**Ameera Yahya Ahmed AL-Hooti**[1]

# THE USE OF BLOCKCHAIN TECHNOLOGY IN ARCHIVAL MANAGEMENT: TOWARD SECURE, TRANSPARENT, AND DECENTRALIZED RECORDS

***Abstract***

**Purpose:** *This paper examines blockchain technologies as instruments to strengthen archival management by providing verifiable authenticity, tamper evidence, and resilient traceability for digital records (Risius and Spohrer 2017; ICA 2021). It situates blockchain within Oman Vision 2040 and evaluates how distributed ledger technology (DLT) can be piloted and integrated with existing archival infrastructures (Oman Vision 2040 2022).*

**Method/Approach:** *A qualitative case-study approach synthesizes three evidence streams: international pilot project reports such as ARCHANGEL (ARCHANGEL Project 2018–2019), peer-reviewed literature and technical white papers (2017–2024), and semi-structured expert interviews and institutional readiness analyses from Oman. Thematic analysis examined three domains: integrity & authenticity, transparency & access, and institutional readiness & governance.*

**Results:** *Blockchain provides a cryptographic chain-of-custody and tamper-evident anchoring model for archival objects by writing content fingerprints to distributed ledgers while storing content off-chain (Kollwitz and Daugherty 2020; Stublić 2023). International pilots show feasibility; however, challenges include governance design, legal recognition, interoperability, cost, and capacity building (Saglik & Lemieux, 2023).*

**Conclusion:** *Blockchain is a promising augmentation to archival toolkits but is not a substitute for core preservation practices (Bendor-Samuel 2022). Recommendations include staged pilots in Oman, a hybrid architecture, standardized hashing and metadata practices, training, and regional consortia for governance and cost distribution.*

**Keywords:** *Blockchain; Digital Archives; Authenticity; Hashing; ARCHANGEL; Oman Vision 2040*

1 Ameera Yahya Ahmed AL-Hooti, PhD student at ALMA MATER EUROPAEA university, email: ameera1yahya2@gmail.com.

# 1. INTRODUCTION

Modern archives face increasing challenges in guaranteeing the authenticity, preservation, and accessibility of records in a digital age. Traditional digital repositories, while advanced, remain vulnerable to cyber-attacks, unauthorized alterations, and centralized failures (Kollwitz and Daugherty 2020). Blockchain technology, with its decentralized ledger system and cryptographic security, emerges as a transformative innovation for archival science (Risius and Spohrer 2017; ICA 2021).

In Oman, the objectives of Oman Vision 2040 highlight the importance of digital transformation, knowledge preservation, and public trust in government records (Oman Vision 2040 2022). Integrating blockchain in archival management aligns with these priorities, offering solutions for authenticity verification, transparent access, and resilient preservation strategies (Saglik & Lemieux, 2023).

Digital records are the principal form of contemporary documentary heritage. Governments, corporations, and cultural institutions generate vast quantities of born-digital and digitized materials that constitute the societal memory. Ensuring the long-term integrity, authenticity, and accessibility of these records poses persistent technical and institutional challenges. Digital objects are prone to format obsolescence, bit-rot, malicious alteration, and losses that arise from centralized failures or weak provenance practices (Risius & Spohrer 2017). Traditional centralized repositories and preservation practices remain necessary, but increasingly insufficient without additional technical mechanisms that produce verifiable, third-party evidence of object integrity.

Distributed ledger technology (DLT), or blockchain, has emerged in the last decade as a means to provide tamper-evident, cryptographically-secure records that can be independently verified by third parties. For archives, the central practical promise of blockchain is the ability to anchor cryptographic fingerprints (hashes) of digital objects in an append-only ledger that resists retroactive tampering. Combined with off-chain storage and robust preservation workflows, blockchain-based anchoring creates a durable evidence trail of a record's existence and fidelity at specific points in time.

Oman Vision 2040 emphasizes digital transformation, public sector trust, and

knowledge preservation as pillars of national development. The National Records & Archives Authority (NRAA) in Oman faces the dual mandate of safeguarding the nation's documentary heritage and enabling transparent, trustworthy government information services. Implementing blockchain technologies can therefore directly support Vision 2040 objectives by strengthening public trust in records, ensuring secure provenance of official documents, and providing auditable trails for vital government records.

This paper aims to synthesize international evidence on blockchain for archives, analyze institutional readiness within Oman, and propose a detailed, practical roadmap for piloting and scaling blockchain solutions in archival management. The research proceeds in three stages: literature and project review; thematic analysis of interviews and documents; and development of a technical and governance roadmap tailored to the Omani archival context.

Research questions addressed in this study are:

1. What demonstrable opportunities does blockchain provide for enhancing security, authenticity, and long-term trust in archival management systems?

2. How can blockchain-supported architectures be designed to preserve confidentiality, manage access, and integrate with preservation repositories?

3. What technical, governance, legal, and organizational conditions are necessary in Oman for feasible adoption and sustainable operation of blockchain anchors?

The following sections elaborate a theoretical framing, review recent literature and pilots (notably ARCHANGEL and Estonia), explain methodology, 'present a technical analysis of blockchain mechanisms adapted for archives, discuss institutional readiness in Oman, and offer a staged implementation roadmap with concrete technical and policy recommendations.

## 2. CONTEXT AND THEORETICAL FRAMEWORK

### 2.1 BLOCKCHAIN TECHNICAL PRIMER

Blockchain is a distributed, append-only ledger in which transactions or data anchors are grouped into blocks, each linked to the prior block by a cryptographic hash. This chaining mechanism makes any retroactive alteration detectable because it would require recalculating and replacing subsequent blocks across a distributed network of nodes. Consensus algorithms (Proof of Work, Proof of

Stake, or permissioned consensus protocols such as PBFT or RAFT) coordinate agreement among nodes as to the current ledger state. For archival uses, the practical configuration is typically a permissioned or consortium ledger that restricts participation to trusted institutions (national archives, universities, cultural institutions) while avoiding the high energy cost and privacy issues associated with public proof-of-work chains.

Key blockchain properties relevant to archives include immutability (tamper evidence rather than absolute immutability of stored content), cryptographic timestamping, decentralization, and programmability (smart contracts). Immutability is operationalized through cryptographic hashing and ledger consensus: a digital object's fingerprint (for example, SHA-256 digest) is computed and anchored on the ledger; later, any stakeholder can recompute the digest of the stored or migrated object and compare it to the anchored value.

## 2.2 ARCHIVAL CHALLENGES IN THE DIGITAL ERA

Archivists confront three interdependent problems: ensuring authenticity, enabling long-term preservation, and maintaining trust and transparency. Authenticated custody is complicated by digital workflows that may produce many derived versions of objects (e.g., scanned images, OCRed text, migrated file formats). Preservation requires active curation—format migrations, bit-level checksums, and storage redundancy—while trust demands verifiable evidence and transparent governance. Without traceable evidence, an institution's claim about a digital object's originality and integrity is vulnerable to challenge. The ledger anchor approach complements, rather than replaces, Open Archival Information System:

- Based preservation frameworks and preservation metadata standards such as PREMIS.
- Record Authenticity: Digital files are vulnerable to tampering and falsification (Kollwitz and Daugherty 2020).
- Preservation: Rapid technological obsolescence risks long-term accessibility (Tscheuschner and Schaefer 2021).
- Transparency: Centralized control limits trust and public confidence (Bendor-Samuel 2022).

### 2.3 THEORETICAL LENS

This study applies to a socio-technical systems perspective and employs records continuum concepts. The socio-technical lens highlights that technological artefacts (like blockchain) derive value through interplay with governance, legal frameworks, human skills, and institutional culture. Records continuum theory posits that evidentiality and authenticity are constructed across creation, capture, organization, and preservation activities; (Risius and Spohrer 2017), blockchain anchoring provides an enduring technical trace linking those continuum stages, which strengthens claims about an object's provenance across time (Stublić 2023).

### 2.4 DEFINITIONS AND SCOPE

For the purposes of this study, the term 'blockchain anchoring' refers to the practice of computing cryptographic digests (hashes) of digital objects and recording these hashes on a distributed ledger at discrete time points. 'Off-chain storage' refers to conventional preservation repositories (OAIS-compliant) where content is stored; metadata and hashes are recorded externally and referenced on-chain. 'Permissioned ledger' denotes an enterprise-style blockchain where node participation, roles, and governance are defined by consortium rules.

## 3. LITERATURE REVIEW AND INTERNATIONAL PILOTS

Over the last decade, literature bridging archival science and blockchain technology has expanded from exploratory conceptual pieces to pragmatic pilot reports and empirical studies. This section synthesizes key findings across three themes: integrity and provenance assurance; access, rights management, and transparency; and preservation architectures (on-chain vs. off-chain trade-offs). It draws heavily on the ARCHANGEL project, Estonia's national-level cryptographic services, and academic reviews published between 2017 and 2024.

### 3.1 INTEGRITY AND PROVENANCE ASSURANCE

A core archival value is the ability to demonstrate that a record is authentic — that it has not been altered since its creation or since its acquisition by the archival repository. Cryptographic hashing and timestamping provide strong technical evidence of such claims. Risius and Spohrer (2017) offer a conceptual framework for blockchain's applications, noting that the technology's immutability properties

are particularly suited for proof-of-existence and tamper-evidence. ARCHANGEL operationalized this concept by generating robust content fingerprints (including AI-derived features) and anchoring them to a distributed ledger to produce long-term, independently verifiable evidence of integrity (ARCHANGEL, 2018–2019). Practical research stresses that the ledger should store only the fingerprint (hash) and essential provenance metadata rather than entire content to preserve confidentiality and manage costs (Kollwitz & Daugherty 2020).

### 3.2 ACCESS, RIGHTS MANAGEMENT, AND TRANSPARENCY

Blockchains' programmability through smart contracts enables conditional access logic: embargo release, automated licensing enforcement, and role-based verification. In cultural heritage settings this has been proposed for managing rights and provenance metadata. However, scholarly critiques emphasize privacy and GDPR-like compliance concerns when metadata or identifiers are placed on-chain; therefore, permissioned ledgers and privacy-preserving techniques (e.g., zero-knowledge proofs, on-chain pointers to encrypted off-chain metadata) are recommended. The Open Data Institute (ODI) and ARCHANGEL produced practitioner-focused guidance emphasizing governance, legal alignment, and stakeholder co-design as preconditions for successful deployments (ODI 2019).

### 3.3 PRESERVATION ARCHITECTURE AND ON/OFF-CHAIN TRADE-OFFS

Empirical pilots indicate hybrid architecture as the pragmatic best practice: store objects and rich metadata in OAIS-compliant repositories (off-chain) and record digest anchors on-chain. ARCHANGEL also explored perceptual hashing and AI features to create fingerprints resilient to format migration (useful when binary-level hashing would fail after transformations). The exact algorithmic choice (e.g., SHA-256 vs. perceptual hashing) depends on whether the archive needs strict bit-level invariance or a more forgiving fingerprint that can verify migrated or transformed derivatives. These choices have long-term governance implications since hashing standards may evolve; archival policies must include re-hashing and migration verification strategies.

### 3.4 NOTABLE INTERNATIONAL IMPLEMENTATIONS

ARCHANGEL (UK) is among the most mature pilots explicitly focused on archives. It combined content-hash anchoring, AI-derived fingerprints, and multi-stakeholder governance to create a prototype verification service (ARCHANGEL reports 2018–2019). Estonia's Guardtime/X-Road efforts represent a national-scale integrity and e-governance model demonstrating how cryptographic integrity services can be applied across governmental registries and health records, with national legal backing for digital signatures and timestamp services (Aru, 2016). Other pilots range from museum provenance tracking and NFT experiments to blockchain-backed cataloguing services in libraries.

### 3.5 CRITIQUES AND LIMITATIONS IN LITERATURE

Critical literature consistently cautions against techno-solutionism: blockchains do not automatically solve provenance disputes, nor do they replace the need for careful appraisal, metadata standards, or legal evidence frameworks. Environmental concerns (particularly with energy-intensive public chains), governance complexities, and the question of ledger permanence (what institutions will operate nodes decades into the future?) are recurring themes. Authors recommend staged, governed pilots and emphasize that blockchain's archival value derives from strong institutional arrangements rather than purely technical properties (Risius & Spohrer 2017; ODI 2019; Kollwitz & Daugherty 2020).

### 3.6 RESEARCH GAPS

Despite growing literature, there is limited empirical work focused on the Middle East and Gulf archival environments. This paper addresses that gap by adapting lessons from global pilots to Oman's legal, institutional, and technical context, proposing a tailored roadmap and pragmatic governance mechanisms for a region where state-driven digital transformation agendas (e.g., Oman Vision 2040) create a conducive policy environment for innovation.

## 4. METHODOLOGY

This study employs a qualitative case-study methodology synthesizing three data streams. The purpose is explanatory and prescriptive: explaining how blockchain has been used internationally and prescribing an implementable pathway for Oman.

### 4.1 DOCUMENT ANALYSIS

Sources included project reports (ARCHANGEL technical documentation and ODI commentary), academic papers (2017–2024), governmental white papers (Estonia), technical standards, and practitioner blogs. The selection emphasized practical pilots and peer-reviewed evaluations to extract transferable lessons.

### 4.2 EXPERT INTERVIEWS

Semi-structured interviews were undertaken with 12 experts selected through purposeful sampling: seven archival professionals (senior archivists and NRAA staff), three IT system architects in Omani public agencies, and two legal/regulatory advisors familiar with digital evidence and records law. Interview topics covered current archival workflows, pain points (e.g., tampering incidents, migration practices), attitudes toward blockchain, perceived benefits, and potential obstacles (budgetary, legal, or technical). Interviews were recorded with consent and anonymized for thematic coding.

### 4.3 THEMATIC ANALYSIS AND TRIANGULATION

Interview transcripts and documents were coded iteratively using NVivo-style thematic approaches (open coding followed by axial coding). Themes aligned with research questions: (1) blockchain's technical fit for authenticity and security, (2) privacy and governance implications, and (3) organizational readiness and resourcing. Triangulation between interviews and documentary evidence increased validity: where interview claims referenced pilot projects, those claims were cross-checked with project documentation.

### 4.4 ETHICAL CONSIDERATIONS

Research adhered to ethical norms for human subjects: informed consent, anonymization, and secure storage of transcripts. Given the sensitivity of archival governance and government IT practices, findings are reported at an aggregate level without attribution to specific individuals or institutions.

### 4.5 LIMITATIONS

Limitations include modest interview sample size and restricted access to some proprietary technical implementations. However, the study draws on publicly

available project documentation and peer-reviewed literature to ground recommendations in broadly observed patterns.

# 5. ANALYSIS AND DISCUSSION

## 5.1 AUTHENTICITY, INTEGRITY AND CONTENT FINGERPRINTING

The combination of content hashing and distributed anchoring provides a practical approach to creating an auditable chain of custody for digital objects. Bitwise hashing (e.g., SHA-256) offers stringent detection of any binary alteration; however, strict bitwise comparison fails after format migration or reprocessing. Consequentially, leading pilots recommend a multi-layered fingerprinting approach: (a) bitwise checksums for archival masters stored off-chain, (b) perceptual or feature-based fingerprints (AI-assisted) for migrated or derivative forms, and (c) comprehensive preservation metadata (PREMIS) linking object versions and transformations. ARCHANGEL's use of AI-driven features demonstrates resilience to transformations while preserving verifiability across time and format conversions.

Case implication: In Omani archives, a practical rule would be to maintain the highest-fidelity archival master (bitstream) in controlled storage with regular fixity checks. For public access or derivative forms, maintain perceptual fingerprints whose anchors are written to the ledger alongside provenance metadata describing transformations and responsible agents.

## 5.2 PERMISSIONED LEDGERS AND CONSORTIUM GOVERNANCE

Most archival and Galleries, Libraries, Archives, and Museums pilots favor permissioned ledgers under a consortium governance model. Permissioned ledgers allow participating institutions to run nodes and define consensus rules, while avoiding the high energy costs and privacy exposure of public chains. Governance is central: the ledger's trustworthiness depends not only on cryptographic properties but also on the governance framework—who operates nodes, how disputes are adjudicated, how consortium membership changes, and how succession is managed over decades. The ARCHANGEL pilot underscores that governance design must be co-produced with stakeholders and legally codified.

Recommendations for Oman: Create a consortium including NRAA, academic partners (e.g., Sultan Qaboos University), and selected ministries to operate

nodes. Legal agreements should define node responsibilities, data stewardship roles, and sustainability financing.

### 5.3 SMART CONTRACTS, ACCESS CONTROL AND LEGAL CONSTRAINTS

Smart contracts can encode time-based releases, embargo rules, and automated verification services. Nevertheless, their immutability raises concerns: a flawed smart contract may be difficult to correct. In addition, placing access policies on-chain could contravene privacy laws if metadata reveal sensitive information. Therefore, smart contract use in archives should be cautious: implement access control pointers to encrypted off-chain metadata and maintain updatable policy references managed via off-chain governance while relying on on-chain anchors for verification only.

### 5.4 INTEROPERABILITY WITH EXISTING ARCHIVAL SYSTEMS

A critical technical requirement is interoperability between existing archival management systems (AMS) and the DLT anchoring service. Integrations should expose a simple Application Programming Interface: when a record is ingested or migrated, the AMS computes the digest(s) and calls the anchoring service to create a ledger transaction containing the hash and minimal provenance metadata. The anchoring service should return a tamper-evident verification token and store the mapping in preservation metadata. This approach minimizes disruption to current workflows while embedding anchors into routine preservation activities.

### 5.5 LEGAL EVIDENTIARY VALUE AND POLICY ALIGNMENT

Anchoring a fingerprint on a ledger gives strong technical evidence of existence at a timestamp, but whether that evidence holds legal weight depends on national law. Estonia's success with state-backed cryptographic services reflects a broader institutional alignment: legal recognition of digital signatures and timestamp services, and national commitment to e-governance. Oman should assess records law and evidence law to determine whether cryptographic anchors need statutory recognition or whether archival policies can operationally adopt anchors as additional provenance controls.

## 5.6 COSTS, SUSTAINABILITY AND ENVIRONMENTAL CONSIDERATIONS

Costs include development, consortium coordination, node hosting, and long-term maintenance. A permissioned consortium model distributes costs but mandates clear funding agreements. Environmental concerns are minimized by permissioned ledgers using energy-efficient consensus engines (e.g., PBFT). Cost models should account for long-term governance: who will ensure node continuity after a decade or more? Regional shared infrastructure (GCC-level archival consortium) could be cost-effective, offering economies of scale and resilience.

## 5.7 HUMAN CAPACITY AND PROFESSIONAL PRACTICE

Interviews show archival professionals are enthusiastic but cautious. Capacity building is required in cryptography basics, hashing strategy, metadata best practices (PREMIS, Dublin Core), Application Programming Interface integration, and governance. Training programs should be co-created with universities and international partners and include hands-on modules for ingesting, hashing, and verifying anchored objects.

## 5.8 ETHICAL CONSIDERATIONS

Anchoring must respect privacy. Even when only hashes are anchored, metadata may reveal sensitive provenance. Data protection (e.g., personally identifiable information in archival metadata) requires either not anchoring sensitive metadata publicly, encrypting metadata off-chain, or using permissioned privacy controls. Smart contracts must be designed to enforce legal and ethical constraints, and retention policies must align with national privacy laws.

## 5.9 SYNTHESIS: A PRAGMATIC ARCHITECTURE

A pragmatic architecture for Oman would combine:

(1) OAIS-compliant off-chain storage for full content,

(2) a hashing service integrated with archival AMS to compute and store hashes and provenance metadata,

(3) a permissioned consortium ledger (Hyperledger Fabric or Quorum) where anchors are written, and

(4) a public-facing verification service that allows researchers and authorized users to verify fingerprints against ledger entries without exposing sensitive content.

Governance and legal frameworks underpin the architecture, ensuring continuity, node succession, and statutory recognition where required.

## 6. RESULTS

This study yields four major results grounded in literature analysis, pilot documentation, and expert interviews. The findings illuminate both technical feasibility and practical considerations for implementing blockchain-based archiving in Oman.

### 6.1 BLOCKCHAIN'S TECHNICAL VIABILITY FOR ANCHORING AUTHENTICITY

Evidence from ARCHANGEL and other pilot projects demonstrates that blockchain anchoring is technically viable and reliable for creating time-stamped fingerprints of archival objects. Implemented with robust cryptographic hashing algorithms and AI-enhanced feature fingerprints, blockchain anchoring provides a tamper-evident mechanism that ensures verifiable integrity across format migrations, reproductions, or derivatives. The use of hybrid models combining on-chain anchors with off-chain content storage reduces storage overhead while maintaining strong auditability. Additionally, AI-assisted fingerprinting enhances anomaly detection, providing an extra layer of verification against potential data corruption or manipulation.

### 6.2 INSTITUTIONAL CONSTRAINTS AND READINESS FACTORS

Interviews with Omani archival and IT professionals highlight strong institutional interest in blockchain-based authenticity mechanisms but reveal notable readiness gaps. These include:

- Limited standardization of hashing and metadata practices across agencies.
- Lack of a formal governance consortium for ledger oversight.
- Unclear legal frameworks regarding the evidentiary status of blockchain anchors.

Despite these constraints, the alignment with **Oman Vision 2040**, the availability of capable universities, and existing IT infrastructure suggest a supportive environment for pilot projects. Institutional readiness could be accelerated through capacity-building programs, legal clarifications, and adoption of metadata standards.

## 6.3 ROADMAP FEASIBILITY AND PREFERRED TECHNICAL MODEL

A staged deployment approach is feasible, moving from feasibility assessment → prototype development → evaluation → scaling. The preferred technical model combines:

- **Off-chain storage** for content (ensuring confidentiality and efficiency).
- **On-chain anchors** written to a permissioned blockchain ledger, governed by a consortium of participating institutions.

This hybrid approach balances cost, confidentiality, and verifiability, while allowing incremental adoption and testing. The model also enables future integration with AI-assisted verification, automated metadata validation, and cross-agency interoperability.

## 6.4 PILOT SELECTION RECOMMENDATIONS

Pilot projects should prioritize high-value public administrative record streams with legal and societal significance, such as:

- Land records and property registrations.
- Crucial administrative communications with public accountability implications.
- Records transitioning from classified to public status.

These records provide strong demonstrable benefits for public verifiability and serve as compelling use cases for policymakers. Selecting record classes with both high public value and legal importance ensures early adoption success and stakeholder engagement.

## 6.5 OBSERVED BENEFITS AND EMERGING INSIGHTS

Pilot evidence and expert feedback suggest that blockchain anchoring not only strengthens trustworthiness and transparency but also promotes long-term digital preservation. The integration of AI-enhanced fingerprints offers early detection of data integrity issues, which could reduce administrative overhead and safeguard public records from inadvertent corruption.

## 6.6 POTENTIAL CHALLENGES AND MITIGATION STRATEGIES

Challenges identified include:

- Technical complexity for small agencies.
- Legal uncertainty surrounding blockchain evidence.
- Interoperability issues among heterogeneous record systems.

Mitigation strategies include capacity building, development of legal guidelines for blockchain evidence, and standardization of data and metadata schemas across participating institutions.

## 7. CONCLUSION AND RECOMMENDATIONS

Blockchain technologies offer archival institutions a powerful tool for strengthening cryptographic evidence of authenticity and building public trust in digital records. However, blockchain is not a replacement for core archival practices but rather a complementary technology that enhances provenance and verification capabilities.

For Oman, the alignment with Vision 2040 and the national digital transformation agenda provides a policy window to pilot blockchain anchoring. The following set of prioritized recommendations emerges from the study:

1. **Establish a National Archival Blockchain Working Group:** Convene NRAA, relevant ministries, universities, and legal advisors to define pilot scope, governance, and standards.
2. **Adopt Hybrid Architectures:** Use OAIS-compliant off-chain storage for content and a permissioned ledger to anchor hashed fingerprints, minimizing exposure of content and controlling costs.
3. **Standardize Hashing and Metadata Practices:** Select SHA-256 (or equally robust) for bit-level checksums, and a perceptual/feature-based fingerprint strategy for migrated derivatives; document these practices and align them with PREMIS metadata.
4. **Launch Scoped Pilots With Clear** Key Performance Indicators**:** Pilot two high-value record streams with clear evaluation metrics (verification success rate, cost per anchored object, stakeholder acceptance, legal robustness).
5. **Build Capacity:** Fund training programs for archivists and IT staff, including practical courses on hashing, verification workflows, and ledger interactions.
6. **Legal and Policy Review:** Engage legal scholars to evaluate the evidentiary status of anchors and propose statutory recognition if necessary; ensure privacy and data protection compliance.

7. **Governance and Sustainability Planning:** Draft consortium agreements that define node operators, succession, dispute resolution, and long-term funding models; explore regional collaborations for shared infrastructure.
8. **Public Engagement and Transparency:** Communicate pilot objectives and results publicly to build trust; provide a public verification portal for non-sensitive records to demonstrate benefits.

By following a staged, carefully governed, and standards-based approach, Oman can realize the benefits of blockchain anchoring while managing risks and ensuring alignment with national priorities. Such an approach would contribute to international knowledge on the application of distributed ledger technologies (DLT) in archives and position Oman as a regional leader in trustworthy digital heritage stewardship.

Moreover, to ensure the enduring reliability and evidentiary value of blockchain-based records, it is critical to anticipate future cryptographic challenges. Integrating a reflection on **quantum computing-resistant cryptographic methods**—such as lattice-based, hash-based, or multivariate polynomial schemes—would further strengthen the recommendations. Considering post-quantum security within the design of archival anchoring systems would safeguard the long-term integrity, authenticity, and verifiability of digital records in the face of advancing computational capabilities.

## APPENDIX A: PROPOSED PILOT TECHNICAL ARCHITECTURE (SUMMARY)

1. Off-chain OAIS repository: High-fidelity masters, replication, fixity checks (bit-perfect checksums).

2. Hashing service: Integrated with AMS, computes SHA-256 and perceptual fingerprints, stores mapping in preservation metadata.

3. Permissioned ledger: Consortium nodes operated by NRAA, university, and selected ministries using Hyperledger Fabric or Quorum.

4. Verification service: Public-facing web service that accepts an object fingerprint and returns ledger-based verification results.

5. Governance layer: Consortium agreement, node management, dispute resolution, sustainability funding.

## APPENDIX B: INTERVIEW PROTOCOL (SUMMARY)

Interview topics:

- Current archival ingest and migration workflows
- Existing fixity and verification practices
- Awareness and attitudes toward blockchain and Distributed Ledger Technology - Perceived legal, policy, and technical obstacles
- Resource and training needs
- Recommendations for pilot scope

## REFERENCES

ARCHANGEL Project. (2018–2019). *ARCHANGEL: Trusted Archives of Digital Public Records*. University of Surrey; The National Archives; Open Data Institute.

Aru, I. (2016, March 9). Estonian government adopts blockchain to secure 1 mln health records. *Cointelegraph*. Retrieved at https://cointelegraph.com/news/estonian-government-adopts-blockchain-to-secure-1-mln-health-records (accessed 7. 10. 2025).

Bendor-Samuel, P. (2022). Blockchain and Digital Trust in Records Management. *Information Management Journal, 56*(3), 45–60.

International Council on Archives (ICA). (2021). *Emerging Technologies in Archives: Blockchain Applications*. Paris: ICA Publications.

Kollwitz, C., and J. Daugherty. (2020). Preserving Trust in the Digital Era: Blockchain for Archives. *Journal of Archival Organization, 17*(2), 123–141.

Oman Vision 2040. (2020). The National Vision for Sustainable Development. Oman Vision 2040 Office. https://www.omanvision2040.om

Open Data Institute (ODI). (2019). ARCHANGEL: Project Reports and Practitioner Guidance.

Risius, M., and K. Spohrer. (2017). A blockchain research framework: What we (don't) know, where we go from here, and how we will get there. *Business & Information Systems Engineering, 59*(6), 385–409.

Tscheuschner, T., and J. Schaefer. (2021). Blockchain for Cultural Heritage: Preserving Authenticity in the Digital Age. *Digital Heritage Journal, 8*(1), 55–72.

Stublić, H. (2023). *Blockchain and NFTs in the Cultural Heritage Domain*. Heritage (MDPI).

Saglik, Ö. and Lemieux, V. (2023). *Will Blockchain Technology Change How Well National Archives Preserve the Trustworthiness of Digital Records?: Preliminary Results of a Survey.* IEEE Conference Proceedings.