Crypto Payment Rails Without Becoming a Custodian: A Representative Modernization Scenario for a Regulated Institution Adding Non-Custodial Crypto Settlement

ACM Global Tech

Abstract

This case study is a *representative modernization scenario* grounded in public industry benchmarks and the underlying Lux, Hanzo, and Zen technology, with outcomes framed as *target* outcomes. It describes how a regulated institution could add crypto payment rails and non-custodial settlement—accepting and settling stablecoin and cryptocurrency payments alongside fiat, with multi-party-computation (MPC) threshold custody so no single party ever holds the keys, real-time anti-money-laundering (AML) screening, and on-chain settlement. The technical substance derives from the Hanzo Crypto Payment Rails architecture [1], the non-custodial threshold-custody construction for regulated venues [2], and the non-custodial ATS design that fixes the 2-of-3 threshold requirement [3]. ACM Global Tech is a Web3 Alliance (W3A, w3a.foundation) member that licenses this intellectual property and partners to resell and co-build it for regulated institutions.

1 The Pressure

A regulated institution—a bank, broker-dealer, or payments company—increasingly faces demand to accept and settle digital-asset payments: stablecoins (USDC, USDT) and major cryptocurrencies, from corporate clients, marketplaces, and cross-border counterparties who already hold these assets. Crypto payment adoption has been held back not by demand but by four structural barriers: exchange-rate volatility between payment initiation and settlement, slow confirmation times on Bitcoin and Ethereum mainnet, the key-management complexity of holding merchant or treasury wallets, and fragmented integration across chains [1].

The institution confronts a sharper tension on top of these. To accept and settle crypto it must be able to authorize asset movements; but the moment it holds customer or treasury private keys it becomes a *custodian*—a single point of catastrophic failure exposed to insider theft and key compromise, and subject to the heightened regulatory burden of holding customer assets [3, 2]. Simultaneously it must satisfy the AML and Travel-Rule obligations that attach to value transfer: under FATF Recommendation 16, originator and beneficiary information must travel with a qualifying transfer, and OFAC sanctions screening must run before settlement. Retrofitting these controls onto legacy rails is brittle. The institution needs to settle crypto *without* any single party being able to move assets unilaterally, and *without* weakening its compliance posture.

2 ACM's Approach: Crypto Rails Plus MPC Custody

ACM's offering composes a crypto payment-rails layer with non-custodial threshold custody, so acceptance and settlement are possible while authorization stays distributed across parties.

Accept and settle crypto alongside fiat.
The rails accept BTC, ETH, and stablecoins (USDC, USDT) as first-class payment methods through the same checkout and settlement pipeline used for cards, with rate-locking, chain-specific confirmation monitoring, automatic conversion to a settlement currency, and optional fiat off-ramp to the institution's bank account [1]. At checkout the exchange rate is locked for a bounded window, sourced from aggregated exchange feeds with TWAP smoothing, removing the volatility gap between initiation and settlement [1].

Non-custodial by construction.
Every payment and settlement wallet is a 2-of-3 MPC threshold address—shares split across the institution (operator, which co-signs only after compliance checks pass), a co-signer, and a disaster-recovery share—so no party ever holds the complete key [1, 2]. A single distributed key-generation ceremony produces signing capability across all supported chains; addresses are derived per payment via HD derivation from the MPC master key [1]. Two complementary protocols cover the relevant chains: CGGMP21 threshold ECDSA over secp256k1 for EVM and Bitcoin, and a threshold construction over ed25519 for EdDSA chains [2, 1]. Shares can be refreshed (reshared) without changing the on-chain address, and an HSM attestation layer co-attests each signing share without weakening unforgeability [2].

On-chain settlement with deterministic finality.
For settlement on the Lux EVM, finality is sub-second and deterministic; once confirmed, a transaction cannot be reverted, gas cost is under $0.01 per transaction, and stablecoins are deployed natively (avoiding bridge risk) [1]. The institution can settle on-chain in the settlement currency or take the fiat off-ramp; end-to-end, a crypto payment can reach a bank deposit within 24 hours [1].

The composition delivers the property that matters to a regulator and to the institution's risk committee alike: because every asset movement requires a 2-of-3 threshold signature, a compromise of the operator alone is insufficient to move assets [3, 2].

3 Architecture

The payment-and-settlement flow follows the cited design [1]:

1. **Initiation.** The payer selects a crypto payment method; the SDK presents available currencies and chains.
2. **Rate lock.** The exchange rate is locked for a bounded window from aggregated exchange feeds with TWAP smoothing.
3. **Address generation.** A unique MPC-derived address is generated for the payment.
4. **Screening (compliance gate).** AML and sanctions checks run before the operator co-signs; the operator's MPC share is released only when checks pass (see Section 4).
5. **Confirmation.** Chain-specific confirmation monitoring applies (1 block final on Lux; staged confirmations on Bitcoin scaled to amount) [1].
6. **Settlement.** Received crypto is converted to the settlement currency (default a stablecoin) and moved to the institution's MPC-managed settlement wallet.

7. **Fiat off-ramp (optional).** The settlement stablecoin is redeemed through an institutional channel and wired to the bank account.

Multi-chain coverage. EVM chains (Lux, Ethereum) derive addresses as `keccak256(pubkey)` and support native and ERC-20 tokens; Bitcoin uses `bech32` native SegWit with confirmation counts scaled to payment size; ed25519 chains use a separate ceremony with single-slot confirmation [1]. For high-frequency flows, bilateral payment channels on Lux allow off-chain micro-payment increments that batch-settle on-chain at channel close [1].

Platform services and APIs. Payment intents, status, refunds, settlements, and webhooks are exposed over a versioned API; all endpoints require IAM authentication via OAuth 2.0 bearer tokens with operation-scoped keys [1]. Identity and onboarding (KYC/AML), key management for MPC material, API routing, and persistence are supplied by the underlying Hanzo platform services (IAM, KMS, Gateway, Base) [2].

4 AML, Travel Rule, and Compliance

The compliance gate sits *in front of* the operator's signing share: a settlement cannot proceed unless screening passes, because the operator co-signs only after compliance checks succeed [1]. This gate maps to the regulatory controls a regulated institution must satisfy:

- **Sanctions screening.** OFAC and address-risk screening before the operator releases its MPC share, so a flagged counterparty never reaches settlement.
- **Travel Rule.** Originator and beneficiary information carried with qualifying transfers, satisfying FATF Recommendation 16 across borders.
- **Real-time AI/ML for AML.** ACM operates a real-time AI/ML transaction-monitoring engine for AML, scoring transactions and counterparties as they flow through the compliance gate so that suspicious activity is caught before the operator releases its signing share. This live monitoring capability composes with the compliance-gated signing flow and KYC/AML onboarding specified in the cited crypto-payment-rails research [1].

Because custody is non-custodial, the institution gains crypto acceptance without assuming the custodial regulatory burden of holding customer keys [3, 2]; the compliance controls (screening, Travel Rule, monitoring) are enforced at the signing boundary rather than bolted on afterward [1].

5 Target Outcomes (versus cited benchmarks)

The figures below are *benchmarks reported in the cited research* [1] and serve as the targets a deployment would be measured against.

1. **Crypto acceptance without custodial risk.** The institution can accept and settle crypto while remaining non-custodial, because every movement requires a 2-of-3 threshold signature and the operator alone cannot move assets [3, 2].
2. **Volatility removed at the point of sale.** Rate-locking with TWAP-smoothed feeds closes the price gap between initiation and settlement [1].

Table 1: Scenario targets, tied to benchmarks reported in the cited research [1].

Metric	Lux	Bitcoin
Median confirmation	1.2 s	∼12 min
On-chain finality	sub-second, deterministic	probabilistic
Gas / fee per payment	<$0.01	fee-market rate
MPC signing latency	∼280 ms	∼280 ms
Settlement to stablecoin	∼1.8 s	∼13 min
Fiat off-ramp (end-to-end)	<24 h	<24 h

3. **Fast, final settlement on Lux.** Sub-second deterministic finality and sub-cent gas are the targets for the on-chain settlement leg [1].

4. **Compliance enforced at the signing boundary.** Screening and Travel-Rule data are conditions for the operator's co-signature, not after-the-fact reconciliation [1].

5. **Operational continuity.** Threshold shares can be rotated without changing on-chain addresses, supporting key hygiene and recovery without disrupting balances [2].

6 Deployment

A deployment would proceed in stages: (i) stand up the 2-of-3 MPC key groups for payment and settlement wallets with the disaster-recovery share held offline [1, 2]; (ii) wire the compliance gate (sanctions/AML screening and Travel-Rule data capture) ahead of the operator co-signer [1]; (iii) enable the target chains and a settlement stablecoin, with the fiat off-ramp configured to the institution's verified bank account [1]; and (iv) integrate the versioned payment API and webhooks into existing treasury or checkout systems under OAuth 2.0 scoped keys [1]. ACM licenses this stack as a W3A member and partners to resell and co-build it for regulated institutions [3].

References

[1] Z. Kelling. *Hanzo Crypto Payment Rails: Multi-Chain Settlement with MPC Custody*. Hanzo Industries Inc. Source: `hanzo:hanzo-crypto-payments/hanzo-crypto-payments.tex`.

[2] Z. Kelling. *Non-Custodial Securities Custody via Threshold Signing*. Lux Industries, Inc. Source: `lux:mpc-custody/mpc-custody.tex`.

[3] Z. Kelling. *Non-Custodial Blockchain ATS: Architecture of a Regulatory-Compliant Securities Exchange*. Lux Partners. Source: `lux:lux-ats-architecture/lux-ats-architecture.tex`.