Quantum Unified Model (QUM)

Benefits for Science and Industry

Author and Inventor: Carlos Daniel Borrego Romero, MBA, BSc Computer Systems, CISA, CRISC, CDPSE, ISO 27001, CASE .NET

The QUM encodes the complete informational identity of any quantum or quantum-hybrid system — its phase-space state, its certainty (uncertainty-proximity) structure, and its measurement context — into a single canonical, cryptographically verifiable descriptor. Identity is declared preserved when the descriptor computed at the origin equals the one recomputed at the destination, giving a reproducible, apparatus-independent test of quantum-state identity across space and time. The genuinely new contribution of Borrego is the verifiable quantum-identity invariant itself — a single canonical descriptor, not present in prior art, that elevates proximity to the uncertainty limit to a first-class 'certainty fingerprint' and binds it cryptographically with full measurement context and provenance, so that quantum-state identity becomes a reproducible, apparatus-independent, hash-verifiable credential with an auditable chain of custody.

Benefits for Science

Verifiable quantum-identity invariant	Introduces a previously non-existent single descriptor that certifies quantum-state identity by hash equality across origin and destination — unifying state characterization, uncertainty quantification, and cryptographic verification into one reproducible credential.
Quantum information science	Introduces a verifiable identity invariant for quantum states, complementing fidelity and tomography with a single reproducible credential that certifies state identity across transmission and storage.
Quantum metrology & uncertainty research	Elevates proximity to the Robertson-Schrödinger uncertainty limit to a first-class, axis-resolved observable (the 'certainty fingerprint'), enabling precise, directional quantification of how close a state sits to minimum uncertainty.
Quantum foundations & measurement theory	Binds measurement context, axis conventions, and provenance into the state description, making context-dependent divergence diagnosable and separating physical change from convention mismatch.

Reproducibility & open science	Canonical serialization with fixed precision and stable encoding yields hash-identical descriptors across labs, directly improving reproducibility and cross-institution verification of quantum experiments.
Quantum-gravity / holographic information	Connects compact informational fingerprints to holographic information-preservation principles, offering a bridge between operational quantum identity and fundamental information conservation.

Benefits for Industry

Quantum computing & networking	Provides chain-of-custody verification for quantum states moved across a quantum network or between processors, with intermediate checkpoint hashes forming an auditable transport record.
Cybersecurity & cryptographic identity	Couples physical quantum state to SHA-3 / Keccak cryptographic binding, enabling tamper-evident, auditable identity credentials for high-assurance systems and secure provenance.
Quantum sensing & instrumentation	Apparatus-independent identity hashes let manufacturers certify that a sensor's quantum state is preserved through calibration and transport, improving traceability and quality assurance.
Regulated industries & compliance (finance, pharma, defense)	Immutable, reproducible identity credentials with full provenance metadata support audit, regulatory compliance, and certified data lineage for quantum-derived measurements.
Metrology institutes & standards bodies	A canonical, unit-aware descriptor offers a candidate standard for declaring and comparing quantum-state identity consistently across institutions and implementations.

Benefits in 10 Years and Beyond — with AI and Emerging Technologies

Global quantum-internet identity layer	As quantum networks mature, the QUM descriptor could become the universal identity and chain-of-custody layer of a planetary quantum internet, with AI continuously verifying state integrity across nodes.
AI-assisted quantum tomography	Machine learning could reconstruct full state capsules from minimal measurements, making certainty fingerprints instant and enabling real-time identity verification on live quantum hardware.
Post-quantum trust infrastructure	Combining physical quantum identity with next-generation cryptography could yield tamper-proof digital trust for finance, health, and government records that survives the post-quantum era.

Autonomous quantum laboratories	Self-driving labs could use QUM credentials to certify, transport, and re-verify quantum states without human intervention, accelerating materials, drug, and sensor discovery.
Holographic information preservation	Linking operational identity to holographic principles could inform far-future technologies for encoding and preserving information at fundamental physical limits.