



Project Continuum

An Ar.io Digital Preservation Initiative

Prepared by the Ar.io Foundation

with authors Jonathan Policke, Philip Mataras, and Scott Jacques,
and review input from members of the Continuum working group,

as part of an open research effort to align decentralized permanence with established digital
preservation standards.

January 19, 2026

v0.1.0

Table of Contents

Table of Contents	1
0. About and Mission Statement	2
0.1 About the Ar.io Foundation.....	2
0.2 Mission Statement.....	2
0.3 Value Proposition.....	2
1. Background	3
1.1 OAIS (Open Archival Information System).....	3
1.2 Purpose and Scope.....	3
2. The Ar.io Digital Preservation Initiative (DPI)	4
2.0 Vision.....	4
2.1 Why It Matters.....	4
2.2 Our Approach.....	5
2.3 Long-Term Goals.....	5
2.4 Our Commitment.....	6
3. OAIS Alignment in the Permanent Cloud	7
3.0 Overview.....	7
3.1 Terminology Equivalence.....	7
3.2 Functional Alignment.....	9
3.3 Principled Alignment.....	11
3.4 Conformance Alignment.....	12
4. DOI ↔ TXID / ArNS Interoperability	14
4.1 Overview.....	14
4.2 Mapping Model Example.....	14
4.3 Preservation Advantage.....	15
5. CrimRxiv Pilot	16
5.1 Purpose & Mission.....	16
5.2 Context.....	16
5.3 Why It Matters.....	16
5.4 Demonstration Walkthrough.....	17
6. Future Vision and Considerations	18
6.1 Limitations and Risks.....	18
6.2 Next Steps.....	18
Appendices	19
A. Glossary.....	19
B. References and Citations.....	21

Copyright © 2026 Ar.io Foundation. All rights reserved.

Continuum - An Ar.io Digital Preservation Initiative (DPI)

This document is part of the Ar.io open research and standards effort to align decentralized, verifiable data permanence with global digital preservation frameworks. Portions of this work may be reused and cited under the terms of the Creative Commons Attribution 4.0 International (CC BY 4.0) license.

For more information, visit: <https://ar.io>

0. About and Mission Statement

0.1 About the Ar.io Foundation

The Ar.io Foundation stewards open protocols and open-source software for naming, indexing, and access on the **Permaweb***. All code and methods relevant to this document are public and independently verifiable. The Foundation welcomes external review and commentary from preservation practitioners and standards bodies as part of an open research and standards-alignment effort.

0.2 Mission Statement

Continuum is an Ar.io Digital Preservation Initiative (DPI) - an open effort to align decentralized, verifiable data permanence with established digital-preservation standards. Built on Arweave's permanent-storage layer and the ar.io gateway network, Continuum demonstrates how decentralized infrastructure can fulfill the same guarantees of authenticity, integrity, and accessibility that underpin frameworks like the Open Archival Information System (OAIS).

Its goal is to bridge the trust models of institutional preservation and decentralized technology, ensuring that cultural, scientific, and public-interest data can remain permanently accessible, verifiable, and independent of any single institution or provider.

0.3 Value Proposition

Continuum provides institutions and archives with a protocol-based architecture for decentralized preservation, aligned with the Open Archival Information System (OAIS) reference model. It enables one-time funding for long-term storage through Arweave's endowment model, eliminating recurring renewals or subscription fees while ensuring verifiable, redundant access across the ar.io gateway network - even if any single provider goes offline.

Each preserved record carries a permanent, verifiable identifier ensuring provenance, integrity, and reliable citation. Network-wide verification and observation maintain authenticity over time, while open standards and open-source software ensure interoperability and freedom from vendor lock-in.

***Note to reader:** A glossary of novel terms has been included in the appendix of this document.

1. Background

Continuum situates ar.io within the global conversation on digital preservation standards, providing a framework for showing how decentralized, verifiable infrastructure can satisfy established expectations for authenticity, reliability, and long-term stewardship.

1.1 OAIS (Open Archival Information System)

The Open Archival Information System (OAIS) is the foundational international standard for long-term digital preservation, formally recognized as:

ISO 14721:2025 (CCSDS 650.0-M-3) - Reference Model for an Open Archival Information System (OAIS)

OAIS defines the concepts and responsibilities required to preserve digital information over the long term and ensure its continued accessibility, authenticity, and intelligibility, independent of any specific producer, technology, or institution.

1.2 Purpose and Scope

The OAIS model:

- Defines the functional components of a trusted digital repository.
- Establishes common terminology and concepts for the preservation community.
- Provides a framework for designing, auditing, and certifying preservation systems.
- Is technology-agnostic and institution-neutral.

OAIS is a reference model, not an implementation. It describes what must be achieved, not how to achieve it.

2. The Ar.io Digital Preservation Initiative (DPI)

A global effort by ar.io to safeguard humanity's digital legacy - ensuring that the stories, discoveries, and public knowledge that define our time remain permanently accessible and verifiable, independent of any single institution or platform.

The DPI embodies the belief that permanence is a public good: that cultural heritage, scientific research, and civic memory deserve the same durability as the medium that carries them.

2.0 Vision

Continuum envisions a world where the integrity and longevity of humanity's digital record no longer depend on the stability of any single institution, platform, or funding cycle. It carries forward the DPI's belief that cultural heritage, scientific knowledge, and civic information should endure as part of our shared memory - not as data trapped within transient systems.

Through a verifiable, standards-aligned foundation built on decentralized infrastructure, Continuum demonstrates that authenticity, accessibility, and permanence can be guaranteed by protocol itself. In doing so, it bridges human trust and technical assurance - ensuring that what matters most remains discoverable and trustworthy for both humans and machines for generations to come.

2.1 Why It Matters

Modern digital preservation relies on centralized infrastructure and short funding horizons. Even the most trusted archives, libraries, and research repositories face risks of:

- **Institutional fragility:** mergers, policy and administration changes, or funding loss can threaten access.
- **Technological drift:** dependence on proprietary formats and cloud services can make existing solutions obsolete.
- **Economic impermanence:** ongoing storage costs that must be continually financed - or risk data loss.

Ar.io and Arweave offer a new model - one in which permanence, provenance, and accessibility are *guaranteed by protocol*, not policy. This architecture forms an open permanent data lake - a decentralized, verifiable preservation substrate that replaces moated access with transparent, interoperable storage and retrieval. Together, these layers comprise what we call the **Permanent Cloud** - a universal, trust-minimized preservation layer built on the permanent internet (the Permaweb) for humanity's digital record.

2.2 Our Approach

1. **Standards-Driven Design**

Continuum aligns decentralized infrastructure with the globally recognized **OAIS (Open Archival Information System)** model. By demonstrating equivalence between OAIS functional entities and ar.io components, Continuum provides a common language for archivists, researchers, and technologists.

2. **Collaborative Validation**

Continuum works with academic and governmental partners, such as CrimRxiv Consortium (“CrimConsortium”), to migrate real-world repositories to the Permanent Cloud - testing interoperability, metadata integrity, and long-term verifiability in practice.

3. **Transparent Permanence**

Each asset preserved through ar.io and Arweave is independently verifiable across multiple gateways. Proof-of-access consensus maintains integrity over time, and the Wayfinder protocol ensures retrieval without reliance on any single service.

4. **Economic Sustainability**

The Arweave endowment model ensures that a one-time payment funds storage for centuries, removing the recurring financial burden that limits most institutional preservation projects. Meanwhile, the ar.io model ensures durable and verifiable access to that data through a decentralized network of gateways and open retrieval and indexing protocols.

5. **Open Governance and Evolution**

Built atop Arweave’s evolution framework, ar.io ensures that future improvements can be introduced without compromising past data, while preserving both the information and the integrity of its preservation method.

2.3 Long-Term Goals

- **Demonstrate Proven Compatibility**

Produce verifiable OAIS-aligned pilot studies proving decentralized systems can meet or exceed existing institutional preservation standards.

- **Build Institutional Bridges**

Form partnerships with digital preservation networks (e.g., DPC, NDSA, IIPC) to co-develop best practices for decentralized archives.

- **Advance Open Standards**

Publish an open, community-driven “Decentralized Preservation Framework,” extending OAIS principles to the Permaweb.

- **Foster a Global Preservation Network**

Establish a network of preservation infrastructure - gateways and archives - that

coordinate through open protocols to ensure persistent access, verification, and provenance.

2.4 Our Commitment

Continuum represents ar.io's commitment to building infrastructure worthy of humanity's collective memory - infrastructure that transcends institutional limits while embracing the rigor, accountability, and trust of professional archival practice.

This initiative commits ar.io to applying those principles in practice, establishing decentralized infrastructure as a peer to institutional preservation systems.

3. OAIS Alignment in the Permanent Cloud

3.0 Overview

Continuum applies the Open Archival Information System (OAIS) Reference Model (ISO 14721) within a decentralized architecture, demonstrating that the core responsibilities of long-term digital preservation can be fulfilled through protocol design as well as institutional process.

Section 3 outlines how ar.io and Arweave collectively meet OAIS functions, principles, and responsibilities.

3.1 Terminology Equivalence

OAIS Concept	Ar.io / Arweave Equivalent	Notes / Explanation
Information Model		
Submission Information Package (SIP)	ANS-104 bundle (Packaging Information) containing content + tags (PDI inputs) submitted via Ar.io Gateway	Encapsulates producer submission, validated and signed before storage.
Archival Information Package (AIP)	Atomic Asset (TXID record): the immutable onchain content + PDI, encapsulated by the ANS-104 bundle (Packaging Information) and described via ArNS and Gateway indexes (Package Description)	Immutable onchain record combining content and preservation metadata.
Dissemination Information Package (DIP)	Retrieved data package via Wayfinder	Verified AIP output delivered to users through gateways.
Content Information	Data item within the bundle	The digital object preserved (e.g., document, dataset).
Preservation Description Information (PDI)	Transaction metadata and tags	Provenance, context, fixity, access rights, and reference information.
Fixity Information	Immutable, permanent content hash + TXID proof	Verifies data integrity and inclusion in the blockweave.
Provenance Information	Blockweave transaction history	Immutable record of custody and submission identity.

OAIS Concept	Ar.io / Arweave Equivalent	Notes / Explanation
Reference Information	TXID + ArNS record	Persistent, resolvable identifiers for discovery and citation.
Functional Entities		
Ingest	Ar.io Gateways using ANS-104	Validation and submission of data and metadata to the network.
Archival Storage	Arweave blockweave	Permanent, globally replicated, protocolized, endowment-funded storage.
Data Management	ArNS + Gateway indexes	Maintains metadata, naming, and discovery capabilities.
Administration	Ar.io Foundation governance and protocolized smart contracts	Policy, evolution, and community oversight at protocol level.
Preservation Planning	Gateway monitoring + open-source evolution	Continuous adaptation to standards and formats.
Access	Wayfinder Protocol + Gateways	Distributed, verifiable retrieval layer ensuring redundancy.
Supporting Concepts		
Designated Community	Institutional and public users of preserved content	Defines audience for usability and intelligibility.
Representation Information	Stored codecs, schemas, and metadata	Preserved with data to maintain interpretability.
Preservation Watch	Gateway observation and verification metrics	Monitors content health and availability over time.

Table 3.1.1: OAIS <> Ar.io Terminology

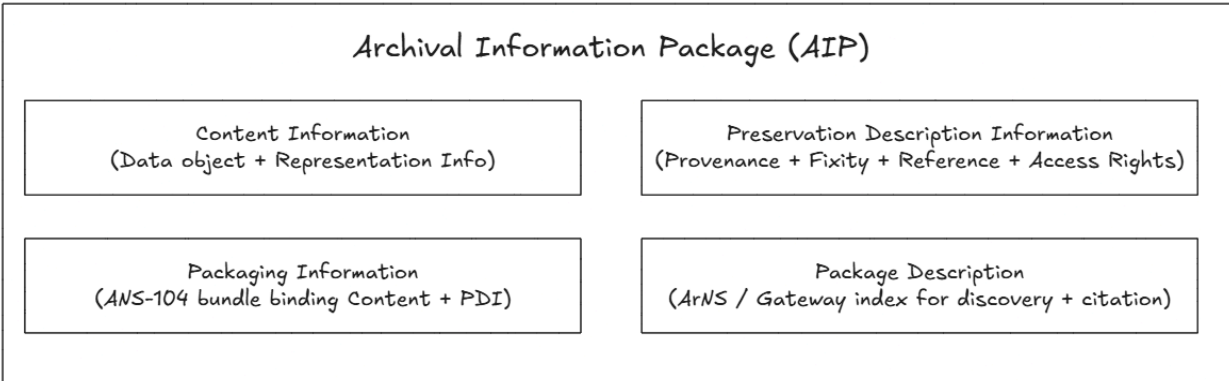


Figure 3.1.1: AIP structure in the Permanent Cloud

The AIP encapsulates all preservation components: the preserved content and its descriptive context (Content Information and Preservation Description Information) are bound together by the ANS-104 bundle (Packaging Information) and made discoverable through ArNS and gateway indexes (Package Description).

3.2 Functional Alignment

OAIS defines six core functional entities that describe how an archive preserves and provides access to digital information. The table below shows how these entities are implemented across the ar.io and Arweave networks, a decentralized architecture where permanence, provenance, and access are enforced by protocol.

OAIS Entity	OAIS Definition (ISO 14721)	Ar.io + Arweave Implementation	Core Capability
Ingest	<i>Processes by which information is submitted to the archive, validated, and prepared for preservation.</i>	Data enters the Permanent Cloud through Ar.io Gateways, which validate content and metadata, bundle submissions using ANS-104, and commit them immutably to the Arweave blockweave.	Verifiable ingestion (proof of submission and inclusion: TXID, tags).

OAIS Entity	OAIS Definition (ISO 14721)	Ar.io + Arweave Implementation	Core Capability
Archival Storage	<i>The secure storage, maintenance, and retrieval of preserved information objects and their associated metadata.</i>	Arweave provides immutable, globally replicated storage secured by a sustainable endowment model. ar.io extends this through decentralized indexes, content verification, and gateway observation, ensuring data remain discoverable and retrievable across time and providers. Gateways maintain local caches for resilience and speed; retrieval is always verifiable against the TXID.	Permanent retention and verifiable availability.
Data Management	<i>Maintenance of metadata, identifiers, and administrative information supporting discovery and preservation operations.</i>	The Arweave Name System (ArNS) and transaction identifiers (TXIDs) provide persistent, verifiable links between preserved content and its descriptive metadata. Ar.io Gateways index this information for discovery and interoperability with institutional catalogs and metadata systems.	Provenance and discoverability through persistent identifiers (TXID/ArNS).
Administration	<i>The functions that manage the operation of the archive, establish policies, and ensure preservation responsibilities are met.</i>	Governance and policy are encoded in smart contracts and managed transparently through the Ar.io Foundation and community processes. Built atop Arweave’s evolution framework, these contracts enable rule-based upgrades without altering or invalidating preserved data.	Accountable stewardship via transparent, rules-based governance.
Preservation Planning	<i>Monitoring the environment and developing strategies to ensure the long-term usability of information.</i>	Permanent storage and open-source architecture minimize manual migrations. As standards evolve, ar.io software and gateways adapt without compromising historical data integrity. Gateways provide Preservation Watch across the network.	Future-proof continuity and format/standards adaptability.

OAIS Entity	OAIS Definition (ISO 14721)	Ar.io + Arweave Implementation	Core Capability
Access	Processes that support the discovery, retrieval, and dissemination of preserved information to users.	The Ar.io Gateway Network and Wayfinder Protocol enable distributed, verifiable retrieval via standard web interfaces (ar://, HTTPS, and GraphQL). Wayfinder cross-verifies responses across multiple gateways, confirming authenticity and ensuring high availability without reliance on any single provider.	Trustworthy access through multi-gateway verifiable retrieval.

Table 3.2.1: OAIS <> Ar.io Functional Alignment

3.3 Principled Alignment

The Permanent Cloud fulfills OAIS preservation principles by translating technical mechanisms (Section 3.2) into enduring assurances of authenticity, accessibility, sustainability, understandability, and accountability.

Continuum also defines measurable Preservation Objectives and reviews them as Designated Community knowledge evolves, aligning with OAIS Issue 3 (CCSDS 650.0-M-3).

OAIS Principle	Permanent Cloud Expression
Authenticity & Integrity	Each preserved object carries permanent provenance and transaction metadata with cryptographic proofs of inclusion and fixity - ensuring that data received, stored, and retrieved remain verifiably identical to what was originally submitted
Accessibility	Open, web-native retrieval through gateways and the Wayfinder protocol ensures durable, redundant access across networks and institutions.
Sustainability	The Arweave endowment model permanently funds storage, while the ar.io network maintains verifiable access through open economics and multi-party operation.
Understandability & Transparency	The Permaweb preserves data, metadata, and the associated software, codecs, and schemas required for interpretation. By storing these elements together through open, permanent transactions, ar.io

OAIS Principle	Permanent Cloud Expression
	ensures that preserved information remains intelligible and usable as technology evolves.
Accountability & Governance	Transparent, rule-based smart contracts and protocol-level consensus provide verifiable stewardship and decision-making independent of central authorities.

Table 3.3.1: OAIS <> Ar.io Principled Alignment

Together these principles demonstrate that the Permanent Cloud satisfies OAIS preservation values in decentralized form.

3.4 Conformance Alignment

The OAIS Reference Model (ISO 14721 / CCSDS 650.0-M-3 § 3.2) defines five core responsibilities that any preservation system must meet to claim conformance. Table 3.4.1 summarizes how the Ar.io Network satisfies these responsibilities through protocol-level mechanisms and verifiable evidence as demonstrated in Section 5.

OAIS Core Responsibility	Ar.io / Arweave Expression	Evidence
Negotiate and accept information from producers	Content enters the Permanent Cloud permissionlessly through Ar.io Gateways, which validate submissions (ANS-104 bundles) and commit data immutably to the Arweave blockweave.	Upload SIP → AIP receipts
Obtain sufficient control to preserve information long-term	Immutable provenance, the Arweave endowment model, and decentralized consensus ensure enduring custody, replication, and verifiable preservation independent of any single institution.	Provenance chain and fixity records
Determine Designated Community and ensure understandability	Ar.io preserves data, metadata, and the associated software or codecs required for interpretation, ensuring intelligibility for future users — satisfying OAIS requirements for Representation Information.	Preservation objectives and community definition

Follow documented policies and procedures for authenticity, integrity, and usability	Transparent governance, open-source smart contracts, and cryptographic proofs of inclusion and fixity provide verifiable authenticity and procedural accountability.	Governance contracts and integrity proofs
Make preserved information available to the Designated Community	Open, web-native retrieval through Ar.io Gateways and the Wayfinder protocol ensures continuous, redundant access across networks and institutions.	Wayfinder multi-gateway verification logs

Table 3.4.1: OAIS <> Ar.io Conformance Alignment

This table demonstrates fulfillment of the OAIS mandatory responsibilities (§3.2) and links each to verifiable evidence demonstrated in Section 5.

4. DOI ↔ TXID / ArNS Interoperability

4.1 Overview

In traditional digital preservation and scholarly contexts, a TXID functions as a content-bound, permanent identifier. Rather than redefining DOI semantics, Continuum bridges DOI → TXID via ArNS so records stay citable in institutional systems while gaining cryptographic permanence.*

Transaction identifiers (TXIDs) are cryptographically verifiable references that permanently bind data to its proof of existence, provenance, and integrity - effectively serving as a permanent digital object identifier (pDOI).

The Arweave Name System (ArNS) extends these identifiers into a persistent, human-readable namespace, supporting metadata registration, discoverability, and record linkage.

By establishing a DOI ↔ TXID ↔ ArNS mapping, Continuum ensures that scholarly records preserved on the Permaweb maintain both:

1. Institutional persistence - through the globally recognized DOI framework (e.g., DataCite, Crossref).
2. Protocol-level permanence - through immutable TXIDs recorded on Arweave and resolved via ArNS.

**In addition to DOIs, other institutional identifier schemes used in archival practice (e.g., Archival Resource Keys, ARKs) function as OAI Reference Information and can be related to Transaction IDs (TXIDs) via ArNS using the same mapping approach described here.*

4.2 Mapping Model Example

Field	Example	Description
DOI	10.17605/OSF.IO/ABC123	CrimRxiv DOI issued via OSF/DataCite.
Arweave TXID	rQ93kGx.....p7ZsB9zE4A	Permanent, cryptographic identifier of the preserved object on Arweave.
ArNS Record	paper-abc123_crimrxiv	Human-readable, versioned name that resolves to the TXID and associated metadata.
Metadata (JSON or Tags)	{ "doi": "10.17605/OSF.IO/ABC123", "txid": "rQ93kGxS2...", "title": "...", "authors": [...], "timestamp": "2025-10-08" }	Minimal interoperable metadata record preserved onchain.

Table 4.2.1: Example DOI Mapping Model

4.3 Preservation Advantage

This bridge model extends the DOI’s concept of persistence from the metadata layer to the data layer, ensuring that both the record’s description and its content remain permanently verifiable.

A DOI functions much like a registry entry - a reference that persists as long as the underlying resolution infrastructure and hosting institutions maintain it. It identifies what something is and where it should be found, but not necessarily what it contains. In that sense, a DOI behaves like a symbolic link: it depends on ongoing curation to keep its target up to date.

By contrast, on the Permaweb, persistence is intrinsic rather than maintained. Each Arweave Transaction ID (TXID) is a cryptographic fingerprint of the asset itself - inseparably binding the data, metadata, and provenance in a single atomic record. It does not matter where the data is stored, because the TXID permanently and verifiably defines what it is. The Arweave Name System (ArNS) then provides human-readable resolution to these immutable assets, merging the accessibility of traditional identifiers with the self-verifying integrity of decentralized permanence.

In OAIS terms, DOI is Reference Information (a component of PDI), while the TXID and ArNS collectively guarantee Fixity Information and Reference Information, satisfying functional requirements for authenticity and provenance.

Concept	DOI (Traditional)	TXID / ArNS (Permaweb)
Persistence Model	Maintained by institutions through registries and redirection	Intrinsic to the data via cryptographic proof and embedded onchain
Scope	Metadata and reference only	Metadata + content + provenance (atomic unit)
Failure Mode	Link rot, metadata drift, institutional loss	Content drift is detectable (hash mismatch); resolution can fall back to independent gateways
Resolution	Centralized resolver (e.g., Crossref, DataCite)	TXID directly, or via the decentralized name system (ArNS)
Guarantee	“It should be here.”	“This is the exact object.”

Table 4.3.1: DOI <> TXID <> ArNS

Together, the DOI ↔ TXID ↔ ArNS bridge establishes a verifiable pathway between institutional identifiers and decentralized permanence - enabling scholarly records to remain both citable and cryptographically guaranteed within the global preservation ecosystem.

5. CrimRxiv Pilot

5.1 Purpose & Mission

The CrimRxiv pilot demonstrates how the Ar.io Network and Arweave can deliver OAIS-aligned, verifiable digital preservation in a live institutional setting.

Conducted in partnership with the CrimConsortium, the pilot tests how decentralized, trust-minimized infrastructure can meet established preservation standards while advancing the principles of open scholarship, reproducibility, and public access.

5.2 Context

CrimConsortium, a global network advancing open-access criminology, maintains CrimRxiv, a hub and repository for criminology research. Its materials are hosted on the PubPub publishing platform, which is scheduled to sunset at the end of 2026. To ensure continuity and permanence, CrimConsortium is migrating CrimRxiv to ar.io's decentralized storage and access stack.

As part of the Continuum framework pilot, CrimRxiv's content was mirrored through November 9, 2025, and is accessible at <https://crimrxiv-demo.ar.io>. This pilot tests decentralized permanence, metadata integrity, and OAIS functional alignment in a production setting, establishing a replicable model for scholarly publishing and repository preservation.

All works are published under Creative Commons licenses, permitting lawful redistribution and permanent archiving on the Permaweb. Through this migration, CrimConsortium demonstrates how decentralized infrastructure can maintain discoverability, verifiability, and access in line with OAIS preservation standards, ensuring that open-access criminology outputs remain permanently available and independently verifiable.

5.3 Why It Matters

The CrimRxiv pilot validates decentralized permanence as a viable path to meeting OAIS preservation standards, transforming an existing repository migration into a formally recognized, standards-aligned demonstration.

It establishes CrimConsortium as the first institutional anchor for Continuum - proving that decentralized infrastructure can achieve archival standards of trust, provenance, and verifiable access, and positioning the Permanent Cloud as a practical substrate for global digital stewardship.

5.4 Demonstration Walkthrough

The CrimRxiv pilot provides a working example of how OAIS-aligned preservation operates in practice. Each record within the archive contains a verifiable link between institutional identifiers and onchain proof of preservation.

On any article page, readers can view both a DOI and a transaction ID (TXID). Selecting the TXID opens its permanent record on Arweave, which displays:

- **Provenance:** submission identity, block height, and timestamp showing who deposited the item and when.
- **Fixity:** the TXID and hash values confirming the exact content of the preserved file.
- **Access rights:** a permanent license tag (for example, CC-BY-4.0) bound to the content.
- **Reference and description:** the DOI, title, authors, and other metadata enabling discovery and citation.

These details allow any observer to verify the object's authenticity, integrity, and provenance without relying on a single host or server. Each article is a self-contained preservation proof.

Because the archive's data and metadata are public, versioned, and addressable by TXID and ArNS, they can be reused and extended. Others can index and analyze preserved outputs, build citation networks or dashboards, train language models on openly licensed material, or maintain independent mirrors while still verifying every byte.

Finally, the pilot demonstrates that the repository interface itself is permanent. Each page is stored on Arweave and resolved through ArNS, ensuring stable addressing, prepaid storage, and resilient access across multiple gateways. The result is an archive that remains open-access, verifiable, and independent of future platform fees or service dependencies.

6. Future Vision and Considerations

6.1 Limitations and Risks

Continuum and the underlying Permanent Cloud model depend on several long-term assumptions that, while reasonable, remain subject to validation over time. The Arweave endowment model, operating reliably since 2018, assumes that economic-value stability and continued network participation will sustain perpetual storage; future market conditions could influence those dynamics. Likewise, durable access through the ar.io gateway network relies on ongoing community operation, software maintenance, and adherence to open standards. Governance, interoperability, and regulatory environments may evolve in ways that require adaptation. Broader institutional adoption of decentralized preservation models also depends on continued education, trust-building, and alignment with existing archival certification practices. These factors are monitored as part of Continuum's preservation-planning process and will inform future iterations of the framework.

6.2 Next Steps

Continuum is designed as a progressive program of validation, collaboration, and standardization.

Following the initial CrimRxiv pilot, the initiative will expand through successive phases - first validating decentralized preservation across multiple institutional repositories, then consolidating these results into a formal, openly published Decentralized Preservation Framework.

This framework will evolve in partnership with the broader digital preservation community, aligning with organizations such as the DPC, NDSA, and IIPC to ensure compatibility with established best practices and certification pathways.

Over time, these efforts aim to position Continuum and the Permanent Cloud as recognized, standards-aligned infrastructure for verifiable, decentralized digital preservation - bridging institutional stewardship and protocol-level permanence across the global preservation ecosystem.

Appendices

A. Glossary

- **Access:** The process of discovering, retrieving, and disseminating preserved information to users. In the Permanent Cloud, access is provided through Ar.io Gateways and the Wayfinder Protocol, which enable verifiable retrieval via standard web interfaces. (*OAIS Functional Entity; CCSDS 650.0-M-3 §4.2*)
- **ANS-104:** Arweave Network Standard defining how bundles of data and metadata are structured for permanent storage. Used by Ar.io Gateways for validated ingestion.
- **Archival Information Package (AIP):** A logical container consisting of *Content Information* and *Preservation Description Information (PDI)* that is preserved within the archive. (*OAIS §1.6.2*)
Example: The canonical, immutable data package permanently stored on Arweave and indexed via ar.io .
- **ArNS (Arweave Name System):** A decentralized, human-readable naming and metadata system that maps names to Arweave transaction IDs (TXIDs) and supports versioned record resolution across gateways.
- **Arweave Blockweave:** A tamper-proof, cryptographically linked data structure that permanently stores immutable transactions replicated across all nodes. Its built-in economic endowment ensures perpetual storage through a decentralized, protocol-level incentive model - forming the base permanence layer of the Permaweb.
- **Atomic Asset:** A single, immutable record combining data, metadata, and provenance in one verifiable transaction on the Permaweb. Identified by a unique TXID, it ensures that what is preserved and how it's described are inseparable and permanently verifiable. Analogous to an OAIS Archival Information Package (AIP).
- **Authenticity:** The degree to which an object is regarded as what it purports to be. In OAIS, authenticity is supported by provenance and fixity evidence; in Arweave, by cryptographic proof of inclusion. (*OAIS §1.6.2*)
- **Content Information:** The digital object that is the target of preservation, consisting of the Content Data Object and its Representation Information. (*OAIS §1.6.2*)
Example: A CrimRxiv research paper or dataset submitted for long-term preservation.
- **Continuum Framework:** The standards-alignment model defining how ar.io + Arweave fulfill OAIS functions through decentralized protocols.
- **CrimRxiv:** A hub and repository for open-criminology articles.
- **CrimRxiv Consortium ("CrimConsortium"):** a global network of institutions and individuals who lead, provide, and support open criminology on and off CrimRxiv.
- **Designated Community:** The group of users for whom preserved information must remain understandable and usable over the long term. Defined by the archive (or protocol) and may evolve over time. (*OAIS §1.6.2 & §2.3.2*)
- **Dissemination Information Package (DIP):** An Information Package, derived from one or more AIPs, that is sent by an archive to a *Consumer* in response to a request. (*OAIS*

§2.3.4)

Example: The verified, retrievable data package delivered to an end user via ar.io and the Wayfinder protocol.

- **DOI (Digital Object Identifier):** A persistent identifier issued within institutional publishing networks (e.g., DataCite, Crossref) to provide long-term reference to digital objects. In Continuum, DOIs are bridged to Arweave TXIDs via ArNS.
- **Fixity Information:** Metadata and mechanisms (e.g., hashes, Merkle proofs) ensuring that a Content Data Object has not been altered in an undocumented manner. (OAI §1.6.2 & §2.3.3)
- **Gateway (ar.io):** A network node providing open access, indexing, querying, and verification of Arweave data. Gateways form the access and validation layer of the Permanent Cloud.
- **Ingest:** The process by which information is submitted, validated, and prepared for preservation. In ar.io , this occurs through gateway-facilitated ANS-104 bundling to Arweave. (OAI Functional Entity §4.2)
- **Metadata Integrity:** The guarantee that descriptive and administrative metadata remain verifiable and cryptographically linked to their preserved content.
- **OAI (Open Archival Information System):** An international reference model (ISO 14721 / CCSDS 650.0-M-3) defining the concepts, responsibilities, and functional entities required for long-term digital preservation.
- **Open Criminology:** Scholarly outputs such as articles (preprints, postprints, versions-of-record), data, and software code; published under an open-source license (e.g., Creative Commons); that inform the study of lawmaking, lawbreaking, and reactions to them.
- **Permanent Cloud:** The verifiable preservation and access layer built on the Permaweb, integrating Arweave storage and ar.io gateway services to provide OAI-aligned permanence, provenance, and accessibility.
- **Permaweb:** The global, immutable web of data permanently stored on Arweave and accessible through open protocols such as ar.io .
- **Preservation Description Information (PDI):** The information necessary to preserve a Content Data Object, including Provenance, Context, Reference, Fixity, and Access Rights Information. (OAI §1.6.2 & §2.3.3)
- **Preservation Watch:** A continuous process within an OAI that monitors the environment, technology, and content to identify risks to long-term usability or integrity. (OAI §2.3.3.6)
- **Provenance Information:** Metadata documenting the origin, custody, and change history of a Content Data Object. In Arweave, provenance is cryptographically recorded in each TXID. (OAI §1.6.2)
- **Submission Information Package (SIP):** An Information Package delivered by the *Producer* to the OAI for use in constructing or updating one or more Archival Information Packages (AIPs). (OAI §2.3.4)

Example: The validated data package submitted to Arweave through an Ar.io Gateway during ingest.

- **TXID (Transaction Identifier):** A cryptographic hash permanently identifying a piece of data stored on Arweave. Serves as an immutable provenance record linking content, metadata, verification proofs, and publisher. Conceptually equivalent to a permanent digital object identifier (pDOI) in scholarly preservation contexts.
 - **Wayfinder Protocol:** An ar.io retrieval mechanism that queries multiple gateways to confirm content authenticity and availability, ensuring verifiable, fault-tolerant access.
-

B. References and Citations

- **ISO 14721:2025 (CCSDS 650.0-M-3):** <https://ccsds.org/Pubs/650x0m3.pdf>
- **Arweave White Paper:** https://draft-17_whitepaper.ar.io/
- **Ar.io White Paper:** <https://whitepaper.ar.io>
- **Continuum Framework (most current version):** <https://continuum.ar.io>
- **CrimRxiv Pilot Project and Demonstration:** <https://crimrxiv-demo.ar.io>