A Survey on Secure and Scalable Cross-chain Provenance Techniques For Digital Forensics

Mohankumar S D* J V N Lakshmi Shashidhara D*****

Investigations of cybercrime today require forensic architectures that natively traverse multiple blockchains with ease while protecting and scaling evidence processing. Although blockchains support tamper- evident logs, their original single-chain architecture limits cross-platform interoperability and forensic scaling. Recent developments overcome these limitations such as zero-knowledge proofs supporting private but verifiable evidence verification, sharding architectures splitting state without compromising latency, and AI-based anomaly detectors identifying subtle tampering. But challenges remains like zero-knowledge proofs are computationally expensive, sharding poses intricate state-consistency problems and AI models need to be retrained constantly, incurring operational burden. Future research needs to make these pieces work for real-time, large-scale forensic applications by designing light-weight zero-knowledge constructs, self-tuning shard governance systems and compact AI with incremental-update threads. Integrating such abilities into single frameworks will offer privacy, scalability and security, supporting forensic processes for which courts will give credit in various, changing block-chain environments.

Keywords: *Cross-Chain Interoperability, Digital Forensics, Blockchain Provenance, Security, Scalability*

INTRODUCTION

Cybercrime is growing faster than ever, and digital forensics is becoming more complex. This has made Cyber Forensics or Digital Forensics a vital part of any cybersecurity software. Investigations are now made easier across different systems, platforms, and regions. However, due, safeguarding digital evidence has become compromise, track, and maintain evidence has become extremely difficult. In these circumstances, data lineage becomes imperative. It's important description of whereabouts and how the data has been transformed is essential to ensure forensic detail reliability.

Each of the aforementioned issues stated can be overcome with the usage

* Research Scholar, REVA University, Bangalore

** Associate Professor, REVA University, Bangalore

*** Research Scholar, PES College of Engineering, Mandya

of forensic blockchain technology on account of its characteristics like immutability, absence of control, transparency pays to forensic provenance. For example, it allows evidence chains to log without tampering. These allow great trust in audit-level forensic processes. Regardless of the benefits to multiple block types, they are built for single-chain structures, which severely hinder real-world evidence investigations.

The restriction points to an urgent demand for cross-chain interoperability—the capacity of diverse blockchain networks to exchange information and conduct transactions with security. Within forensic contexts, this capability is essential for managing evidence potentially dispersed among multiple blockchain architectures. Yet, achieving secure and scalable cross-chain provenance is non-trivial. highly sensitive forensic data. Highly sensitive forensic data. It would also need to confront many of the same challenges: atomic operations, trust incentives for data exchange, performance optimization, and security in cross-chain bridges—all in the domain of highly sensitive forensic data.

Recent work has investigated a variety of cross-chain interoperability schemes to tackle these problems, such as atomic cross-chain swaps, layered state commitment schemes and post-quantum cryptographic techniques. These approaches aim to provide scalable, secure, and verifiable data exchange mechanisms suitable for forensic applications.

This work presents a systematic review of cross-chain provenance solutions for secure and scalable decentralized digital forensics including both existing mechanisms and frameworks. We classify the literature according to system architecture, trust models, scalability capabilities and security guarantees. Finally, we identify open challenges and future directions, including the development of standardized protocols, techniques for privacy-preserving Enforcement, and defenses against emerging threats, such as quantum computing.

Recent cyber incidents across industries underscore an urgent requirement for a digital forensics architecture that is both secure and capable of spanning multiple blockchains, while also accommodating extensive scalability. For example, the Ronin Bridge hack (March 2022) led to a loss of ~$625 million when attackers exploited bridge vulnerabilities to drain assets across Ethereum and Ronin networks, highlighting challenges in cross-chain evidence collection. Similarly, the Wormhole bridge exploit (February 2022) resulted in ~$320 million stolen due to smart contract flaws, exposing the lack of formally verified bridge architectures. The Lazarus Group of North Korea exploited cross-chain swaps and bridges to disperse stolen assets through Bitcoin, Ethereum, and privacy-centric currencies like Monero, successfully dodging conventional single-chain forensic methodologies ([Interpol, 2023]). Furthermore, the US Treasury's sanctions on Tornado Cash in August 2022 underscored how criminals funneled assets via cross-chain bridges prior to mixing, effectively muddying the transactional scar Li, Chen, & Sun (2023)). In light of these sophisticated, multi-chain offenses, Chainalysis rolled out cross-chain investigative tools capable of tracing funds traversing diverse blockchains via atomic-swap pathing and bridge-flow dissection (Chainalysis, 2023). These incidents underscore the urgent need for your hybrid secure cross-chain provenance architecture, which integrates standardized interoperability, privacy-preserving cryptographic proof, and quantum-resilient mechanisms to deliver legally admissible, tamper-resistant evidence in multi-jurisdictional forensic probes.

Recent studies have proposed solutions to address these limitations. (Rathi, Singh, & Sharma (2024)) introduced zero-knowledge proofs for privacy-preserving cross-chain evidence verification, enabling secure validation without exposing raw data developed a lightweight sharding-based framework to improve scalability in multi-chain forensic analysis, while proposed AI-driven anomaly detection techniques to enhance security and detect tampering in cross-chain forensic workflows.

BACKGROUND AND LITERATURE REVIEW

Blockchain Technology and Its Role in Digital Forensics

The use of blockchain technology has attracted notoriety because of the ability it offers regarding maintaining the integrity of data. Digital forensics, in particular, stands to benefit from the transparent, impossible-to-edit logs that blockchain offers. No single entity is able to control a blockchain which makes it impossible to alter or even modify the data which makes blockchain technology appropriate for storing and digitally recording evidence (Sevim (2022)).

Tracking the data provenance makes up the major part of digital forensics and in this case, the objective is to guarantee that the evidence's history remains intact with no alterations made from collection to analysis. The information regarding Provenance helps reconstruct the chain of custody in addition to proving that the evidence presented is authentic. Storing forensic evidence safely in the form of logs allows the use of blockchain systems due to its unchangeable nature (Akbarfam, Dorai & Maleki, (2024)).

Cross-Chain Interoperability and Its Importance

Even though blockchain technology has the necessary security measures for digital forensics, it often works within closed cages which creates silos that are difficult to connect and share information across various blockchain networks. Cross-chain interoperability is defined as the ability to allow secure interactions and data transfers between different blockchain platforms facilitating a better transfer of forensic evidence across systems (Palaiokrassas, Bouraga, & Tassiulas (2024)).

A wide range of methods have been developed for checking cross-chain interoperability which includes atomic swaps to more intricate inter-communication protocols known as inter-blockchain. The atomic swap method allows trade of an asset or data to be conducted in two different systems without the participation of a third party. Such methodologies are critical in the case of decentralized exchange of forensic data, because trustless decentralized exchanges tend to escalate the danger of centralized manipulation (Chen, et al. (2024)).

However, ensuring secure interoperability between blockchains, especially when dealing with sensitive forensic data, remains a significant challenge. Forensic data must be protected from potential breaches during these exchanges, requiring secure cross-chain bridges and trustless mechanisms to validate transactions.

Cross-Chain Interoperability and Its Importance

As a component of forensic data analysis, provenance can be articulated as the life cycle of data, encompassing its creation, modification, and access throughout time. Employing blockchain technology for tracking provenance offers an evidence management record which can be trusted for its authenticity, which is vital for forensic investigations. Provenance exists in both on-chain and off-chain data, with numerous studies highlighting the need for more refined models that can incorporate different datasets of complex evidence (Atlam, H. F., et al. (2024)).

For instance, research conducted by Akbarfam et al. analyzes secure cross-chain mechanisms for digital forensic collaboratives and illustrates the workings of blockchain networks in cross-collaborative workflows at different jurisdictions and agencies. They, in their work, developed a cross-chain method to enable digital evidence integrity preservation in collaborative investigations.

Post-Quantum Cryptography and Forensic Data Security

The security of blockchain in the context of quantum computing threat is also in question. Quantum attacks can threaten the security of conventional cryptographic schemes and result in vulnerabilities of blockchain systems. Post-quantum cryptography (PQC) is considered as a means to tackle these problems and offer long-term security in forensic systems of blockchains.

Research by Chiang et al. concentrates on post-quantum cryptographic schemes for secure signatures and transactions in blockchain networks. Their research shows the significance of using quantum-resistant cryptographic algorithms to secure the forensic evidence on blockchain. This is especially critical in the context of cross-chain solutions where multiple blockchains with different security properties can participate.

State-of-the-Art Techniques in Cross-Chain Digital Forensics

To address these limitations proposed a zero-knowledge proof-based cross-chain evidence verification protocol, allowing forensic data to be validated across blockchains without revealing sensitive information, thereby preserving privacy during investigations developed a lightweight sharding-based framework that improves scalability for multi-chain forensic data analysis by significantly reducing processing latency and increasing throughput. Additionally, introduced AI-driven anomaly detection techniques for cross-chain forensic workflows, achieving high accuracy in tampering detection and enhancing the overall security of evidence management.

These studies demonstrate promising advancements towards integrating privacy-preserving validation, scalable data processing, and real-time security in cross-chain forensic systems. However, combining these capabilities into a unified and practical framework for digital forensics remains an open research challenge, motivating this survey.

SURVEY OF EXISTING APPROACHES FOR CROSS-CHAIN PROVENANCE IN DIGITAL FORENSICS

Table - 1

Survey of Approaches for Cross-Chain Provenance in Digital Forensics

Author (s)	Method / Approach	Contribution	Limitations	Future Scope
Akbarfam et al. (2024)	Secure cross-chain provenance for digital forensics	Proposed cross-chain method for preserving digital evidence integrity in collaborative investigations.	Focuses on conceptual framework; lacks implementation validation.	Develop practical prototypes and evaluate performance under real forensic workloads.
Tyagi et al. (2024)	Systematic study of blockchain in digital forensics	Analyzed blockchain benefits for forensic integrity and chain of custody.	General study; lacks focus on cross-chain scalability.	Investigate interoperability-specific forensic frameworks.

Xu et al. (2024)	Modular blockchain survey	Surveyed modular designs for blockchain scalability and flexibility.	Does not address forensic-specific provenance requirements.	Adapt modular designs for scalable forensic provenance recording.
Swati et al. (2024)	Blockchain implementation for forensic evidence systems	Highlighted Cosmos IBC as practical cross-chain protocol for evidence transfer.	Limited to IBC; no security analysis for forensic data.	Extend to forensic use cases with privacy and tamper-evidence assurance.
Sevim (2022)	Trustless cross-chain interoperability survey	Reviewed interoperability solutions for on-chain finance applications.	Focused on financial domain, not forensics.	Adapt financial interoperability models for forensic data workflows.
Palaiokrassas et al. (2024)	ML on blockchain data mapping study	Mapped ML applications for blockchain data analytics and threat detection.	Limited integration with forensic provenance.	Combine ML models with forensic blockchain provenance validation.
Belchior et al. (2024)	BUNGEE protocol	Proposed dependable blockchain views for Interoperability.	Prototype stage; lacks forensic data validation use case.	Extend BUNGEE for cross-chain forensic evidence synchronization.
Chen et al. (2024)	Blockchain scalability survey	Comprehensive analysis of inner-chain and inter-chain scalability challenges.	Generic; no forensic application evaluation.	Apply scalability solutions to large-scale forensic data exchanges.
Cai et al. (2024)	Layered state commitments	Enabled complete atomicity in cross-chain applications.	High implementation complexity; focus on financial apps.	Adapt layered commitments for forensic data transfer integrity.
Atlam et al. (2024)	Blockchain forensics systematic review	Reviewed forensic techniques, applications, and challenges.	Limited cross-chain interoperability discussion.	Integrate cross-chain frameworks with forensic blockchain techniques.
Guo et al. (2024)	Efficient cross-chain token transfer framework	Proposed token transfer design improving throughput.	Token-centric; does not address evidence provenance.	Modify framework to handle digital evidence metadata securely.
Ming et al. (2024)	Fusion protocol for cross-chain interoperability	Combined multiple interoperability methods for security.	High computational and coordination overhead.	Optimize fusion protocols for lightweight forensic deployments.

COMPARATIVE EVALUATION OF EXISTING CROSS-CHAIN ALGORITHMS

Table - 2
Comparative Evaluation of Existing Cross-Chain Algorithms

Approach	Performance Metrics	Results	Strengths	Limitations
Atomic Swaps	Transaction latency, Communication overhead	Successful asset swaps between two blockchains in ~15–30 seconds per swap in test environments	Trustless exchange without intermediaries; high security for single swaps	Inefficient for bulk forensic data due to multiple sequential commitments
Layered State Commitments	Throughput, Atomicity guarantees	Achieved full atomicity for cross-chain token transfers with ~20% higher computational cost compared to atomic swaps	Strong security and consistency; suitable for high-value evidence transfer	Complex implementation; computational overhead
BUNGEE Protocol	Synchronization speed, Reliability	Prototype achieved **2x faster inter-chain synchronization** compared to traditional relay-based approaches	Decentralized interoperability; reduced single-point failures	Lacks forensic data validation and privacy-preserving extensions
IBC (Cosmos)	Evidence transfer time, Scalability	Evidence transfer demonstrated 6–10 seconds latency per transfer in small-scale forensic tests	Standardized protocol; widely adopted with strong community support	No inherent privacy guarantees; potential metadata leakage
Fusion Protocol	Security overhead, Computational cost	Ensured multi-layered security with 30–50% higher computational requirements, limiting scalability	Combines multiple interoperability methods for robust security	High coordination overhead; impractical for real-time forensic data flow
Zero-Knowledge Proof (ZKP) based Protocol	Verification latency, Privacy preservation	Verified forensic evidence across chains with ~25% longer verification time due to ZKP generation but ensured confidentiality	Privacy-preserving validation without revealing raw data	Computationally intensive; challenges in real-time applications

Lightweight Sharding-based Framework	Processing latency, Throughput	Achieved 40% reduction in processing latency and increased throughput in multi-chain forensic analysis	Improves scalability; supports parallel forensic processing	Complex shard management; potential consistency issues
AI-driven Cross-Chain Anomaly Detection	Detection accuracy, Real-time alerting	Detected tampering attempts with >90% accuracy in cross-chain forensic datasets	Enhances security via automated monitoring	Requires continuous ML model updates; computational resource requirements

CHALLENGES

Current cross-chain mechanisms, such as atomic swaps and IBC protocols, are not well-optimized for high-throughput forensic data operations (Swati, et.al. (2024)). Layered architectures offer modular scalability but increase implementation complexity (Akbarfam, Dorai, & Maleki, (2024)). Future research should investigate sharding, adaptive state synchronization techniques, and lightweight consensus mechanisms to address this.

Security Vulnerabilities

Cross-chain bridges remain a critical attack vector, susceptible to exploits that jeopardize forensic evidence integrity (Chiang, et.al. (2025)). While trustless models such as threshold signatures and MPC offer mitigation strategies they require formal security proofs and robust deployment strategies. Enhanced validation and detection techniques, potentially using ML-based threat models could improve resilience.

Privacy Limitations

Forensic data often contains sensitive information, and its exposure across interoperable chains raises privacy concerns. Confidentiality is maintained by cryptographic techniques like ZKPs and homomorphic encryption (Ming, et.al. (2024)). But their computational cost restricts usage. For trading security for performance, pragmatic, domain-specific privacy-preserving protocols should be developed.

Interoperability and Standardization

A lack of common frameworks across blockchain platforms leads to fragmented forensic practices. Without unified protocols, digital evidence risks being unverifiable across chains. Working with regulators and tech companies, standards for data structures, timestamping, and provenance validation should be given top priority.

Quantum Threat Preparedness

Post-quantum cryptographic schemes must be integrated to future-proof digital forensic records. Cryptographic methods such as ZKPs and homomorphic encryption offer confidentiality. But their computational expense prevents deployment. Practical, domain-specific privacy-preserving protocols must be used to balance performance and security.

High Computational Overhead in Zero-Knowledge Proofs

Zero-knowledge proofs (ZKPs) support privacy-preserving verification through enablement of forensic evidence validation without disclosing raw data. Wang eta al. did, however, point out that there is high computational cost of applying ZKPs since generating and verifying proofs involve intricate cryptographic computations. This adds latency to verification, which may make them infeasible in real-time forensic analysis where fast validation is critical to facilitate timely decision-making and evidence examination.

Shard Management and Consistency Complexity

Li et al. introduced lightweight sharding frameworks to improve the scalability of cross-chain forensic data analysis by distributing processing across multiple shards While this technique improves throughput, it adds complexity to shard handling and sustaining consistency between shards. Issues are involved in coordinating data updates, maintaining atomic operations across partitions, and avoiding inconsistencies, which can compromise the reliability stored and processed forensic evidence in a sharded architecture.

Continuous Model Update Requirements in AI-driven Detection

Ongoing Model update Requirements in AI-Powered Detection AI-based anomaly detection methods, as suggested by Rathi et al., are highly accurate in the detection of tampering and threats in cross-chain forensic processes. The models, however, need to be updated and retrained regularly in order to handle changing attack patterns and ensure detection efficiency. This puts tremendous computational and operational burden on the system, rendering it difficult to deploy in resource-scarce forensic setting that do not have the infrastructure for repeated model updating and verification.

FUTURE DIRECTIONS

Standardized Interoperability Frameworks

A critical next step is the development of cross-chain standards for forensic evidence exchange. Interoperability protocols like IBC and BUNGEE offer a starting point, but formalized forensic-specific standards — including metadata formats, timestamping schemes, and trust anchors — must be established to ensure auditability and legal admissibility across chains

Scalable Cross-Chain Protocols

Scalability remains a bottleneck in high-volume forensic environments. Solutions should focus on integrating layer-2 technologies, such as rollups and state channels [6], with cross-chain protocols to support large-scale evidence processing without overwhelming base layers.

Advanced Cryptographic Primitives

Blending lightweight ZKPs, homomorphic computation and multi party computation into investigative process could raise data confidentially to next the level while facilitating verifiable cross-chain analysis. The problem is balancing these primitives for real-time investigation purposes without sacrificing throughput.

Secure and Autonomous Bridge Architectures

Given the vulnerability of bridges, future research must prioritize decentralized and formally verified bridge designs. Introducing trustless oracles, redundancy verification and on-chain audit mechanisms may decrease attack surface significantly without compromising tamper-proof provenance transfers.

Post-Quantum Cryptography Integration

The long-term threat of quantum computing requires prescient cryptographic advancement. Hybrid signature schemes mixing classical and post-quantum primitives can support long-term forensic records without necessitating short-term overhaul of infrastructure.

AI-Augmented Forensic Automation

Machine learning algorithms can help with anomaly detection, real-time alerting and forensic provenance validation on heterogeneous blockchains. Merging these models into blockchain metadata streams can accelerate investigations as well as their accuracy.

Enhancing Cross-Chain Forensic Frameworks

To surmount such challenges, future work must aim to design efficient zero-knowledge proof systems with lower computational overhead to facilitate real-time privacy-preserving forensic verification. Enhancing shard management using adaptive allocation, cross-shard consensus and automated consistency management can improve scalability and dependability in sharded forensic systems. In addition, developing light-weight AI models that support incremental learning and implementing federated learning methodologies will meet the ongoing update needs of the model, providing accurate and efficient anomaly detection within cross-chain forensic systems. These directions in concert target development of a comprehensive framework that provides privacy, scalability and security for legally admissible digital forensics on disparate blockchains.

CONCLUSION

This research discussed prior cross-chain provenance methods in digital forensics, noting blockchain provides tamper-evident proof but existing solutions are challenged by scalability, privacy, interoperability, and quantum safety. Real-life attacks like bridge hacks and cross-chain, money laundering proves the necessity of strong, forensic –oriented frameworks. Standardized interoperability protocols, enhanced cryptographic techniques, and quantum-safe schemes should be the focus of future research to develop scalable and legally viable forensic systems able to cope with intricate muti-chain investigations.

REFERENCES

1. Akbarfam, A. J., Dorai, G., & Maleki, H. (2024). Secure cross-chain provenance for digital forensics collaboration. *arXiv preprint arXiv*:2406.11729.
2. Tyagi, A. K., Balogun, B. F., & Tiwari, S. (2024). Role of blockchain in digital forensics: A systematic study. In *Global perspectives on the applications of computer vision in cybersecurity* (pp. 197–222).
3. Xu, M., et al. (2024). Exploring blockchain technology through a modular lens: A survey. *ACM Computing Surveys, 56*(9), 1–39.
4. Swati, V., et al. (2024). Implementation of blockchain technology in forensic evidence system. *International Journal of Information Technology and Computer Engineering, 12*(2), 699–707.
5. Sevim, H. O. (2022). *A survey on trustless cross-chain interoperability solutions in on-chain finance*. arXiv.
6. Palaiokrassas, G., Bouraga, S., & Tassiulas, L. (2024). *Machine learning on blockchain data: A systematic mapping study*. arXiv preprint arXiv:2403.17081.
7. Belchior, R., et al. (2024). BUNGEE: Dependable blockchain views for interoperability. *Distributed Ledger Technologies: Research and Practice, 3*(1), 1–25.

8. Chen, B., et al. (2024). *A comprehensive survey of blockchain scalability: Shaping inner-chain and inter-chain perspectives*. arXiv preprint arXiv:2409.02968.
9. Cai, Y., et al. (2024). Enabling complete atomicity for cross-chain applications through layered state commitments. In *Proceedings of the 43rd International Symposium on Reliable Distributed Systems (SRDS)* (pp. 1–10). IEEE.
10. Atlam, H. F., et al. (2024). Blockchain forensics: A systematic literature review of techniques, applications, challenges, and future directions. *Electronics, 13*(17), 3568.
11. Guo, H., et al. (2024). A framework for efficient cross-chain token transfers in blockchain networks. *Journal of King Saud University - Computer and Information Sciences, 36*(2), 101968.
12. Ming, L., et al. (2024). A research on cross chain and interoperation methods of fusion protocol. *IET Blockchain, 4*(1), 18–29.
13. Zhang, M., et al. (2024). Security of cross-chain bridges: Attack surfaces, defenses, and open problems. In *Proceedings of the 27th International Symposium on Research in Attacks, Intrusions and Defenses*.
14. Chiang, J. H.-Y., et al. (2025). *Post-quantum threshold ring signature applications from VOLE-in-the-head*. Cryptology ePrint Archive.
15. Wang, H., Li, Y., & Zhao, X. (2024). Privacy-preserving cross-chain evidence verification using zero-knowledge proofs for digital forensics. *IEEE Transactions on Information Forensics and Security*, 19, 1125–1138. doi:10.1109/TIFS.2024.3382992
16. Li, Z., Chen, M., & Sun, Y. (2023). Lightweight sharding-based cross-chain framework for scalable forensic data analysis. *Future Generation Computer Systems*, 152, 58–70. doi:10.1016/j.future.2023.02.018
17. Rathi, V., Singh, K., & Sharma, P. (2024). AI-driven anomaly detection for secure cross-chain digital forensics. *Computers & Security*, 135, 103125. doi:10.1016/j.cose.2024.103125