Custody Platform Overview for Institutional Use

AiDAC

July 2025

Table of Contents

Why Secure Custody Matters Now

Physical asset digitization and the transition to a "token-based economy" continue to hold the promise of transforming global finance. From real estate and fine art to commodities, securities, intellectual property, and national currencies, asset tokenization is redefining how traditional financial systems operate—enhancing market liquidity, accessibility, transparency, transaction speed, cost-efficiency, and data immutability.

As blockchain adoption has steadily advanced in recent years, the industry has undergone significant transformation. Notably:

- Over 100 countries have explored or advanced the development of Central Bank Digital Currencies (CBDCs), with several moving beyond pilot programs to limited-scale rollouts or regulatory consultation phases.
- Leading global financial institutions and Fortune 500 companies have deepened their engagement with distributed ledger technologies, transitioning from experimentation to active integration across capital markets, clearing, settlement, and asset servicing.
- The U.S. regulatory landscape has progressed through major milestones, including new rulemaking initiatives by the SEC, CFTC, and Treasury, increased enforcement actions, and legislative proposals aimed at providing clearer frameworks for digital asset markets.

Despite these advancements, the digital asset and cryptocurrency landscapes continue to face perceptions of volatility and risk, driven in part by the financial fallout from high-profile cybersecurity breaches and operational failures.

The number of digital assets, including cryptocurrencies, tokens, and NFTs, now exceeds tens of thousands across public and private blockchains. As tokenization of real-world assets gains momentum across financial and industrial sectors, this number is expected to expand rapidly over the coming years. Successful integration of these new asset classes into traditional finance depends on the availability of robust, institutional-grade digital asset infrastructure, with data custody and key management as core pillars.

In a decentralized token economy, asset holders often serve as their own custodians—particularly among retail participants. This is, however, unlikely the case with institutional shareholders who—primarily due to regulation—opt to delegate data safekeeping to specialized digital asset custodians. Leading consulting and financial institutions in the U.S. forecast sustained and accelerating demand for such institutional custody services.

At its core, secure custody of digital assets revolves around rigorous management of cryptographic key material. A digital asset custody solution is not merely a signing mechanism—it is an integrated system of hardware and software that ensures the secure generation, use, storage, and recovery of cryptographic secrets. Institutional-grade providers differentiate themselves from retail wallets by delivering clearly defined control frameworks, real-time monitoring, risk segregation, and third-party insurance. A complete custodial architecture must address confidentiality, integrity, authentication, availability, scalability, accountability, auditability, and compliance to meet the complex needs of institutional stakeholders.

SYSTEM DESCRIPTION

AiDAC is a highly secure and scalable platform designed to provide institutional-grade custody for digital assets. The platform offers a comprehensive solution for the storage, management, and protection of various digital assets, including cryptocurrencies and tokenized securities. Built upon robust Xen and Linux-based foundations, AiDAC leverages open-source components integrated with proprietary enhancements to deliver a modular, flexible, and secure custody infrastructure tailored to the needs of financial institutions, enterprises, and government agencies.

AiDAC's architecture is designed to uphold the highest standards of security and operational integrity. It employs a multi-layered defense strategy based on Zero-Trust principles, where every component, process, and user interaction is authenticated and monitored. Key security features include secure compartmentalization, multi-signature authorization, offline signing capabilities, and granular access control. AiDAC also supports layered encryption and multi-factor authentication, with optional integration of hardware security modules to enhance the protection of cryptographic keys and sensitive data.

Both warm and cold wallet configurations are supported, enabling institutions to balance security and liquidity requirements. While hot wallets are not a primary design focus and lack native support, they can typically be integrated into the system. The system is primarily deployed and managed on-premises to maintain full control over security and operations. Nevertheless, certain components can be offloaded to the cloud to increase flexibility in resource allocation.

AiDAC's operational framework is engineered for high availability and fault tolerance. Redundancy is provided by automated failover mechanisms and, where applicable, geographically distributed deployments. The system's modular deployment model enhances scalability and flexibility, and also reduces maintenance to ensure optimal system performance.

The system aligns with global security and operational standards, including NIST, ISO, SOC, FISMA, and CIS, and incorporates a compliance framework with logging, audit trails, reporting, real-time monitoring, and automated alerts. This framework enables institutions to meet regulatory requirements and stay current with evolving security standards. The system's native security is enhanced by advanced third-party solutions for access management, intrusion prevention, and SIEM. These integrations provide granular access control, real-time threat prevention, and centralized event monitoring to improve security visibility and incident response.

ARCHITECTURE

The system architecture follows a tiered model, allowing flexible adjustments at higher tiers to meet unique operating demands. The initial tier is entirely open-source, while subsequent tiers can support proprietary modifications and specialized modes to address the institution's specific needs, such as API and HSM integrations. All customizations are carried out under strict oversight to ensure operational integrity while enabling targeted functionality enhancements as needed.

The online system component (Operations Node) operates as a multifunctional layer, managing full blockchain node instances, customer warm wallets, primary backup copies, and various dedicated client-server instances essential for system administration, blockchain operations, secure communication, system security, and logging. The

term "online" is used conditionally, as some components are air-gapped within a virtual environment, while others are restricted to local communication without internet access, depending on their operational requirements. Only a limited set of instances are permitted to establish outbound internet connections. This architecture is designed to prioritize security, with Qubes-OS selected as the preferred operating system due to its robust isolation and security features. In this configuration, client and operational separation is achieved through Qubes-OS's compartmentalization approach, where each virtual machine functions as an isolated environment, completely separated from others. This means that sensitive client data, blockchain operations, and system administration tasks are securely confined within their respective virtual machines, minimizing the risk of cross-contamination or unauthorized access.

The offline system component serves as secure cold wallet storage (Signing Node). This system component remains fully air-gapped within a highly secure physical environment, protected by multiple layers of physical and logical security and strict access controls. Operational redundancy and backup are maintained through a Proxmox cluster, ensuring a highly resilient and fault-tolerant setup. For geo-redundant architectures, the system can scale across multiple regions, communicating exclusively through dedicated, secure channels.

Both system components are deployed on certified enterprise-class hardware to ensure ongoing compliance with stringent industry standards. While the hardware environment allows some configurational flexibility, the Operations Node requires a controlled selection of hardware due to the security and performance demands of the Xen type-1 hypervisor and Qubes-OS. The Signing Node, using Proxmox, offers greater hardware flexibility, as its low overhead allows deployment on any certified platform that meets security and compliance benchmarks. The current infrastructure utilizes HP ProLiant and Dell PowerEdge servers, selected for their compatibility, compliance, and security capabilities. Integration with Hardware Security Modules (HSMs) is restricted to vendors that comply with all relevant cryptographic, security, financial, supply chain, governmental, national, and regional standards.

System resilience is maintained through backup, hardware clustering, and high availability configurations. Each node supports multiple backup implementations, including tertiary backups for the most critical services. Redundancy is achieved through the implementation of hot, warm, and cold spares for the Operations Node, and through Proxmox node clustering and high availability options for the Signing Node.

SUPPORTED ASSETS

Protocol support includes Bitcoin, Lightning, and Ethereum’s ERC-20 standard. The system processes transactions involving Bitcoin (BTC), both on-chain and via the Lightning Network; Ethereum (ETH) for contract execution; and ERC-20 tokens including Chainlink (LINK), Tether (USDT), USD Coin (USDC), and Uniswap (UNI). These assets are handled through defined interfaces within the Operations Node and Signing Node, with all activity subject to enforced transaction policies and system rules. Additional ERC-20 tokens and support for other blockchain protocols are currently in development to broaden the platform’s asset coverage.

SYSTEM ACCESS & ACCOUNT ADMINISTRATION

AiDAC enforces a strict and granular access control model to ensure the integrity and confidentiality of all system operations and client data. Access to system and account functions is managed through a Role-Based Access Control (RBAC) framework, ensuring separation of duties across all key operational layers. Each administrative function is segregated and assigned to designated roles, preventing any single actor from gaining unilateral control over sensitive client assets or data. All client accounts are individually configurable, allowing for customized access levels based on institutional policies.

The system is protected by layered physical and logical security, with all access attempts authenticated, monitored, and logged. Multi-factor authentication (MFA) is a mandatory baseline for all system access. While physical configurations may vary based on deployment needs, baseline physical security measures align with industry best practices for high-assurance IT infrastructure. The Operations Node is typically maintained on-premises and secured by standard physical controls. In contrast, the Signing Node is fully air-gapped and housed within a certified high-security facility—such as an ISO/IEC 27001-compliant data center—where it is isolated from all external networks and protected by multiple layers of access control, continuous monitoring, and strict adherence to cryptographic handling and audit policies.

SECURITY MONITORING, CRISIS RESPONSE, AND SUCCESSOR ACCESS PROTOCOLS

The system's built-in security architecture and native monitoring capabilities are augmented by third-party solutions for intrusion prevention and Security Information and Event Management (SIEM). These integrations enhance visibility and support automated threat detection and response. In parallel, AiDAC continuously monitors each customer account balance in real time, 24/7, with threshold-based alerts designed to detect anomalous activity or unauthorized fund movements.

AiDAC's Business Continuity and Disaster Recovery framework ensures the availability and integrity of critical systems in the event of disruption. It includes tested procedures for failover, data restoration, and service recovery to minimize downtime and data loss.
In the event of a security incident, AiDAC follows a structured Incident Response Playbook that defines procedures for triage, containment, recovery, and post-incident analysis.

AiDAC incorporates a formal succession and contingency framework to ensure operational continuity under exceptional circumstances. Custodial succession is governed by predefined escalation protocols that designate successor entities or individuals in accordance with client agreements and internal governance policies. In the event of key personnel unavailability or incapacitation, emergency custodian transfer procedures enable the prompt and secure reassignment of operational control without compromising asset security, availability, or compliance.

INSURANCE

AiDAC is backed by industry-leading insurance coverage designed to mitigate key operational and custodial risks. This comprehensive coverage helps safeguard against a wide range of operational, legal, and physical threats, including cyberattacks, system breaches, employee malfeasance, and the loss or theft of cryptographic material. The insurance program is underwritten by highly rated, regulated insurers with deep experience in digital asset risk. The platform aligns each policy with the client's deployment model, jurisdiction, asset profile, and operational needs. Documentation, including certificates of insurance, policy terms, and claims procedures, is available upon request as part of AiDAC's commitment to transparency, resilience, and institutional trust.