The Price of Proof

Verification is becoming the scarce resource of the machine-speed economy

Arkaya Risk · v2 · 4 August 2026

Built to the Arkaya AI Production Standard. Locked formulations verbatim. Numbered references with substantive content. Sources authenticated. Page boundaries verified.

Executive summary

- In August 2026 IBM and its partners claimed quantum advantage: computations no classical computer can practically repeat. Their central difficulty was not the computing but proving the answers could be trusted, because once a task exceeds classical reach, the familiar means of checking it disappears.
- The same problem is arriving everywhere at machine speed. Autonomous AI systems produce decisions, transactions and records faster than any auditor can re-check by redoing the work, and every traditional form of assurance rests on the assumption that a checker can.
- Where recomputation becomes impractical, verification shifts from reproducing the work to validating the evidence that the work was done correctly. Evidence, not re-performance, becomes the object of trust.
- As assertions become nearly free to produce, verification becomes the scarce function, and evidence that reduces a counterparty's uncertainty is reflected in prices, capital and terms. The paper carries this as a hypothesis with a stated failure condition, not as settled fact.
- Arkaya addresses one class of this problem: governance evidence for organisational decisions. A verification layer must be neutral, independent and permanent, and permanence includes surviving the quantum transition in its own cryptography.

The example

In August 2026, IBM and its research partners claimed quantum advantage: computations that no classical computer can practically repeat [1]. The physics drew the headlines. The economics sat in a quieter sentence. Under IBM's own definition, advantage exists only if the outcome can be rigorously validated, and once a task exceeds classical reach, the familiar means of checking it disappears. The most advanced computation in the world was worth exactly as much as the trust its answer could command.

The response is instructive. The teams did not answer the problem by computing harder. They designed verification into the production of the answer: error detection encoded into the computation itself, carrying a statistical lower bound on its fidelity [2]; replication of the work on independent hardware

from a different manufacturer; and publication of the claims on a public tracker, with an open invitation to prove them wrong [1]. One of the three papers describes its estimate as the most credible among the approaches considered, not as established ground truth [3]. Assertion and verification were held apart, deliberately, in the authors' own words.

The general problem

Quantum computing is the extreme case of a shift already under way. Autonomous AI systems now produce decisions, transactions and records at a speed and volume no auditor can re-perform. Every traditional form of assurance, whether audit, attestation or compliance review, rests on a quiet assumption: that a checker can re-perform or sample the work after the fact. Machine-speed systems break that assumption, not because the checkers lack effort or skill, but because the cost of independently reproducing the work has become prohibitive.

The consequence is a change in what verification means. *Where recomputation becomes impractical, verification shifts from reproducing the work to validating the evidence that the work was done correctly.* Evidence, not re-performance, becomes the object of trust.

The economics

Every market rests on three functions: information, verification and settlement. For most of the modern era, information was the binding constraint, and the institutions we built, from accounting standards to credit ratings, were answers to information scarcity. Machine intelligence is now making information abundant and assertions nearly free to produce. As the cost of making a claim approaches zero, the scarce function is no longer stating what is true but establishing that it is. We call this the Verification Age, and we carry it as a hypothesis rather than a settled fact: if markets shown independently verifiable evidence do not begin to differentiate price, capital or terms against merely asserted alternatives, the proposition fails [6].

The economic mechanism beneath the hypothesis is older than the technology. Wherever capital is allocated under asymmetric information, independently verifiable evidence that reduces epistemic uncertainty will tend to be reflected in the price, in the capital held against the exposure, or in the terms of the deal, to the extent that the market can observe, trust and incorporate it. That principle is a synthesis of established results, from Knight on uncertainty and Akerlof on quality uncertainty to Spence on signalling and Duffie and Lando on default risk under incomplete information; it is not an original theorem [4]. What is new is not the mechanism but the volume of economic activity now flowing through it. As machine output grows, the share of value resting on claims nobody can re-check grows with it, and so does the return to proof.

One property makes verification institutional rather than commercial. Bilateral judgement scales linearly; markets scale through shared institutions. A single counterparty can always investigate a single assertion, at cost, one relationship at a time. A market of many parties cannot form on bilateral investigation, any more than trade could scale on private weights and measures. A verification layer is therefore an institution, not a product, and its value rests on properties a product does not need: neutrality, independence and permanence.

Honesty requires a boundary. Governance loss has three sources: adverse selection, moral hazard and correlated tail. The evidence layer addresses adverse selection, the question of whether an assertion can be relied on before the event; it does not by itself change behaviour after contracting, nor de-correlate a systemic tail, which remain the counterparty's to price and to bear.

What a verification layer must be

Trust is the willingness to act despite residual uncertainty. Independently verifiable evidence reduces that uncertainty without eliminating it. Evidence is independently verifiable only when it is comparable, portable and adjudicable across parties, which is what the schema supplies and no single engine or self-certification does.

Independence is the load-bearing property, and independence asserted is not independence enforced. In Arkaya's case the enforcement is structural: under the Schema Independence Charter, no commercial counterparty and no commercial function inside Arkaya may overrule a schema decision, and schema custody is not a revenue line [7]. The steward issues no rating and assigns no level. Verification does not route through Arkaya: a counterparty checks the evidence offline, without any Arkaya service in the path, exactly as IBM's reviewers test a quantum claim without IBM in the room.

Permanence is the quieter requirement. Evidence that must hold across years of renewals, refinancings and exits must remain verifiable for as long as it matters, which is why the cryptography beneath a verification layer must itself survive the quantum transition. The post-quantum signature standards finalised by NIST in August 2024 make that migration a scheduling decision, not a research problem [5].

Where this begins

Arkaya is building the governance evidence layer the insurance and capital markets need to price governance risk explicitly. That is one class of the wider verification problem: governance evidence for organisational decisions. Other classes belong to other instruments, from hardware attestation and secure enclaves to zero-knowledge proofs and independent audit, and this paper claims none of them.

Insurance is the canary: the first place the missing infrastructure draws blood. An underwriter must price the operational control of an insured organisation that neither party can re-perform or observe directly, at renewal, on twelve months of assertions. Every pressure described above concentrates at that desk first, which is why a thesis about the economics of verification begins, in practice, as a thesis about insurance.

The direction

The quantum advantage claims may yet fall; the public tracker exists to invite exactly that, and the claims are stronger for it. What will not reverse is the direction underneath them. Computation is becoming abundant. Proof is not.

A price is only as sound as the proof beneath it. In the age of abundance, that proof is increasingly scarce.

Resilience Capital is built. Not asserted.

References

1. IBM Think, "Why establishing trust matters for quantum computing", 3 August 2026. Reports the three quantum advantage claims, IBM's definition of advantage as requiring rigorous validation, and the public Quantum Advantage Tracker inviting classical refutation. Verified by direct retrieval, 4 August 2026. https://www.ibm.com/think/news/why-establishing-trust-matters-quantum-computing

2. IBM and the University of Chicago, arXiv:2607.25941. A 70-qubit logical computation encoded across 97 physical qubits with error detection designed in, establishing a statistical lower bound on fidelity: the worked example of verification built into the production of an answer rather than added after it.

3. Algorithmiq, arXiv:2607.25998. Presents its quantum estimate as the most credible among the approaches considered, not as independently established ground truth: the distinction between an asserted answer and a verified one, held in the authors' own words.

4. The information-economics canon: Knight (1921) on risk and uncertainty; Akerlof (1970) on quality uncertainty; Spence (1973) on signalling; Leland and Pyle (1977) and Stiglitz and Weiss (1981) on informational asymmetry in credit; Merton (1974) and Duffie and Lando (2001) on default risk under incomplete information. The synthesis these results support is the principle stated in the economics section; the paper adds no theorem to them.

5. NIST post-quantum cryptography standards, finalised August 2024: FIPS 203 (ML-KEM), FIPS 204 (ML-DSA) and FIPS 205 (SLH-DSA). The basis of the permanence requirement: long-lived evidence must migrate to quantum-resistant signing before large-scale fault-tolerant machines arrive.

6. Salim Ismail, Moonshots podcast, Episode 256 (2026), on the migration of scarcity from information to trust as intelligence becomes abundant. Cited as an external anchor for the Verification Age hypothesis, not as proof of it; the hypothesis stands or falls on whether markets price the difference between verified and asserted claims.

7. Schema Independence Charter v1.1, 28 May 2026. The institutional enforcement of schema neutrality: no commercial counterparty and no commercial function inside Arkaya may overrule a schema decision; schema custody is not a revenue line. Counterparty-disclosable; available on request.

Revisions. v2, 4 August 2026: executive summary added at co-founder review; no other change. v1, 4 August 2026: first issue.

David J McKibbin · Simon Hudson Co-Founders

djm@arkayarisk.com · +44 (0)7972 178759 · smh@arkayarisk.com · +1 (914) 309-6397

Arkaya Risk is currently being formed in the UK and is presently a trading style of Centinel 10 Ltd, a company registered in England and Wales (no. 11906608).