ISSN: 3007-9640 DOI: https://doi.org/10.70114/acmsr.2026.9.1.P18

A Delegatable Accumulator-Based Framework for Lightweight Cross-Chain Copyright Ownership Verification

Yi Wei [a], Hengtong Chang [b], and Jing Dong [c] *

Nanfang College Guangzhou, China.

[a] weiy@nfu.edu.cn, [b] changhengtong@nfu.edu.cn, [c] dongj@nfu.edu.cn

Abstract. Cross-chain copyright ownership verification is difficult for lightweight clients because copyright states evolve through registration, transfer, and revocation, rendering existing membership witnesses outdated for the updated state. This paper proposes a delegatable RSA-accumulator framework that separates one-time trust establishment from routine verification. A BFT committee authenticates an initial accumulator anchor; thereafter, untrusted relays update membership witnesses and return verifiable transition evidence. Copyright identifier, owner, rights type, status, and version are encoded into one prime representative, enabling existence and current ownership to be verified with a single constant-size proof. A multi-chain prototype shows that verification remains approximately 174 kGas and 0.44 KB as the scale increases to 500, while lightweight storage remains about 0.874 KB. The design therefore reduces reliance on trusted relays without requiring clients to retain source-chain ledgers.

Keywords: blockchain interoperability; copyright management; delegatable accumulator; lightweight verification; cross-chain authentication.

1. Introduction

Blockchain supports copyright traceability and automated rights management [1–3], but cross-chain ownership verification remains challenging for lightweight clients. Many existing approaches require state synchronization or reliance on external relays. Registration, transfer, and revocation further complicate verification by changing copyright records and requiring membership witnesses to be updated.

Cross-chain approaches balance trust, synchronization, and proof-generation costs [4–6]. TrailChain traces ownership across marketplaces [7], FastDCV supports batched consistency verification [8], and CAVer reduces verification overhead through message accumulation [9]. Cryptographic accumulators offer compact set commitments [10], while recent advances support delegatable proofs [11], private proof-update delegation with constant-time client-side operations [12], and lightweight universal constructions [13]. However, integrating owner-bound copyright representation, authenticated cross-chain initialization, and verifiable witness updates remains a challenge.

We propose a delegatable RSA-accumulator framework combining these mechanisms. Copyright elements bind ownership, status, and version, while a committee authenticates the initial accumulator anchor once. Subsequently, untrusted relays update membership witnesses across versions, and lightweight clients verify both state transitions and membership against the authenticated state. This design outsources witness maintenance without requiring continuous relay trust or full-ledger storage. A multi-chain prototype evaluates verification gas consumption and proof size against TrailChain, FastDCV, and CAVer.

2. Proposed Framework

2.1 System Model and Threat Assumptions

The source chain C_h maintains active copyright records and commits an accumulator A_t and state version v_t to its authenticated state. A verifier V on C_v stores public parameters pp, its latest authenticated accumulator and version, and a witness for the tracked element. A committee of $n = 3f + 1$

ISSN: 3007-9640 DOI: https://doi.org/10.70114/acmsr.2026.9.1.P18

members certifies initialization with at least $2f + 1$ valid signatures. Subsequent witness updates may be outsourced to any relay.The overall framework is illustrated in Fig. 1.

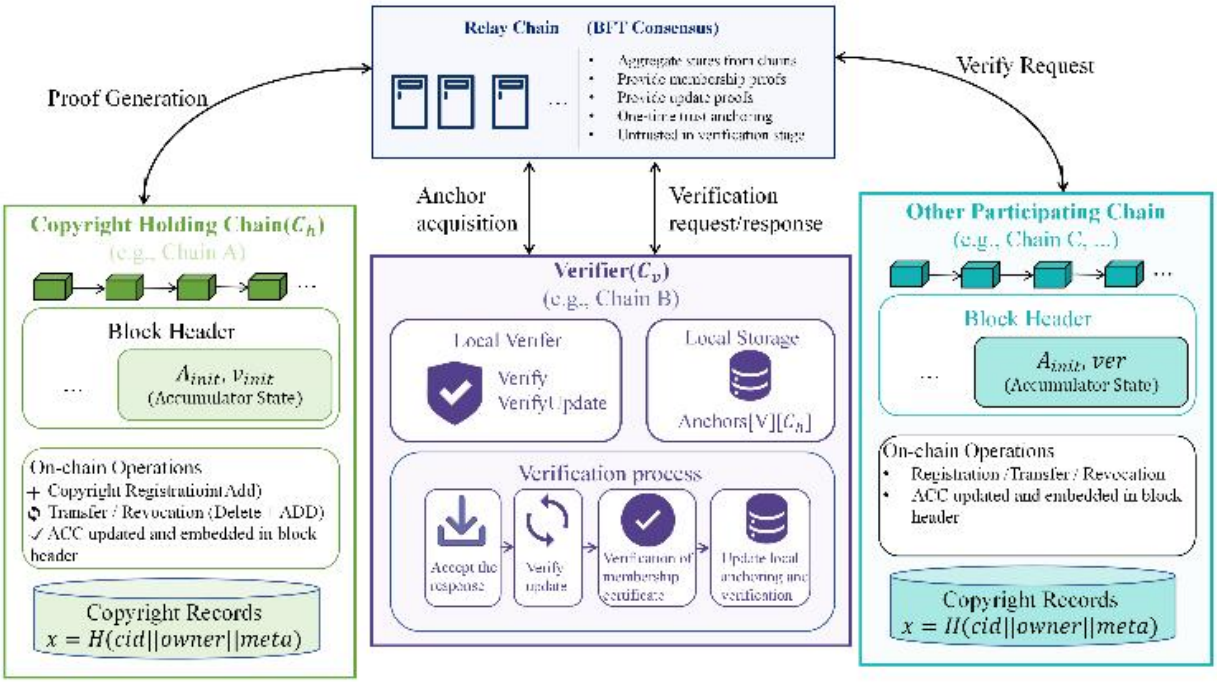


Fig. 1. Framework model

Relays may return forged, incomplete, stale, or replayed responses. The adversary cannot factor N, break source-chain finality, forge threshold signatures, or control more than f committee members at anchoring time. Availability attacks remain possible, but invalid ownership must not be accepted.

2.2 Copyright Accumulator

Let $pp = (N, g, H, H_p)$, where $N = pq$ is an RSA modulus with unknown factorization, $g \in QR_N$, H is collision resistant, and H_p is a domain-separated hash-to-prime function. Let r denote a record version, distinct from the accumulator version v_t. Encode a record using an unambiguous serialization:

$$m_t = COPYRIGHT \parallel cid \parallel owner \parallel rights \parallel status \parallel v_t, e_t = H_p(m_t) \quad (1)$$

The record version changes only when that record changes. For an unchanged record, its representative e remains fixed across accumulator updates. Let S_t be the set of prime representatives of active records:

$$P_t = \prod_{x \in S_t} x, \quad A_t = g^{P_t} \bmod N \quad (2)$$

$$P_{t,e} = \prod_{x \in S_t \setminus \{e\}} x, \quad \pi_e^t = g^{P_{t,e}} \bmod N \quad (3)$$

Membership is accepted only if the witness reconstructs the current state:

$$(\pi_e^t)^e \equiv A_t \pmod N \quad (4)$$

2.3 Dynamic Operations and Delegation

Setup generates pp for security parameter λ. Registration inserts a new element; transfer atomically deletes the old element and inserts its replacement; revocation deletes the active element. Add and Delete produce the updated accumulator and public update evidence. Prove generates a membership witness, and Verify checks (4).

For an unchanged element $e \in S_t \cap S_{t+k}$, DelegateUpdate refreshes its witness using public evidence $\delta_{t:t+k}$ and returns an update proof $\rho_{t:t+k}$. VerifyUpdate checks the delegated computation:

$$(\pi_e^{t+k}, \rho_{t:t+k}) \leftarrow \text{DelegateUpdate}(\text{pp}, A_t, A_{t+k}, \delta_{t:t+k}, \pi_e^t) \quad (5)$$

A transferred record has a new representative and requires a newly generated membership witness; the former owner's witness is not converted into a witness for the replacement element. Deleted

ISSN: 3007-9640 DOI: https://doi.org/10.70114/acmsr.2026.9.1.P18
elements cannot be accepted against the authenticated successor accumulator under membership soundness.

3. Cross-Chain Verification Protocol

3.1 Phase I: One-Time Trusted Anchoring

The verifier requests an anchor for C_h using a fresh nonce. Committee members validate a finalized source-chain state and its accumulator commitment, then sign a common message binding the chain identifier, header, accumulator, state version, nonce, and public-parameter digest $H(\mathrm{pp})$.

The committee returns the message, public parameters, and a quorum certificate containing at least $2f + 1$ valid signatures. After checking the certificate, request binding, and parameter digest, V stores (A_t, v_t, pp). This establishes the initial trust anchor under the committee threshold assumption.

3.2 Phase II: Autonomous Verification

For a copyright claim $q = (cid, owner, rights, status)$, the verifier sends $VerifyReq(C_h, q, v_t, nonce)$ to an arbitrary relay. The relay obtains the latest finalized state (A_{t+k}, v_{t+k}), collects the public update evidence $\delta_{t:t+k}$, and evaluates (5). It then returns $Resp = (C_h, q, A_{t+k}, v_{t+k}, \pi_{e,t+k}, \rho_{t:t+k}, nonce)$. This computation requires no verifier secret.

The verifier rejects the response if the chain or copyright identifiers differ from the request, the nonce is invalid, the source state lacks the required finality, or $v_{t+k} < v_t$. It then derives e_{t+k} from (1) and performs the following checks:

$$b_1 = VerifyUpdate(pp, A_t, A_{t+k}, \delta_{t:t+k}, \rho_{t:t+k}) \quad (6)$$

$$b_2 = Verify(pp, A_{t+k}, e_{t+k}, \pi_{\mathrm{e}}{}^{t+k}) \quad (7)$$

$$Accept(q) = 1 \Leftrightarrow (b_1 = 1) \wedge (b_2 = 1) \wedge (v_{t+k} \geq v_t) \quad (8)$$

Upon acceptance, V replaces its local verification state with $(A_{t+k}, v_{t+k}, \pi_{e,t+k})$. The update evidence $\delta_{t:t+k}$ is consumed as transition input rather than retained as a permanent history. Hence, the lightweight verifier stores only its latest authenticated state and membership witness.

4. Security Analysis and Evaluation

Completeness. For honestly generated states and updates, the membership relation in (4), VerifyUpdate, and the combined decision rule in (8) all evaluate successfully.

Membership soundness. Under the Strong RSA assumption, an adversary cannot construct a witness $\pi*$ that satisfies the membership equation for A_t when $e* \notin S_t$ with non-negligible probability.

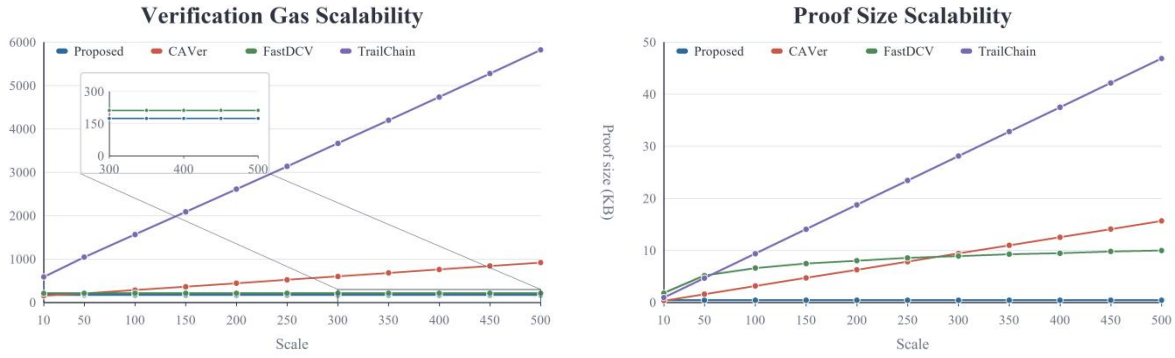
Transition authenticity. Collision resistance and the soundness of delegated updates prevent a forged proof $\rho*$ from validating an accumulator state that is not derived from the stored anchor through the claimed update evidence $\delta*$.

The combined ownership statement follows because acceptance requires both transition authenticity and membership soundness. Given a trusted anchor A_t and a successfully verified transition to A_{t+k}, the adversarial success probability is bounded by

$$Pr[Verify(pp, A_{t+k}, e*, \pi*) = 1 \wedge e* \notin S_{t+k}] \leq negl(\lambda)$$

Forging the initial state additionally requires breaking the threshold signature or violating the assumption that at most f committee members are Byzantine. Version monotonicity rejects a stale but otherwise valid state, while the nonce prevents response replay. The scheme is therefore trust-minimized rather than absolutely trustless: bootstrap security depends on the committee threshold and source-chain finality, whereas relay correctness after anchoring is verified cryptographically.

ISSN: 3007-9640 DOI: https://doi.org/10.70114/acmsr.2026.9.1.P18



(a) (b)

Fig. 2. (a)Verification gas scalability and (b)Proof-size scalability

The prototype contains three Ethereum-compatible chains and one PBFT relay chain, using Geth v1.10.26, Docker Desktop 4.36.0, and Ganache v6.12.2 for controlled comparison. Experiments run on an Intel Core Ultra 7 155H with 32 GB RAM. Baselines are CAVer, FastDCV, and TrailChain.

As shown in Figs. 2(a) and (b), the proposed scheme maintains nearly constant verification gas consumption and proof size over scales of 10–500, reaching 174 kGas and 0.44 KB at scale 500. Gas consumption is 17.9%, 81.1%, and 97.0% lower than that of FastDCV, CAVer, and TrailChain, respectively.

5. Conclusion

This paper presents a delegatable accumulator framework for lightweight cross-chain copyright ownership verification. A one-time BFT-certified anchor authenticates the initial source-chain state, after which untrusted relays update witnesses for local verification. Copyright elements bind record identity, owner, status, and version, enabling joint verification of membership and ownership against the authenticated state. At scale 500, the prototype requires approximately 0.44 KB proofs and 174 kGas per verification, while maintaining nearly constant verifier storage. The framework reduces reliance on trusted relays without requiring full-ledger storage.

References

[1] García R, Cediel A, Teixidó M, Gil RM. A review of media copyright management using blockchain technologies from the academic and business perspectives. Information. 2025 Jan 21;16(2):72.

[2] Madapati SL, Pradhan NR. Decentralizing video copyright protection: a novel blockchain-enabled framework with performance evaluation. Frontiers in Artificial Intelligence. 2025 Aug 18;8:1655709.

[3] Hanif M, Munir EU, Rehan MM, Ahmad SG, Khan I, Setchi R. Tiered blockchain framework: A secure, trustworthy, and cost-efficient solution for the digital rights protection. Blockchain: Research and Applications. 2025 May 14:100308.

[4] Li W, Liu Z, Chen J, Liu Z, He Q. Towards blockchain interoperability: A comprehensive survey on cross-chain solutions. Blockchain: Research and Applications. 2025 Apr 7:100286.

[5] Li M, Weng J, Li Y, Wu Y, Weng J, Li D, Xu G, Deng R. Ivycross: A privacy-preserving and concurrency control framework for blockchain interoperability. Cryptology ePrint Archive. 2021.

[6] Xie T, Zhang J, Cheng Z, Zhang F, Zhang Y, Jia Y, Boneh D, Song D. zkbridge: Trustless cross-chain bridges made practical. InProceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security 2022 Nov 7 (pp. 3003-3017).

[7] Gupta P, Dedeoglu V, Kanhere SS, Jurdak R. TrailChain: Traceability of data ownership across blockchain-enabled multiple marketplaces. Journal of Network and Computer Applications. 2022 Jul 1;203:103389.

ISSN: 3007-9640 DOI: https://doi.org/10.70114/acmsr.2026.9.1.P18
[8] Xu Y, Zeng J, Dai S, Xiang Q, Tao J, Cheng G. FastDCV: An efficient cross-chain data consistency verification scheme supporting batch processing. Peer-to-Peer Networking and Applications. 2025 Oct;18(6):301.

[9] Guo Y, Wang Y, Huang J, Duan T, Jia L, Zhang H, Sun Y. Caver: Compacting accumulation to reduce cross-chain verification overhead. Blockchain: Research and Applications. 2025 Sep 8:100381.

[10] Loporchio M, Bernasconi A, Maesa DD, Ricci L. A survey of set accumulators for blockchain systems, Comput. Sci. Rev. 49 (2023) 100570 [Internet]. 2023

[11] Barthoulot A, Blazy O, Canard S. Cryptographic accumulators: new definitions, enhanced security, and delegatable proofs. InInternational Conference on Cryptology in Africa 2024 Jul 3 (pp. 94-119). Cham: Springer Nature Switzerland.

[12] Soóki-Tóth B, Glasz B, Kavousi A, Seres IA. Private Delegation of (Non-) Membership Proof Updates in Cryptographic Accumulators. Cryptology ePrint Archive. 2026.

[13] Jiang W, Li J, Guo Y, Zhang H. An ordered universal accumulator based on a hash chain. Applied Sciences. 2025 Feb 27;15(5):2565.