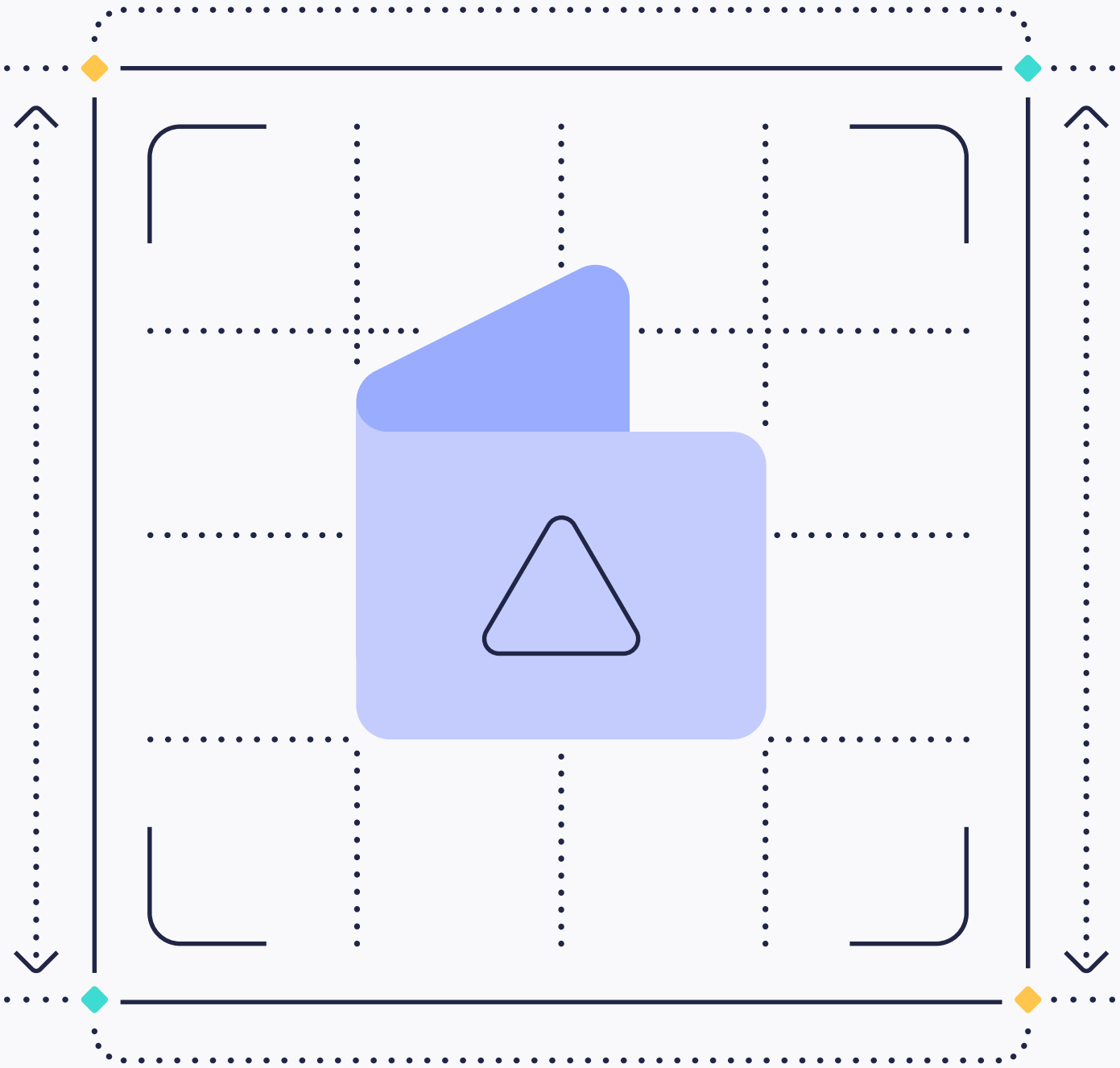
Fireblocks

Wallet Infrastructure for Banks: A Blueprint for Building Digital Asset Operations



Fireblocks

Table of contents:

Introduction 3

Digital Asset Custody for Banks: What Changes and Why 4

The Strategic Foundation: Custody Model and Wallet Infrastructure 4

The Strategic Fork in the Road: Your Custody Model 4

Building Your Wallet Infrastructure: Six Steps 4

STEP 1: Define Your Control Requirements 4

STEP 2: Choose Your Key Management Architecture 4

STEP 3: Build the Transaction Control Layer 4

STEP 4: Connect to the Networks That Matter 4

STEP 5: Financial Reporting and Audit Readiness 4

STEP 6: Integrate With Core Banking Systems 4

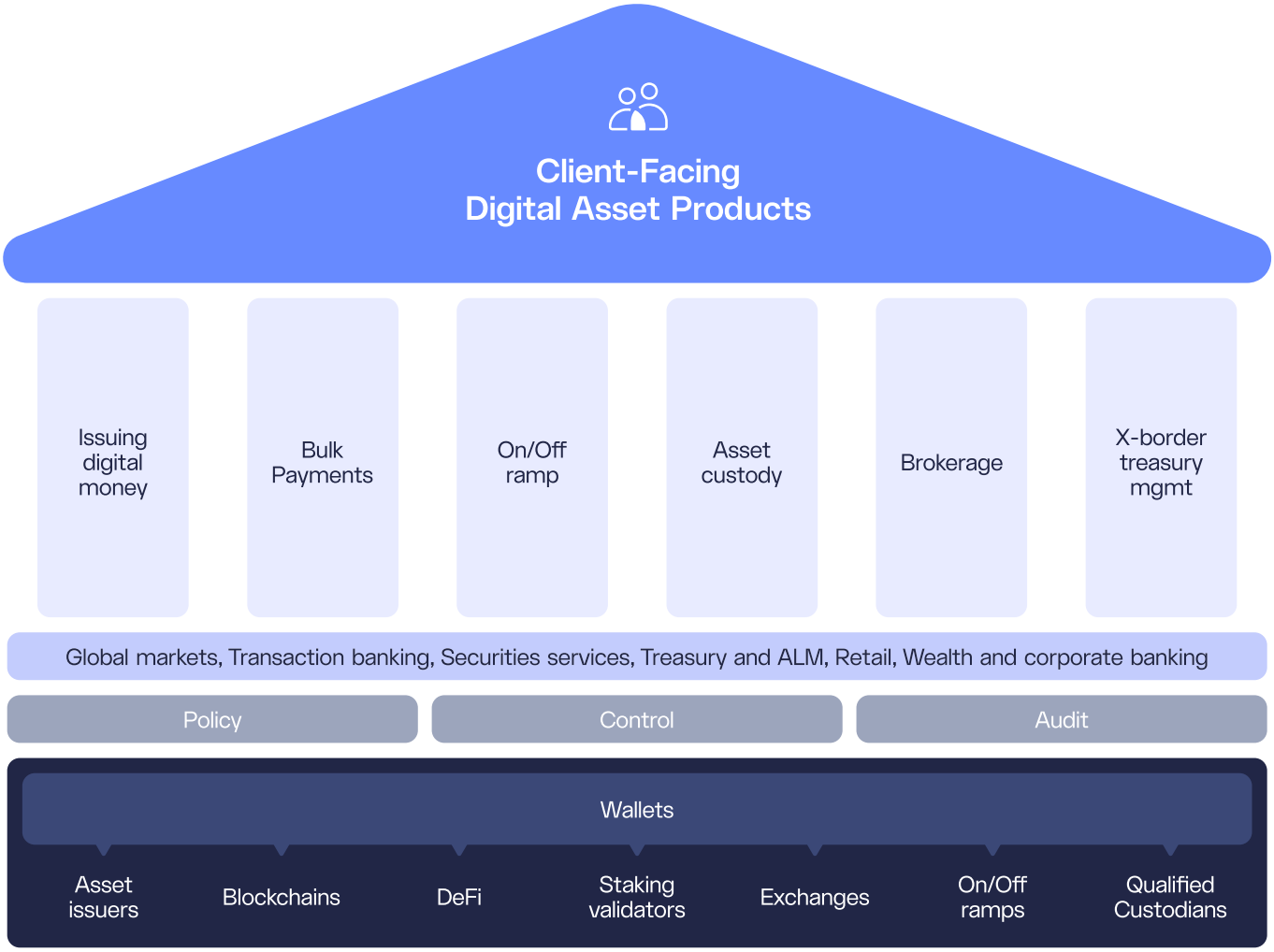
Summary: Requirements for Bank Wallet Infrastructure 4

Building a digital asset capability isn't one decision. It's a stack of decisions, each one dependent on the layer below it. The architecture above shows how that stack is structured: connectivity and wallet infrastructure at the foundation, compliance and risk controls above it, day-2 operations running the whole thing in production, and client-facing products at the top.

This blueprint series covers each layer in turn. In this Part 1, we start at the foundation: wallet infrastructure.

Get it right and you have infrastructure that supports multiple use cases, scales without rebuilding, and keeps control where it belongs. Get it wrong and you're re-architecting mid-flight, sharing economics you should be capturing, and explaining to regulators why your governance framework doesn't match your operational reality.

The good news is banks across every major jurisdiction are already running this in production, and this blueprint is the framework for getting the foundational decisions right.



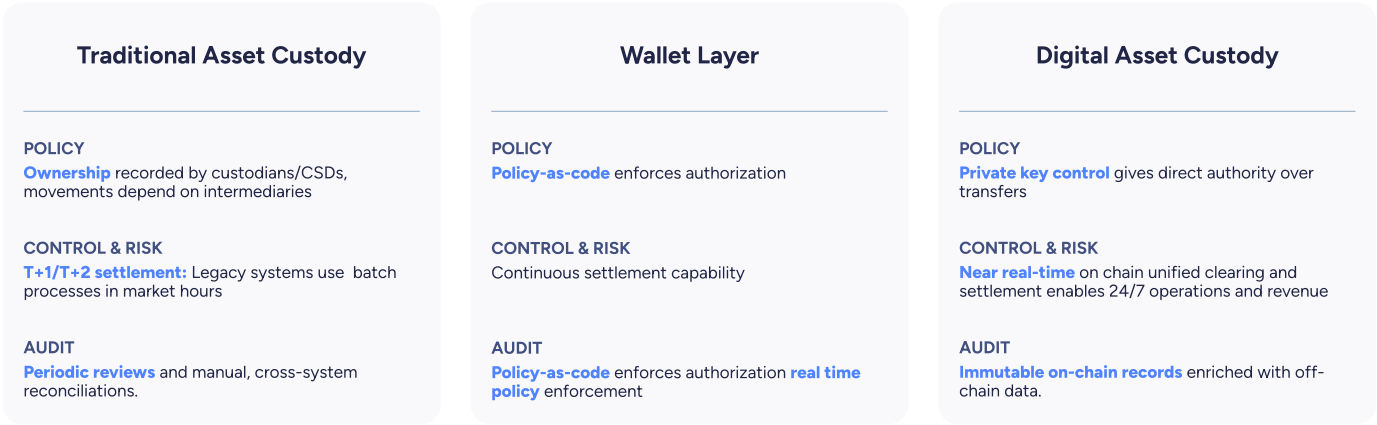
Fireblocks

Digital Asset Custody for Banks: What Changes and Why

Most banks enter the digital asset space carrying assumptions from traditional custody. That's where implementation projects can get into trouble.

The Foundations: Traditional vs. Digital Asset Custody

Custody in digital assets is not an adaptation of traditional models. It is the control point that determines whether a bank can safely issue, move, settle, and scale new products.



Banks that want to scale digital assets must start at the wallet layer. It's the control boundary for your entire franchise.

In traditional banking, custody sits behind core systems. Control is distributed across relationships and counterparties: the bank manages records, settlement and safekeeping happen through established intermediaries. In digital asset operations, control is cryptographic and direct. Private keys govern asset movement. Whoever controls the keys controls the assets.

Wallet infrastructure is where that control lives. It is not a custody product bolted onto existing systems. It is the operating layer where every critical function lives:

- Security: key management, MPC, hardware security modules
- Compliance: transaction policies, sanctions screening, Travel Rule
- Governance: approval workflows, role-based access, audit trails
- Connectivity: blockchain networks, liquidity providers, payment rails

Commercial operations run by your bank will be controlled through the wallet layer. The architecture you choose now determines what is possible later.

The Strategic Foundation: Custody Model and Wallet Infrastructure

Building digital asset infrastructure starts with two structural decisions: the custody model and the wallet architecture. Get both right and they compound each other. With the right custody model, every wallet decision is easier, and the right wallet architecture makes every use case that follows possible.

The Strategic Fork in the Road: Your Custody Model

This decision comes before you start building: direct custody or sub-custody. Your wallet infrastructure will then be Step 1 of your build.

The Strategic Fork in the Road for custody

Evaluating whether custody or sub-custody is right for your business.

For a detailed explanation of the direct vs. sub-custody comparison and implementation frameworks, see our White Paper Why Direct Custody is the Future for Financial Institutions.

Sub-custody

Sub-custody means outsourcing the major components of your digital asset infrastructure to a third party: key management, technology risk, and balance sheet risk all sit outside your institution. It can look attractive at the outset. Faster time to market, lower initial investment, reduced operational build. In practice, regulated banks rarely choose this path. For a bank still validating client demand or running a limited pilot, it can make sense as a starting position.

But the constraints compound quickly. When a third party holds the keys, your ability to move assets depends on their operational model: their hours, their processes, their risk thresholds, their product roadmap. In markets that operate 24/7, dependency on a custodian with batch processing windows is not a minor friction. It is a ceiling on what you can offer.

Direct custody

Direct custody removes that ceiling. Your institution retains full control over your assets and your clients' assets, eliminating counterparty risk and keeping governance, policy controls, data, and reporting within your own perimeter. You control how assets move, how compliance is enforced, and how services connect to the broader ecosystem. And because your roadmap is your own, you can respond to market needs and regulatory obligations without waiting on a third party to develop their product. You also capture the full economics of the services you offer rather than sharing them with an external custodian.

Decisions and Long-term Impacts

This decision has long-term consequences. Banks that start with sub-custody and later seek to migrate face a re-architecture project while managing live client relationships.

Before you decide, answer these three questions:

> Does your 12-24 month roadmap contain more than one use case: custody, tokenization, stablecoin payments,stablecoin issuance, and/or trading & brokerage?

> What are your revenue ambitions? Every service a sub-custodian delivers on your behalf is revenue you don't capture directly.

> Do your internal policies or regulatory obligations require you to remain in full control of your assets, governance, and policies?

Building Your Wallet Infrastructure: Six Steps

For many banks working through those three questions, direct custody is the answer. The six steps that follow are the framework for building on that foundation: from defining your control requirements through to core banking integration. Each step builds on the one before it.

Step 1: Define Your Control Requirements

The design of the control layer requires the input of a combination of Treasury, Ops, Risk, and Compliance teams and is the backbone of the solution. Getting this stage right ensures the right transaction flows, approval quorums, and experience is optimally enforced to balance risk, regulatory adherence, and operational overheads.

Before you choose a key management architecture or configure a policy engine, you need to answer a prior question: what level of control do you actually need over asset movement, and at what granularity?

Segregation of duties

Who can initiate a transaction? Who must approve it? What quorum is required for high-value movements?

Define these governance structures before you configure them into infrastructure. Banks that skip this step end up with governance frameworks that were never designed for digital asset workflows and require manual workarounds as volume scales.

Wallet architecture

Different wallet types have different risks and operational profiles:

- hot wallets for operational liquidity
- warm wallets for intermediate balances
- cold wallets for long-term safekeeping

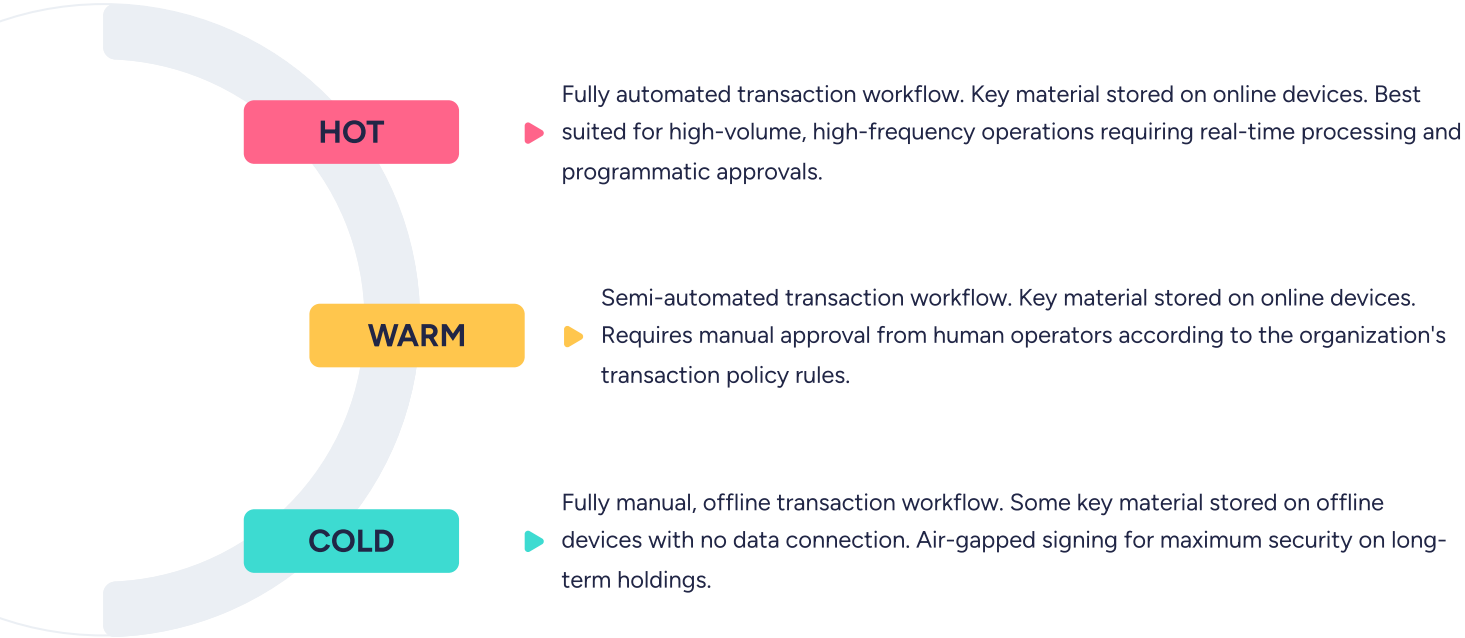
Match your configuration to your use case: a bank running stablecoin payments has different liquidity requirements than one offering institutional safekeeping.

For client-facing services, a custodial wallet model enables the bank to stay in control on behalf of their customers, generating millions of wallets whilst applying a common control and governance structure across all assets.

This is the foundation for institutional custody services, digital asset safekeeping, and Wallets-as-a-Service offerings for corporate and wealth clients.

If you are using wallet infrastructure to manage your own digital asset holdings, the configuration looks different: fewer wallets, larger holdings, and a cold and warm storage architecture weighted toward security over operational throughput. This applies to proprietary trading desks, stablecoin reserve management, and cross-border treasury operations.

Hot, Warm and Cold: Choosing the Right Wallet Architecture



Policy engine scope

Transaction policies can be configured to enforce rules based on wallet origin, destination address, asset type, transaction size, counterparty identity, and jurisdiction. This includes the ability for banks to integrate their own policy rules engine to achieve segregation of duties along with maker/checker rules. Define the scope before implementation so policies reflect your actual risk framework, not a default template.

Step 2: Choose Your Key Management Architecture

Key management is the technical foundation of digital asset custody. Your choice here has operational, security, and regulatory implications that persist for the life of your infrastructure.

> MPC (Multi-Party Computation): Distributes transaction signing across multiple devices or parties, eliminating single points of failure. Supports flexible deployment (cloud or on-premise), scales well across wallet volumes, and is the architecture used by the majority of institutional-grade digital asset platforms.

> HSM-based key management: Keeps private keys inside your own hardware, with all key generation, storage, and signing occurring within your infrastructure. HSM-based key management suits institutions where regulatory or policy requirements mandate full control of cryptographic key material, or if you have significant existing HSM investments you need to leverage rather than replace.

> Hybrid: MPC for operational wallets, HSM-backed cold storage for long-term safekeeping. Suits banks with large, heterogeneous custody operations across multiple asset classes and risk tiers.

Your selection criteria here go beyond the technical. Consider how each architecture supports the governance requirements you defined in Step 1, how it aligns with regulatory expectations in your primary jurisdictions, and how it performs as transaction volumes scale.

Step 3: Build the Transaction Control Layer

Compliance in digital asset custody is not a layer added after infrastructure is built. It is embedded in the transaction layer itself. This is one of the most significant operational differences from traditional banking.

This layer has two components: the policy engine, which governs how transactions are authorized and executed, and the compliance controls, which ensure every transaction meets regulatory requirements across jurisdictions.

Your Policy Engine: Authorization Before Execution

A policy engine sits at the center of this layer. It evaluates every transaction against a defined rule set before execution: wallet origin, destination address, counterparty risk tier, asset type, transaction size, and jurisdiction. Transactions that don't meet policy requirements are blocked or escalated before they reach the blockchain.

This matters because blockchain transactions are final. There are no reversals, no clawbacks, no reconciliation windows. Enforcement must operate before execution, not after.

Your transaction control layer needs to handle:

> **Transaction simulation:** Simulate transactions before they execute onchain to verify that intended outcomes match what will actually happen. Critical for smart contract interactions, where the gap between intended and actual execution has been the vector for significant industry losses.

> **Audit trails:** Log every transaction, approval decision, policy check, and exception in a tamper-evident audit Log every transaction, approval decision, policy check, and exception in a tamper-evident audit trail. This supports internal governance, supervisory examination, and the continuous monitoring regulators increasingly expect.

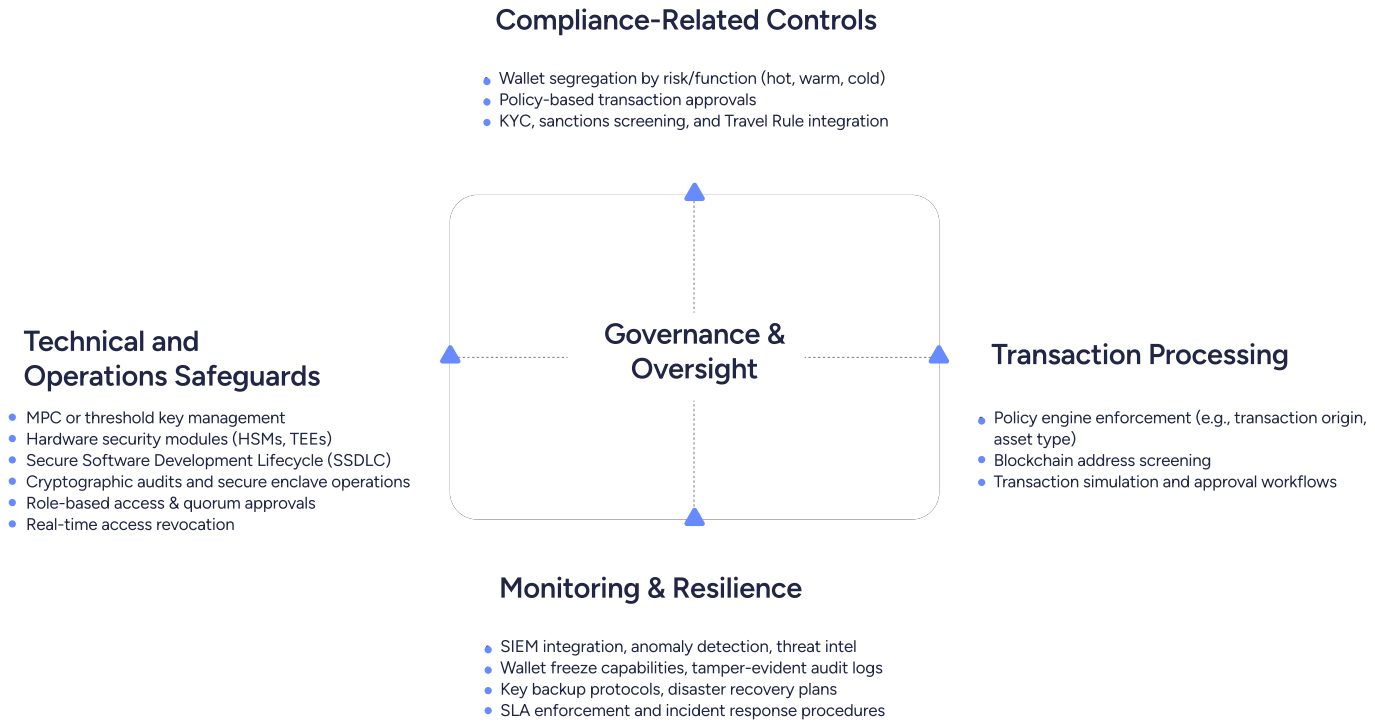
Your Compliance Controls: Embedded, Not Bolted On

Where the policy engine governs authorization, compliance controls govern regulatory obligations. These operate at the transaction level, running continuously across every wallet action, transfer, and counterparty interaction, not as a periodic review but as a live enforcement layer, providing:

> **Blockchain address screening:** Screen destination addresses against sanctions lists and blockchain intelligence data in real time. This requires integration with providers such as Chainalysis or Elliptic and must operate continuously given 24/7 market conditions.

> **Travel Rule compliance:** FATF's Travel Rule requires transmission of originator and beneficiary information for transfers above defined thresholds. Implement this via a Travel Rule solution such as Notabene, configured across jurisdictions with different threshold requirements.

For banks in the US, the OCC's 2023 Cybersecurity Supervision Work Program addresses many of these requirements directly. The Anchorage Digital consent order and the NYDFS consent order against Block, Inc. are concrete examples of where control frameworks have been found inadequate. These are the supervisory baselines you should be building toward.



Step 4: Connect to the Networks That Matter

Your wallet infrastructure is only as valuable as the ecosystem it connects to. Operational value in digital assets is realized through connectivity: to blockchain networks, liquidity providers, on/off-ramp partners, exchanges, and counterparties.

Building these connections from scratch produces fragile, expensive infrastructure. Each bilateral integration requires:

- Legal agreements
- Technical build
- Ongoing maintenance
- Its own operational risk management

If you're managing 30 bilateral connections, you're managing 30 points of failure and 30 integration maintenance burdens.

The alternative is a network model: a single integration point that gives you access to a pre-connected, pre-vetted ecosystem of counterparties and infrastructure providers. New connections can be activated in days rather than months.

The same logic applies to blockchain connectivity. Supporting 150 blockchains through a single platform is operationally different in kind from maintaining 150 independent node connections. Protocol upgrades, network incidents, and new chain support all flow through one operational relationship rather than many.

This includes permissioned and private chain deployments (EVM-compatible subnets and enterprise networks), which require the same single integration approach alongside additional network-specific access and compliance configuration.

Step 5: Financial Reporting and Audit Readiness

Digital asset operations generate reporting obligations that cannot be met by custody infrastructure alone. The data that governs wallet operations and the data required for financial reporting and regulatory audit serve different purposes, are held to different standards, and require different infrastructure to produce.

Banks offering digital asset services are responsible for three categories of reporting that regulators across all major jurisdictions are actively enforcing:

> **Customer asset segregation and balance reporting:** Regulators require continuous, demonstrable evidence that client assets are segregated and accounted for. In the EU, MiCAR Articles 80 and 83 make this mandatory. In Hong Kong, the SFC requires a full monthly VASP return. The obligation exists regardless of whether your bank is live at scale or in early-stage production.

> **Transaction and custody reporting:** Transaction-level records must be produced at the cadence regulators require: monthly in most APAC jurisdictions, per-transaction on demand in others. These records must be accurate, complete, and traceable to source data.

> **Cost basis reporting:** As digital asset tax reporting obligations come into force, banks need per-customer cost basis tracking that is accurate from day one, not reconstructed after the fact. The US 1099-DA is the most significant near-term example,

The challenge is data. Blockchain data is not self-certifying for financial reporting purposes. Getting accurate, complete, audit-ready data from multiple chains, cleaning and enriching it, and producing it in the format regulators require is a distinct infrastructure problem. A typical G-SIB will submit between 10,000 and 20,000 regulatory reports annually. That volume cannot be managed manually.

Your reporting infrastructure needs to sit between your wallet layer and your regulatory obligations, pulling onchain data continuously, reconciling it to your internal books, and producing structured outputs that are ready for regulatory submission without manual assembly at period end.

Build this in from the start. Banks that treat reporting as a post-launch problem face a rebuild under live operational conditions and regulatory scrutiny.

Step 6: Integrate With Core Banking Systems

This is the step that determines whether digital asset operations become a real business line or remain a standalone product. Integrating with your existing financial, risk, and reporting infrastructure converts digital asset activity from an isolated ledger into something that can be governed through your established processes.

Reconciliation

Onchain transaction records must map to internal ledger entries in real time. Blockchain transactions are final and settlement is continuous, while most core banking systems expect batch processes. Your reconciliation architecture must handle this mismatch without creating gaps in the audit trail.

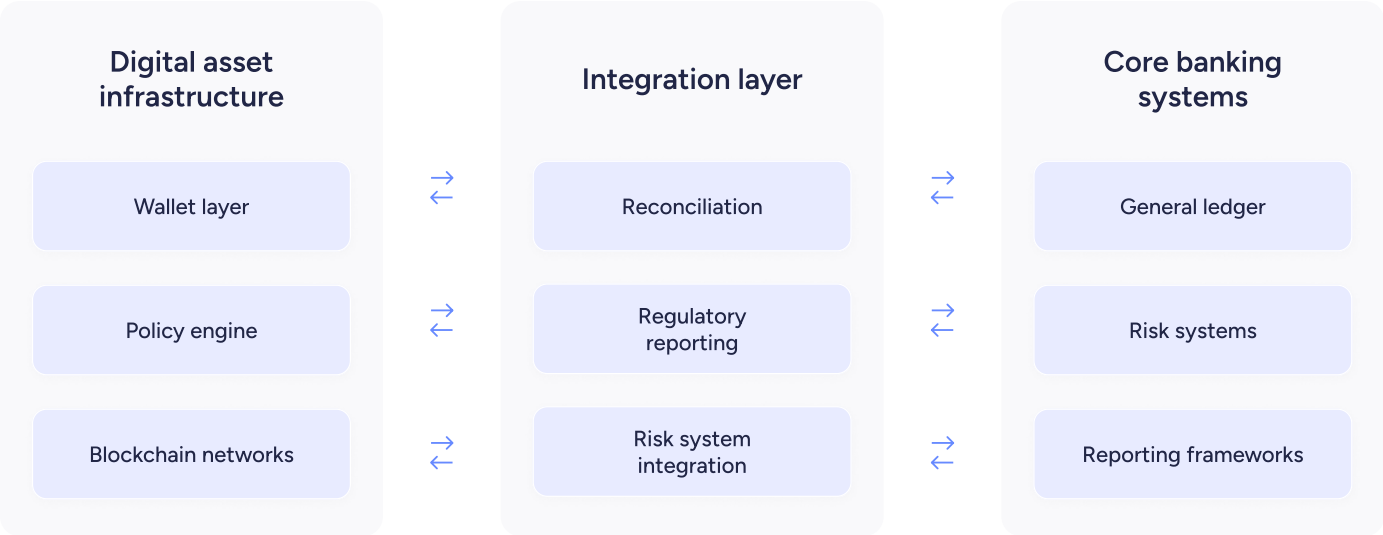
ERP integration

Corporate treasurers managing digital asset positions expect the same visibility and control they have over traditional assets. Digital asset activity needs to flow directly into ERP systems such as SAP and Oracle: wallet balances, transaction confirmations, and settlement records updating automatically rather than requiring manual intervention. This is where programmable digital money meets embedded finance: banking functions operating seamlessly within the corporate's own systems.

Risk system integration

Real-time position data, counterparty exposure, and transaction monitoring outputs must feed into your risk management systems. This is what allows your risk function to govern digital asset activity through the same frameworks it applies to other business lines.

Digital Asset Infrastructure and Core Banking Integration



Bidirectional integration keeps digital asset activity visible across existing systems

Flexible, well-documented APIs are the connective tissue here. They accelerate integration and reduce the technical debt that accumulates when connections are built as one-off solutions rather than a systematic architecture.

Summary: Requirements for Bank Wallet Infrastructure

Your wallet infrastructure is the foundation everything else builds on. Get these seven requirements right and you have an architecture that supports every use case on your roadmap, meets the supervisory expectations your regulators are moving toward, and scales without forcing a rebuild mid-flight.

1. Security architecture: MPC or HSM-based key management with no single point of failure. Multi-layered defense including hardware isolation, behavioral analytics, and proactive threat detection. Integration-compatible deployment for banks with existing HSM infrastructure.

2. Governance and policy engine: Programmable transaction approval logic enforced at the wallet layer before execution. Role-based access controls, quorum requirements, and real-time revocation capability. Configurable across asset class, counterparty risk tier, jurisdiction, and transaction type.

3. Compliance integration: Native support for sanctions screening, Travel Rule compliance, blockchain address screening, and suspicious activity monitoring. Integration with leading blockchain intelligence providers. Tamper-evident audit trails supporting continuous monitoring and supervisory examination.

4. Network connectivity: Pre-connected ecosystem of exchanges, liquidity providers, on/off-ramp partners, and payment counterparties accessible through a single integration point. Support for 150-plus blockchains without the operational overhead of independent node management.

5. Financial reporting and audit readiness: Purpose-built financial data infrastructure sitting between your wallet layer and your regulatory obligations. Automated production of customer asset segregation reports, transaction and custody records, and cost basis data. SOC 1-certified outputs ready for regulatory submission without manual assembly at period end.

6. Core banking integration: Flexible APIs enabling real-time reconciliation between onchain activity and internal ledgers. Direct integration with ERP systems ensures digital asset activity flows into existing financial and operational workflows. Risk system integration delivering real-time position data and exposure monitoring.

7. Operational scalability: Architecture that scales from pilot to production without rebuilding. The same security model, policy engine, and governance framework that manages initial volumes should operate identically at institutional transaction throughput.

Fireblocks

What Comes Next:
The Blueprint Series Continues

Wallet infrastructure is the foundation. But building a digital asset capability that operates at institutional scale, meets regulatory expectations across jurisdictions, and runs reliably in production requires more than getting the foundation right.

The decisions you make here create the conditions for what follows. Your compliance and risk architecture can only be as strong as the wallet layer it sits on. Your Day-2 operations can only be as resilient as the infrastructure they're running.

The banks moving now are not just solving for today's use case. They are building infrastructure that supports a multi-year digital asset strategy.

More than 95 banks are already building their digital asset operations on Fireblocks, securing over $10 trillion in transactions across 150-plus blockchains. The infrastructure exists. The regulatory framework is clearing. Your clients are asking.

Contact us to discuss your wallet infrastructure strategy with our banking team.