2025 Q3 Newton Protocol Disclosures Update

October 31, 2025

Protocol Evolution

Since the publication of the initial Newton Protocol transparency report, the project has undergone a significant technical and conceptual evolution. Originally envisioned as a keystore rollup built for key management, the design has matured into a broader, more foundational layer: a decentralized policy engine for onchain compliance and the agentic economy.

This evolution reflects both developer and community feedback as well as architectural learnings. The original keystore rollup design focused specifically on verifiable automation and delegated authorization for agents, allowing onchain execution through controlled, cryptographically verified permissions. Over time, it became clear that the same primitives enabling verifiable automation for agents could extend far beyond agent authorization to a broader framework for programmable verification and policy enforcement for agentic AI, stablecoins, RWAs & the $250T asset market.

The updated Newton Protocol builds on these foundations, evolving from key- and intent-level verification to a generalizable policy engine that governs what actions may occur, under what conditions (including both onchain and offchain conditions), and with what attestations. The Protocol retains the deterministic guarantees and cryptographic integrity of the rollup model while expanding its scope into a universal policy layer, enabling compliant, verifiable, and composable automation across agents, applications, and financial systems.

1) Overview[1]

What's changed: Newton Protocol has progressed from an agent-focused automation framework to a decentralized policy engine that governs onchain actions with verifiable, programmable rules. It now provides pre-transaction policy enforcement and real-time authorization for any intent initiated by agents, applications, or users, extending trustless automation into compliant and verifiable finance. Through cryptographic attestations and zero-knowledge proofs, Newton Protocol allows offchain data and policies, such as KYC

[1] The section numbering that follows corresponds to the initial Transparency Report and outlines the architectural shift and update to the Protocol's scope, roadmap, and technology stack to reflect the policy-engine direction.

credentials or regulatory constraints, to be enforced onchain with the same deterministic guarantees as native protocol logic.

What Newton Protocol is now: A modular policy layer that lets application owners define, enforce, and prove rules (before settlement) using reusable policies ("NewtonPermissions"). Policies are enforced by a decentralized operator quorum (AVS), with attestations that contracts can verify onchain.

What this enables:

- **Agent safety & alignment:** Agents act only within user- or app-defined constraints.
- **Compliance as code:** Stablecoins, RWAs, exchanges/vasps, and treasury/payment flows can embed programmatic KYC/AML, travel-rule, limits, and business and jurisdictional logic.
- **Composability & neutrality:** Rules are programmable and portable; Newton Protocol doesn't just dictate *what* to allow but also provides verifiable *how*.

2) Project & Protocol

Newton Protocol has evolved into a foundational policy engine for verifiable authorization, enabling any onchain or offchain system to define, enforce, and prove behavioral rules before execution. It moves the focus of trust from *who signs* a transaction to *what conditions must be satisfied* for that transaction to occur.

Purpose and Design Philosophy

At its core, Newton Protocol introduces programmable policy enforcement: a neutral layer that ensures every action taken by an agent, application, or smart contract adheres to transparent, verifiable criteria. Policies can encode business logic, compliance requirements, or user-defined safety rules, all validated cryptographically before an action executes.

This approach delivers three essential outcomes:

- **Deterministic trust:** Applications can prove that each action was authorized under a verifiable policy, without relying on centralized gatekeepers.
- **Interoperability:** Policies are portable and composable across chains, contracts, and agent frameworks.
- **Transparency and auditability:** Each authorization event produces a verifiable receipt, forming a permanent record of compliant behavior.

Core Entities

Newton Protocol is organized around three cooperating roles that mirror traditional real-world control systems:

1. **Applications** – define policies and request evaluations for specific actions or transactions.

2. **Operators** – decentralized validators who evaluate those policies by verifying whether proposed intents comply with the stated rules.

3. **Data Providers** – sourced by application developers to supply onchain and off-chain inputs required for policy evaluation, such as identity attestations, risk scores, or regulatory lists.

Together, these entities create a continuous authorization loop: policies are defined → evaluated → enforced → recorded.

Policy Evaluation Flow

When an application initiates an action, it submits a task evaluation request to the Newton Protocol AVS (Actively Validated Service).

1. The Task Manager contract broadcasts the request, which is picked up by the registered operators.

2. Operators verify that the intent meets the policy's criteria, signs their results, and sends them to an Aggregator, which produces a single BLS-aggregated signature.

3. The application then embeds this aggregated authorization receipt into its transaction, which the target contract verifies before execution.

This process ensures every transaction is validated *before* it is finalized on-chain.

Verification

Newton Protocol provides enforcement via AVS crypto-economic consensus. More specifically, a quorum of restaked operators evaluate policies using Rego (OPAL/OPA) rules and co-sign a BLS-aggregated authorization receipt. Operators are slashable for misbehavior, ensuring economic security.

Data Providers and External Inputs

The modular Data Provider architecture extends Newton Protocol beyond onchain data. It allows policies to reference offchain facts, such as KYC credentials or sanctions lists, through verifiable adapters. Each adapter must produce proof of freshness and integrity using trusted execution environments (TEEs), ZK proofs, or cryptographic signatures. This architecture enables Newton Protocol to serve as a compliance and risk layer for decentralized finance and agentic systems without sacrificing privacy or composability.

Developer Experience

Developers interact with Newton Protocol through lightweight client contracts and SDKs:

1. **Define a policy** by deploying a `NewtonPolicy` instance and registering its hash.
2. **Submit an intent** for evaluation via the Newton Protocol API or SDK.
3. **Receive a verifiable authorization receipt** containing the aggregated signature or proof.
4. **Verify on-chain** using the `NewtonPolicyClient` mixin in the application contract.

This flow keeps integration simple while providing formal proofs of policy adherence.

Key Advantages

- **Programmable Compliance:** Encode and enforce regulatory or risk rules directly in smart contracts.
- **Agent Safety:** Constrain AI or autonomous agents to pre-approved actions within their mandates.
- **Audit Trail:** Each authorization is verifiable and recorded, offering clear transparency for users and regulators.
- **Chain-Agnostic:** Newton Protocol operates as a layer across EVM chains and can extend to other execution environments over time.

3) Roadmap

The next phase of Newton Protocol's development focuses on translating the policy engine architecture into robust, verifiable infrastructure that can serve both developer and institutional use cases. Following the transition from the keystore rollup design, the near-term roadmap emphasizes establishing the core authorization network, enabling policy programmability, and demonstrating end-to-end verifiable execution across key integrations.

In the initial alpha mainnet phase, the project has deployed the Actively Validated Service (AVS) layer responsible for decentralized policy evaluation. This network will allow developers to submit intents for validation and receive cryptographic receipts confirming policy compliance before a transaction executes. Alongside the AVS, a set of developer tools will make it possible to compose and test policies directly in application environments. These tools will include SDKs, example contracts, and a Policy Explorer which enables public task and policy exploration similar to a blockchain explorer. The alpha mainnet phase will focus on building with a permissioned group of developers for early use-case testing, stability and performance observations, validator on-ramping, and initial audit of the policy and task management contracts.

As the protocol transitions over time to mainnet general availability ("MGA"), Newton Protocol will formalize its verification standards. The MGA phase will introduce the early stages of decentralized policy evaluation, to be supported by threshold-based operator quorums, and a public challenge mechanism to ensure correctness. Zero-knowledge (ZK) verification paths will be integrated for policies requiring cryptographic proofs rather than human-readable evaluations. This release will also include an open indexer and explorer, providing transparent data on operator health, policy performance, and attestation history.

Subsequent phases will extend Newton Protocol's capabilities into data connectivity and institutional adoption. Through various Data Provider adapters, developers and partners will be able to reference verifiable data inputs directly in policy logic, such as sanctions lists, KYC credentials, or risk scoring feeds. This will enable compliant asset transfers, permissioned DeFi participation, and agent-level controls for enterprise or regulated users.

Overall, the roadmap reflects Newton Protocol's evolution from an experimental keystore rollup into a foundational policy verification layer for programmable, compliant automation. Each milestone builds toward a system capable of enforcing complex policies transparently and interoperably across onchain ecosystems.

4) Technology & Infrastructure

The Newton Protocol now operates as a modular system that connects onchain policy enforcement with offchain cryptographic validation. Its design is structured around a simple principle: before any transaction is executed, the conditions governing that transaction must be provably satisfied.

At its core, Newton Protocol consists of two complementary layers. The onchain layer, including the `NewtonPolicy`, `NewtonProverTaskManager`, and `NewtonPolicyClient` contracts, defines how policies are referenced, authorized, and verified. This layer ensures determinism: an action can only proceed if the submitted authorization matches an attested policy outcome. The offchain layer, implemented through Newton Protocol's AVS (Actively Validated Service) network, handles policy evaluation. Independent operators validate whether an intent conforms to the stated policy and co-sign a verifiable authorization receipt using aggregated BLS signatures. These receipts can be verified by any smart contract, providing strong cryptoeconomic guarantees that policy conditions were honored.

Complementing these two layers is the Data Provider, which bridges offchain information into policy evaluation. Using trusted execution environments (TEE), cryptographic attestations, or zero-knowledge proofs, this subsystem allows policies to rely on verifiable external data, such as identity attestations, risk signals, or compliance lists, without exposing private user information. Together, these components enable flexible yet trustworthy policy enforcement across a range of financial, agent, and application contexts.

Security and transparency are built into the architecture. Each policy evaluation produces an auditable trail of onchain events (e.g., `TaskCreated`, `TaskResponded`, `AttestationSpent`) allowing independent observers to confirm when and how decisions were made. Operator behavior is economically secured through stake-backed slashing, ensuring that invalid attestations can be challenged and penalized. The system's modularity also allows different proof types to coexist: ECDSA and BLS signatures for lightweight authorization, SP1-compatible zk proofs for higher assurance, and eventually, Groth16 or RISC0 proofs for privacy-preserving use cases.

From an operational standpoint, Newton Protocol is designed for performance and observability. The AVS aims to maintain sub-second response times for common policy evaluations, with verification steps reduced to a single proof and a single aggregated signature. An open indexer and explorer will make policy data, operator statistics, and attestation health publicly viewable, providing transparency for both users and developers.

Through this architecture, Newton Protocol extends the reliability once reserved for execution consensus into the domain of policy consensus. This represents a critical step in enabling safe, compliant, and verifiable automation across the onchain ecosystem.

6) Token Characteristics & Utility

The Newton Protocol token (NEWT) underpins the network's economic and security model. It aligns incentives among participants, enforces accountability, and enables the decentralized validation and governance functions that power policy evaluation and compliance-as-code infrastructure.

The token's role has not changed in its financial or economic fundamentals, but its functional utility has expanded to reflect the evolution of the Protocol from a keystore-focused rollup to a policy validation and compliance engine. Whereas the original model primarily tied NEWT to functions within a keystore ecosystem, the updated model positions NEWT as the native coordination asset that secures the Actively Validated Service (AVS) layer and facilitates permissionless participation in the policy network.

Core Functional Roles of NEWT

1. **Network Security and Staking**
   Operators participating in policy evaluation will stake NEWT to register and maintain active status within the Newton Protocol's AVS. Staking aligns economic incentives: operators are rewarded for accurate and timely policy evaluations and are subject to slashing penalties for provable misbehavior, downtime, or submission of invalid attestations. This staking mechanism ensures that the integrity of the network scales with economic weight, creating a verifiable trust model anchored in the token itself.

2. **Delegation and Restaking**
   Token holders who do not wish to operate infrastructure directly can delegate NEWT to trusted operator nodes. Over time, Newton Protocol will integrate with restaking frameworks such as EigenLayer, allowing NEWT holders to secure multiple AVS instances and earn cross-protocol yield while contributing to network resilience.

3. **Policy Evaluation Fees**
   Applications that submit transaction intents or policy evaluation requests to the network pay service fees denominated in NEWT (or ETH-equivalent assets). These fees are distributed to active operators (and NEWT holders that delegate to operators) in proportion to their contribution to the policy evaluation and proof-generation process. This fee structure incentivizes continuous participation and high performance among validator sets while creating recurring demand for the token.

4. **Challenge and Dispute Resolution**
   Challengers play a vital role in maintaining accountability by verifying operator responses and submitting fraud proofs during challenge windows. Challengers must stake NEWT to raise a dispute and receive rewards if the challenge is upheld, ensuring rational behavior and strong adversarial checks throughout the system.

In summary, NEWT continues to function as both collateral and an economic coordination asset, but its utility has deepened with the Protocol's evolution from keystore rollup to policy engine. As Newton Protocol matures, the token's purpose extends beyond simple staking to become the economic fabric that ensures fair participation, data integrity, and decentralized control across all layers of verifiable policy enforcement.

11) Protocol Governance

Newton Protocol's governance framework continues to evolve toward its long-term goal of becoming a secure, neutral, and decentralized policy infrastructure that can serve both traditional and crypto-native ecosystems. Governance remains central to ensuring that the Protocol's evolution reflects the interests of its participants while maintaining the highest standards of security, transparency, and credible neutrality.

Following the initial framework established in the original Transparency Report, the Foundation has formally initiated Phase 0: Governance Planning. This phase focuses on establishing the groundwork for responsible decentralization: clarifying roles, principles, and participation structures before any formal voting or protocol-level decision-making begins. For more information on Phase 0 of governance, please see the Foundation's official governance update: https://docs.newt.foundation/governance/governance-model. This is the beginning of the structured progression as part of the original framework, confirming that the Foundation remains responsible for oversight during the early build-out period, with decentralization proceeding as the Protocol matures and adoption broadens.

Additional Reporting

As the Newton Protocol continues its transition from a keystore rollup to a policy engine—and from concept to implementation—the immediate focus remains on building and validating its technical foundations rather than activating its economic subsystems. Because the Protocol is still in an alpha mainnet stage, the economic functions described above, such as staking, delegation, challenge resolution, and policy evaluation fees, are not yet active as part of a MGA phase.

The Protocol's tokenomics, outlined previously, represent the intended long-term structure, but these mechanisms will not meaningfully operate until the system is fully developed and reaches a sufficiently mature phase. Until that time, reporting will center on technical progress: engineering milestones, system readiness, and protocol validation. Once the Newton Protocol achieves full operational maturity, the Foundation will initiate its regular financial and token reporting consistent with its long-term transparency commitments.

Exhibit A: Onchain Addresses

An additional Foundation multi-sig wallet is added under Liquidity Support:

0xba555FEf68C54D94ed19b564b1791e088d79B5cf