



[Home](#) [Licensing](#) [Patents](#) [Articles](#)

Post-Quantum Alignment: Hash-Based Security Without Vulnerable Hardness Assumptions

by [Nick Clark](#) | Published March 27, 2026 | [PDF](#)

Security based on hash preimage resistance and per-step unpredictability rather than hardness assumptions vulnerable to quantum algorithms. Within the keyless identity system, this capability operates as a structural primitive at the identity level. It is not an optional enhancement or a configurable plugin but a mandatory architectural property that every participant encounters. The result is a system where post-quantum alignment is enforced by construction rather than by convention, policy, or external oversight.

What It Is

Security based on hash preimage resistance and per-step unpredictability rather than hardness assumptions vulnerable to quantum algorithms. This is a structural mechanism within the keyless identity system that operates at the identity level. It is not advisory, not configurable at the discretion of individual participants, and not dependent on external enforcement infrastructure.

Every interaction within the system encounters this mechanism as a mandatory constraint. The behavior it produces is deterministic: given the same inputs and the same system state, the outcome is identical regardless of which node evaluates it, when the evaluation occurs, or what substrate hosts the computation.

Why It Matters

Conventional identity systems address this problem through persistent cryptographic keys, certificates, or biometric databases. These approaches function adequately under controlled conditions but introduce structural fragility when keys are compromised, certificates expire, or databases are breached. The underlying assumption that stored credentials remain secure over their lifetime becomes a liability precisely when reliability matters most.

Post-quantum alignment removes this fragility by embedding the relevant capability directly into the identity layer. There is no external dependency that can fail independently, no middleware that can be misconfigured, and no trust assumption that can be violated by a single compromised participant. The guarantee is structural.

How It Works

The mechanism operates through deterministic evaluation embedded in the keyless identity system. When a relevant operation is initiated, the system evaluates the applicable structural constraints against the current state. This evaluation consults the fields, policies, and lineage records that travel with the objects themselves rather than relying on external state that may be stale, unavailable, or compromised.

The outcome of each evaluation is recorded in an append-only lineage structure. This record is cryptographically committed, ensuring that the complete history of decisions, transitions, and state changes remains auditable and tamper-evident. No evaluation outcome can be retroactively altered without breaking the cryptographic chain.

Because the evaluation logic and the data it operates on travel together, the mechanism functions identically across network partitions, substrate migrations, and administrative boundaries. There is no central evaluation point that must be available for the system to operate correctly.

What It Enables

With post-quantum alignment as an architectural primitive, systems built on this foundation can operate autonomously while maintaining the structural guarantees that centralized architectures achieve through oversight. The capability is not a tradeoff between autonomy and governance but a resolution of the apparent conflict between them.

This enables deployment across centralized cloud infrastructure, federated multi-party environments, fully decentralized networks, and edge installations with intermittent connectivity. The structural guarantees hold regardless of deployment topology because they are properties of the objects and protocols themselves, not properties of the infrastructure that hosts them.

[Keyless Identity All 21 steps →](#)

Identity from accumulated continuity. Post-quantum by construction.

Patent

[US 19/388,580](#) · published

Primary Technical Disclosure

◦ [Stateless Device Pseudonymity and Secure Messaging in Cognition-Native Systems](#)

Secondary Technical

◦ [Continuity-Based Biological Identity Using Trust-Slope Validation](#) ◦ [Trust Slope as Identity Primitive: Cumulative Hash Chains Replace Static Credentials](#) ◦ [Dual-Source Identity Derivation: Hardware Anchors and Local State Vectors Combined Per Epoch](#) ◦ [Stateless Symmetric Encryption: Session Keys Derived From Current Identity State](#) ◦ [Two-Stage Message Authentication: Transport Continuity Screening Before Semantic Validation](#) ◦ [Agent-Substrate Slope Entanglement: Binding Every Mutation Step to Its Execution Host](#) ◦ [Append-Only Mutation Lineage Log: Forward-Secure Identity Transition Chains](#) ◦ [Cumulative Slope Validation Across Substrates: Multi-Node Provenance Verification](#) ◦ [Quorum-Based Identity Recovery: Peer Attestation After Memory Loss](#) ◦ [Entropy Anchor Rotation: Proactive Identity Reseeding With Forward Links](#) ◦ [Biometric-Assisted Reseeding: Privacy-Preserving Fuzzy Extractors for Anchor Rotation](#) ◦ [Delayed Slope Validation: Bounded Proof Windows for Disconnected Environments](#) ◦ [Sparse Trust Slope Recovery: Compact Checkpoints for Resource-Constrained Devices](#) ◦ [Predictive Identity Validation: Drift Detection Before Full Discontinuity](#) ◦ [Legacy PKI Fallback: Session-Scoped Adapters With Strict Isolation Boundaries](#) ● [Post-Quantum Alignment: Hash-Based Security Without Vulnerable Hardness Assumptions](#)

Applications (General)

◦ [Trust Slope Entanglement: Cryptographic Lineage for Semantic Agents](#) ◦ [Post-Quantum Enterprise Identity Migration](#) ◦ [Billions of IoT Devices Need Authentication Without Keys](#) ◦ [Financial Identity Without Credential Databases](#) ◦ [Patient Identity Through Behavioral Continuity](#) ◦ [Supply Chain Authentication Without PKI](#) ◦ [Smart Building Access Through Continuity](#) ◦ [Vehicle Operator Identity Binding](#) ◦ [Displaced Person Identity Without Documents](#)

Applications (Specific)

◦ [Okta Centralized Enterprise Identity. The Keys That Prove It Are Still Stored Somewhere.](#) ◦ [Auth0 Made Developer Identity Easy. The Credential Model Underneath Did Not Change.](#) ◦ [YubiKey Made Hardware Authentication Practical. The Key Is Still the Vulnerability.](#) ◦ [CLEAR Made Airport Identity Fast. It Built a Biometric Database to Do It.](#) ◦ [Worldcoin Scans Irides to Prove Humanity. The Proof Depends on a Central Enrollment System.](#) ◦ [Jumio Automated ID Verification. The Verification Still Depends on Documents.](#) ◦ [Microsoft Entra Unified Cloud Identity. Identity Still Depends on Stored Credentials.](#) ◦ [Ping Identity Built Enterprise Federation. The Federation Depends on Shared Secrets.](#) ◦ [OneLogin Simplified Enterprise SSO. The SSO Token Is Still a Credential.](#) ◦ [Duo Security Made MFA Ubiquitous. The Second Factor Is Still a Credential.](#) ◦ [Thales HSMs Protect Key Material. The Keys Still Exist.](#) ◦ [Entrust Issues Digital Certificates. The Certificate Is a Stored Credential.](#) ◦ [DigiCert Secures the Web With TLS Certificates. The Certificate Model Has Structural Limits.](#) ◦ [Let's Encrypt Made TLS Free. The Certificate Model Is Still the Same.](#)

[Keyless Identity overview →](#)

AQ
deterministic
autonomy

Legal

Subject to one or more pending U.S. and international patent applications, see [Patents](#) for the current list and status. No license, express or implied, is granted. Any use requires a separate written agreement—see [Licensing](#). Patent applications referenced on this site are pending. Claim scope, if any, is subject to examination and may issue in altered form or not at all. See [Legal](#) for terms and conditions.

Adaptive Query™ is a trademark of Nicholas Clark. U.S. federal registration is pending. federal registration. AQ™, AQ Inside™, Adaptive Index™, Adaptive Network™, Semantic Agent™, @AQ™, AQID™, and Adaptive Coin™ are used as trademarks in connection with the Adaptive Query platform and brand. Other names may be trademarks of their respective owners.

Platform operated by Adaptive Query LLC, which provides patent and trademark licensing services. Copyright © 2025-2026 Nicholas Clark. All rights reserved.

Last updated: 2026-03-03



-
- [Inventive Steps](#)
- [Licensing](#)
- [Patents](#)

- [Articles](#)
- [Legal](#)
- [Opportunities](#)
- [Sitemap](#)



-
- nick@qu3ry.net
- 72 28 14 36 01



[Invented by Nick Clark](#) | Founding Investors: Devin Wilkie