Enhancing Blockchain Transaction Tracking: A Systematic Review of DLT-Based Financial Systems

Mario Trerotola
Dept. of Control and Computer Engineering
Politecnico di Torino
Turin, Italy
mario.trerotola@polito.it

Davide Calvaresi
Institute Informatique
HES-SO Valais-Wallis
Sion, Switzerland
davide.calvaresi@hevs.ch

***Abstract*—Distributed Ledger Technologies (DLTs) fuse cryptographic immutability with decentralized consensus, transforming global finance, simultaneously hindering the forensic reconstruction of illicit value flows. This paper presents a systematic mapping of financial transaction tracing on DLTs through a rigorously designed Systematic Literature Review (SLR). Six research questions - covering enabling technologies, privacy primitives, tracking methods, structural limits, proposed mitigations, and future directions - guided the search. Three reviewers screened 120 publications from 2017-2025, resolving disagreements by adjudication and distilling 21 primary studies (17.5 % acceptance). The corpus converges on four technical pillars: heuristic/graph-based address clustering, machine-learning anomaly detection, cross-ledger correlation frameworks, and privacy-enhancing constructs such as ring signatures and zk-SNARKs. Our synthesis exposes a persistent tri-lemma among scalability, attribution accuracy, and privacy compliance, exacerbated by heterogeneous protocol designs and data-retention costs. To reconcile these issues, we articulate a four-layer tracing architecture that integrates high-throughput multi-chain ingestion, cache-efficient temporal graph indexing, explainable risk scoring, and privacy-preserving off-chain fusion with KYC anchors. This blueprint offers regulators, investigators, and researchers a scalable, GDPR-aligned pathway for illuminating opaque financial networks, while establishing a consolidated knowledge base and a forward research agenda for next-generation DLT traceability.**

***Index Terms*—Blockchain, DLT, Transaction tracing, Privacy-preservation, AML**

I. Introduction

The rapid adoption of Distributed Ledger Technologies (DLTs) in sectors such as finance, supply chain, and healthcare has underscored the dual promise of transparency and decentralization, alongside the challenge of cryptographic pseudonymity [1], [2]. Immutable transaction records enhance auditability but can also facilitate illicit asset flows—ransomware payments, darknet transactions, and money laundering—by obscuring participant identities [3], [4]. Consequently, there is a pressing need for scalable and robust tracing methodologies capable of linking on-chain pseudonymous addresses to real-world entities, particularly at centralized exchange gateways where Know Your Customer (KYC) protocols provide identity anchors [5].

Early blockchain analysis methods leveraged heuristics and clustering to group addresses under common control [6], while recent advances apply graph-based search and machine learning techniques to detect anomalous flows in real time [7], [8], [9], [10]. Cross-ledger frameworks further extend these capabilities across multiple blockchains [11], [3]. However, sophisticated privacy mechanisms—mixing services, ring signatures, and zero-knowledge proofs (e.g., zk-SNARKs) [12] —pose significant obstacles, demanding innovative solutions that balance confidentiality with regulatory requirements.

This paper presents a systematic literature review (SLR) structured leveraging six research questions to assess the state of the art in financial transaction tracing on DLTs. The review examines foundational technologies, privacy-preserving techniques, tracing methodologies, limitations, proposed solutions, and future research directions.

II. Background and Definitions

Distributed Ledger Technologies (DLTs) provide a decentralized, tamper-resistant framework for recording transactions across peer-to-peer networks [1], [13], [2]. Blockchain, the most prevalent form of DLT, relies on cryptographic consensus mechanisms—Proof of Work (PoW) or Proof of Stake (PoS)—to ensure data integrity and network agreement [2]. Two primary ledger models exist: the Unspent Transaction Output (UTXO) model (Bitcoin) and the account-based model (Ethereum) [13], [11].

Despite public ledgers, users transact via pseudonymous addresses, hindering direct identity attribution. Privacy-enhancing techniques—coin mixers, CoinJoin, ring signatures (Monero), and zk-SNARKs (Zcash) [3]—further obfuscate transaction trails. Centralized exchanges (CEXs) bridge blockchain and fiat systems through KYC [5], while decentralized exchanges (DEXs) enable peer-to-peer swaps without identity verification [3]. Understanding these concepts is vital for evaluating tracing techniques in DLT ecosystems.

III. Systematic Literature Review Methodology

This paper adopts a rigorous and reproducible systematic literature review methodology, following the framework outlined by Kitchenham [14]. This approach has been validated and utilized in similar contexts, including the works of Palmarini et al. [15], Anjomshoae et al. [16], Mualla et al. [17], and Calvaresi et al. [18], [19]. Additionally, the review incorporates insights from recent studies, such as Pinto et al. [20], which

highlight the importance of methodological rigor in addressing complex topics.

Figure 1 illustrates the methodology adopted for this review, which is structured into three main stages. The first stage, **Planning the Review (P1)**, focuses on defining the primary research question(s) and formulating the Structured Research Questions (SRQs). This stage emphasizes the establishment of a comprehensive search protocol to ensure methodological rigor and reproducibility, which is subsequently validated to ensure alignment with the research objectives. The second stage, **Performing the Review (P2)**, involves the execution of the planned activities. This encompasses the collection and selection of relevant literature, data extraction and analysis, and the resolution of any disagreements among reviewers to maintain consistency throughout the process. The final phase, **Results Analysis (P3)**, is dedicated to the analysis of the findings, the documentation of insights, and the presentation of outcomes. This phase summarizes key lessons learned and provides actionable recommendations based on the evidence gathered.

IV. Review Planning

This section outlines the process for defining Structured Research Questions (SRQs) and establishing the review protocol. The protocol encompasses several key elements: the **Search Strategy**, which details the methods for identifying relevant literature, including databases, keywords, and search operators; the **Inclusion and Exclusion Criteria**, which set clear guidelines for determining the relevance of studies; **Bias and Disagreement Resolution**, which describes mechanisms to mitigate biases and resolve conflicts during the review process; and the **Quality Assessment Criteria**, which defines metrics for evaluating the quality and relevance of the selected studies. This structured approach ensures the review is comprehensive, systematic, and aligned with the research objectives.

A. Research Questions

The overarching objective of this study is to assess the feasibility of connecting wallets to individuals within the context of existing DLT-based systems for economic transactions. To this end, we define the following research framework.

1) General Research Question (GRQ): The **General Research Question (GRQ)** guiding this investigation is as follows:

With respect to current off-the-shelf DLTs for economic transactions, is connecting a wallet to an individual possible, and how can it be done?

This question encapsulates the dual challenge of assessing the technological capabilities of current systems and identifying methodologies to bridge the gap between pseudonymity and identifiable ownership.

2) Structured Research Questions (SRQs): To decompose the General Research Question (GRQ) into more manageable components, we adopt a series of **Structured Research Questions (SRQs)** that focus on specific aspects of the problem. These SRQs are outlined as follows:

SRQ1: Technology *What technologies are utilized to implement Distributed Ledger Technologies (DLTs) for economic transactions, and how are these technologies characterized?* This question aims to identify the core technologies underlying DLT systems, including their architectural frameworks, consensus mechanisms, and scalability features.

SRQ2: Privacy-Preserving Techniques *What privacy-preserving techniques are employed to enhance the confidentiality of transactions and asset tracing on DLTs? What are their strengths and limitations in terms of security and transparency?* This question examines techniques such as zero-knowledge proofs, ring signatures, and mixing protocols, assessing their effectiveness in balancing privacy concerns with traceability requirements.

SRQ3: Transaction Tracing *Is transaction tracing conducted on DLTs? How is this tracing performed?* This question investigates the existing methodologies and tools used to trace transactions across blockchain networks, including heuristic-based approaches and clustering algorithms.

SRQ4: Limitations *What are the primary limitations in transaction tracing on DLTs (e.g., issues with anonymity, scalability challenges, and cross-chain tracing complexity)?* This question aims to identify the key obstacles that hinder effective transaction tracing, such as the use of privacy-enhancing coins, limited data interoperability, and computational bottlenecks.

SRQ5: Proposed Solutions *What solutions have been proposed to overcome the existing limitations of transaction tracing on DLTs?* This question highlights innovative approaches and frameworks developed to address the challenges identified in SRQ4, including advancements in machine learning and cross-chain analysis.

SRQ6: Future Directions *What are the primary research directions proposed by leading studies to advance asset and transaction tracing on DLTs?* This question explores emerging trends and opportunities in research, such as decentralized identity frameworks, enhanced cryptographic techniques, and the integration of regulatory compliance measures.

Search Strategy

The search strategy focused on selecting pertinent information sources to ensure the collection of comprehensive and high-quality literature. The databases utilized included: IEEE Xplore (http://ieeexplore.ieee.org), ScienceDirect (http://www.sciencedirect.com), ACM Digital Library (http://dl.acm.org), Citeseerx (http://citeseerx.ist.psu.edu/index), and Google Scholar (https://scholar.google.com).

The selection of keywords was guided by the reviewers' domain expertise and included terms relevant to Distributed Ledger Technologies (DLTs), transaction tracing, and privacy preservation. Keywords were aggregated to refine results, forming the following query combinations:

- DLT,
- DLT + transaction,
- DLT + transaction + tracing,
- Blockchain + transaction,
- Blockchain + transaction + tracing,

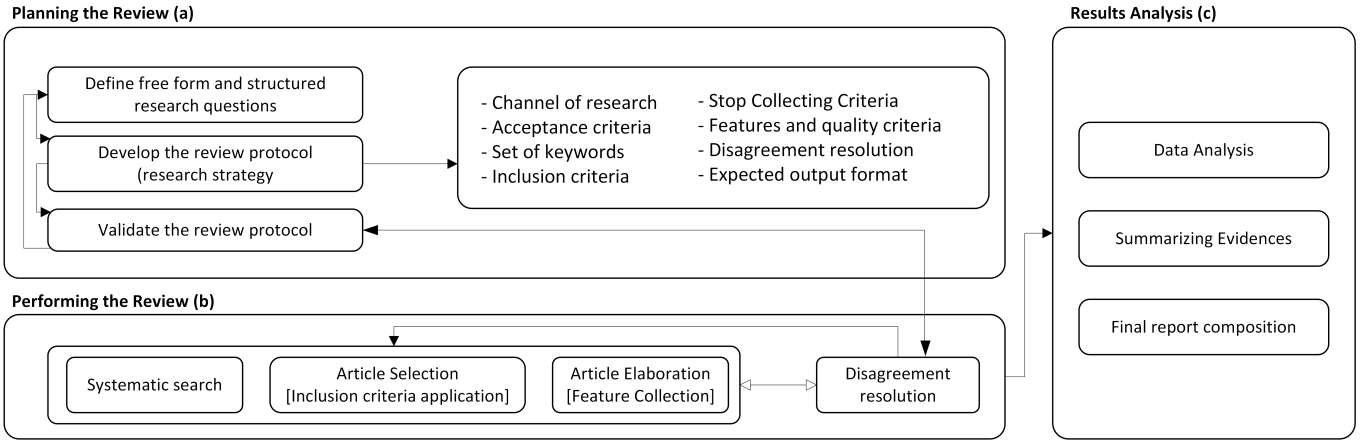

Fig. 1. Schematic representation of the systematic literature review methodology.

- Wallet identification + pseudonymity,

Each search query produced a set of articles, which were subsequently screened based on title and abstract for coherence with the research objectives.

Inclusion and Exclusion Criteria

The initial search yielded 120 papers, which were then filtered using the following criteria:

- **Temporal**: Studies published between 2017 and 2025 to capture recent advancements in DLT technologies.
- **Originality**: Exclusion of papers that presented minor variations or duplicates of existing work.
- **Purpose**: Focus on studies addressing economic transactions or asset tracing using DLTs.
- **Relevance**: Inclusion of studies with a clear contribution to privacy-preserving techniques or wallet identification.
- **Theoretical foundation**: Inclusion of studies proposing innovative formulations, definitions, or system designs.
- **Practical contribution**: Inclusion of studies providing implementations, tests, evaluations, or critical analyses.

After applying these criteria, the set of primary studies was narrowed down to 16 contributions.

Bias Resolution and Conflict Management

To mitigate biases and resolve disagreements, three reviewers independently evaluated the studies. Conflicts were addressed through periodic meetings, and a study was included if at least two reviewers agreed on its relevance. Table I summarizes the outcomes of the conflict resolution process.

Features and Quality Criteria

The quality of the extracted information was evaluated based on several criteria, including: publication year and geographical location, main purpose and application context, architectural and technological evidence (classified as Conceptual, Prototype, or Tested Frameworks), and technical limitations and future challenges.

These features were categorized using the DARE [14], ensuring a structured evaluation of the selected studies.

V. Review Execution

The semi-automatic search (Sect. III) retrieved 120 unique records, which were divided equally among three reviewer pairs. Each pair performed an initial title–abstract screening, applying the inclusion/exclusion rules from Sect. III , yielding 40 candidates. Those underwent full-text review in double-blind fashion; any disagreement (27 cases) was resolved by the third reviewer according to the protocol summarized in Table I.

After conflict resolution, 21 articles were accepted (17.5 % overall acceptance rate) and advanced to data extraction. Reviewers collaboratively populated a structured data sheet—capturing publication metadata, methodological features, and identified limitations—while clearly separating objective results from expert interpretation. This streamlined process ensured consistency, minimized bias, and produced a high-quality corpus for subsequent analysis.

VI. Review results and analysis

In the following, we structure the results of the SLR according to the research questions defined in Sect. IV

SRQ1: Technologies Used to Implement DLTs for Economic Transactions

DLTs secure transactions via consensus protocols that balance security and efficiency: early PoW systems like Bitcoin provide strong tamper-resistance at high energy cost [21], [1], PoS networks lower energy consumption but introduce stake-based risks [2], and permissioned ledgers adopt BFT variants (e.g., PBFT, Tendermint) for low-latency finality [22]. State representation follows either the UTXO model (Bitcoin, Zcash), treating outputs as discrete coins for parallel validation [13], or the account-based model (Ethereum), maintaining a global state object for contract logic [1]; enterprise frameworks like Hyperledger Fabric further decouple execution, ordering, and validation to enhance modularity and privacy

TABLE I
SUMMARY OF THE INCLUSION/EXCLUSION PHASE OF THE COLLECTED PAPERS

Rev	Conflict Solver	Y–Y	N–N	Conflicts	Accepted out of Conflicts	Total	Accepted	Acceptance %
$A \Leftrightarrow B$	C	7	23	10	2	40	9	22.5%
$A \Leftrightarrow C$	B	5	29	6	3	40	8	20.0%
$B \Leftrightarrow C$	A	3	26	11	1	40	4	10.0%
Sum		**15**	**78**	**27**	**6**	**120**	**21**	**17.5%**

[23]. To tackle on-chain limits, Layer-2 solutions (state channels, sidechains) [24], rollup schemes—Optimistic and zk-Rollups—aggregate transactions into succinct proofs [24], and cross-chain bridges with atomic swaps enable asset transfers across heterogeneous ledgers [25], [26], though fragmentation persists without unified standards [5], even as multi-agent integration offers decentralized coordination potential [18].

SRQ2: Privacy-Preserving Techniques in DLTs

Blockchain systems leverage advanced cryptographic primitives to protect transaction confidentiality while preserving verifiability. Early theoretical foundations of non-interactive zero-knowledge proofs enable succinct shielded transactions, as later instantiated in zk-SNARK-based protocols like Zcash [27] [13]. Ring signatures and stealth addresses in Monero provide sender and recipient anonymity by blending outputs within a decoy set, though they incur significant verification overhead [1] [3].

More recent Layer-2 constructions—such as zk-Rollups—aggregate batches of transactions off-chain and publish compact proofs on-chain, reducing both gas costs and data leakage while retaining full auditability [24]. Mixing services and CoinJoin further obfuscate on-chain links, but their non-deterministic behavior complicates automated tracing and invites regulatory scrutiny [4]. Overall, these techniques reflect a continual trade-off between privacy guarantees, computational efficiency, and forensic transparency.

SRQ3: Transaction Tracing on DLTs

Transaction tracing on DLTs employs a range of methods—including heuristic clustering, graph analytics, cross-ledger correlation, and machine learning—to uncover illicit asset flows. UTXO-based clustering groups addresses that share inputs or outputs to infer common control [6], while heuristic detection of mixing services and CoinJoin transactions reveals obfuscation tactics [3]. Graph-based frameworks build an account–transaction network and apply targeted traversal: TRacer uses local subgraph expansion and ranking for near–real-time tracing on Ethereum [7], TPGraph temporally partitions the ledger to bound memory and computation [9], and MFGSCOPE optimizes in-memory layouts and parallel traversal for lightweight forensic analysis [10]. Cross-ledger approaches such as CLTracer correlate deposit and withdrawal events across heterogeneous chains to follow funds through bridges and DEXs [8]. Network-analysis studies link on-chain patterns to replicated phishing infrastructures via domain and content similarity metrics [28]. Machine-learning models—including graph neural networks and link-prediction algorithms—flag suspicious edges with high precision in Ethereum's account graph [4], [11]. Finally, unsupervised anomaly-detection techniques adapted from cybersecurity demonstrate potential for uncovering novel illicit transaction motifs without labeled training data [20].

SRQ4: Limitations in Transaction Tracing on DLTs

Despite significant progress, transaction tracing on DLTs remains constrained by several fundamental limitations. First, the pseudonymous nature of blockchain addresses makes it inherently difficult to link on-chain identifiers to real-world entities without auxiliary data sources or heuristic inference, leading to reliability concerns in deanonymization efforts [6], [8]. Second, the computational and storage overhead required to build and traverse large transaction graphs in real time imposes severe scalability bottlenecks, as demonstrated by the performance bounds of current graph-based tools [7], [9]. Third, advanced privacy mechanisms—such as ring signatures and stealth addresses in Monero, zk-SNARKs in Zcash, and mixing protocols—while strengthening confidentiality, substantially increase forensic opacity and analysis complexity [4], [3].

Cross-chain tracing is additionally hindered by heterogeneous protocol designs and the lack of unified interoperability standards, resulting in fragmented tool support and coverage gaps across different ledgers [25], [26]. Clustering and heuristic methods are also prone to false positives and negatives—particularly in noisy contexts like replicated phishing infrastructures—undermining attribution accuracy [28], [11]. Finally, many regulatory agencies and smaller investigative teams face resource constraints in terms of computational power, storage capacity, and domain expertise, limiting their ability to deploy and maintain sophisticated tracing infrastructures [10], [5].

SRQ5: Proposed Solutions to Overcome Transaction Tracing Limitations on DLTs

The literature converges on integrated approaches that address pseudonymity, scalability, privacy, and interoperability in a unified framework. Scalable graph-based systems such as TRacer utilize local sub-graph expansions and ranking heuristics to limit search complexity on account-based ledgers [7], while TPGraph temporally partitions the transaction graph to reduce memory and computation demands [9], and MFGSCOPE applies optimized in-memory layouts and parallel traversal for lightweight analysis on resource-constrained nodes [10]. Machine learning—with graph neural

networks and link-prediction techniques—has demonstrated high precision in identifying illicit clusters and forecasting suspicious edges in Ethereum's network [4], [11], and unsupervised cybersecurity methods detect novel threat motifs without requiring labeled data [20]. Hybrid on-chain/off-chain fusion frameworks like CLTracer combine on-chain heuristics with KYC and sanction-list records to enhance attribution accuracy and minimize false positives [8], [5]. Refined heuristic clustering for phishing and advance-fee fraud domains leverages domain registration and content similarity metrics to accurately link replicated scam infrastructures [28]. The integration of explainable AI techniques ensures that tracing decisions remain interpretable and auditable by analysts [16], [18]. Concurrently, ongoing standardization of cross-chain bridge APIs, atomic swap protocols, and interoperable zk-proof schemas aims to eliminate fragmentation and enable seamless multi-ledger traceability [25], [26].

SRQ6: Future Directions

Dynamic and Streaming Graph Analytics. Building on TP-Graph's temporal sharding [9] and MFGSCOPE's cache-aware in-memory layouts [10], future research should enable continuous ingestion of high-velocity transaction streams. This entails developing adaptive subgraph indexing strategies and incremental graph-update algorithms (e.g., memory-efficient edge eviction policies) to sustain low-latency analysis as ledger throughput and node populations increase.

Unsupervised and Self-Supervised ML/AI Models. To detect novel laundering patterns without relying on labeled examples, work must advance graph neural networks and link-prediction frameworks that employ contrastive learning and cybersecurity-inspired motif discovery. Such self-supervised techniques have shown promise in uncovering "zero-day" transaction anomalies in Ethereum's account graph [4], [11] and smart-grid contexts [20].

Explainability and Interpretability. Automated alerts should be accompanied by human-readable rationales. Integrating attention mechanisms and Explainable AI toolkits (e.g., post-hoc feature attribution) will allow investigators to audit and justify each flagged transaction or cluster, thereby enhancing trust and regulatory compliance [16], [18].

Privacy-Preserving On-Chain/Off-Chain Fusion. Combining on-chain heuristics with off-chain datasets—including KYC records, IP logs, and public registries—must preserve user confidentiality. Protocols based on Secure Multi-Party Computation or Federated Learning can enrich attribution accuracy while ensuring GDPR compliance and minimizing data exposure [8], [5].

Cross-Chain Interoperability Standards. To eliminate current fragmentation, it is essential to define unified transaction metadata schemas, interoperable zero-knowledge proof wrappers, and standardized audit-log formats. Promoting common bridge and atomic-swap APIs will enable seamless multi-ledger traceability and foster a cohesive ecosystem of tracing tools [25], [26].

VII. Discussion: Toward a Unified Tracing Stack

Our systematic review of 21 primary studies highlights that no existing approach fully reconciles the competing demands of **scalability**, **attribution accuracy**, and **privacy compliance**. Current solutions tend to prioritize one or two aspects while neglecting the third.

This gap emphasizes the need to move beyond isolated tools toward an integrated framework. Therefore, we propose a modular architecture that synthesizes and extends the most effective, albeit incomplete, techniques identified in our review, aiming to address the tri-lemma through critical trade-offs.

Layer 1 – Multi-Chain Data Ingestion for Scalability: A key challenge is managing fragmented, high-volume data streams from multiple blockchains. To address this, we refine the temporal sharding strategy from TPGraph [9], which segments transaction data into rolling time windows. This approach enables continuous, memory-efficient stream processing, offering a stable foundation for algorithms that prioritize accuracy.

Layer 2 – Cache-Efficient Graph Indexing for Performance: As transaction graphs grow, real-time forensic analysis becomes computationally intensive. This layer combines MFGSCOPE's [10] compressed graph structures with TRacer's [7] local subgraph expansion technique. The result is a responsive indexing layer that enables efficient query execution, even on large datasets.

Layer 3 – Adaptive Risk Scoring for Explainable Accuracy: To improve attribution accuracy while avoiding rigid rule-based systems or opaque black-box models, this layer uses a self-supervised GraphSAGE encoder. It generates adaptive risk scores, with attention-based explanations, ensuring not only accuracy but also auditability and trust, which are critical for regulatory compliance [16].

Layer 4 – Privacy-Preserving Correlation for Compliant Attribution: The final challenge is to enhance accuracy while maintaining privacy. Building on CLTracer's cross-chain heuristics [8], this layer introduces secure multi-party computation to fuse on-chain and off-chain data. It enables the system to access identity information from KYC anchors when necessary, ensuring GDPR compliance and solving the privacy component of the tri-lemma.

These four layers together form a unified tracing stack, balancing performance, forensic capabilities, and regulatory alignment. The modular design allows for flexible deployment and progressive adoption, providing a concrete solution to the persistent challenges in the field.

VIII. Conclusions

This systematic literature review explores the feasibility and methodologies for linking pseudonymous Distributed Ledger Technology (DLT) wallet addresses to real-world identities. Our analysis of 21 primary studies reveals that while multiple transaction tracing techniques exist, no single solution is currently sufficient. The review demonstrates that while

connecting a wallet to an individual is possible under certain conditions, significant structural challenges still limit its widespread application.

The central finding is the identification of a persistent tri-lemma: the challenge of balancing *scalability*, *attribution accuracy*, and *privacy compliance* simultaneously. Current tracing solutions are hindered by computational bottlenecks from growing ledgers, the forensic opacity introduced by advanced privacy technologies, and the fragmentation caused by inconsistent interoperability standards.

To address these challenges, this paper proposes a modular, four-layer tracing architecture that systematically tackles the tri-lemma. The framework balances scalability, accuracy, and privacy by distributing tasks across distinct layers. Specifically, the **Ingestion and Indexing** layers address **scalability** with memory-efficient processing and compressed graph structures. The **ML Scoring** layer enhances **attribution accuracy** using adaptive, explainable machine learning models, while the **Cross-Ledger Correlation** layer ensures **privacy compliance** by securely correlating on-chain data with off-chain identity anchors through privacy-preserving computation.

By integrating these techniques into a unified architecture, our approach offers a scalable and actionable solution for regulatory and investigative bodies. Future research should focus on developing realistic benchmarks and creating interoperable data standards to advance this architecture toward deployable, trustworthy, and compliant forensic systems.

REFERENCES

[1] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *IEEE international congress on Big Data*. Ieee, 2017, pp. 557–564.

[2] B. Lashkari and P. Musilek, "A comprehensive review of blockchain consensus mechanisms," *IEEE access*, vol. 9, pp. 43 620–43 652, 2021.

[3] H. Yousaf, G. Kappos, and S. Meiklejohn, "Tracing transactions across cryptocurrency ledgers," in *28th USENIX Security Symposium (USENIX Security 19)*, 2019, pp. 837–850.

[4] J. Wu, J. Liu, Y. Zhao, and Z. Zheng, "Analysis of cryptocurrency transactions from a network perspective: An overview," *Journal of Network and Computer Applications*, vol. 190, p. 103139, 2021.

[5] A. Panwar and V. Bhatnagar, "Distributed ledger technology (dlt): The beginning of a technological revolution for blockchain," in *2nd International Conference on Data, Engineering and Applications (IDEA)*. IEEE, 2020, pp. 1–5.

[6] H. Kuzuno and C. Karam, "Blockchain explorer: An analytical process and investigation environment for bitcoin," in *2017 APWG symposium on electronic crime research (eCrime)*. IEEE, 2017, pp. 9–16.

[7] Z. Wu, J. Liu, J. Wu, Z. Zheng, and T. Chen, "Tracer: Scalable graph-based transaction tracing for account-based blockchain trading systems," *IEEE Transactions on Information Forensics and Security*, vol. 18, 2023.

[8] Z. Zhang, J. Yin, B. Hu, T. Gao, W. Li, Q. Wu, and J. Liu, "Cltracer: a cross-ledger tracing framework based on address relationships," *Computers & Security*, vol. 113, p. 102558, 2022.

[9] X. Chen, T. Wang, K. Huang, and Z. Shao, "Tpgraph: A highly-scalable time-partitioned graph model for tracing blockchain," in *Proceedings of the 17th ACM International Systems and Storage Conference*, 2024.

[10] Y. Hu, Y. Sun, Y. Chen, Z. Chen, B. He, L. Wu, Y. Zhou, and R. Chang, "Mfgscope: A lightweight framework for efficient graph-based analysis on blockchain," *IEEE Transactions on Dependable and Secure Computing*, 2024.

[11] D. Lin, J. Wu, Q. Xuan, and C. K. Tse, "Ethereum transaction tracking: Inferring evolution of transaction networks via link prediction," *Physica A: Statistical Mechanics and its Applications*, vol. 600, p. 127504, 2022.

[12] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin," in *2014 IEEE symposium on security and privacy*. IEEE, 2014.

[13] Y. Yuan and F.-Y. Wang, "Blockchain and cryptocurrencies: Model, techniques, and applications," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no. 9, pp. 1421–1428, 2018.

[14] B. Kitchenham, O. P. Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering–a systematic literature review," *Information and software technology*, vol. 51, no. 1, pp. 7–15, 2009.

[15] R. Palmarini, J. A. Erkoyuncu, R. Roy, and H. Torabmostaedi, "A systematic review of augmented reality applications in maintenance," *Robotics and Computer-Integrated Manufacturing*, vol. 49, 2018.

[16] S. Anjomshoae, A. Najjar, D. Calvaresi, and K. Främling, "Explainable agents and robots: Results from a systematic literature review," in *18th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2019), Montreal, Canada, May 13–17, 2019*. International Foundation for Autonomous Agents and Multiagent Systems, 2019.

[17] Y. Mualla, A. Najjar, A. Daoud, S. Galland, C. Nicolle, E. Shakshuki *et al.*, "Agent-based simulation of unmanned aerial vehicles in civilian applications: A systematic literature review and research directions," *Future Generation Computer Systems*, vol. 100, pp. 344–364, 2019.

[18] D. Calvaresi, A. Dubovitskaya, J. P. Calbimonte, K. Taveter, and M. Schumacher, "Multi-agent systems and blockchain: Results from a systematic literature review," in *Advances in Practical Applications of Agents, Multi-Agent Systems, and Complexity: The PAAMS Collection: 16th International Conference, PAAMS 2018, Toledo, Spain, June 20–22, 2018, Proceedings 16*. Springer, 2018, pp. 110–126.

[19] D. Calvaresi, S. Eggenschwiler, Y. Mualla, M. Schumacher, and J.-P. Calbimonte, "Exploring agent-based chatbots: a systematic literature review," *Journal of ambient intelligence and humanized computing*, vol. 14, no. 8, pp. 11 207–11 226, 2023.

[20] S. J. Pinto, P. Siano, and M. Parente, "Review of cybersecurity analysis in smart distribution systems and future directions for using unsupervised learning methods for cyber detection," *Energies*, vol. 16, no. 4, 2023.

[21] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[22] L. Ismail and H. Materwala, "A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions," *Symmetry*, vol. 11, no. 10, p. 1198, 2019.

[23] M. N. M. Bhutta, A. A. Khwaja, A. Nadeem, H. F. Ahmad, M. K. Khan, M. A. Hanif, H. Song, M. Alshamari, and Y. Cao, "A survey on blockchain technology: Evolution, architecture and security," *Ieee Access*, vol. 9, pp. 61 048–61 073, 2021.

[24] A. Gangwal, H. R. Gangavalli, and A. Thirupathi, "A survey of layer-two blockchain protocols," *Journal of Network and Computer Applications*, vol. 209, p. 103539, 2023.

[25] G. Suciu, C. Nădrag, C. Istrate, A. Vulpe, M.-C. Ditu, and O. Subea, "Comparative analysis of distributed ledger technologies," in *2018 Global Wireless Summit (GWS)*. IEEE, 2018, pp. 370–373.

[26] W. Ou, S. Huang, J. Zheng, Q. Zhang, G. Zeng, and W. Han, "An overview on cross-chain: Mechanism, platforms, challenges and advances," *Computer Networks*, vol. 218, p. 109378, 2022.

[27] A. De Santis, S. Micali, and G. Persiano, "Non-interactive zero-knowledge proof systems," in *Advances in Cryptology—CRYPTO'87: Proceedings 7*. Springer, 1988, pp. 52–72.

[28] R. Phillips and H. Wilder, "Tracing cryptocurrency scams: Clustering replicated advance-fee and phishing websites," in *IEEE international conference on blockchain and cryptocurrency (ICBC)*. IEEE, 2020.