Originals: Authentic Decentralized Digital Assets

Version 1.1 — August 2025

Brian Richter (Aviary Tech)

Abstract

Originals is a minimal protocol for creating, discovering, and transferring digital assets with cryptographically verifiable provenance. Assets are represented by Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) that migrate through three infrastructure-native layers: private (`did:peer`), public (`did:webvh`), and transferable (`did:btco`). Ownership moves only on Bitcoin, ensuring that economic value is secured by the world's most resilient consensus network, while discovery and experimentation incur no blockchain cost. The protocol requires no smart contracts, trusted third parties, or bespoke blockchains.

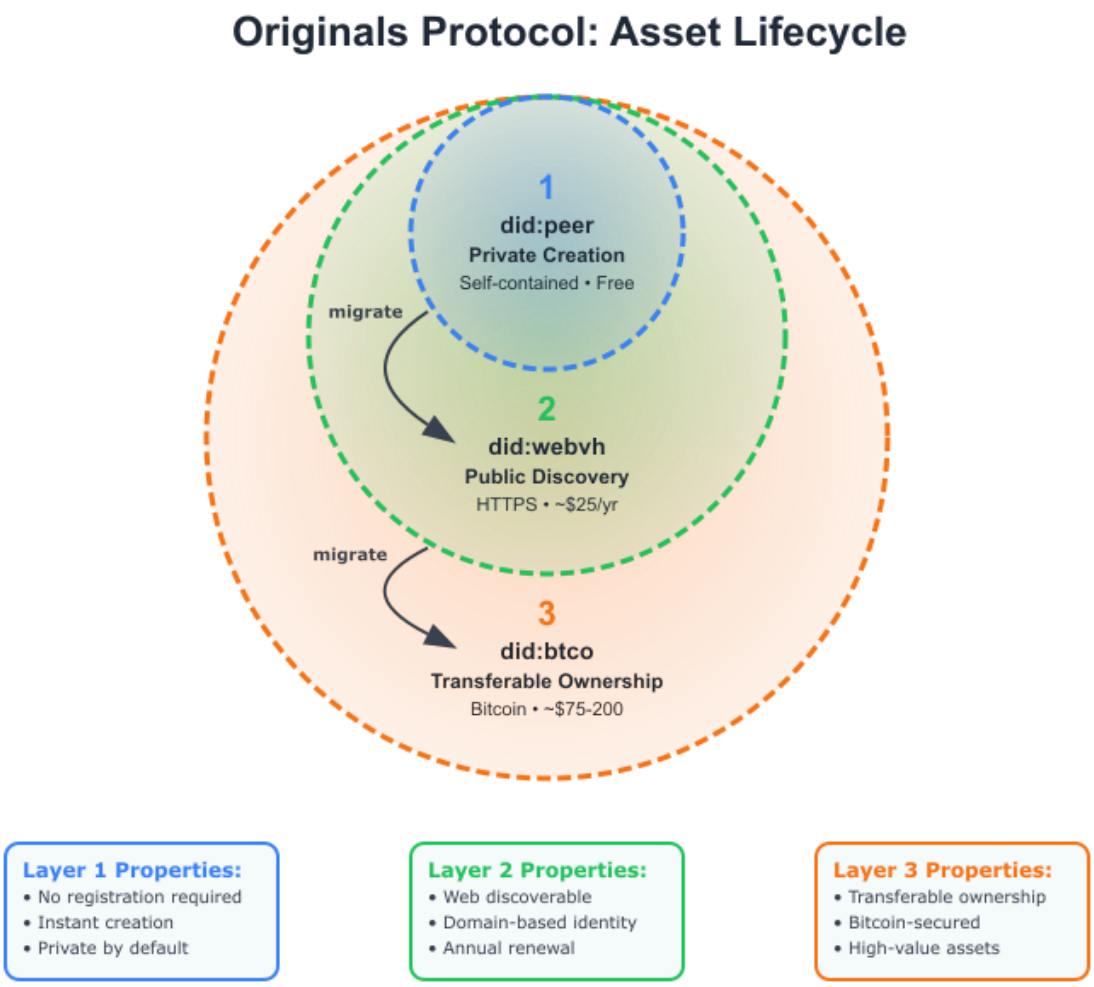
1. Introduction

Digital assets today depend on platforms that can vanish or mutate content, undermining authenticity. Existing NFT systems pin hashes but trade mutable URLs. Mainstream web media offers discoverability without cryptographic guarantees or ownership. Conversely Originals ensure provenance is inseparable from the asset and security organically scales with value. This delivers what existing platforms fail to provide.

2. System Overview

Originals organizes the asset lifecycle into three layers with the ability to migrate in one direction using digital signatures to form an auditable chain: `did:peer` → `did:webvh` → `did:btco`

1. Private Creation — `did:peer`: A self-contained DID document embeds resource URLs and resource credentials. Verification is offline and free.
    a. `did:peer` (short form) credentials can be published directly to `did:webvh` or `did:btco` for public resource provenance or timestamping. This allows creators to assert authorship or claim existence of a resource prior to full migration.
2. Public Discovery — `did:webvh`: The DID document is hosted on any HTTPS server, making the asset indexable by existing web crawlers. No economic activity occurs here.
3. Transferable Ownership — `did:btco`: Critical state is inscribed on Bitcoin via the Ordinals protocol. A unique satoshi anchors the final DID, enabling censorship-resistant transfers.



3. Data Model

Each layer shares the same verification stack:

1. DID Document — keys and services
2. Verifiable Credentials — `ResourceCreated`, `ResourceUpdated`, `ResourceMigrated`
3. Resources — digital content (images, text, code, data, etc.)

Uniform proofs let wallets and applications verify any asset with identical code, regardless of layer.

4. Economic Layer Separation

Only Bitcoin prevents double-spending; therefore all trades must settle in `did:btco`. Lower layers handle creativity and distribution where consensus is unnecessary. Market forces push valuable assets upward, aligning security spend with asset value.

Layer	Security	Cost	Economic Role
did:peer	High (self-contained)	0	None
did:webvh	Medium (HTTPS)	≈ $25 / yr	None
did:btco	Maximum (Bitcoin)	≈ $75–200 one-time	All transfers

5. Incentives

Creators pay nothing to experiment, modestly to be discovered, and only migrate to Bitcoin when a buyer emerges. Collectors gain the strongest guarantees when value justifies the fee. No party subsidises unused security.

6. Security Considerations

1. Data Integrity: All credentials include W3C standard proofs.
2. Key Rotation & Recovery: Compromised keys can be revoked and rotated via DID operations without breaking historical provenance.
3. Front-Running: Unique satoshi assignment thwarts front-running attacks.
4. Layer Resilience: Failure in web hosting affects discoverability but not ownership; Bitcoin anchoring is final.

7. Related Work

Originals builds directly on the interoperability of W3C DID and VC standards, and the finality of Bitcoin's Ordinals protocol, but deliberately separates the processes of asset creation, discovery, and settlement.

8. Conclusion

Originals offers a simple path from creation to permanent ownership without inventing new blockchains. By letting economic gravity decide when an asset deserves Bitcoin immutability, the system pairs mainstream web usability with maximal security, creating a pragmatic bridge for decentralized digital provenance.

Appendix 1: Example Use Cases for Originals

Digital Art Provenance and Transfer

- An artist creates an image and issues a `did:peer` version for experimentation and feedback among peers.
- Once the piece sparks interest, the artist migrates it to `did:webvh`, making it discoverable on a personal domain for wider public viewing.
- Upon sale, the work is migrated to `did:btco` and inscribed on Bitcoin, ensuring both the artist and buyer can prove the asset's origin and ownership chain is immutable and publicly auditable.

Scientific Data Publication

- A researcher documents original datasets with a `did:peer` identifier for internal lab use and collaboration.
- When ready to publish, the dataset is migrated to `did:webvh` and hosted on an institutional server for public referencing and indexing.
- Following peer review or receipt of a grant, the data's origin and record are finalized by migrating to `did:btco`, making its provenance tamper-resistant and allowing future citations to reference its Bitcoin-inscribed authenticity.

DAO Governance

- A DAO establishes its community by issuing `did:peer` credentials to early members, representing identity and participation rights without cost.
- As the DAO grows, membership credentials are migrated to `did:webvh`, making them discoverable and verifiable on the open web while still off-chain. This enables public recognition of contributors, roles, and proposals.
- When decisions, commitments, or treasury actions require permanence, they are finalized by migrating to `did:btco`. These inscriptions on Bitcoin create an immutable, censorship-resistant record of governance outcomes and membership proofs, ensuring long-term transparency, accountability, and trust.

Software Release with Verifiable Supply Chain

- An open-source project maintains `did:peer` credentials for unreleased or developmental branches.
- Minor releases are migrated to `did:webvh` for web-wide indexing and downloads.
- Major releases are further migrated to `did:btco`, enabling governments and enterprises to verify provenance and source integrity, reducing supply chain risks.

Heritage Collectibles

- Archivists, museums, or estates catalog rare items with `did:peer` credentials, creating verifiable records without needing a blockchain.
- `did:webvh` migration makes these records publicly discoverable and indexable for researchers and the public.
- `did:btco` anchoring ensures provenance persists even if institutions dissolve or servers disappear — preserving cultural heritage with Bitcoin's permanence.

Consumer Goods with Provenance Trails

- A manufacturer issues `did:peer` credentials for limited-run sneakers, instruments, or other goods.
- `did:webvh` provides a verifiable public registry of authentic items, reducing counterfeiting risk.
- `did:btco` anchoring secures the full chain of custody, ensuring authenticity survives through resales, market shifts, or brand collapse.