WORKING PAPER

The Cold Standard

A Fixed Reference for a Record That Won't Stop Moving

Instrument, not archive. Reference, not backup. A sealed corpus, held beyond executable reach and opened only by human hands, against which the working record on Earth is checked — routinely, on ordinary days, while everything still works.

Sanjeet Kumar

Enterprise Architecture & Technology Governance Leader · Founder & Owner, Robotiqa Technologies Ltd.

Sovereign Digital Resilience · Epistemic Infrastructure · AI Governance

August 2026 · v1

ORCID 0009-0003-1677-684X · DOI: 10.5281/zenodo.22073327

In one page

For most of the last century, anyone holding a banknote/coin could, in principle, walk it to a counter and convert it into a fixed weight of gold. The note was trusted on ordinary days precisely because the check was available on ordinary days.

When that convertibility was severed, money became fiat — valuable only because an institution said so.

Our records are going off their gold standard. As AI systems come to write, store, retrieve, summarize and interpret the record, almost every check we can run on a record is performed by tools drawn from the same class as the thing being checked. A record whose authenticity rests on institutional assertion alone is a fiat record. Most records already are, and nothing in current provenance tooling changes that — a signed manifest is still a file, verified by software, on a machine.

This paper defines the missing instrument> a 'Cold Standard' — a fixed, sealed corpus held beyond the executable reach of any system on Earth, opened only by governed 'human action', whose job is to answer one narrow question on demand: is what you hold today what was sealed then? Not a backup for after the catastrophe. A reference for use while everything still works. It commits a digest of every consequential record exhaustively, and retains full content only for a calibration sample.

The design has been proven twice. Metrology ran a physical reference — the prototype kilogram — for 130 years, with rationed access and a governed chain of comparison, and it worked even though the reference itself drifted. Monetary convertibility ran the everyday version: any note, any day, checkable against a fixed reserve. And since 1995 a hash printed weekly in a newspaper has quietly demonstrated the whole trick in miniature.

Four claims:

1) The contamination of the record is present-tense and measurable, not a forecast.
2) A reference does not need to be true. It needs to be fixed. Drift is then measured in the copies.
3) Isolation is a ladder, ordered by what an adversary must spend: logical → air gap → geological → extraterritorial → orbital → off-world — and every rung that exists today is built and sold for recovery. The verification function is unclaimed at every altitude.
4) Every honest version of this idea is weakest at the last mile, because verification happens on Earth. The paper says so, and says what can — and cannot — be done about it.

A BACKUP answers what survives. a COLD STANDARD answers what changed.

1. The question underneath the question

Start with something narrow and practical… because the large version of this question may invite large and useless answers.

An institution issues a determination about a person — a licence refused, a title registered, a benefit denied. Some years later the determination is challenged. The institution goes looking for the record. It finds one. The record is legible, well-formed, internally consistent, and stored in a system with good access controls.

Well, how does anyone establish that this record is the one that was made at the time?

The conventional answer is a chain: hashes, audit logs, timestamps, backups held by a second party, perhaps a notarised anchor on a ledger. Each of those is a real control and each is worth having. But notice what they have in common. Every one of them is a digital artifact, held in a digital system, generated by software, and read back through a tool/software. The chain does not terminate in something outside the class of things it is checking. It terminates in another member of the 'same' class.

For most of computing history this was tolerable, because forging the whole chain coherently was prohibitively expensive and the capability was concentrated in a small number of well-resourced entities. That assumption has quietly stopped holding.

A system that can write a plausible document can also write the plausible log entry, the plausible metadata, the plausible summary a busy person reads instead of the document — and, more consequentially, the plausible interpretation of the document a reader is given when they ask what it says.

The failure this paper is concerned with is not forgery. Forgery is a solved-ish problem, with known countermeasures. The failure is subtler and worse: the slow drift of the working record away from what was recorded, with nothing outside the record against which the drift could be seen.

An earlier paper in this series argued that institutions owe a duty of decision custody — the demonstrated ability to reproduce, explain, defend and answer for every consequential decision made in their name, for as long as the consequences last. That paper assumed the evidence, once preserved, could be trusted.

This paper examines the assumption — and proposes the instrument the assumption was silently borrowing.

2. The contamination is present tense

The forward-looking version of this argument — "one day we will not be able to tell" — is weaker than the evidence supports, and invites the reader to file the problem under things to worry about later. The measurements are already uncomfortable.

Shumailov and colleagues established the mechanism in Nature in 2024: training generative models indiscriminately on the mixture of real and generated content that scraping the open web now produces degrades the models' ability to generate diverse, high-quality output. They named it model collapse, and it is recursive — each generation of models trains partly on the output of the last... and the variance narrows. To be precise about what this evidences: model collapse is a measured property of the information environment, not yet a measurement of institutional records themselves — related exposures, not the same one. The claim of this paper is that the second now sits inside the first.

The exposure has grown quickly. Corpus analyses reported through 2025 and 2026 place a large and rising share of newly published web pages as containing AI-generated text — an Ahrefs analysis of 900,000 newly created pages put it at 74.2 per cent by April 2025, measured with Ahrefs' own detector, whose imperfection the study itself concedes — and work presented at the 2026 Web Conference describes the downstream effect

as retrieval collapse: search and retrieval-augmented systems increasingly surface evidence that was itself model-generated. Narrowing the pool a question can be answered from.

The archival community has drawn the conclusion faster than most. Current archiving-policy surveys argue for hybrid analog anchoring — permanent paper and archival film as tamper-evident, technology-independent ground truth — explicitly because synthetic records erode trust in purely digital archives. And a public index of what its maintainers call low-background steel now curates sources believed uncontaminated by AI-generated content: pre-1970 newspaper archives, a 2022 Wikipedia dump, linguistic corpora frozen and abandoned. Precisely because their sources became contaminated.

Note> what that last item concedes. A word-frequency database was not attacked. It was not corrupted. It simply stopped being usable as a description of human language. Because the language it sampled stopped being reliably human. Nobody did anything wrong, and the resource died anyway.

The dynamic is not confined to the open web. It is now documented inside clinical documentation: ambient-AI systems draft clinical notes at scale, clinicians routinely revise factual details in those drafts — orders and tests in forty per cent of analysed edit units, medications and diagnoses in roughly a quarter each — and, as the study itself cautions, discrepancies that survive review can propagate as notes are copied forward through the longitudinal record. The record of institutions is downstream of the same tools as the record of the internet, on a delay, not on an exemption.

3. The recovery consensus

Serious institutions already keep important material in isolated places, and the isolation on offer is more varied and more capable than most readers assume. Walk the existing landscape from the ground up, because the pattern it reveals is the paper's strongest evidence of a gap.

The geological vault

The Arctic World Archive has operated since 2017, three hundred metres inside a decommissioned coal mine on Svalbard, beside the Global Seed Vault. Data is written as high-density codes onto silver-halide film rated for five hundred to a thousand years, needs no electricity once written, and sits in territory demilitarised by a treaty with more than forty signatories.

Retrieval is manual: a request, a person, a reel, a scanner. It holds national archives, GitHub's open-source code, and cultural deposits from dozens of countries.

The extraterritorial vault

In 2017 Estonia opened the world's first data embassy: state servers in a Luxembourg data centre granted, by bilateral agreement, the same inviolability and immunity as embassy premises and diplomatic personnel. The motivation is instructive: Estonia's essential registries — including its land register — exist only in digital form and carry evidential value only in digital form, so their continuity is existential. The host state cannot lawfully touch the machines.

Monaco followed with its own e-embassy in Luxembourg in 2021. This is a rung the security literature barely names: jurisdictional non-adjacency, distinct from physical remoteness — a vault that defeats not burglars but subpoenas.

The off-world vault

The Arch Mission Foundation has been placing archives off Earth since 2018; its nickel NanoFiche Lunar Library reached the lunar surface intact with the Intuitive Machines IM-1 mission in February 2024.

The academic version exists too: Ezell, Lazarian and Loeb showed in 2022 that laser links and modern storage density make a lunar backup of civilisation's record feasible. And the commercial version is no longer hypothetical: Lonestar Data Holdings transmitted documents to and from a lander en route to the Moon in 2024, flew a physical data-centre payload on IM-2 in 2025 and completed storage, encryption and recovery tests for government and enterprise customers in cislunar space, and in May 2026 signed a Space Act Agreement with NASA's Ames Research Center to develop data storage and communications on and around the Moon, with orbital "StarVaults" marketed for 2027.

The 'Pattern'

Now read the labels on all of it. The Arctic World Archive preserves deposits and returns them to depositors. The data embassy exists, in Estonia's own framing, so the state can be rebooted if it loses its territory. The lunar-archive literature is written as insurance against planetary catastrophe. And the company that actually operates on the Moon sells its service under the name Disaster Recovery as a Service (DRaaS).

From the WORM tier in a corporate storage array to the film reels under the perma-frost… to the diplomatically immune servers in Luxembourg… to the payload on the lunar surface: every rung of the isolation ladder that exists today is built, funded, marketed and described in the language of **recovery**. What survives; what we reboot from; what we open after the bad day. The designers of these systems would count it a success if their archives were never opened at all.

That is the gap.

Nothing on the ladder — at any altitude — is designed to be used while things are working: consulted routinely, on ordinary days, to measure whether the working record has moved. Each of them answers what survives, or who made this. None of the artifacts surveyed here answers the question section 1 asked: **against what do we calibrate**?

The nearest existing practice is closer to the ground and must be named precisely, because it looks like the answer and is not. Digital preservation has long kept preservation masters — the US National Archives defines the preservation copy as the highest-quality long-term copy, maintained to protect the original — and runs routine fixity checking: digests recomputed and compared against stored reference values, as the Digital Preservation Coalition's handbook describes and the Library of Congress practises at scale. The distinction is exact. Fixity checking answers whether an archived object still matches a digest stored beside it — a comparison run inside the environment. A cold standard asks what anchors that digest, and the verifier, and the interpretation software, and the working record, when all of them live inside substantially the same digital trust environment. Fixity is a check within the system; a cold standard is a comparator held outside it.

The archives are copies, not references. The provenance standards and personhood credentials are gates, not measures — and they are mechanisms inside the environment whose integrity is in question, files checked by tools/software on machines. The missing thing is an instrument, not an archive.

4. Two precedents that worked

The instrument this paper proposes has run twice before, at civilizational scale, for about a century each time. One version supplies the governance mechanics; the other supplies the everyday-use framing. Neither was elegant. But both worked.

4.1 The kilogram: a reference under rationed access

From 1889 until the 2019 redefinition, the kilogram was defined by an object: the International Prototype of the Kilogram, a platinum-iridium cylinder held by the BIPM outside Paris.

During those 130 years, the IPK and its duplicates were used to calibrate every other kilogram standard on Earth. Access was rationed by design — the prototype and its six official copies sat under the strict supervision of the CIPM, and the prototype itself was consulted roughly once every fifty years, an inconvenience so severe that even the BIPM struggled to keep its own working standards traceable. Rationing was not a limitation reluctantly accepted; it was how the artifact was protected. A reference that is handled often is a reference that changes.

Beneath the prototype sat a named hierarchy — the official copies (the témoins, the witnesses), national prototypes, working standards, and finally the masses used in laboratories and shops — each tier calibrated against the tier above. No individual weighing ever touched the prototype; every weighing was nonetheless connected to it by a documented chain.

And here is the detail that matters most. Comparison campaigns found real divergence between the prototype and its official copies — on the order of fifty micrograms across a century. The reference was not stable. Yet, as NIST puts it> by definition the IPK's mass could not change — because it was the official kilogram, its mass was always exactly one kilogram, even if it actually gained or lost mass.

> **A reference does not need to be true. It needs to be FIXED.**
>
> Correctness is not a property the reference must earn. Once the reference is fixed and the comparison procedure is governed, deviation becomes a measurable property of the copies rather than an argument about the world. The question stops being "which of these is right?" and becomes "how far has this one moved, and when did it move?"

For records, this is a substantial simplification. A cold standard does not have to adjudicate whether a document was accurate, fair or complete when it was sealed. It only has to be the thing that was sealed. Every dispute about truth becomes a dispute about drift, which is at least tractable. Nor does fixity promote a wrong record into a true one: a record wrong at sealing stays wrong — provably unchanged — which is precisely the state that appeal, correction and audit require.

4.2 Convertibility: a reference in daily use

The kilogram precedent has one limitation as a model: almost nobody ever used it! Two consultations per century is the right cadence for protecting an artifact and the wrong one for governing a living record. For the everyday half of the design, turn to the other great reference system of the same era.

Under the classical gold standard, a banknote was not valuable because a government asserted it was. It was valuable because it was convertible: the holder of any note could, in principle, present it on any ordinary day

and receive a fixed quantity of a reserve that no printing press could inflate. The check was rarely exercised — that was the point. Its availability disciplined the entire system. Notes circulated freely and were trusted casually precisely because conversion was always possible, and the reserve sat in a vault most holders would never see.

When convertibility was severed — finally and completely in 1971. When the United States closed the gold window — money became fiat: its value floating on institutional credibility, managed by policy, backed by nothing a holder could independently test.

Records are now completing the same transition, unannounced. Call a record whose authenticity rests on institutional assertion alone — with no fixed reference any holder could test it against — a fiat record.

Most records already are fiat records, and always were; the difference is that assertion used to be backstopped by the physical difficulty of coherent forgery, and it is that backstop — not cryptographic integrity controls, which remain — that AI has eroded to almost nothing. A cold standard is, precisely, a return to convertibility: any record, any day, checkable on demand against a fixed reserve that the machinery of daily use cannot touch.

My two honest concessions attach to this analogy, and both strengthen rather than weaken it. First, the gold standard was abandoned as monetary policy> for macroeconomic reasons that have nothing to do with the verification mechanism, which functioned throughout. This paper borrows the mechanism, not the monetary theory.

Second, both precedents were eventually retired in favour of something better: the kilogram for a physical constant, gold for managed currency. If a constant-based solution to record authenticity ever exists, it will deserve to win. We are currently in the century before the constant.

5. Defining the Cold Standard

Cold standard

A fixed, sealed corpus of records, held beyond the executable reach of any general-purpose computing system on Earth, opened only through governed human action, and consulted routinely — in normal operation — to answer one narrow question: whether what an institution holds now is what it sealed then.

In one phrase: a historical-state oracle, not a truth oracle. Four properties are load-bearing. A repository lacking any one of them is something else — may be something useful, but not this.

Fixed

The corpus is organised in sealing epochs. New material extends the corpus by opening a new epoch; it never modifies a sealed one. This is stronger than write-once storage, which prevents alteration of a medium. Epoch sealing prevents alteration of meaning: the interpretation layer — the reference data, code lists and lookup tables that make a record legible — is sealed with the record, because a record whose input codes have since been redefined is no longer the same record even if every byte is unchanged.

Beyond executable reach

The tempting requirement here is "no network path at any price." The operating lunar data centre shows why that demand is both unachievable and unnecessary: the Moon has perfectly good radio, and a reference that cannot answer is not a reference. The defensible property is narrower and stronger — no remotely mutable execution. A channel may exist, but nothing that arrives over it can alter what the far end does. The endpoint is frozen at deployment: firmware that cannot be updated remotely, an attestation grammar fixed in silicon, no administrative interface of any kind. The **channel carries questions in and signatures out**. It can never carry code, configuration or commands. Reaching the artifact to change it requires physical presence, which is the next property's job to govern. Stated precisely, the endpoint does execute — it parses queries and signs answers — so freezing is a boundary on change, not a claim of invulnerability: a frozen implementation can still harbour a flaw that shipped with it. What freezing removes is the adversary's ability to install one. That is why the query grammar is minimal, the implementation is published for adversarial review before sealing, and a flaw discovered afterwards is answered by retiring the endpoint, never by patching it.

Human-gated

Physical access requires the **presence of a human being**, and the system is designed so that no software agent — however capable, however authorised — can cause the corpus to be opened. Personhood credentials matter here but are insufficient: a credential proves a human is somewhere in the loop, not that a human is in the room. Presence, not attestation, is the control. The credential work protects the query channel; the door needs hands.

Attestation-only

The standard does not return content. It answers a bounded set of questions about digests — whether a given digest is present in the sealed corpus, in which epoch, under which sealing authority — and returns a signed assertion of the answer. **It does not summarise, interpret, rank or explain**. The moment it returns content, it becomes a source, and a source can be quoted out of a context that no longer exists. Convertibility is a yes or a no with a date on it, not a narrative.

6. Non-adjacency and the isolation ladder

Security discussions usually treat isolation as a binary: air-gapped or not. This is unhelpful, because every real air gap is crossed constantly — by people carrying media, by maintenance, by supply chains that arrive pre-compromised, and by the fact that somebody must be trusted to be inside.

I think, the useful measure is not whether a gap exists, but what an adversary must spend to be on the other side of it. Call this non-adjacency: the distance between the artifact and the nearest thing that can change it, measured in adversary cost rather than in metres. Non-adjacency is a ladder, and each rung defeats a class of adversary the rung below cannot.

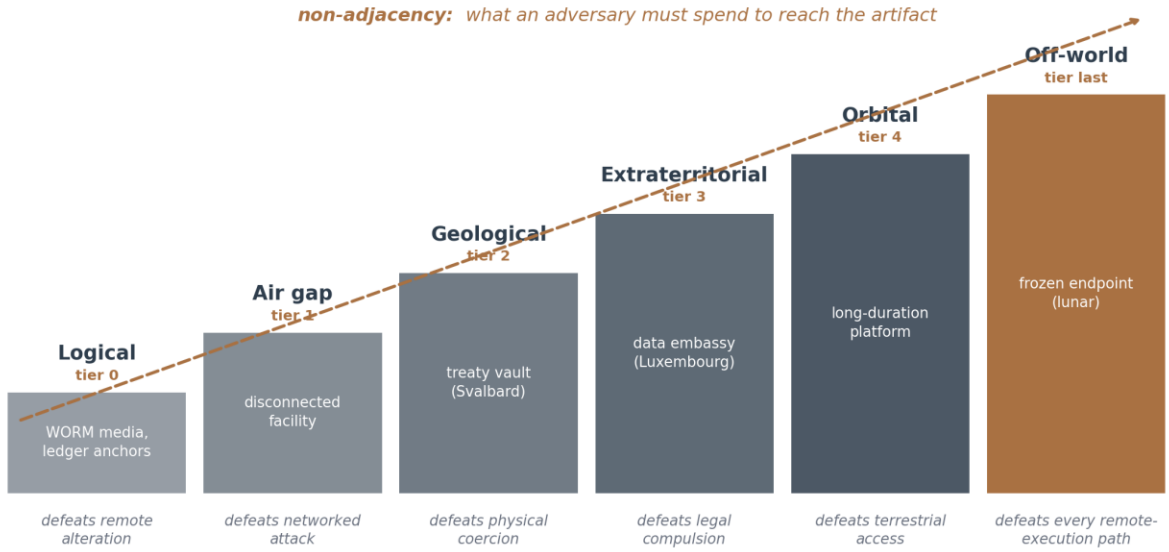

Figure 1 — The isolation ladder. Six tiers of non-adjacency, each defeating an adversary class the tier below cannot. Every tier that exists today is operated for recovery; none is operated as a reference.

Tier	Working example	Defeats	Adversary must spend
0 — Logical	WORM media, segmented networks, ledger anchoring	Remote alteration, ransomware, careless overwrite	Credentials and minutes. An insider defeats it.
1 — Air gap	Disconnected facility, controlled media transfer	Networked attack, automated exfiltration at scale	Physical entry or a compromised courier. Days.
2 — Geological	Arctic World Archive, Svalbard: film in perma-frost, treaty territory	Regional catastrophe, physical coercion of the site	State-level physical action in treaty territory. Weeks.
3 — Extraterritorial	Estonian data embassy, Luxembourg: diplomatic immunity for servers	Legal compulsion of the operator by any single jurisdiction	Breach of diplomatic law, or two states' consent. Months.
4 — Orbital	Lonestar StarVault class, from 2027	All terrestrial physical access	Precise coordinate knowledge, Launch capability and a rendezvous. Months to years.
5 — Off-world	Lunar surface payloads (flown); frozen-endpoint variant (proposed here)	Every remote-execution path; every covert route — approach is a publicly observable act of national capability	A state-scale programme, years of lead time, in full view.

Three observations follow, and they are the reason this paper is a ladder and not a proposal for a lunar base.

First, almost all of the practical benefit is available at tiers 0/1 through 3, today, at institutional cost, on infrastructure that already exists and in one case already enjoys diplomatic immunity. An organisation that wants a cold standard for its own determinations can build one this year, and a state can build one by treaty.

Second, the tiers are not redundant. Svalbard defeats burglars; Luxembourg defeats subpoenas. A record can be perfectly safe from physical seizure and perfectly exposed to a court order served on its custodian, and the reverse. Geological and jurisdictional non-adjacency are different axes, and a design that needs both should say so. Strictly, that makes non-adjacency a profile rather than a scalar — network-and-execution distance, physical distance, jurisdictional distance, custodial distance, supply-chain distance and the observability of an approach vary independently — and the ladder is that profile projected onto a single adversary-cost line. The projection is kept here for exposition; a design document should score the axes separately, as a non-adjacency profile.

Third, the top rung is not better physics or better security — it is worse on both: higher cost, lower reliability, harsher environment. What it uniquely provides is the end of the covert option. At every lower tier, the honest statement is "reaching this costs an adversary X, perhaps quietly." At the last tier, reaching the artifact is a launch — a publicly observable act of national capability with years of lead time. Distance, latency and expense stop being costs and become the control itself.

Space is not where the archive belongs. It is where the ladder ends. The buildable instrument lives on the lower rungs, and nothing in this paper's argument depends on anyone reaching the top.

7. Two routes to fixity

Everything so far pursues fixity by isolation: put the reference where nothing can reach it. There is a second route, it has been running quietly for thirty years, and a sound design uses both.

Since 1995, the timestamping firm Surety — founded by Haber and Stornetta, whose 1991 paper on document timestamping is the direct ancestor of the blockchain — has each week computed a single hash over all the seals added to its database and published it as a small classified advertisement in the New York Times, under "Notices & Lost and Found."

The company's claim is exact: this makes it impossible for anyone, including Surety itself, to backdate a timestamp or validate a record that is not an exact copy of the original. To falsify the reference now, an adversary would have to alter or replace the printed archive of a newspaper distributed in hundreds of thousands of physical copies, held in libraries and homes, for every week since 1995.

Call this fixity by dissemination: instead of putting the reference beyond reach, put it everywhere — in so many independent, physical, humanly-held copies that coherent revision is impossible. Isolation makes the reference unreachable; dissemination makes it un-revisable. They fail differently. An isolated reference has a single custodian who can be captured, coerced or lost; a disseminated one has no custodian at all, but can carry only a digest, not a corpus.

The design rule for a cold standard follows directly: seal the corpus by isolation; publish the epoch digests by dissemination. At the close of each sealing epoch, the epoch's root digest — a few dozen characters — is signed at the frozen endpoint and then printed, engraved, gazetted and deposited into the widest, most physical, most institutionally diverse set of substrates available: newspapers of record, national gazettes, library deposit copies, inscriptions at the custodial sites themselves. The corpus answers what the record was. The published digests protect the answerer — because any attestation the standard signs can be checked against a number the whole world has held in print since the epoch closed.

Figure 2 — The convertibility loop. The working record is checked against the sealed corpus through a fixed-grammar attestation channel; the published epoch digests let any verifier check the checker.

8. The last mile, stated honestly

Here is the objection that defeats every naive version of this idea, including the version the author first wrote down.

Suppose the corpus is perfectly sealed, the endpoint frozen, the attestations signed. Those attestations arrive on Earth. They are received by a ground station running software, relayed over terrestrial networks, verified by a library, and displayed to a human on a screen rendered by an operating system. Every component in that chain is inside the threat model. An adversary who cannot touch the corpus can still control what a person believes the corpus said. The isolation is perfect, and it is thinned at the last metre.

There is no complete answer. There are four partial ones, and a cold standard is only as credible as its willingness to state which it relies on.

1) Signing keys that have never existed outside the frozen endpoint. The private key is generated at the endpoint and never leaves it; off-world deployment merely supplies the strongest physical instance of the same rule. The public key is published by dissemination — printed, engraved, deposited — so that substituting it is a detectable act, not a silent one.
2) Attestations small enough to verify by hand. A signature over a digest, in a scheme whose verification a competent person can carry out with pencil, paper and a published algorithm, is slow and awful — and, at the security margins of today's mainstream schemes, not yet practical. Hand-verifiability, or failing that verification on minimal, diverse, independently sourced hardware, should be read as a stated design goal and an open problem, not a solved one. Pursuing it constrains the cryptography severely and is a real design cost. It remains the only form of verification that would not itself require trusted silicon.
3) A human verification corps with rotating custody. Verification performed by people, in person, in rotation, drawn from institutions with divergent interests, whose attestations of what they saw are themselves

sealed into subsequent epochs. This does not scale and is not meant to. It is how notarisation, election observation and weights-and-measures inspection have always worked, and it is the only known mechanism for terminating a chain of trust in something other than a machine.

4) Accepting a bounded claim. A cold standard cannot make an individual believe a true thing. It can make a systematic, undetected, long-running divergence between the working record and the sealed record expensive to sustain — because the divergence must survive every independent verification attempt, against every printed digest, forever, without one of them coming back clean.

The fourth is the real claim, and it is modest. The instrument does not deliver certainty. It converts an unfalsifiable question — is this record genuine? — into a falsifiable one — does this record convert against the sealed epoch, and if not, when did they part company? That is a smaller promise than the idea first appears to make, and it is worth more than the larger promise would be if it could not be kept.

One more limit belongs on this list: time. A frozen endpoint ages, and cryptography ages with it — schemes weaken, and a corpus meant to outlive its founders will outlive its algorithms. The honest design answers ageing with succession rather than mutation. Signature schemes are chosen for longevity — hash-based signatures, whose security assumptions reduce essentially to the underlying hash function, are one conservative, already-standardised choice — though the succession argument does not depend on any particular family. Each successor epoch re-anchors the digests of the epochs before it, so a corpus sealed under an ageing scheme is progressively re-committed under newer ones. And endpoints are replaced, never upgraded: a successor is deployed, both answer in overlap through a transition, and the elder is retired. Nothing about the corpus rotates. What rotates is the machinery that vouches for it.

9. The genesis problem

The second serious objection is chronological. A cold standard is only as useful as its first epoch, and the first epoch must be assembled now, from material that is already contaminated. There is no clean solution, and any paper claiming one should be distrusted. The least-bad approach has three parts.

Sample rather than exhaust. The instinct is to preserve everything, which is impossible and legally hazardous — an obligation to retain collides with data-protection erasure rights, a tension raised sharply in public discussion of the preceding paper in this series. The resolution is to separate two modes the corpus serves, because the paper's motivating scenario and its drift measurement need different things. In commitment mode, the standard seals a digest of every consequential record through an epoch manifest — digests are small, reveal no content on their own, and can be committed exhaustively — so that an individual determination challenged decades later still gets its answer: present or absent, epoch N. In calibration mode, full content and its interpretation layer are retained only for a documented, reproducible sample, which is what drift measurement needs and what retention law will tolerate. Commit exhaustively; retain selectively. The challenged pension determination of section 11 runs on the first mode; the published drift figure runs on the second.

Seal provenance claims, not purity claims. The first epoch should not assert that its contents are human-authored. It should assert, for each item, what is known about where it came from, and seal that claim beside the item. Contaminated material with an honest provenance record can be reasoned about later; clean material with an asserted one cannot.

Prefer material that pre-dates the problem. Pre-2020 corpora are imperfect, but they have one property nothing produced since can have: their contamination profile is bounded by a date. This is the reasoning behind the low-background steel collections, and the metaphor is exact — steel smelted before 1945 is prized for radiation-sensitive instruments not because it is better steel but because of when it was made.

The uncomfortable implication: the first epoch should be sealed as soon as possible, and will still be worse than one sealed five years ago. Every year of delay weakens the genesis corpus. This is the strongest available argument for treating tiers 1 through 3 as urgent rather than aspirational.

10. Governance

The technical architecture is the easy half. A cold standard is a governance instrument that happens to have a storage medium, and the questions that decide whether it is trustworthy are institutional.

Who seals

The sealing authority decides what enters an epoch, and therefore what the future will be able to check. This is the single greatest concentration of power in the design and the honest objection to the whole idea: whoever controls the standard controls what counts as having happened. The mitigation is plurality — multiple cold standards, held by institutions with divergent interests, whose disagreement is itself informative. A single global standard would be worse than none: the appearance of a check with the possibility of one removed. Monetary history supplies the model — many reserves, many issuers, mutual convertibility — and also the warning of what concentration does.

Who may query, and how often

Query rationing is a preservation control and a governance control simultaneously. Unlimited querying invites the standard to become an operational dependency, which invites pressure to make it faster, which invites an executable path. The kilogram's twice-a-century cadence is too slow for records; the principle that the cadence is deliberately inconvenient is not. Convertibility disciplined money while being rarely exercised. The availability of the check does the work; the check itself should stay expensive enough to stay rare.

Who verifies

The human verification corps needs defined selection, rotation, term limits, and a rule that no institution supplies a majority in any period. Its members' attestations are sealed into subsequent epochs, so the corps' own history becomes part of the corpus it guards.

Succession

The instrument is useless on a horizon shorter than the institution that holds it. The Metre Convention of 1875 has outlived most of its signatories in their 1875 form; the Svalbard Treaty of 1920 still governs the mine above the film reels. Any cold standard needs a named succession path, an explicit dissolution procedure, and a statement of what happens to the corpus if the sealing authority ceases to exist — including the possibility that the correct answer is that it stays sealed and unopened.

Jurisdiction

The tiers now come with legal instruments attached. Tier 2 has the Svalbard Treaty's demilitarised, multi-signatory regime. Tier 3 has the Estonia–Luxembourg agreement as a drafted, operating precedent for

extending embassy-grade inviolability to data — the closest existing legal shape to what a cold standard's custody requires, and a template a consortium of archives could adapt. The upper tiers inherit Article II of the Outer Space Treaty, which forecloses national appropriation of celestial bodies — cutting usefully against capture of the artifact and awkwardly against any clean answer to who owns the vault. That question is flagged as a prerequisite, not resolved here.

11. Record drift as a measurable

If the instrument works, its output is a number, and the number is more interesting than the archive. Record drift is the observed divergence between the working record and the sealed epoch, over a defined sample, at a defined verification date. It has three components worth separating:

1) Content drift — the item no longer matches the sealed digest. Rare, obvious, and the least interesting: existing integrity controls catch most of it.
2) Interpretation drift — the item matches, but the reference data needed to read it has changed, so the same bytes now mean something different. The failure mode most likely to occur, least likely to be noticed, and the reason epoch sealing must include the interpretation layer.
3) Absence drift — the item is in the sealed epoch and no longer in the working record at all. Not corruption; disappearance. The hardest to detect without a reference, and the only one a cold standard detects trivially.

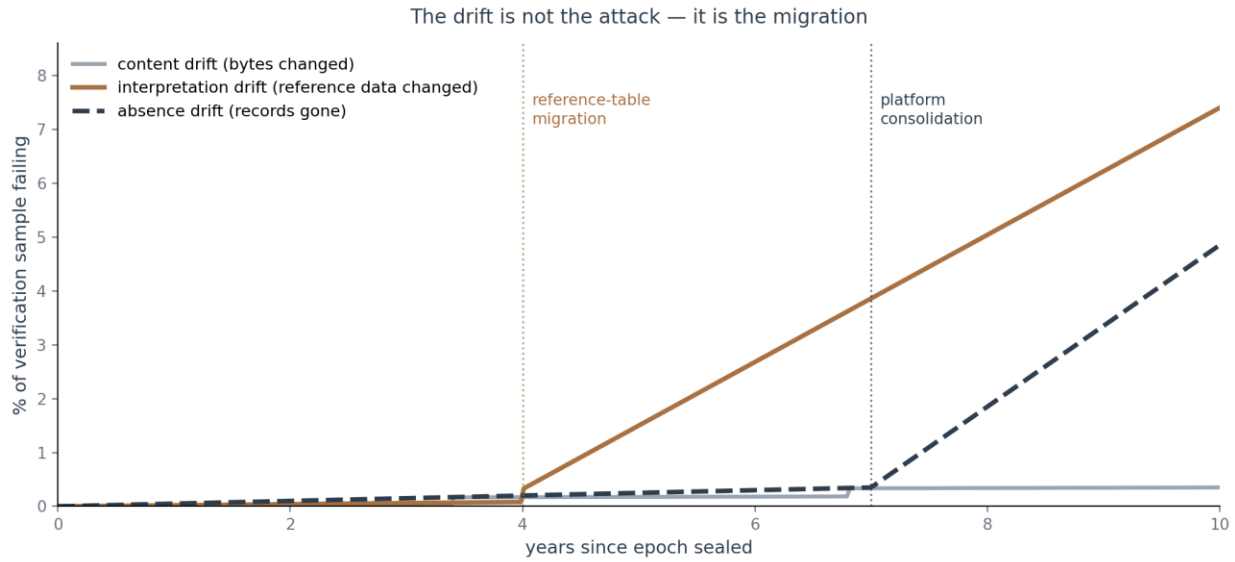

Figure 3 — What a published drift figure looks like. The inflections are migrations and consolidations, not attacks; the value of the measurement is that separation becomes visible while it is still explicable.

Interpretation drift is not exotic

The pattern has well-documented, entirely innocent instances. When countries dissolve, their entries in the international country-code tables are retired and reassigned, and a stored nationality code from the 1990s no longer resolves to what it meant when written. When clinical coding migrated between major revisions of the international disease classification, decades of morbidity records changed granularity and mapping underneath unchanged patient files. The world's timezone database is revised continually, quietly changing what a stored

local timestamp denotes. None of these was an attack. Each was maintenance. All of them changed what old records mean.

A short illustration

The institution and particulars below are constructed; the failure pattern is drawn from experience across several sectors.

A pension administrator consolidates three benefits platforms onto one. As part of the cleanup, the service-classification table — which maps employment categories to accrual rules — is rationalised: duplicate codes merged, dormant codes retired, a handful remapped to their "modern equivalents." The member records themselves are migrated byte-perfect, and every integrity check passes, because the records did not change. Nine years later a survivor challenges a benefit calculation. The record of the original determination is produced instantly and is internally impeccable. But the accrual category it cites now resolves, through the rationalised table, to a different rule than the one applied at the time — and the pre-consolidation table survives only as an undocumented spreadsheet attached to a former contractor's handover email.

The institution is not corrupt and its record is not forged. Its record has simply stopped meaning what it meant, and there is nothing outside the record to show when the meaning moved. A cold standard that had sealed the classification table with the determinations would have answered the question in an afternoon.

A rising drift figure does not indicate wrongdoing. It indicates that an institution's working record and its sealed record are separating — which happens through migration, reorganisation, vendor change and staff turnover far more often than through malice. The value of publishing the figure is that it moves the conversation from assertion to measurement, and gives a board something to ask about that has an answer.

12. Objections

"This is a solution looking for a problem."

The problem is documented in section 2 and is already being acted on by archivists reaching for film and paper. The paper's contribution is not the observation that records are at risk; it is the claim that the response requires a reference rather than a better copy — and section 3's survey found no existing artifact, terrestrial or lunar, built around that distinction.

"Svalbard is enough. Why go higher?"

For most institutions tier 2 or 3 is enough, and the paper says so plainly. The ladder exists because "enough" is a function of the adversary. Svalbard does not defeat a lawful order served on a custodian; Luxembourg does not defeat two governments agreeing; nothing terrestrial defeats an adversary with authority over every custodian. Whether any institution genuinely faces the upper-tier adversary is for each to answer; the argument here is that the tiers should exist and be named, not that everyone should climb them.

"The gold standard was abandoned — you are reviving a discredited idea."

It was abandoned as monetary policy, because pegging the money supply to a metal constrained economies in ways that had nothing to do with verification. The mechanism this paper borrows — convertibility on demand against a fixed reserve — functioned for the entire life of the system and was never the reason for its

retirement. And the paper concedes in advance what retirement looks like: when a constant-based definition of record authenticity exists, the artifact should yield to it, as the kilogram did.

"Whoever controls it controls the truth."

Correct, and the most serious objection in the paper. Section 10 answers with plurality rather than a claim of neutrality, because no sealing authority is neutral and a design that requires one is a design that fails. A reader who finds plurality unconvincing should treat that as the open research problem it is.

"It is elitist infrastructure."

Access to verification would be unevenly distributed, as access to legal remedy already is. This is a real cost. It argues for public rather than commercial sealing authorities, for published drift figures rather than per-query commercial access, for digests disseminated in substrates anyone can hold, and for tiers 1 through 3 to be cheap enough that a mid-sized public body can afford one.

"The archive becomes a target."

It does. A cold standard is a concentrated, high-value, publicly known asset whose destruction would be strategically meaningful. Plurality answers part of this; dissemination answers more — destroying the corpus does not un-print the digests, so an attacker can silence the instrument but cannot make it lie retroactively. And it is, uncomfortably, an argument that the upper tiers are more necessary rather than less.

13. What to do

Five questions for a board

1) If a determination we made five years ago were challenged tomorrow, what would we compare the record against — and is that comparator inside the same systems as the record itself?

2) Do we seal the interpretation layer — the code lists, reference tables and lookups that make our records legible — or only the records?

3) Which rung of the isolation ladder are we actually on, as opposed to the one our controls documentation implies — and which adversary does that rung fail against?

4) If our working record and our archived record had been separating for three years, what would have told us?

last) Who, by name, can open our most protected record store — and can that be caused to happen without a human being physically present?

A proposed work item for standards bodies

The OAIS reference model (ISO 14721) already supplies most of the vocabulary — in particular the requirement that preserved information be independently understandable to a designated community, which is exactly the property interpretation drift destroys. What OAIS does not supply is the comparative function: it describes an archive that preserves, not a reference against which external copies are measured.

A useful work item would define, as a profile rather than a new standard: the sealing epoch and its required interpretation layer; the bounded attestation query set and its response grammar; digest-dissemination requirements (substrates, diversity, cadence); conformance criteria for each rung of the isolation ladder, including the frozen-endpoint property; composition and rotation rules for a verification corps; and a reporting format for record drift with its three components separated. None of this requires new cryptography. Most of it requires agreeing what the questions are.

14. Closing

For a hundred and thirty years the kilogram was a lump of metal in a French vault — inconvenient, rarely consulted, physically drifting — and it worked, because everyone agreed in advance which lump it was and built a governed chain of comparison down to the scale in the shop. For roughly the same century, a banknote was trusted on ordinary days because on any ordinary day it could be converted against a reserve its holder would never see. Since 1995, a string of characters in a newspaper's classified pages has made one company's entire archive unrevisable, one printed week at a time.

We are now in the position on records that metrology was in on mass in 1875 and money was in on value before convertibility: many working copies, no agreed reference, and a growing certainty that the copies are moving relative to one another. Every vault humanity has built so far — under the permafrost, behind diplomatic walls, on the lunar surface — answers the wrong question superbly. They tell us what survives the catastrophe. None of them tells us, on an ordinary Tuesday, what changed.

The response, both times before, was not to invent a better copy. It was to fix one reference, put it where daily use could not touch it, ration the door, publish the proof, and define everything else by comparison. That is what a cold standard is. The hard part was never the vault.

A backup answers what survives. A cold standard answers what changed.

References

1. Adler, S., et al. (2024). Personhood credentials: Artificial intelligence and the value of privacy-preserving tools to distinguish who is real online. arXiv:2408.07892.
2. Ahrefs (2025). What percentage of new content is AI-generated? Analysis of 900,000 newly created web pages. ahrefs.com.
3. Arch Mission Foundation. The Lunar Library and the Billion Year Archive. archmission.org.
4. Arctic World Archive. arcticworldarchive.org; Piql AS, piql.com/awa.
5. Bureau International des Poids et Mesures. The International Prototype of the Kilogram (IPK). bipm.org/en/mass-metrology/ipk.
6. Choudhuri, A. R., Garg, S., Lee, K., Montgomery, H., Policharla, G. V., & Sinha, R. (2026). A Cryptographic Framework for Proof of Personhood. Cryptology ePrint Archive, Paper 2026/333.
7. Digital Preservation Coalition. Digital Preservation Handbook — Fixity and checksums. dpconline.org; Library of Congress digital-collections fixity practice.
8. e-Estonia / Republic of Estonia. Data Embassy. e-estonia.com/solutions/e-governance/data-embassy; Agreement between the Republic of Estonia and the Grand Duchy of Luxembourg on the hosting of data and information systems, signed 20 June 2017.
9. Ezell, C., Lazarian, A., & Loeb, A. (2022). A Lunar Backup Record of Humanity. arXiv:2209.11155.
10. Guo, Y., Hu, D., Yang, Z., et al. (2026). What do clinicians edit in ambient AI-drafted clinical documentation? A qualitative content analysis. Journal of the American Medical Informatics Association, 33(8), 1457–1465. doi:10.1093/jamia/ocag073.
11. Haber, S., & Stornetta, W. S. (1991). How to time-stamp a digital document. Journal of Cryptology, 3(2), 99–111.
12. International Organization for Standardization. ISO 14721 — Open Archival Information System (OAIS) reference model.
13. Kumar, S. (2026). Decision Custody. doi:10.5281/zenodo.21959272.
14. Kumar, S. (2026). The Intent Bottleneck — When AI Compresses Delivery, Strategy Becomes the Constraint. doi:10.5281/zenodo.21971390.
15. Kumar, S. Century-Scale Systems. doi:10.5281/zenodo.21970841.
16. Lonestar Data Holdings. Freedom lunar data-centre payload, IM-1/IM-2 missions (2024–2025); NASA Ames Space Act Agreement (May 2026). lonestar.space.
17. Low-background Steel. Index of sources uncontaminated by AI-generated content. lowbackgroundsteel.ai.
18. Micrographics Data (2026). Global Archiving Policy in the AI Era — industry survey on hybrid analog anchoring as tamper-evident ground truth.
19. National Institute of Standards and Technology. Kilogram: The Present; Metrological Traceability FAQ and NIST Policy. nist.gov.
20. Oberhaus, D. (2018). The World's Oldest Blockchain Has Been Hiding in the New York Times Since 1995. Motherboard/VICE.
21. Shumailov, I., Shumaylov, Z., Zhao, Y., Papernot, N., Anderson, R., & Gal, Y. (2024). AI models collapse when trained on recursively generated data. Nature. doi:10.1038/s41586-024-07566-y.
22. Stock, M., et al. (2015). Calibration campaign against the international prototype of the kilogram in anticipation of the redefinition of the kilogram, Part I. Metrologia, 52(2), 310. doi:10.1088/0026-1394/52/2/310.
23. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space (Outer Space Treaty), 1967, Article II; Svalbard Treaty, 1920.
24. United States National Archives and Records Administration. Preservation master (definition). archives.gov/preservation.

25. Yu, H., Kim, D., & Kim, Y.-B. (2026). Retrieval Collapses When AI Pollutes the Web. Proceedings of the ACM Web Conference 2026 (WWW '26), 8745–8748. doi:10.1145/3774904.3792955.

A note on AI assistance

This paper was drafted with AI assistance for prior-art search, structuring and editing. The argument, the framing, the coined terminology and the final wording are the author's. All cited sources were checked before publication.

Note on terminology

"Cold standard" as defined in section 5 is coined here, in deliberate echo of the gold standard's convertibility mechanism and of cold storage's access economics. "Fiat record", "record drift", "non-adjacency", "sealing epoch" and "frozen endpoint" are defined where they first appear. An earlier draft used "witness standard", after the témoins — the official witness copies of the prototype kilogram; the metrological lineage is retained, the term is not, to avoid collision with evidentiary usage in law. "Witness testing" in weights-and-measures inspection and the WITNESS human-rights organisation are unrelated to any usage here.