Title: arcHIVE and C2PA: Two-Factor Provenance for the Digital Age

Abstract

This paper introduces arcHIVE, a decentralized media provenance and authenticity system designed as a complementary safeguard to centralized implementations of the Content Authenticity Initiative (C2PA), primarily governed by Adobe and partner corporations. Unlike models that root trust solely in certificate authorities and proprietary infrastructure, arcHIVE uses self-sovereign cryptographic identities, IPFS content addressing, and blockchain tokenization to create a public, verifiable, and censorship-resistant chain of custody for media. This paper explores the technical architecture, comparative trust models, and the socio-political implications of layering decentralized assurance on top of centralized authenticity systems.

1. Introduction

As misinformation and synthetic media proliferate, C2PA has emerged as a proposed standard for digital content authenticity. Backed by Adobe, Microsoft, Intel, Truepic, Nikon, BBC, Arm, WITNESS, and several others, the initiative aims to ensure that users can trace the origins and modifications of media files (C2PA, 2023). However, its reliance on centralized certificate authorities and closed infrastructure raises concerns about control, access, and bias. This paper proposes arcHIVE not as a replacement, but as a cryptographic second factor--offering grassroots content authentication that complements existing infrastructure by enabling provenance without exclusive dependence on corporate verification.

Analogy: arcHIVE as Two-Factor Provenance

Just as two-factor authentication (2FA) complements passwords to enhance digital security, arcHIVE complements C2PA to enhance media authenticity. C2PA functions like a password: it verifies identity through a trusted authority. arcHIVE is like 2FA -- a second, decentralized layer of verification based on public keys, tokenization, and distributed storage. Even if centralized trust is compromised, the arcHIVE layer remains independently verifiable, public, and tamper-resistant.

2. C2PA: Promise and Pitfalls

C2PA combines signed manifests with metadata to show a file's provenance. It allows for digital signatures, annotations of edits, and assertions of authorship. While the standard is open, its implementation is not: Adobe dominates tooling, verification services, and trust anchors. This limits accessibility, especially for marginalized creators or communities without Adobe accounts or recognition. Furthermore, signed data is typically stored and verified within Adobe's ecosystem, not on decentralized or user-controlled infrastructure (Content Authenticity Initiative, 2023).

3. The Need for a Decentralized Counterpart

Centralized media authentication systems risk replicating the failures of DRM, surveillance-heavy platforms, and digital gatekeeping. arcHIVE addresses these risks by enabling:

- Self-signed Ed25519 keys (user-generated)
- IPFS storage of hashed media and manifest content
- Smart contract-based minting of authenticity tokens (ERC-721/1155)

This offers an open, inspectable verification path, making media verifiable by anyone, from any machine, without dependence on a proprietary cloud (IPFS Project, 2024).

4. The arcHIVE System

arcHIVE consists of:

- A WASM or Python-based C2PA-compliant signer
- IPFS integration to pin media or manifest hashes (e.g., `Qm...`)
- A tokenization engine that mints a smart contract token to formalize authorship and timestamp
- A decentralized verification portal (on-device or webapp)

Each signed file links to a content hash pinned on IPFS. The smart contract embeds this hash as the canonical reference. The resulting NFT acts as a digital title registry, optionally enriched with metadata, video proof, and human-readable claims.

Figure 1. arcHIVE Signing and Verification Flow

```
[ Media File ]

    ->

[ C2PA Manifest ]

    -> (SHA-256)

[ IPFS Hash Qm... ]

    ->

[ Token Minted (ERC-721) ]

    ->

[ Verification Portal / App ]
```

5. Trust Models Compared

Feature	C2PA (Adobe-centric)	arcHIVE
Certificate Authority	Centralized (Adobe, Microsoft, Intel, Truepic, Nikon, etc.)	Decentralized (self-sign or DAO-based anchors)
Manifest Verification	Adobe Content Credentials	Open source CLI/UI verifier
Hash Storage	Cloud-hosted (Adobe servers)	Public IPFS content addressing
Ownership Registry	None	On-chain ERC token with public metadata
Identity Model	Adobe/Microsoft Cloud IDs	Wallet addresses or DIDs
Accessibility	Enterprise-first	Community-first
Revocation/Control	Platform-enforced	Signer-controlled with optional DAO overrides

Figure 2. Centralized vs. Decentralized Trust Models

C2PA (Adobe)

User -> Adobe Signer -> Adobe Credential Graph -> Manifest

arcHIVE

User -> Local Signer -> IPFS + Token Minting -> Manifest + NFT -> Public Verification

6. Socio-Political Implications

C2PA's structure risks creating a two-tiered authenticity economy, where large institutions dominate visibility and trust. arcHIVE counters this by empowering individuals and local communities to assert authorship and provenance independently. This matters especially in regimes with censorship, in activist documentation, or in regions without reliable legal or governmental backing (Miller & Stiegler, 2003).

7. Conclusion

C2PA is a meaningful step forward, but its current trajectory risks entrenching centralized authority over media truth. arcHIVE offers a complementary safeguard -- a decentralized, open, and cryptographically sound system that restores trust at the edge, not just the core. Its use of IPFS and tokenization reimagines provenance as a public good, not a corporate asset.

Future Work

- Cross-verification between arcHIVE and C2PA manifests
- Integration with hardware camera signatures
- Reputation graphs for voluntary decentralized trust scores
- Zero-knowledge metadata reveal protocols for sensitive content

Acknowledgments

The authors thank the open-source C2PA, IPFS, and Ethereum communities. Special thanks to Mark S. Miller and Nick Szabo for laying the conceptual groundwork this project builds upon.

References

C2PA. (2023). C2PA Technical Specification Version 1.3. https://c2pa.org/specifications/specifications/1.3/

Content Authenticity Initiative. (2023). Adobe's vision for content authenticity. https://contentauthenticity.org

IPFS Project. (2024). The InterPlanetary File System. https://docs.ipfs.tech

Miller, M. S., & Stiegler, M. (2003). The Digital Path: Smart Contracts and the Third World. In Markets, Information and Communication: Austrian Perspectives on the Internet Economy. Routledge.

Szabo, N. (1997). Formalizing and Securing Relationships on Public Networks. https://szabo.best.vwh.net/formalize.html