eCurrency: A Post-Quantum Proof-of-Stake Currency Architecture

eCurrency Core Contributors

March 27, 2026

Abstract

eCurrency (ECR) is a decentralized, open-source cryptocurrency designed to combine the UTXO-based strengths of Bitcoin with major advances in consensus, security, and functionality. Initially launched as a legacy PoW eCurrency network in 2018, eCurrency transitioned in 2025 to a UTXO-based Proof-of-Stake (PoS) mechanism using coin age for staking weight and fluid validator participation.

Key innovations include a 10-second block interval, lattice-based post-quantum cryptography (PQC), and a simplified P2SH-by-default address model. The monetary base is capped by the legacy PoW eCurrency supply and is issued onto the PoS ledger through one-way migration rather than ongoing PoS minting. Validator incentives are funded by transaction fees and a reward-fund smoothing model. eCurrency is architected for scalable, client-side smart contracts and long-term ecosystem growth.

Contents

1 Introduction: Currency-First Evolution

Bitcoin demonstrated that mathematically rigorous algorithms can produce decentralized monetary systems with durable security assumptions [1]. eCurrency builds on those strengths while targeting key limitations in throughput, security posture, and functional extensibility.

The project began as a legacy PoW eCurrency network in 2018, with an initial codebase derived from a Litecoin fork [2], and evolved through a major 2025 upgrade to a UTXO-based Proof-of-Stake architecture. The historical lineage is important: early design priorities reflected rapid network bootstrap and distribution-era assumptions inherited from that fork lineage, while the 2025 transition reoriented eCurrency toward long-horizon operation as a practical, secure digital currency.

Most capabilities described in the present document are enabled by that PoS-era upgrade and were not fully available in the legacy PoW architecture. The upgrade path is designed to introduce these capabilities with minimal operational friction, allowing the network to transition seamlessly from legacy operation to fast confirmations, robust validator incentives, post-quantum readiness, and an implementation path for scalable client-side smart contracts. The protocol preserves auditable ledger behavior and fixed-supply discipline while modernizing core primitives.

The remainder of the paper is structured as follows: Section 2 defines the architectural and economic challenges addressed by the protocol. Section 3 presents the system design. Section 4 explains supply and validator economics. Section 5 formalizes PoS security and fork choice. Section 6 details cryptographic and script upgrades. Section 7 outlines the smart-contract model. Section 8 presents rollout phases, and Section 9 concludes.

2 Background and Problem Statement: Requirements for a Durable Digital Currency

A modern digital currency must satisfy three constraints simultaneously: strong monetary credibility, durable cryptographic security, and efficient consensus operation under real-world demand. Legacy architectures often optimized initial distribution and early network bootstrapping, but did not fully optimize long-horizon operation as a mature currency system. In eCurrency's case, the original network also inherited practical code-level assumptions from its Litecoin-fork origin [2], which were suitable for launch conditions but not sufficient for long-term evolution targets.

2.1 Consensus and Security Budget Design

Proof-of-Work (PoW) systems established decentralized issuance and censorship resistance, but they also couple security to ongoing external energy expenditure [1]. As a network matures, security budget design should prioritize predictable long-term validator incentives, lower operational friction, and consistent transaction finality.

eCurrency adopts Proof-of-Stake (PoS) to align consensus security with native asset ownership and protocol-level incentives. The PoS model reduces dependency on persistent external compute races while maintaining decentralized block production and verifiability.

2.2 Transaction Security and the Quantum Threat

Digital signatures based on classical hardness assumptions face known long-term risks from fault-tolerant quantum computing. In particular, elliptic-curve signature systems are vulnerable to Shor-class attacks when sufficiently capable quantum hardware becomes available [3].

To address the quantum threat, eCurrency integrates post-quantum signature primitives and migration-safe key management patterns. The resulting cryptographic framework provides forward-looking transaction authentication and reduces exposure to delayed cryptographic obsolescence.

2.3 Upgrade and Governance Friction

Protocol modernization is often constrained by social and technical coordination overhead. eCurrency addresses the coordination challenge through staged upgrades that preserve core monetary invariants while evolving implementation layers, including decoupled smart-contract components.

These constraints motivate eCurrency as a currency-first architecture focused on sustained security, low-friction operation, and post-quantum readiness.

3 System Overview: The eCurrency Architecture

eCurrency is a decentralized digital currency architecture that evolved from a legacy PoW eCurrency chain into a 10-second UTXO-based PoS protocol with post-quantum transaction security. The system preserves deterministic UTXO accounting while modernizing consensus, incentives, and transaction throughput for currency-scale operation.

The architecture is organized as a currency-first upgrade stack. At the ledger layer, UTXO accounting and script-based spend validation are retained to preserve auditability and infrastructure familiarity. At the consensus layer, authority is derived from coin-age-weighted UTXO participation rather than computational races. The age component of weight enables validator circulation over time, while the validation mechanism preserves asset liquidity without rigid lock-heavy staking structures.

At the incentive layer, fee routing and Reward Fund subsidy smoothing provide baseline validator continuity under variable transaction demand. The Reward Fund is capitalized by both transaction fees and the fixed upgrade fee applied when legacy PoW coins are migrated to the PoS chain. At the cryptographic layer, lattice-based post-quantum signatures and a simplified P2SH-by-default script model reduce integration complexity while improving long-horizon security posture.

Figure 1 summarizes the layered upgrade path from legacy PoW operation to the post-quantum PoS currency stack.

The economic core is fixed-supply bounded by legacy PoW eCurrency issuance. Coins can still enter circulation after PoS initialization, but only through one-way migration from the legacy PoW blockchain; no additional PoS-side inflation is introduced beyond that legacy cap. Validator incentives are sustained through fee routing and Reward Fund mechanics rather than perpetual inflation. The fee-routing and Reward Fund model positions eCurrency for long-duration operation where security expenditure is internalized by protocol economics and user activity.

For external baseline context, Table 1 compares eCurrency against Bitcoin and Ethereum (post-Merge) [4], summarizing primary architectural characteristics.

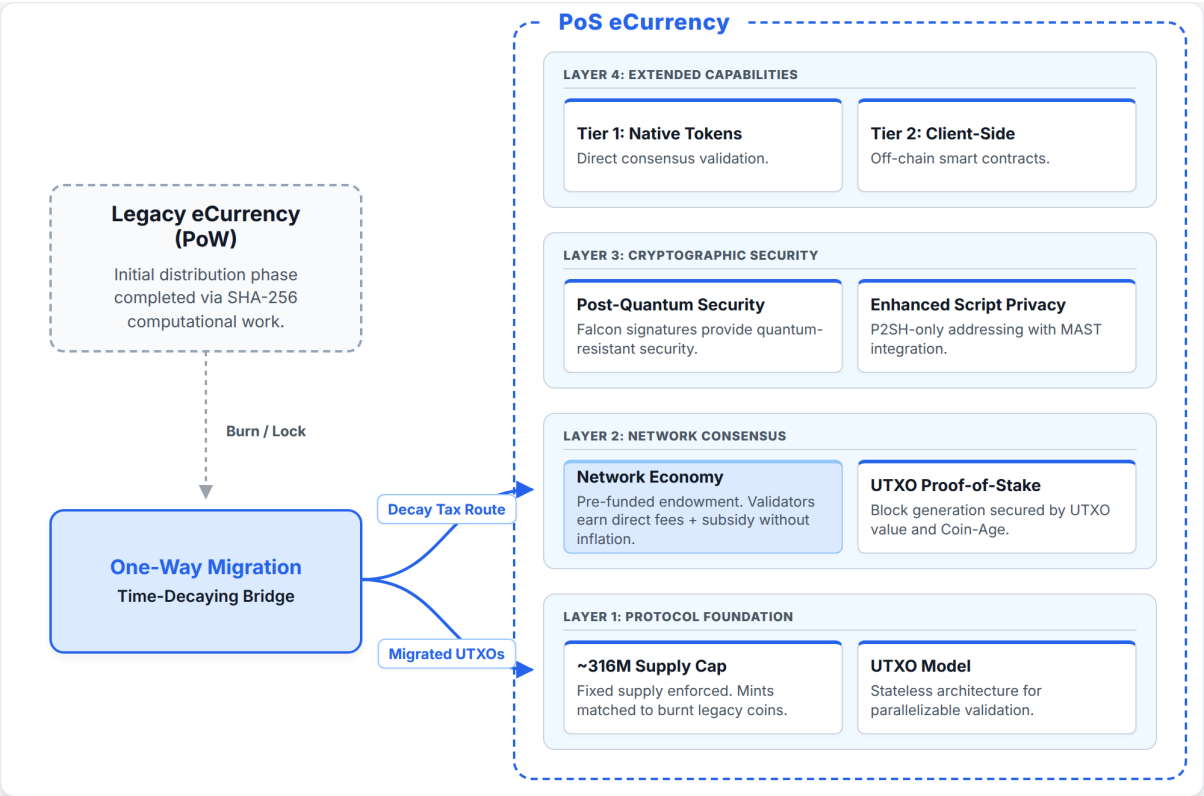

Figure 1: Overview of the eCurrency system architecture from legacy PoW eCurrency operation to post-quantum PoS currency stack.

Table 1: Comparison of major cryptocurrency design choices.

oprule **Feature**	**Bitcoin**	**Ethereum (Post-Merge)**	**eCurrency (ECR)**
Consensus	Proof-of-Work	Proof-of-Stake	UTXO Proof-of-Stake
Avg. Block Time	∼10 minutes	∼12 seconds	10 seconds
Emission Model	PoW issuance	PoS issuance + fee burn	Legacy migration; no PoS minting
Quantum Resistance	No	No (in protocol core)	Yes (lattice-based PQC)
Total Supply	21 Million	Uncapped (low inflation)	∼316 Million (Fixed)
Smart Contracts	Limited scripting	Native Turing-complete VM	Tiered: native + client-side
Native Ticker	BTC	ETH	ECR

4 Supply Migration and Validator Economics

eCurrency follows a capped-supply monetary policy and a validator reward framework designed for long-term network operation without ongoing inflationary issuance. Rather than depending on perpetual new coin creation, the system combines one-way migration from the legacy PoW eCurrency ledger, transaction-fee participation, and a protocol-managed reward reserve.

4.1 Legacy-to-PoS Upgrade Minting Path and Supply Bound

The maximum supply of eCurrency (ECR) is bounded by the legacy PoW eCurrency monetary base. Units are introduced onto the PoS ledger through one-way migration from the legacy chain rather than through discretionary issuance or PoS inflation after launch. The one-way

migration constraint enforces monetary predictability and concentrates network security design on sustainable reward routing rather than inflation.

The upgrade path follows a lock-and-claim flow aligned with the original design: a user first creates a verifiable locking transaction on the legacy PoW chain, then submits a claim transaction on the PoS chain referencing that legacy event, and validators mint the corresponding PoS-side UTXOs only after validating the legacy lock proof. A fixed migration fee is applied during the lock-and-claim conversion and routed into protocol incentives, while migrated legacy balances remain the hard cap on total PoS-side circulation.

Figure 2 summarizes the legacy-to-PoS migration and minting mechanism described above.

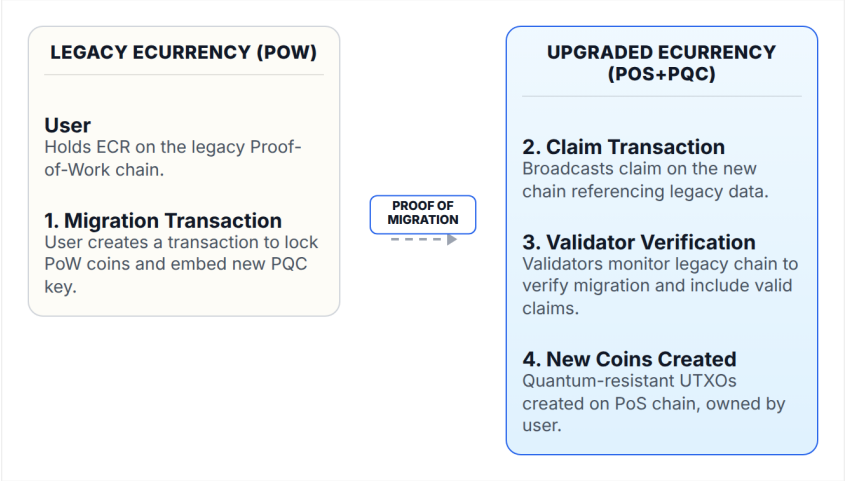

Figure 2: eCurrency legacy-to-PoS upgrade flow: lock-proof migration and capped minting on the new ledger.

4.2 Consolidated Economics: The Network Reward Fund

eCurrency maintains a Network Reward Fund that supports baseline validator compensation and smooths fee-cycle volatility. Consistent with the original design, the fund is seeded and replenished by two primary inputs: (i) a fixed migration fee applied when legacy PoW balances are upgraded to PoS, and (ii) a routed portion of transaction fees from normal block activity.

For each block with total fees F_{total}, the validator receives the payout defined in Eq. 1:

$$R_{\text{validator}} = (F_{\text{total}} \times \beta) + S_{\text{block}} \tag{1}$$

where $\beta \in [0, 1]$ is the direct validator fee-share parameter and S_{block} is a subsidy drawn from the Reward Fund. The remaining fee share, $F_{\text{total}} \times (1 - \beta)$, is routed back to the fund, matching the fee split shown in the reward-flow illustration.

Figure 3 shows the Reward Fund fee-smoothing loop used to stabilize validator compensation.

The motivation for subsidy-based smoothing is not only income stability, but also protocol liveness under low-fee conditions. In particular, it provides a durable incentive resource for zero-fee transaction handling and protocol-mandated heartbeat blocks, both of which are specified in Section 5.2. The fee-split and subsidy structure preserves market incentives for efficient block inclusion while reducing sensitivity to transient fee spikes and troughs.

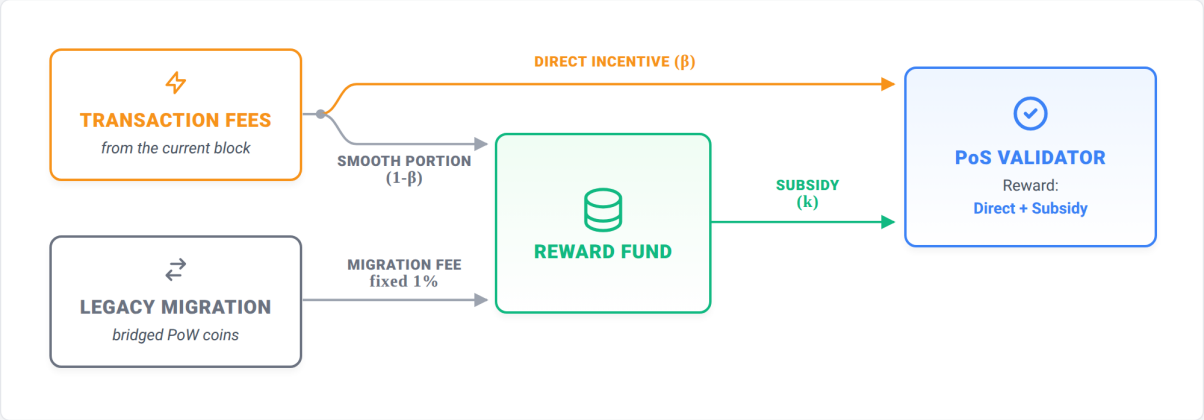

Figure 3: eCurrency Reward Fund dynamics and fee-smoothing mechanism.

4.3 Economic Rationale for Migration and Low-Fee Policies

Migration and low-fee transaction policies are designed to support safe network transition and liveness without violating capped-supply constraints. During the upgrade window, elevated migration-transaction priority improves completion reliability for legacy-to-PoS conversion under contention, while Reward Fund routing provides the economic buffer needed for low-fee operating conditions.

Protocol-level rule definitions (including heartbeat blocks, zero-fee limits, and non-mandatory zero-fee reward constraints) are specified in Section 5.2. In the present section, these mechanisms are treated as economic policy tools that balance validator continuity, user accessibility, and migration throughput.

5 Consensus: UTXO Coin-Age Proof-of-Stake

With the network capitalized through the migration-capped supply model and Reward Fund routing (Section 4), eCurrency secures the ledger using a UTXO coin-age Proof-of-Stake (PoS) protocol. The mechanism is designed to preserve asset liquidity while enabling validator circulation over time: stake weight is calculated directly as value $\times$ age (in blocks) for each staking UTXO, as formalized in Eq. 2, decoupling security from external energy expenditure and re-anchoring chain authority in native asset participation. Building on the stake-weight rule of Eq. 2, the following subsections define two additional consensus pillars: network-health transaction policies (heartbeat blocks, zero-fee boundaries, and migration priority) and a depth-sensitive fork-choice policy for deterministic finality under adverse conditions.

5.1 Block Generation and Coin-Age Weight

Validators do not compete via hash grinding. Instead, a candidate proposer assembles a stake transaction T_{stake}, and authority is computed deterministically from stake weight derived from input UTXOs.

$$W_{\text{stake}} = \sum_{i=1}^{n} (v_i \cdot a_i) \tag{2}$$

where n is the number of staking inputs, v_i is the nominal value of input i, and a_i is UTXO

age in blocks. The proposer with the highest valid W_{stake} in the timeslot wins block production rights. Because v_i and a_i are historical ledger facts, validators cannot improve winning probability through nonce-style computational search.

Upon successful proposal, the consumed stake inputs are spent and replaced by new outputs with age zero. The coin-age reset creates a natural rotation effect in stake influence, preserving liquidity while discouraging static concentration of block-production authority.

5.2 Network Health and Transaction Prioritization

Because validator compensation is jointly sourced from direct fee share and Reward Fund subsidy, eCurrency can safely enforce liveness and migration-priority policies:

- **Mandatory Heartbeat Blocks:** To preserve synchronization and confirmation progress under low demand, the protocol requires a mandatory block every 100th timeslot. Mandatory blocks may be empty (containing no transactions) and remain reward-eligible under Reward Fund subsidy rules. Empty blocks produced outside mandatory timeslots are considered invalid and are rejected by the network.
- **Zero-Fee Transaction Allowance:** The protocol allows at most one zero-fee transaction per block. However, a validator receives no reward for producing a non-mandatory block that contains only that zero-fee transaction to prevent network flood with low-value transactions.
- **Migration Transaction Priority:** Transactions bridging balances from the legacy PoW eCurrency chain to eCurrency are assigned an intrinsic scheduling multiplier $\gamma_{\text{mig}} > 1$. The elevated multiplier raises inclusion priority during contention and accelerates safe migration completion.

5.3 Fork Choice and Reorganization Policy

Nodes adopt the valid chain with maximal cumulative stake weight W_{chain}. To harden short- and medium-depth history against malicious rewrites while preserving long-horizon partition recovery, fork adoption is gated by a depth-sensitive reorganization penalty.

For a competing fork C_{fork} attempting to replace canonical history C_{current}, the acceptance condition is given by Eq. 3:

$$W_{\text{chain}}(C_{\text{fork}}) > W_{\text{chain}}(C_{\text{current}}) \cdot P(d_{\text{eff}}) \tag{3}$$

where d_{eff} is reorganization depth minus a 16-block propagation buffer. The penalty function is defined in Eq. 4:

$$P(d_{\text{eff}}) = \begin{cases} 1 & \text{if } d_{\text{eff}} < 8 \\ d_{\text{eff}}/8 & \text{if } 8 \leq d_{\text{eff}} < 256 \\ 32 & \text{if } 256 \leq d_{\text{eff}} < 900 \\ 960/\sqrt{d_{\text{eff}}} & \text{if } 900 \leq d_{\text{eff}} < 921600 \\ 1 & \text{if } d_{\text{eff}} \geq 921600 \end{cases} \tag{4}$$

The penalty curve of Eq. 4 yields five deterministic security regimes:

- **Grace Window:** Low-depth reorganizations pass with unit multiplier, accommodating normal latency.
- **Linear Ramp:** Required competing weight scales linearly with depth.
- **Plateau:** A 32x threshold protects medium-depth history.
- **Decay:** The threshold decays by $1/\sqrt{d_{\text{eff}}}$ to permit eventual reconvergence after major partitions.
- **Normalization:** Very deep historical divergence reverts to baseline cumulative-weight comparison.

The resulting policy combines practical near-term finality with deterministic long-term healing behavior.

Figure 4 visualizes the depth-sensitive penalty profile used by the fork-choice rule.

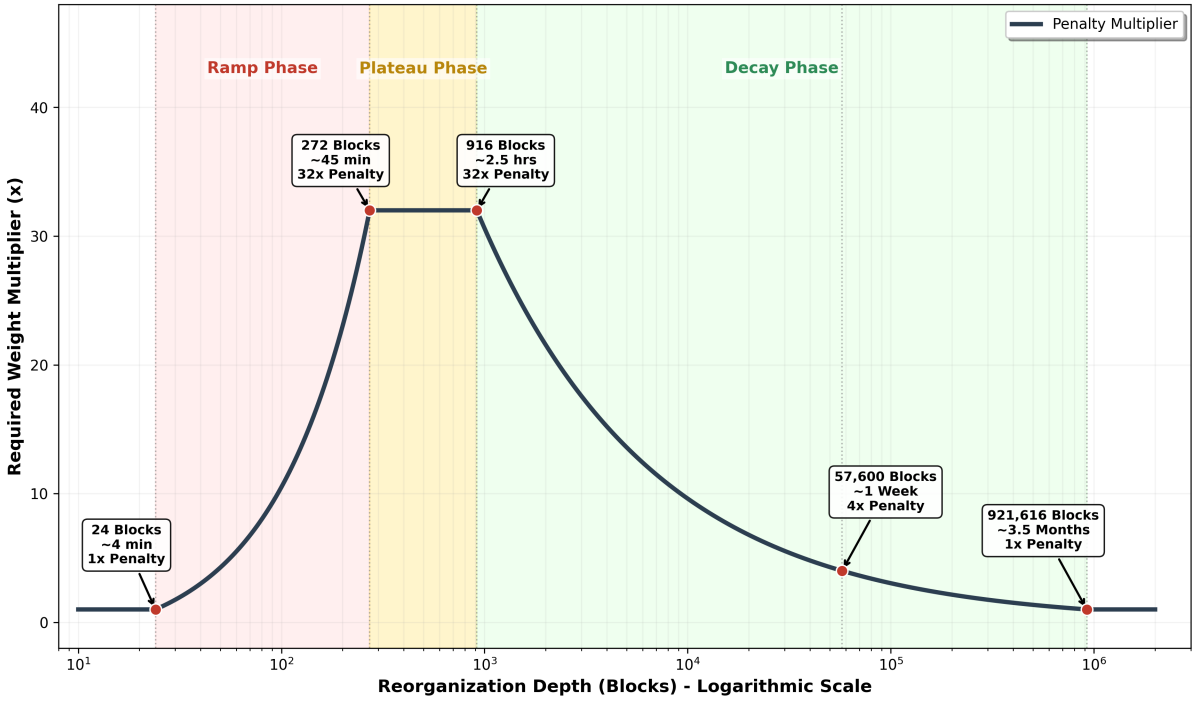

Figure 4: Reorganization penalty profile for PoS fork-choice protection.

6 Cryptographic and Architectural Upgrades

With the economic foundation and consensus mechanisms established, the eCurrency architecture introduces key cryptographic upgrades. These upgrades enhance robustness, privacy, and efficiency, including a simplified P2SH-only address system, the integration of lattice-based post-quantum cryptography, and enhanced script privacy through Merklized Alternative Script Trees (MAST).

6.1 Simplified Address System (P2SH-Only)

To eliminate the complexity associated with multiple address types (e.g., P2PKH, P2SH, SegWit), the upgraded protocol exclusively utilizes a Pay-to-Script-Hash (P2SH) model. Transaction outputs commit to the hash of the script, while inputs provide the pre-image script itself alongside signatures. The P2SH-only model inherently prevents transaction malleability and simplifies protocol integration for wallets and developers.

6.2 Post-Quantum Cryptography (PQC)

The advent of quantum computers poses an existential threat to cryptocurrencies relying on elliptic curve cryptography (ECDSA) [5]. Specifically, Shor's algorithm renders legacy secp256k1 signatures vulnerable to future private key derivation. To address the quantum threat, eCurrency mandates the use of a standardized post-quantum signature algorithm for all transactions.

We propose the adoption of Falcon [5], an algorithm selected for standardization by the U.S. National Institute of Standards and Technology (NIST) [3]. While all post-quantum signature schemes inherently require larger key and signature sizes than classical ECDSA, Falcon is well-suited for blockchain applications compared to other NIST finalists (such as Dilithium/ML-DSA or SPHINCS+). Its security is based on the hardness of the Short Integer Solution (SIS) problem over NTRU lattices, which allows it to generate compact digital signatures paired with fast verification times.

By integrating Falcon, eCurrency achieves the following:

- **Long-Term Security:** The chain is proactively secured against future threats from quantum adversaries, protecting supply integrity and user funds over long horizons.
- **Optimized Scalability Trade-offs:** While PQC introduces a larger data footprint than legacy ECDSA, Falcon minimizes the inevitable size increase relative to alternative schemes and offers fast verification to reduce CPU overhead during validation.
- **Standardization and Auditability:** Relying on a NIST-selected algorithm ensures that the cryptographic primitives have undergone extensive public and academic scrutiny.

6.3 Enhanced Script Privacy with MAST

To further enhance user privacy, minimize on-chain data footprint, and reduce public-key exposure to quantum threats, eCurrency integrates a mechanism inspired by Bitcoin's Merklized Alternative Script Trees (MAST) and the conceptual goals of Pay-to-Merkle-Root (BIP 360). Crucially, rather than introducing a separate address type, eCurrency embeds the MAST capability directly within the existing P2SH standard.

The UTXO still pays to a standard script hash, but new opcodes allow the underlying script to support Merkle path and target-script verification. The extended script model allows a UTXO to be locked to the Merkle root of a tree containing multiple alternative spending conditions.

When the UTXO is spent, only the script branch that is actually used and its corresponding Merkle proof are revealed on-chain. The existence of all other possible branches remains private and does not consume block space.

MAST capability is enabled through two new opcodes, `OP_MASTVERIFY` and `OP_EXEC`, designed to work within a standard P2SH redeem script, for example:

```
<MerkleRoot> OP_MASTVERIFY OP_EXEC
```

- **OP_MASTVERIFY:**
  - **Operation:** Verifies that a script is a valid leaf of a Merkle tree rooted at a specific hash.
  - **Stack Transition:**
    `<LeafScript> <MerklePath> <MerkleRoot>` $\rightarrow$ `<LeafScript>`
  - **Logic:** The opcode computes the Merkle root from `LeafScript` and `MerklePath`. It then verifies that the recomputed root matches `MerkleRoot`. If the check passes, path and root are popped, leaving only `LeafScript`; if it fails, the transaction is invalidated.
- **OP_EXEC:**
  - **Operation:** Treats the data on top of the stack as a script and executes it.
  - **Stack Transition:**
    `<LeafScript>` $\rightarrow$ `<Result>`
  - **Logic:** The top stack item is deserialized as executable script code and run in the current context.

The resulting spend flow is compact and deterministic: signatures, the selected leaf script, and the Merkle proof are provided; membership is verified first; then only the verified branch is executed.

6.4 Open Source and RPC Interoperability

To ensure immediate viability and developer adoption, eCurrency node software is open-source. The node exposes an RPC API compatible with familiar Bitcoin-style infrastructure workflows, allowing exchanges, explorers, and related services to integrate with minimal friction. The software is also deployable through standard containerization workflows (Docker), improving cross-platform reproducibility.

7 Smart Contracts and Extended Capabilities

7.1 Design Philosophy: Hybrid Validation for Scale

The eCurrency smart-contract architecture follows a hybrid validation model intended to preserve base-layer determinism while enabling broad application expressiveness. Rather than forcing arbitrary computation onto every validating node, the protocol separates lightweight consensus-native asset logic from advanced client-side execution pathways [6, 7].

7.2 Tiered Execution Model

Tier 1: Native Embedded Tokens. For standard tokenized assets, validation is integrated into consensus rules. Nodes recognize a dedicated token transaction class without maintaining a global virtual-machine state. The consensus-native approach keeps validation pathways compact, predictable, and compatible with consumer-grade hardware.

A native token transaction carries a `token_id` field, defined as the hash of the asset-genesis transaction. If `token_id` is empty, the transaction is interpreted as genesis for a new token class. To preserve fast verification, each token transaction is constrained to a single token type.

Token outputs are separated into two deterministic categories:

- **Transfer Outputs:** Carry token amount as a fixed-width integer.
- **Control Outputs:** Carry ordered administrative attributes, including a `permissions` bitmask and metadata fields such as `decimals`, `name`, and `symbol`. The `decimals`, `name`, and `symbol` fields are accepted only at genesis.

Unknown control attributes are ignored by consensus to preserve forward compatibility and reduce hard-fork pressure. The deterministic, non-Turing-complete token path is intentionally aligned with UTXO-script reliability and avoids gas-estimation uncertainty.

Tier 2: Client-Side Contracts. For higher-complexity applications, execution is externalized to participating clients and services. The chain acts as a commitment and data-availability layer: transaction outputs may include arbitrary `data` payloads, while interpretation and state progression are managed off-chain by contract-aware participants.

The client-side execution model prevents base-layer state bloat and avoids global execution contention while retaining verifiable settlement anchors on-chain.

Figure 5 illustrates the multi-party UTXO flow for client-side contract interaction with deterministic on-chain settlement anchors.

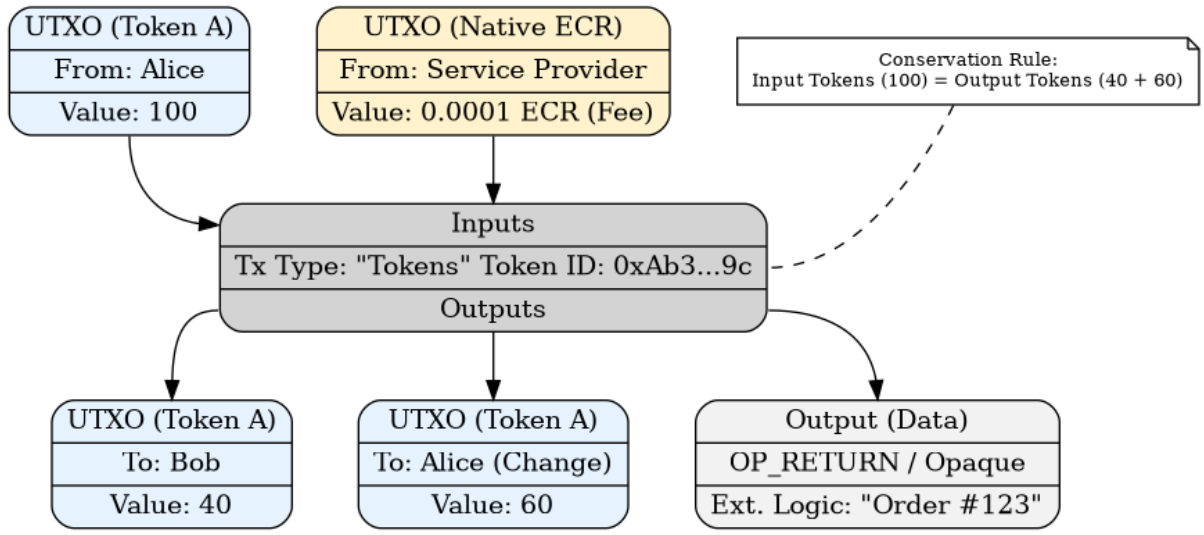

Figure 5: Example multi-party UTXO transaction flow supporting client-side contract logic and deterministic on-chain settlement anchoring.

7.3 UTXO Implementation and Exchange Semantics

The UTXO model enables atomic value movement without account-style global state transitions. Fees are deterministic and independent of virtual-machine execution outcomes.

For decentralized exchange behavior, eCurrency supports cryptographically linked transfer patterns (e.g., hash/timelock-linked swaps) across coordinated transactions:

- **Transaction A:** Party 1 transfers Token A to Party 2.

- **Transaction B:** Party 2 transfers Token B to Party 1.

Settlement conditions are constructed so one leg cannot finalize safely without the other, enabling trust-minimized exchange without global AMM-state overhead.

7.4 Design Lineage and Security Properties

The model synthesizes several proven approaches:

- **Mint-Authority Baton Pattern (SLP lineage):** Administrative mint rights are represented by explicit control outputs and consumed/reissued by rule [8].
- **Consensus-Level Asset Validation (Ravencoin lineage):** Token conservation is verified by consensus rather than trusted indexers [9].
- **Client-Side Validation (CSV/RGB lineage):** Rich contract logic executes client-side while base-layer commitments remain auditable [6, 7].

7.5 Planned Ecosystem Deliverables

Near-term priorities include token standards, wallet capabilities, developer documentation, and integration pathways for exchanges and payment tooling. The project provides an official non-custodial web wallet at https://ecurrency.org, intended as a baseline self-custody access layer for users and integrators [10]. In parallel, eCurrency (ECR) is actively traded on the BlackBit exchange, which presently functions as the initial liquidity hub while broader exchange integrations are pursued [11].

Longer-term priorities include advanced contract modules, scaling layers, and interoperability research.

8 Roadmap: Currency-First Rollout

8.1 Phase 1: Legacy Foundation and Transition Readiness (2018–2025)

- **Legacy PoW eCurrency Operation:** Establish baseline distribution, network participation, and ecosystem primitives.
- **Transition Design Finalization:** Define fixed-supply invariants, migration policy, and PoS security objectives.

8.2 Phase 2: PoS Activation and Security Hardening (2025–2026)

- **Consensus Launch:** Activate UTXO-based PoS with value-age stake weighting, heartbeat blocks, and reorganization-penalty fork policy.
- **PQC Deployment:** Enable post-quantum signature pathways, key-rotation tooling, and P2SH-by-default transaction standardization.
- **Economic Reserve Activation:** Enable Reward Fund routing, fee-smoothing parameters, and subsidy controls for stable validator incentives.

8.3 Phase 3: Migration Completion and Ecosystem Expansion (2026–2027)

- **Migration Throughput Prioritization:** Sustain elevated inclusion weight for legacy-to-PoS migration transactions until operational migration goals are met.
- **Wallet and Custody Integrations:** Broaden support for consumer and institutional access, including official non-custodial web pathways.
- **Market and Payments Tooling:** Expand exchange integrations beyond initial liquidity venues and improve merchant-settlement UX.

8.4 Phase 4: Utility Scale and Governance Maturity (2027+)

- **Contract and Throughput Extensions:** Expand Tier-2 client-side contract tooling and optional scaling layers.
- **Governance Maturity:** Establish stable upgrade cadence with transparent policy constraints and long-horizon operational controls.
- **Steady-State Security Budget:** Operate with fixed-supply monetary discipline and validator incentives sustained by fees plus Reward Fund dynamics.

Figure 6 provides a visual summary of these phased rollout milestones.

9 Conclusion

eCurrency represents a currency-first evolution of decentralized ledger design: fixed-supply discipline, efficient UTXO-based PoS consensus, and post-quantum transaction security. Critically, the eCurrency architecture preserves historical monetary continuity by recognizing the legacy PoW era as the initial supply-distribution phase, then transitioning security to PoS through a one-way validated upgrade mechanism from the legacy chain.

The protocol combines practical throughput, predictable validator incentives, and a scalable smart-contract roadmap while preserving open-source operability and ecosystem integration paths. By coupling PoW-origin supply distribution with an orderly PoW-to-PoS migration and stewardship model, eCurrency is positioned as a long-horizon digital currency architecture oriented toward durability, security, and real-world utility.

Disclaimer

This document is provided solely for informational and technical discussion purposes. It does not constitute financial, investment, legal, tax, accounting, or other professional advice, and it should not be interpreted as an offer, solicitation, or recommendation to purchase, sell, or hold any asset, token, instrument, or security in any jurisdiction.

No representation or warranty is made regarding future performance, liquidity, regulatory treatment, or market adoption of the eCurrency network or related assets. Participation in digital-asset networks involves substantial risk, including but not limited to extreme market volatility, technological failure, smart-contract or protocol defects, cybersecurity incidents, adverse regulatory action, reduced liquidity, and partial or total loss of principal.

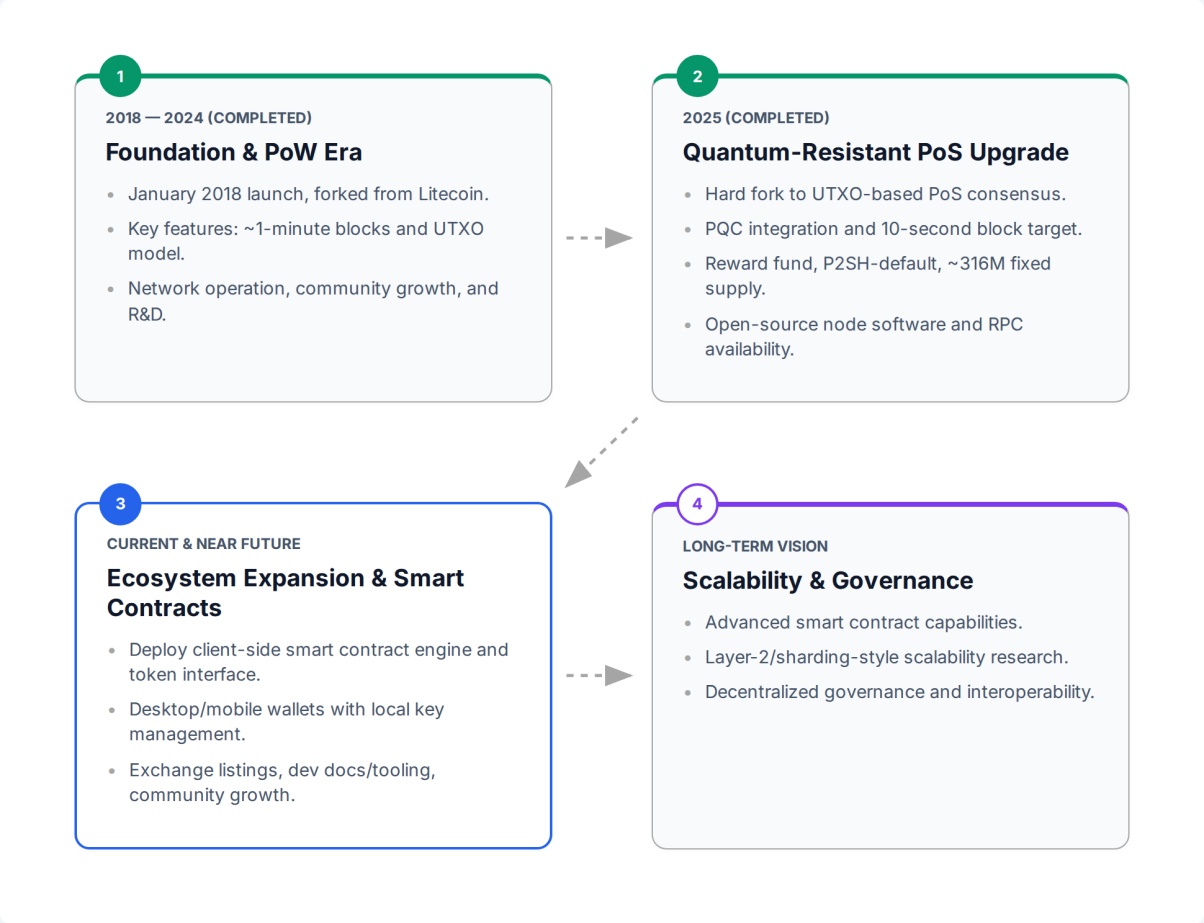

Figure 6: eCurrency phased rollout from protocol launch to mature currency operations.

Readers and participants are solely responsible for conducting independent due diligence and for obtaining advice from qualified professional advisers before making any financial or legal decisions related to eCurrency, including the ECR token.

References

[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Self-published whitepaper, 2008.

[2] Litecoin Project. Litecoin official website. https://litecoin.org, 2026. Accessed: 2026-03-15.

[3] National Institute of Standards and Technology. Nist announces first four quantum-resistant cryptographic algorithms, July 2022. Official Announcement. Available at https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms.

[4] Ethereum Foundation. Ethereum official website. https://ethereum.org, 2026. Accessed: 2026-03-15.

[5] Thomas Prest, Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang. Falcon: Fast fourier lattice-based compact signatures over NTRU, 2020. Submission to the NIST Post-Quantum Cryptography Standardization Process, Round 3. Available at https://falcon-sign.info/falcon.pdf.

[6] Peter Todd. Scalable semi-trustless asset transfer via single-use-seals and proof-of-publication. https://petertodd.org/2017/scalable-single-use-seal-asset-transfer, 2017. Accessed: 2026-03-15.

[7] LNP/BP Standards Association. RGB blackpaper: Client-side validation for Bitcoin & Lightning. Technical report, LNP/BP Standards Association, 2023. Accessed: 2026-02-07.

[8] Jonald Lundeberg et al. Simple ledger protocol (SLP) specification. https://github.com/simpleledger/slp-specifications, 2018. Accessed: 2026-02-22.

[9] Tron Black, Bruce Fenton, and Joel Weight. Ravencoin: A peer-to-peer electronic system for the creation and transfer of assets. https://ravencoin.org/whitepaper/, 2018. Accessed: 2026-02-07.

[10] eCurrency Project. ecurrency official website and non-custodial wallet. https://ecurrency.org, 2026. Accessed: 2026-03-14.

[11] BlackBit Exchange. Blackbit exchange market listing for ecr. https://blackbit.exchange, 2026. Accessed: 2026-03-14.