all important activities. Once an event is recorded on the decentralised ledger, it cannot be altered or removed, providing a tamper-proof history of the contract's behaviour. Such on-chain audit trails greatly simplify compliance reporting and regulatory examination, since auditors can independently verify all administrative and token transfer events against the public ledger. In effect, the smart contract itself maintains a **self-auditing** record of its operations. OpenZeppelin's tooling further supports capturing and monitoring these events, underscoring the emphasis on transparency and accountability. By using OpenZeppelin libraries, the token inherits these proven event emission patterns, ensuring that compliance audits have access to a complete and trustworthy activity log.

What this means: OpenZeppelin smart contracts keep permanent records of everything. Every time someone uses the token the system automatically records this on the blockchain. These records can never be deleted or changed. This makes it easy for auditors and regulators to see the complete history of every transaction and event.

> **Macropod has chosen an enhanced version of ERC-20 that follows OpenZeppelin standards to provide functionality for risk, compliance and governance controls. This will allow Macropod to upgrade the smart contract without significant disruption to AUDM Stablecoin users. Macropod smart contracts have been deployed using code independently audited by OpenZeppelin[17,18]. Other blockchains will follow, with EVM compatible chains representing a lower barrier for deployment by using the existing smart contracts. Macropod deployed AUDM Stablecoin with audit trail features ensuring complete transparency for AUDM Stablecoin users and regulators.**

3.2.2 Customised Smart Contract

Access Registry (Allow/Deny Lists)

Smart contracts issuing stablecoins can delegate access control to a specialised registry contract for dynamic compliance management. In practice, this means the token's smart contract queries an external **Access Registry** to decide if a given address is permitted to interact — hold or transfer token balances. This registry maintains an **AllowList** (addresses explicitly permitted) or a **DenyList** (addresses barred from participation) on-chain. Crucially, these lists can be updated or expanded **without altering the token contract**, allowing compliance updates in real time. Multiple token contracts (i.e., several stablecoins by one issuer) may even point to the **same registry contract**, ensuring consistent enforcement across products.

This dual approach enables compliance with regulatory requirements, allowing institutions to block sanctioned addresses or restrict access to verified participants only. The access control mechanisms provide support for regulatory requirements and Know Your Customer (**KYC**) requirements.

Token Recovery (Address Seizure)

Authorised administrators may claw back tokens from addresses that become disallowed (i.e., added to the DenyList). This feature ensures that tokens held by an ineligible address can be removed or reassigned in compliance with regulations. OpenZeppelin's libraries make such **token recovery** possible through privileged roles. For example, a Recovery role is able to **forcibly transfer or burn tokens** held by an address that "has lost access". In practical terms, if an investor's address is later sanctioned or found to violate terms, the issuer can retract the tokens from that address – preventing those funds from remaining in limbo or being used illicitly.

Contract Uniform Resource Identifier (On-Chain Metadata Reference)

The token contract provides a pointer to an external Uniform Resource Identifier containing metadata and documentation about the token. By design, this metadata is stored off-chain in a decentralised manner making it censorship-resistant, tamper-evident, and **permanently accessible** to stakeholders. The Uniform Resource Identifier content typically includes the token or project name, a description, logos or images for branding, and relevant external links. In a regulatory context, this can point to the latest compliance documentation, legal

disclosures, or even a security contact for vulnerability reporting. The smart contract holds only a pointer and ensures that **anyone** (i.e., investors, exchanges, auditors) can fetch the token's current official documentation directly from the blockchain reference, confident that it's the issuer's authentic and up-to date publication. This melding of on-chain reference with off-chain storage provides the best of both worlds: a **permanent, verifiable record on-chain** that points to detailed, human readable information stored off-chain, thereby meeting legal disclosure requirements without cluttering the blockchain with large documents.

> **Macropod has deployed AUDM Stablecoin with an Access Registry that implements a DenyList. This function enables Macropod to comply with our sanction obligations. AUDM Stablecoin is also deployed with a recover function as an additional compliance control, the access to this is restricted to the compliance business function. Finally, AUDM Stablecoin is also deployed with a Contract URI function to provide holders of the token timely access to the latest legal documentation.**

3.3 Controls

An AFS licensee must have risk management systems embedded into the technology to prevent unauthorised access. This would generally include controls to govern the submission and signing of on-chain transactions with both on and off-chain controls.

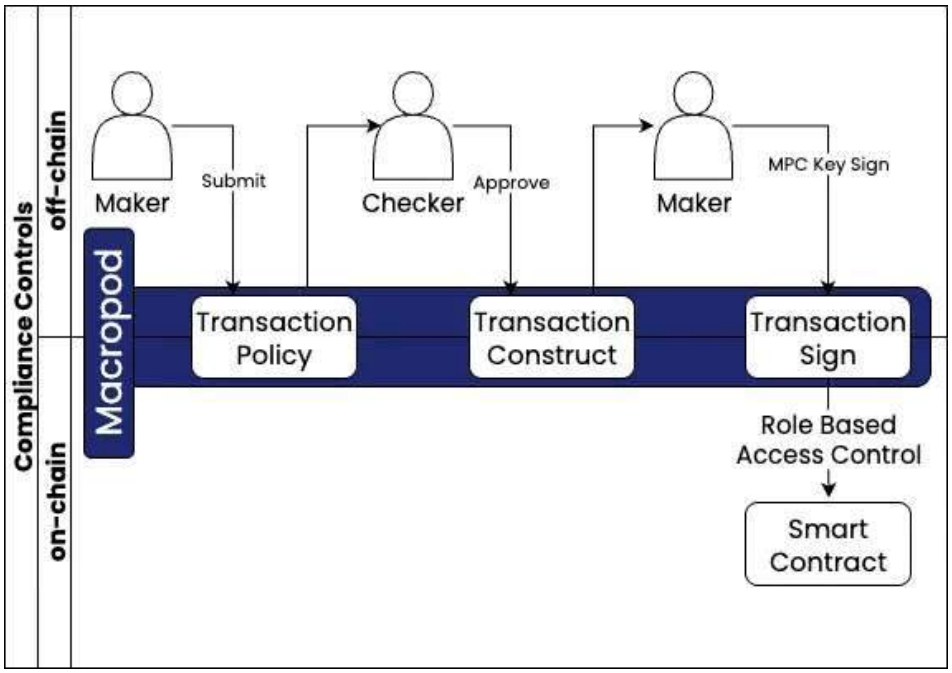

Figure 1: Transaction Security Controls

Macropod uses two types of controls implemented at the system level: controls implemented off-chain — prior to signing — and those that operate on-chain as part of the smart contract. The flow of these controls is illustrated in Figure 1 and implements a maker/checker process.

3.3.1 Off-chain controls

A **Transaction Authorisation Policy** enables stablecoin issuers to define granular rules around who can initiate, approve, and sign transactions submitted to the blockchain. These policies are implemented before any private key signing and also require multiple authorised individuals to participate in transaction signing, thereby reducing the risk of fraud and unauthorised activity. Additional granular off-chain rules governing initiation, approval, and signing should also include the segregation of key operations between business functions. This segregation is called Role-Based Access Controls.

The activity of any token on a blockchain is public and viewable on a block-explorer. The blockchain records the wallets a stablecoin moves between and other smart contracts with which it interacts. This gives a complete history of where the token goes and what it does. A stablecoin issuer can manage AML/CTF risk with the application of a Know-Your-Transaction policy to monitor these transactions for financial crime.

Macropod applies a Transaction Authorisation Policy before a transaction is constructed for signing. This policy is customisable and any proposed change requires a quorum of the Responsible Managers and/or Executives. Approval requires multi-factor authentication, passphrase and biometric verification. Macropod has implemented RBAC to segregate duties across key business domains — namely operations, compliance, and technology. This ensures no single group or actor has unilateral control over multiple critical functions. Finally, Macropod monitors the activity of AUDM Stablecoin with an off-chain process and applies a risk rating to the wallets with which AUDM Stablecoin interacts. This includes monitoring attempts to transact with known sanctioned entities and high risk activities.

3.3.2 On-chain controls

A smart contract contains multiple functions which are accessed through the blockchain. The functions have two types; either **read** or **write**. The read functions do not require a private key to access, they only return some characteristic — current state — of the smart contract, such as the name or ticker code. A write functions requires a private key to access, which performs some action on the smart contract that changes the current state — such as minting new tokens.

A stablecoin smart contract can be designed to grant access to write functions — such as minting — to a specific private key (i.e., a specific wallet). Applying such a control framework on a smart contract to segregate functions to different private keys is also called Role-Based Access Controls , this time at the smart contract level not business function.

> **Macropod has implemented RBAC to segregate smart contract operations across multiple private keys — mint/burn (operations), various contract administration functions (technology), and stablecoin Denylist/salvage/ recovery functions (compliance). This ensures no single group or actor has unilateral control over multiple critical operations.**

3.3.3 Role-Based Access Controls

RBAC provides granular permission management of operations. The modular design approach can be applied to all smart contracts governing a token.

> **Macropod has implemented RBAC with an architecture that segregates duties between business functions and is shown in Figure 2.**

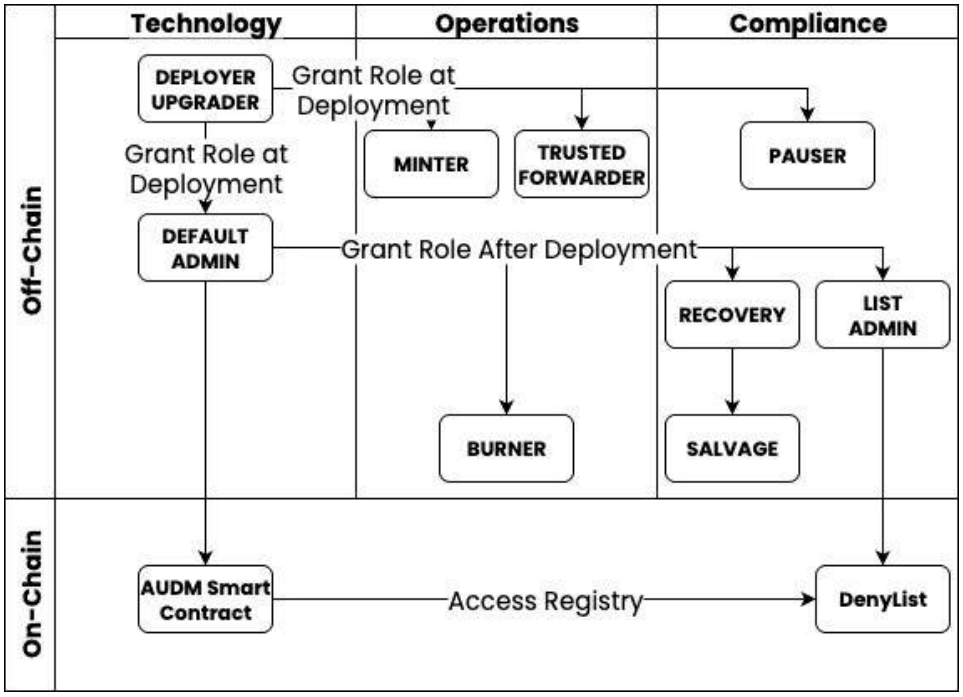

Figure 2: Role Based Access Controls

3.3.4 Risk Controls

Part of the OpenZeppelin contract library defines a **pause** mechanism, such that a token smart contract can immediately suspend all token operations during security incidents or regulatory actions. When paused, all transfer, mint, and burn operations are blocked. This provides a critical safety mechanism for institutional deployments, where regulatory compliance, security incidents, or operational emergencies may require immediate suspension of token operations. It halts all token transfer operations while preserving the underlying token balances and contract state. When a contract is paused, the "whenNotPaused" modifier prevents execution of core transfer functions.

This effectively freezes all token movements across the network.

Importantly, while transfers are blocked during the paused state, administrative functions such as contract upgrades, role management, and access control updates remain operational, allowing administrators to implement necessary fixes or policy changes. The pause state is reversible through an **unpause** function, which restores normal token operations once the emergency has been resolved. This dual-state system provides a robust safety mechanism that balances operational flexibility with emergency response capabilities, making it a

useful feature for institutional token deployments where risk management and regulatory oversight are paramount concerns.

> **Macropod has deployed AUDM stablecoin with a pause/unpause function as a risk control. The access to this is restricted to the compliance function.**

3.3.5 Fiat Payments

Finally, the integration with traditional banking systems requires the coupling of decentralised and centralised systems. In Australia this can be achieved by connecting a stablecoin issuer to a variety of payment gateways.

> **Macropod has integrated into the New Payments Platform[19], creating an on/off ramp for converting AUD reserves into AUDM Stablecoin tokens on a blockchain. The New Payments Platform offers almost instant settlement of AUD into Macropod's reserve account, and likewise from Macropod's reserve account into an account of the AUDM Stablecoin holder on redemption. A representation of this system is shown in Figure 3.**

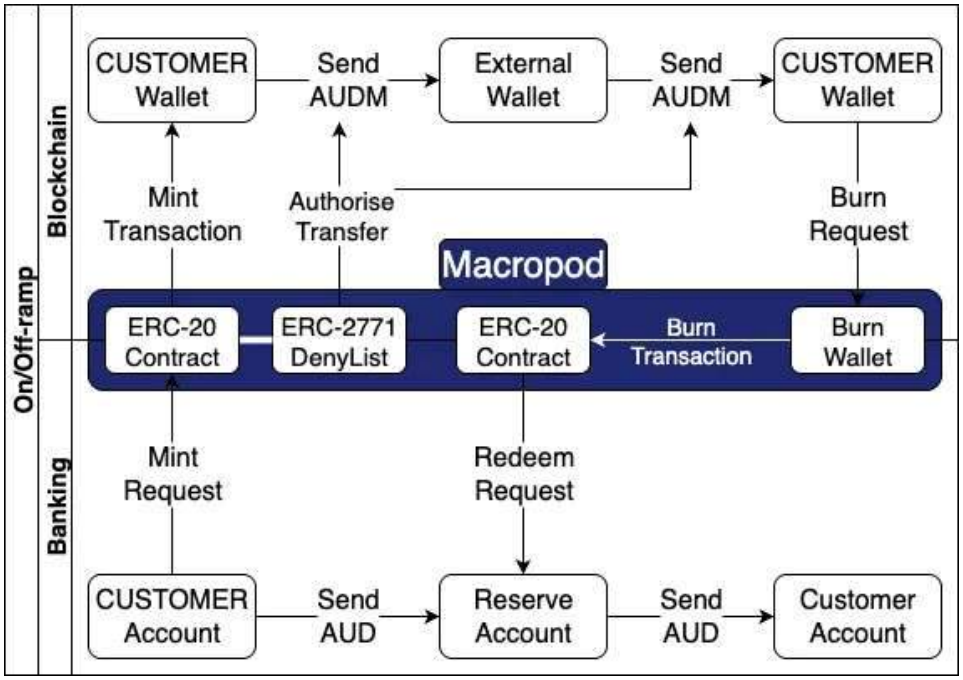

Figure 3: on/off-ramp of AUD into AUDM stablecoin and back to AUD

4. Final Word

The Macropod Platform and AUDM Stablecoin represent a significant advancement in Australia's digital financial infrastructure, bridging the gap between traditional banking systems and emerging blockchain technology. By issuing AUDM Stablecoin, an Australian dollar-pegged stablecoin, Macropod addresses a critical market need for compliant, fiat-pegged digital assets that maintain price stability while offering the benefits of blockchain-based transactions.

As an AFSL-holder and AUSTRAC registrant, Macropod operates within a regulatory framework that prioritises consumer protection, financial stability, and compliance with regulatory requirements. This regulatory oversight provides the necessary trust and confidence for institutional adoption while maintaining the transparency and auditability that blockchain technology enables.

From a technical perspective, Macropod's implementation demonstrates enterprise-grade security and operational excellence. The use of Multi-Party Computation for private key management, Role-Based Access Controls for operational segregation, and upgradeable smart contracts built on audited OpenZeppelin standards create a robust foundation for institutional use. The integration with Australia's New Payments Platform ensures seamless fiat on-ramp and off-ramp capabilities, making the platform accessible to both retail and institutional users.

The compliance features embedded within the AUDM Stablecoin token—including access controls, transaction monitoring, and recovery mechanisms—demonstrate Macropod's commitment to meeting regulatory obligations while maintaining operational efficiency. These features are particularly important in the context of Australia's AML/CTF framework and the need for ongoing monitoring of digital asset transactions.

Macropod's approach to reserve management, with reserves held in segregated trust accounts on behalf of AUDM Stablecoin holders, provides the necessary mechanism for maintaining the stablecoin's peg to the Australian dollar. This conservative approach to reserve management aligns with regulatory expectations and ensures Macropod can meet redemption requests even during periods of market stress.

The platform's deployment on multiple blockchains, starting with Ethereum and Redbelly Network, demonstrates a commitment to interoperability and accessibility. This multi-chain approach allows users to access AUDM Stablecoin across different blockchain ecosystems while maintaining the same regulatory compliance and security standards.

As the digital asset ecosystem continues to evolve, Macropod's regulated approach positions it as a trusted partner for institutions seeking to leverage blockchain technology for payments and financial services. The platform's focus on compliance, security, and operational excellence provides a foundation for sustainable growth and adoption in the Australian market.

The success of Macropod will depend not only on its technical implementation but also on its ability to navigate the evolving regulatory landscape and build trust with users, regulators, and financial institutions. By maintaining its commitment to regulatory compliance, operational transparency, and technological innovation, Macropod has the potential to become a cornerstone of Australia's digital financial infrastructure.

In conclusion, Macropod represents a thoughtful and well-executed approach to bringing regulated stablecoins to the Australian market. The platform's comprehensive regulatory compliance, robust technical architecture, and focus on operational excellence creates a foundation for sustainable growth and adoption. As the digital asset ecosystem matures, Macropod's regulated approach positions it well to serve the growing demand for stable, compliant, and efficient digital payment solutions in Australia.

Bibliography

[1] Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*

[2] Buterin, V. (2013). *Ethereum: A next-generation smart contract and decentralized application platform*

[3] ASIC. (2024). *Our vision: A fair, strong and efficient financial system for all Australians*.

[4] Chapter 7, *Corporations Act 2001* (Cth).

[5] Section 911, *Corporations Act 2001* (Cth).

[6] ASIC. (June 2022). *Regulatory Guide 105: AFS licensing: Organisational competence*

[7] ASIC. Professional Registers: AFSL 566313.

[8] Section 763D, *Corporations Act 2001* (Cth).

[9] *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth).

[10] Section 912, *Corporations Act 2001* (Cth).

[11] ASIC. (June 2022). *Regulatory Guide 104: AFS licensing: Meeting the general obligation*

[12] Australian Signals Directorate. (November 2023). *Essential Eight explained*.

[13] Fireblocks. (October 2024). What is MPC

[14] Ethereum. (2024). ERC-20.

[15] Ethereum. (July 2020). Ethereum Improvement Proposals, no. 2771.

[16] Redbelly Network. (July 2025). Whitepaper.

[16] OpenZeppelin. (2025). Contracts.

[17] OpenZeppelin. (2025). Audits.

[18] Fireblocks. (2024). Contract Audit.

[19] Treasury of Australia. (September 2022). *New Payments Platform*.

