

Digital assets: From wallet visibility to verifiable trust

Standard Chartered · Mei Lam · 2026-09-23 · English original

How can financial institutions scale digital assets with confidence? Trust, identity and governance hold the key.

This article is featured in Issue 3 of our Transaction Banking: Bankable Insights e-magazine. Download a copy to view this and more insights.

Digital asset markets are moving from experimentation to institutional adoption. For financial institutions (FIs), the question is no longer whether blockchain can record value or improve market efficiency.

The harder question is whether institutions can establish enough trust in the people, entities and controls behind wallet activity to participate safely, at scale and across borders.

This matters because institutional engagement is becoming more disciplined. Investors, banks, custodians, asset managers and market infrastructures are exploring use cases across tokenised funds, stablecoins, collateral, custody, settlement and asset servicing. But wider participation raises the trust bar. Digital assets may offer transparency, programmability and speed, but regulated institutions still need confidence in identity, ownership, authority, controls and accountability.

Institutional participation raises the trust bar

Traditional finance is built on a familiar trust architecture: regulated entities, account structures, legal agreements, beneficial ownership checks, sanctions screening, transaction monitoring, governance forums and defined lines of accountability. These controls may not be perfect, but they give institutions a common basis for understanding who they are dealing with, what they are exposed to and where responsibility sits.

Blockchain networks operate differently. They make transactions visible, traceable and auditable – a major selling point – but trust requires more than visibility. A wallet address may show where value moved, but it does not automatically prove who owns the wallet, who controls the keys, whether the wallet is authorised for the transaction, or whether the control environment remains valid after onboarding.

For the FI community, this is the central compliance challenge. The move to tokenised assets and digital money does not remove the need for KYC, sanctions, surveillance and governance. It changes how those controls need to be evidenced, connected and maintained in a wallet-based environment.

The practical problem: pseudonymity creates control gaps

The defining challenge is pseudonymity. Blockchain ledgers may be transparent, but wallet addresses do not inherently reveal the real-world identity of the controller. A wallet may belong to an individual, legal entity, custodian, exchange, smart contract, decentralised protocol, omnibus structure or third-party service provider. Control may also sit across multi-signature arrangements, delegated authorities or outsourced technology workflows.

That creates practical questions for mid- and senior- level leaders responsible for risk, compliance, operations, product and client delivery. Who owns the wallet? Who controls the private keys? Is the wallet self-custodied or managed by a regulated custodian? Who can approve transfers? Can the wallet be changed after onboarding? How are changes validated? What happens if control is delegated to another entity?

These are not theoretical questions. In traditional markets, institutions rely on onboarding files, account records, legal agreements, signatory mandates and regulatory obligations. In a wallet-based model, the same questions remain, but the evidence may be technical, contractual and behavioural. Institutions therefore need to connect off-chain identity with on- chain activity in a way that is repeatable, auditable and proportionate to risk.

This is where Know Your Wallet becomes important. KYW should not be treated as an add-on or one-off screening exercise. It should form part of a broader control framework.

Such frameworks link customer identity, wallet ownership, authority, transaction behaviour, sanctions exposure, governance and ongoing monitoring.

The operating model matters. Teams need a shared definition of acceptable evidence for wallet ownership and control, clear hand-offs between onboarding and transaction monitoring, and escalation routes for exceptions. Controls should also be calibrated by use case: a tokenised fund subscription, stablecoin payment, custody account or collateral arrangement may each require a different level of verification, monitoring and approval.

Move from wallet screening to a trust stack

Wallet screening is necessary, but insufficient. Blockchain analytics can identify exposure to sanctioned addresses, scams, hacks, illicit finance typologies, darknet markets and high-risk services. It can also support transaction monitoring and investigation. But a clean screening result does not prove that the wallet belongs to the client, that the client has authority to use it, or that the control environment remains unchanged over time.

Institutional-grade trust requires a layered model. The objective is not to replicate every traditional process exactly, but to preserve the control outcomes that matter: knowing the customer, understanding the asset, verifying authority, monitoring behaviour and governing exceptions.

A practical trust stack should include five components.

- Identity: Confirm the legal entity, beneficial ownership, regulatory status, business activity and risk profile.
- Wallet ownership and control: Evidence that the wallet is linked to the customer and that the customer has authority to use it, through technical confirmation, custodian attestation, contractual representation or controlled test transaction.
- Eligibility: Confirm that the client, product and jurisdiction are aligned.
- Ongoing traceability: Monitor transaction behaviour, typology changes and emerging red flags.
- Governance: Define approval forums, exception handling, periodic review and control effectiveness testing.

Digital identity frameworks, permissioned networks, trusted registries and reusable attestations may

help reduce duplication across the ecosystem. But they will only be useful if they are interoperable, privacy-conscious, legally recognised and aligned with financial crime, sanctions, data protection and operational resilience expectations. The goal is not more documentation; it is stronger evidence, clearer accountability and better scalability.

A practical scenario: Tokenised fund distribution

Wallet screening is only the start. Discover how institutions can build a trusted, auditable framework for distributing and managing tokenised funds across the investment lifecycle.

What FI leaders should do now

For FI leaders, the priority is to move from conceptual discussion to practical readiness. That means embedding trust and control considerations into product design, client journeys and operating models from the outset, rather than bolting them on after launch.

This requires collaboration across the ecosystem. Regulators need confidence that institutional adoption will not weaken financial crime controls or accountability. Clients need clarity on what information they must provide and why. Technology providers need to support auditability, privacy, interoperability and resilience. Financial institutions need operating models that are scalable, commercially viable and risk-sensitive.

Five actions for practical readiness

- Define the minimum evidence required: to link a customer to a wallet, including how that evidence differs for self-custody, third-party custody and omnibus structures.
- Create a wallet lifecycle process: covering onboarding, changes, suspension, revalidation and offboarding.
- Align KYC, KYW, sanctions screening, and transaction monitoring: so that on-chain and off-chain risk indicators are viewed together.
- Define clear decision rights: across compliance, legal, operations, product and technology.
- Test controls against real use cases: such as tokenised fund distribution, stablecoin settlement or collateral movement.

The institutions that make this practical will have an advantage. They will be able to help clients access digital asset opportunities while maintaining the standards of trust, safety and governance expected in institutional finance.

The next phase: Trust as infrastructure

The next phase of digital asset adoption will not be determined by technology alone. Tokenised assets, digital money and programmable settlement will only scale if institutions can establish confidence in the controls around them.

That requires trust frameworks that operate across both traditional and digital environments. Institutions must be able to connect an on-chain address to an off-chain customer, evidence ownership and control, monitor activity over time and govern exceptions when risk changes.

FI leaders should ask three questions now: What evidence do we require before we trust a wallet? How do we know that trust remains valid after onboarding? And how do we design controls that are strong

enough for effective safeguarding, but practical enough for implementation and scalable enough for growth?

Unlocking capital for clean cooking and emissions reductions

Find out how we helped the World Bank unlock affordable capital for clean energy projects in Ghana.

A practical scenario: Tokenised fund distribution

Consider a regulated asset manager distributing a tokenised money market fund to institutional investors. The fund token may allow faster subscription, redemption and transfer. The asset manager wants a scalable distribution model. The distributor needs to confirm investor eligibility. The custodian needs confidence over safekeeping and settlement. Compliance teams need to connect the on-chain wallet to the off-chain investor.

In this scenario, a clean wallet-screening result is only the starting point. Institutions also need to know whether the investor has completed onboarding, whether the product is suitable and permitted in the relevant jurisdiction, whether the wallet is self-custodied or held through a regulated custodian, who has signing authority, and what evidence is required if the investor later changes wallet details.

A robust model would connect onboarding, wallet verification, transfer controls, monitoring and exception management. For example, only wallets linked to approved investors may be whitelisted to receive or hold the token. Wallet detail changes may require renewed validation. Transfers may be restricted to eligible addresses. Monitoring may combine on-chain analytics with off-chain customer records. Exceptions may be reviewed through defined governance forums.

The real compliance challenge is therefore whether every participant can evidence that the token is being issued, distributed, held and transferred within a trusted, accountable and auditable framework.

Source: <https://www.sc.com/en/news/corporate-investment-banking/digital-assets-from-wallet-visibility-to-verifiable-trust/>