ADDX Go

Pioneering Self-Custody in Private Markets
with The Industry Leading Compliant-Ready Wallet

By ADDX

Author
Lai Sep Riang
Co-founder &
Lead Product Manager

Abstract

The transition of private market assets onto public blockchains requires a new generation of infrastructure that balances compliance with user empowerment. This whitepaper presents the ADDX Go Wallet, a pioneering self-custody solution designed specifically for the era of tokenized Real-World Assets (RWAs). It moves beyond the limitations of existing platforms to provide a secure, compliant, and user-centric gateway to the decentralized economy.

The ADDX Go Wallet is built on a robust Multi-Party Computation (MPC) framework that eliminates single points of failure while embedding regulatory oversight directly into its architecture. Its key innovation lies in using Soul-Bound Tokens (SBTs) to transform the wallet into an intelligent access tool, one that programmatically verifies investor eligibility before allowing interaction with regulated securities. This "compliance-by-design" approach is reinforced by a smart contract-level backstop, rendering non-compliant investments impossible.

Validated in a Proof of Concept aligned with the principles of MAS's Project Guardian, the ADDX Go Wallet demonstrates its readiness to set a new market standard. It offers financial institutions and investors a scalable, interoperable, and user-friendly platform that finally unlocks the promise of a truly global and liquid market for private assets.

Acknowledgements

ADDX gratefully acknowledges the pivotal support of the Monetary Authority of Singapore (MAS), which was provided through the Financial Sector Technology and Innovation (FSTI) grant.

This grant not only provided the necessary resources for the research and development of the ADDX Go platform but also served as a crucial validation of our mission to innovate at the intersection of capital markets and decentralized technology.

We are proud that this work contributes to the ambitious vision of Project Guardian and strengthens Singapore's role as a global hub for financial technology. We remain committed to pushing the boundaries of what is possible in the digital finance landscape.

ADDX

Contents

01 | Executive Summary

This paper details the architecture, security framework, and validated results of the ADDX Go Proof of Concept (PoC), a self-custody system engineered to address the fundamental infrastructure deficit in the tokenized Real-World Asset (RWA) market. Historically, private market platforms have operated on private, permissioned blockchains, which provided secure yet isolated "walled gardens." This paper contends that the subsequent phase of market expansion necessitates bridging these regulated assets to public blockchains.

The PoC validates a hybrid Multi-Party Computation and Threshold Signature Scheme (MPC-TSS) wallet architecture designed to serve as this critical conduit. Employing a {2,3}-threshold scheme, it establishes a "Compliance Bridge" for real-time policy enforcement while providing an "Escape Hatch" that ensures a provably non-custodial state for users. We elaborate on how this architecture securely anchors on-chain identity via Soul-Bound Tokens (SBTs) to programmatically govern user access to regulated offerings. Furthermore, we provide a thorough analysis of the security model, addressing risks such as collusion and application-layer threats. The outcomes of the PoC affirm the viability of this model as a secure, compliant, and scalable foundation to unlock the full potential of the RWA economy.

02 | Introduction: From Walled Gardens to Open Ecosystems

The financial industry has arrived at a clear inflection point, propelled by the tokenization of RWAs and the maturation of stablecoins as a settlement layer. The initial wave of private market democratization, which platforms like ADDX pioneered, logically commenced on private, permissioned blockchains. This strategy offered a controlled environment to ensure rigorous adherence to KYC/AML protocols, transactional privacy, and predictable performance, making it an ideal proving ground for establishing trust with both users and regulators.

However, this "walled garden" architecture, while a crucial first step, inherently presents a fundamental obstacle to scale. Its limitations are significant:

- **Fragmented Liquidity:** Assets remain confined within a single platform's ecosystem, unable to access the expansive, global liquidity pools present on public chains like Ethereum.
- **Lack of Interoperability & Composability:** A tokenized private equity fund on a private chain cannot natively serve as collateral in permissionless DeFi lending protocol (e.g., Aave, Compound), be traded on a public decentralized exchange (e.g., Uniswap), or be integrated into diversified portfolio management tools that operate on public networks. This severely curtails the asset's utility.
- **Capped Network Effects:** Growth is limited to the user base a single platform can onboard, precluding access to the millions of existing, active wallets on public blockchains.

The ADDX Go project was conceived as the strategic evolution to resolve this predicament. The objective was not merely to construct a wallet, but to engineer a secure gateway that enables high-value, regulated assets to safely exist and transact on public blockchains, thereby connecting the curated world of private markets to the open, liquid world of Web3.

03 | The Problem Statement: A Trilemma of Custody in a Public Environment

The transition from a controlled private chain to an open public chain magnifies the challenge of custody. Beyond asset security, it introduces critical compliance complexities, especially concerning securities regulations that forbid general solicitation. The problem thus becomes a trilemma of harmonizing three core requirements:

1. **Security & Recovery:** Standard Externally Owned Accounts (EOAs) introduce a catastrophic single point of failure.
2. **Regulatory Compliance:** A robust mechanism is required to enforce investor eligibility rules not just at the point of transaction, but also at the point of discovery, preventing unaccredited investors from viewing offerings for which they are not qualified.
3. **User Self-Sovereignty:** The fundamental value proposition of public chains is user ownership and control.

04 | Proposed Architecture: A Hybrid MPC-TSS Model as the Bridge

The ADDX Go PoC validates a hybrid architecture founded on Multi-Party Computation and Threshold Signature Schemes (MPC-TSS). It is engineered to be the secure bridge from private ecosystems to public ones.

4.1. The {2,3} Threshold Scheme

The system generates three private key shares for each user wallet through a Distributed Key Generation (DKG) process, with a signature threshold of two (t=2, n=3) required for authorization. The shares are distributed to create a deliberate balance of power:

- **Share 1 (Device Share):** Stored in the secure enclave or equivalent hardware-level keystore of the user's mobile device.
- **Share 2 (Recovery Share):** Stored in the user's personal, encrypted cloud backup (e.g., Google Drive, iCloud).
- **Share 3 (Policy Share):** Held within ADDX's secure, hardware-based infrastructure.

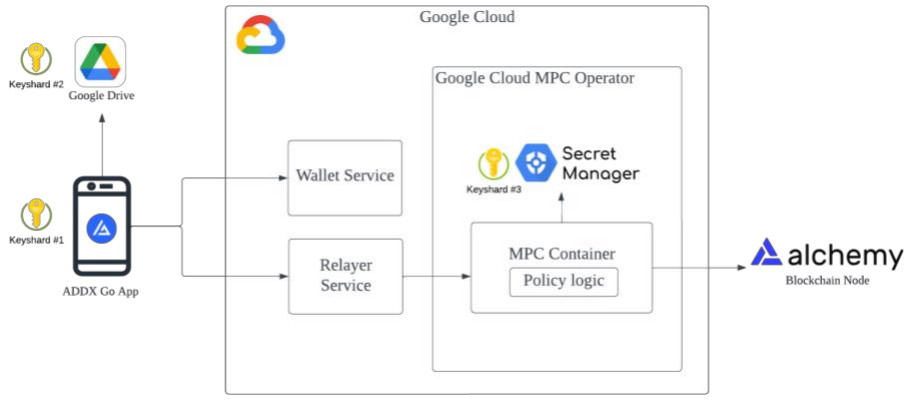

Figure 1. Overview of the Hybrid MPC-TSS Architecture, illustrating distribution of keyshards

4.2. The Wallet as a Dynamic Key: Gating Access with Soul-Bound Tokens (SBTs)

The wallet's most potent compliance function is its role as a "dynamic key," utilizing SBTs to manage access to the platform's core offerings. This constitutes a two-layered approach:

- **Layer 1: UI-Level Access Gating:** Before a user can view or interact with the "Private Markets" section of the ADDX Go application, a local check is performed for a valid KYC/Accreditation SBT in the user's wallet. The absence of this SBT renders the section inaccessible, ensuring compliance with securities marketing laws by preventing general solicitation to non-qualified individuals.
- **Layer 2: Smart Contract-Level Enforcement:** This UI gate is reinforced by an immutable on-chain enforcement mechanism. The smart contract for each RWA offering is programmed to require the presence of the relevant SBT in an investor's wallet before it will accept any funds. This provides a cryptographically secure backstop, rendering non-compliant investment impossible.

4.3. The "Compliance Bridge" for Transactions

This is the linchpin for operating securely on a public chain. For standard transactions, the signing ceremony utilizes the Device Share and the Policy Share. This creates a powerful point of intervention where the ADDX MPC node can programmatically enforce compliance rules before a transaction is broadcast to the public network.

4.4. The "Escape Hatch"

A core principle of our architecture is ensuring users are never permanently locked out from their assets due to the unavailability of the ADDX platform. To this end, the system includes an "Escape Hatch" mode. In the event of a prolonged ADDX service disruption, a user can initiate a transaction signing ceremony using only their Device Share and their cloud-backed Recovery Share.

This procedure operates entirely independently of ADDX's online infrastructure and provides an undeniable, cryptographic guarantee of the user's authority over their wallet. It allows them to sign any valid transaction, proving ownership and intent.

It is important to distinguish between transaction signing and transaction settlement. While the Escape Hatch guarantees the ability to sign, the ultimate transfer of the RWA token is still governed by the rules of its on-chain smart contract. For a transfer to succeed, the user's wallet must still hold the required Soul-Bound Token (SBT) attesting to their eligibility. This two-layer system ensures that even in a disaster recovery scenario, the fundamental compliance framework of the asset remains intact.

05 | Security Model & In-Depth Risk Analysis

A secure system is predicated on the principle of defense-in-depth, acknowledging and mitigating risks at every layer.

5.1. Foundational Security Principles

The architecture is designed to protect against both external adversaries and internal failures. The security posture relies not on a single mechanism but on the interplay between cryptographic guarantees, hardware security, and programmatic policy enforcement.

5.2. Trust Assumptions & Threat Model

Threat Actor: We model a sophisticated adversary aiming to exfiltrate user assets by attempting to compromise user devices, cloud accounts, or institutional infrastructure.
Trust Assumptions: We assume the underlying GG18 cryptographic protocol is secure. We also assume the user is the sole controller of their device and cloud account. The system is designed such that even if a single component (device, cloud, or ADDX backend) is compromised, user funds remain secure.

5.3. Mitigation of Institutional Risk via a Hardware-Secured Policy Engine

The primary institutional risk is that ADDX could misuse its role in the transaction process. We mitigate this risk by securing our key share (the Policy Share) within a FIPS 140-2 Level 3 certified Hardware Security Module (HSM). This specialized hardware acts as a secure "policy cage," programmed with specific rules to automatically reject any transaction that violates them.

However, using an HSM is only the first step. To minimize trust, users must be able to verify our system's integrity themselves.

Our roadmap focuses on making our policy engine transparent and verifiable for our users:

- **Remote Attestation:** The user's application will be able to challenge our HSM, which will respond with a cryptographic proof confirming it is running the correct, approved software before any transaction is co-signed.
- **Code Transparency:** We will open-source the code for our policy engine. This allows anyone to audit the rules and verify that the public code matches the software running in our HSM.
- **Public Policy Logs:** All significant updates to the policy rules will be published to a public blockchain. This creates a permanent and unchangeable audit trail that anyone can inspect.

5.4. Mitigation of Application-Layer Threats

The "Compliance Bridge" architecture provides a unique opportunity to mitigate common user-level threats.

- **Address Spoofing and "Dusting" Attacks:** The ADDX Policy Share node maintains a secure, user-specific address book. The UI will prominently flag any transaction to a new, non-vetted address with a clear warning, compelling the user to consciously approve the interaction.
- **Malicious Smart Contract Interaction & Phishing:** The Policy Share cross-references the destination contract against a real-time, aggregated database of known malicious addresses, blocking transactions to known scam contracts outright.

5.5. Liveness and Fault Tolerance

- **Temporary Outages:** If the ADDX Policy Share node is temporarily unavailable, standard transactions will fail gracefully with a clear message, prioritizing security over uptime.
- **Prolonged Outages:** If an outage persists, users are guided via the app and external communications to activate the "Escape Hatch" to manage their assets independently.

06 | PoC Outcomes & Key Validations

6.1. Validation of the Hybrid MPC-TSS Architecture

The PoC demonstrated the end-to-end viability and robustness of the {2,3} MPC-TSS model. Key functional validations included:

Successful Key Generation: The Distributed Key Generation (DKG) process consistently and securely created the three distinct key shares (Device, Recovery, and Policy) and distributed them to their intended locations.

Standard Transaction Flow: The "Compliance Bridge" mechanism was proven effective. Standard transactions, requiring the user's Device Share and the ADDX Policy Share, were correctly co-signed only after passing pre-defined policy checks.

"Escape Hatch" Functionality: The disaster recovery flow was successfully tested, confirming that a user could sign transactions using only their Device Share and cloud-backed Recovery Share, operating entirely independently of the ADDX infrastructure.

This confirmed that the hybrid model is not merely a theoretical construct but a practical and resilient architecture for guarded self-custody.

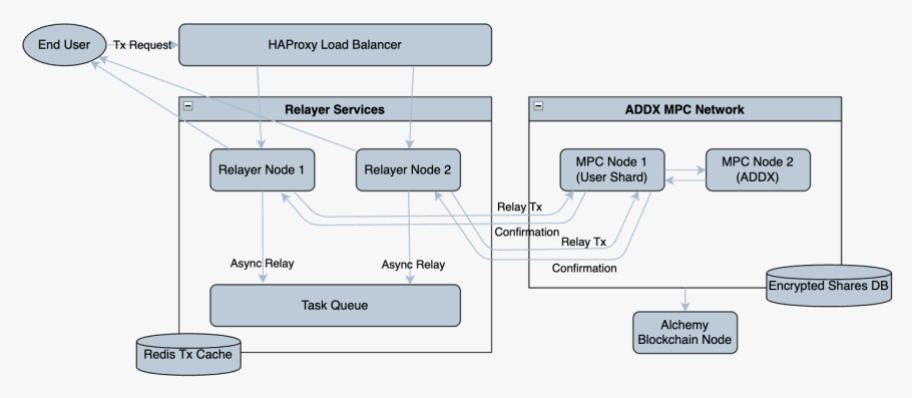

Figure 2. Implementation of Relayer & MPC services and integration to Alchemy blockchain nodes

6.2. Demonstration of Programmatic, On-Chain Compliance

A primary objective was to validate the Soul-Bound Token (SBT) workflow as an effective mechanism for automated, on-chain compliance. The PoC confirmed the efficacy of the two-layered approach:

Layer 1 (Access Gating): The application interface successfully restricted access to investment offerings, programmatically checking for the presence of a valid investor SBT before rendering the private market section. This directly addresses rules against general solicitation.

Layer 2 (Transaction Enforcement): At the smart contract level, attempts to transfer assets to a wallet without the requisite SBT were consistently rejected on a public testnet. This provides a cryptographically secure backstop, ensuring that compliance rules are enforced at the point of final settlement.

The outcome validates that portable, on-chain identity credentials like SBTs can automate compliance for both asset discovery and transaction authorization, forming a scalable foundation for regulated digital assets.

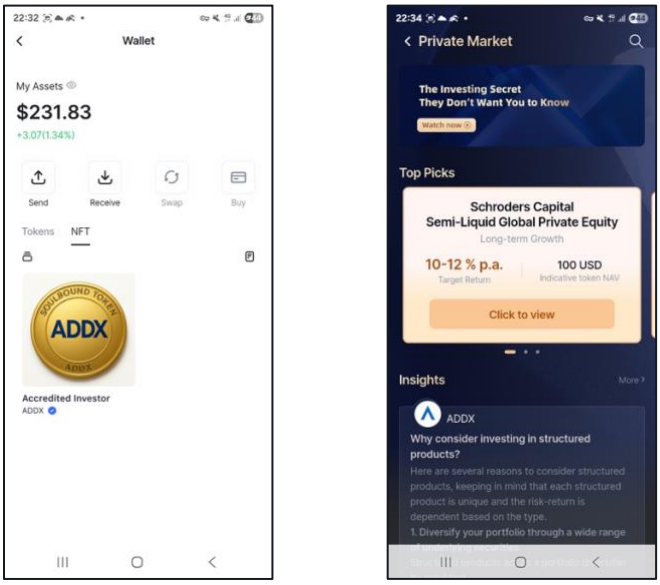

Figure 3. ADDX Go with ADDX Accredited Investor SBT (left), Private Market section after SBT Access Gating (right)

6.3. Performance Benchmarks and Transaction Latency

Quantitative testing was conducted to measure the system's performance under simulated normal load conditions. End-to-end signing latency—from user initiation to the generation of a valid signature—averaged between 800ms and 1.5 seconds.

This performance level was deemed well within acceptable parameters for high-value, low-frequency transactions. For this use case, the marginal increase in latency compared to standard EOA signing is a negligible trade-off for the significant gains in security, compliance, and user-friendly recovery.

6.4. Affirmation of User Experience and Security Model

Elimination of Single Point of Failure: The absence of a user-managed seed phrase was cited as the most significant enhancement. This removed a primary source of user error and anxiety associated with traditional self-custody wallets.

Intuitive Recovery Process: The social-login-based recovery mechanism was perceived as both highly usable and secure, as it aligns with the familiar multi-factor security models of modern financial applications.

The PoC confirmed that abstracting cryptographic complexity through familiar paradigms results in a superior user experience and a mental model of security that users find more trustworthy and approachable.

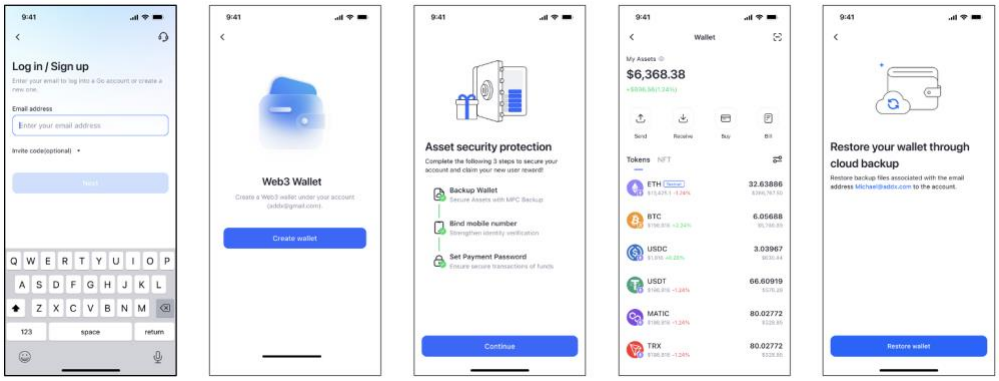

Figure 4. MPC Wallet creation flow

07 | Lessons Learnt

7.1. Security Depends on Provable Institutional Integrity

Our {2,3} MPC design intentionally removes the risk of a single user losing their key. However, this shifts a portion of the security responsibility to the institution holding the third key share (the "Policy Share").

When this shift is made, an institution's operational security must be provable, not just promised. It is not enough to say we are secure; we must demonstrate it. This is why our future work focuses on verifiable systems, like remote attestation and public logs, which allow users to confirm our policy engine is running correctly. Trust must be earned through transparency.

7.2. Designing a Reassuring User Experience for High-Value Transactions

The brief delay (~1 second) during an MPC transaction signing could be seen as a flaw. We redesigned the experience to frame it as a valuable feature. For important transactions, an instant result can feel unsettling.

For high-value operations, the user interface should clearly communicate that security and compliance checks are happening. This turns the short wait into a moment of reassurance. It confirms to the user that the system is working to protect them, making the experience feel more robust and secure.

7.3. Making Security Intuitive Through Familiar Models

Seed phrases are a major barrier for mainstream users. They are a new and unforgiving security method that most people are not prepared to manage.

Complex Web3 security should be mapped to models that people already understand and trust. Our combination of on-device biometrics and encrypted cloud backups mirrors the multi-factor authentication (MFA) used by modern platforms. This provides strong security without forcing users to learn a difficult new process.

7.4. Compliance Must Be Engineered into the System's Core

This PoC proved that compliance cannot be an add-on or a simple interface check. To be effective, it must be a fundamental part of the system's design.

The key lesson is to integrate compliance directly into the cryptographic signature process itself. By requiring the ADDX Policy Share to co-sign transactions, we make it impossible for a non-compliant transaction to be created in the normal flow. This ensures that compliance is not a feature that can be bypassed; it is a core property of every transaction.

7.5. The Need for a New Model: "Guarded Sovereignty"

The concept of "self-sovereignty" in Web3 often implies total, unrestricted control. This ideal is incompatible with regulated financial markets.

The industry needs a more practical model, which we call "Guarded Sovereignty." This model provides a clear balance:

- **User Sovereignty:** Users are protected from platform risk. The "Escape Hatch" guarantees they can always access their assets, even if ADDX goes offline.
- **Regulatory Guardrails:** Transactions must follow the rules programmed into the system, ensuring compliance with securities laws.

This balanced approach protects both the user and the integrity of the market, offering a realistic path to bring high-value assets onto public blockchains.

08 | Future Work & Broader Implications

The successful validation of this architecture provides a foundation for broader ecosystem development.

Standardization of Identity SBTs: Future work involves active collaboration with regulatory bodies and industry peers to develop a common standard for on-chain identity attestations.

Strategic Liquidity Integration: Our ultimate objective is to unlock the composability of RWAs. This requires a strategic approach. Future work will focus on collaborating with leading DeFi protocols to design and build compliant, permissioned liquidity pools. These specialized pools would be architected to interact with our 'Compliance Bridge,' allowing RWAs custodied via the ADDX Go wallet to be used as high-quality collateral. This initiative paves the way for a new class of regulated DeFi, bridging institutional-grade assets with the innovative capital efficiency of decentralized finance.

Intelligent Policy Engine Evolution: Future iterations will integrate machine learning models for anomaly detection, requiring step-up authentication for transactions that are out-of-character for a user.

Institutional-Grade Governance and Policy Controls: To serve the complex operational needs of institutional clients such as asset managers, family offices, and corporate treasuries, the ADDX Go wallet will be enhanced with a suite of enterprise-grade features. Future work will focus on developing a sophisticated governance layer built upon the core MPC architecture. This will include programmable M-of-N transaction approval workflows, granular role-based access controls (RBAC), and dynamic policy enforcement based on transaction size, velocity, or counterparty. An API-first approach will ensure seamless integration with existing institutional treasury and portfolio management systems, transforming the wallet into a comprehensive digital asset management platform for enterprises.

09 | Conclusion

The ADDX Go PoC provides a definitive and holistic solution to the challenges hindering the growth of private market tokenization. It demonstrates that the journey from the safety of private "walled gardens" to the liquid expanse of public blockchains is not only possible but can be achieved with a higher standard of security and regulatory integrity than previously available.

By architecting the wallet as a dynamic key, the system moves beyond simple asset custody. It creates an end-to-end compliant environment where a user's verified on-chain identity—represented by Soul-Bound Tokens—programmatically dictates their access to deal flow, ensuring adherence to securities laws from the moment of discovery to the final settlement. The hybrid MPC-TSS model, with its dual "Compliance Bridge" and "Escape Hatch" modes, proves that the perceived conflict between on-chain self-sovereignty and off-chain regulation is a false dichotomy. This architecture represents the critical infrastructure required to build a more transparent, liquid, and accessible future for all market participants, finally unlocking the multi-trillion-dollar promise of the tokenized economy.

About ADDX

The ADDX platform is established and operated by ICHX Tech. Pte. Ltd. ('ICHX'.) ICHX is regulated by the Monetary Authority of Singapore as a capital markets services licensee for dealing in capital markets products and providing custodial services, and a Recognised Market Operator. Company Registration Number 201731973M.

Disclaimer

This whitepaper is for general informational purposes only and has not been independently verified to ensure its accuracy and fairness. This whitepaper does not constitute any advice from ADDX or ICHX. No representation, warranty, or other assurances of any kind, expressed or implied, is made with respect to the accuracy, completeness, adequacy, reliability validity or availability of any information in this whitepaper. Under no circumstance shall ADDX or ICHX have any liability to the reader for any loss or damage of any kind incurred because of the use or reliance on any information provided in this whitepaper. This whitepaper may not be modified, reproduced, copied, distributed, in whole or in part and no commercial use or benefit may be derived from this whitepaper.