BLOCKCHAIN AND DISTRIBUTED LEDGER TECHNOLOGY

# A Systematic Literature Review of Blockchain and Distributed Ledger Technology for the Detection and Prevention of Phishing Attacks

Temitope Olufunmi Atoyebi Egbele Wilfred Odianosen*, Prema Kirubakaran Ridwan Kolapo

Department of Information Technology and Information Systems, Faculty of Computing, Nile University of Nigeria, Abuja, Nigeria

Published November 2026

**Abstract**

This study systematically reviews blockchain and distributed ledger technology (DLT) for phishing detection and prevention. It also identifies two related research streams: the use of DLT as the infrastructure for anti-phishing intelligence and analytical methods for identifying phishing in blockchain and Web3. The review synthesizes 45 publications through 2026 using PRISMA and reports descriptive mapping, thematic analysis, and evidence identification. Some of the functions of the ledger proposed include decentralized URL blacklists and auditable threat intelligence. In blockchain ecosystems, the dominant analytical methods include machine learning on account and transaction data, analysis of transaction graphs and other temporal graph models, contrastive learning, cross-chain adaptation, and payload inspection. The studies reviewed are largely focused on the Ethereum blockchain from 2023 to 2025. Other limitations identified in the studies include imbalanced classes, ambiguous or absence of labels, lack of both internal and external validation, and privacy and governance concerns. The report suggests the protective measures proposed may not substantially prevent financial loss. It concludes that, despite its potential for improving provability and accountability, the actual effect on phishing is limited without evidence of protective measures, and a timely, off-chain corrective and dispute process.

**Keywords:** blockchain; distributed ledger technology (DLT); phishing detection; phishing prevention; Web3 security

## 1 Introduction

Modern digital ways of working encompass a range of activities, from using digital identities to make online payments, accessing cloud services, and using social media, all the way to utilizing decentralised applications. These digital ways of working increase opportunities for attackers to exploit people's trust using deceptive messages, fraudulent websites and URLs, fake QR codes, phony prompts for wallets, and cloned decentralised applications. As such, phishing impacts traditional online services as well as blockchain services [1], [2]. Industry reports describe large volumes of the traditional type of phishing, and other reports describe deceitful transactions, wallet drainers, and signed transactions [3], [4]. These describe different groups, and their figures cannot be aggregated.

Blockchain is a type of DLT whereby records are linked in the form of cryptographically closed blocks; DLT in general are shared, replicated and distributed ledgers. Some key traits of blockchain technology are provenance and auditability, as well as tamper evidence and programmable rules. The value of these traits depends on the architecture and governance [5]. There are two ways by which blockchain technologies relate to phishing. First, blockchains can facilitate the development of shared

blacklists, threat intelligence, reporting, and reputation systems [6], [7]. Second, blockchain applications can fall prey to phishing attacks through deceitful signatures and approvals as well as fake decentralized applications, wallet drainers and fraudulent smart contracts [8], [9].

While closely related, detection and prevention are distinct outcomes. Models can detect malicious URLs, accounts, contracts, transactions, etc., but preventing loss due to those malicious elements requires that the models intervene before loss occurs. Additional socio-technical controls, such as user-centered mitigations, permission reviews and transaction cancellations, and other controls, like phishing-resistant authentication, should be complemented with analytical detection controls [10], [47]. There is little existing work integrating ledger and user-facing Web3 technologies. This fragmentation is exemplified in reviews that address traditional phishing, Ethereum phishing detection, and blockchain fraud (in general) [11]-[13], [38]. This study classifies existing approaches, integrates worked examples, identifies gaps, analyzes trends in research, and defines future research and innovation priorities. This study focuses on threats and research areas, rather than on innovative solutions. It provides an evidence framework integrating threats, data, analytics, ledger, protective measures, and evaluation.

## 2 Literature review

General phishing research is the benchmark for evaluating blockchain-related systems. Surveys describe the blacklist, heuristic, lexical, host-based, visual-similarity, machine-learning, deep-learning, and hybrid approaches [1], [2], [11], [22], [37], [45], [46]. The machine-learning approaches encounter challenges related to limited evidence at decision time and are adversely influenced by concept drift, adversarial attack adaptation, imbalanced data sets, and weak external validation. Their results cannot be generalized to blockchain transactions. Furthermore, blockchain transactions are different from the entities of analysis in phishing (i.e., URLs, page content, account behaviors, contracts, and graph structures).

Proposals based on DLT for anti-phishing solutions focus on provenance and multi-party accountability. PhishChain records phishing URL assessment on a public ledger. MLPhishChain combines ML and blockchain for classification and recording respectively and reevaluation [6], [7]. Phish Block uses blockchain-based filtering in a cloud environment, and BlockIntelChain broadens the discussion to threat intelligence in a similar context [21], [42]. Although these designs improve traceability, they cannot prove the correctness of the submitted evidence. Open reporting also raises Sybil attacks, privacy, cost, latency, governance, dispute resolution, and false-label correction.

On-chain phishing detections usually depict accounts as nodes and transfers/interactions as edges. Initial studies utilized transaction features of Ethereum, ensemble learning, graph classification and subgraph evidence [14]-[16]. Related work on Bitcoin analyzed behavior of malicious addresses in the context of temporal and graph properties [17]. Feature engineering models like Eth-PSD and approaches utilizing graph-neural networks integrated account features, transaction neighborhoods, temporal and aggregation, heterogeneity in transaction types and self-supervised learning [18]-[25]

Sequence fusion and graph-contrastive methods further combine structural, temporal, and behavioural information [26], [27].

Recent work addresses imbalance and sparse labels, behavioral dynamics, streaming data, cross-chain transfer, and computational scalability. Examples of directions are sampled GNNs, streaming graphs, adversarial domain adaptation, multiscale feature fusion, data augmentation, ego-graph

construction, attention-enhanced gradient boosting, temporally evolving GNNs and dynamic graph coding [28]-[36]. EPAD and other contrastive approaches focus on label efficiency. Later approaches extend benchmarking and temporal self-supervision [39], [40], [43], [44]. Nevertheless, differences in labels, sampling, time windows, graph construction, baselines and train-test splits make a justified universal model ranking difficult

Research is transaction and contract centered, moving towards the point of user authorization. TxPhishScope examines transaction-based phishing attacks that target signing decisions. Phishing-Hook uses opcodes of the Ethereum Virtual Machine to identify phishing smart contracts [41]. Research that informs wallet warnings, transactions simulation, contract-risk labels, and revocation mechanisms is discussed. While these studies offer a basis for phishing defense, evidence of Integration with user interface and a reduction in user loss are still missing. Therefore the papers included in the review are structured using a six component framework illustrated in Figure 1..

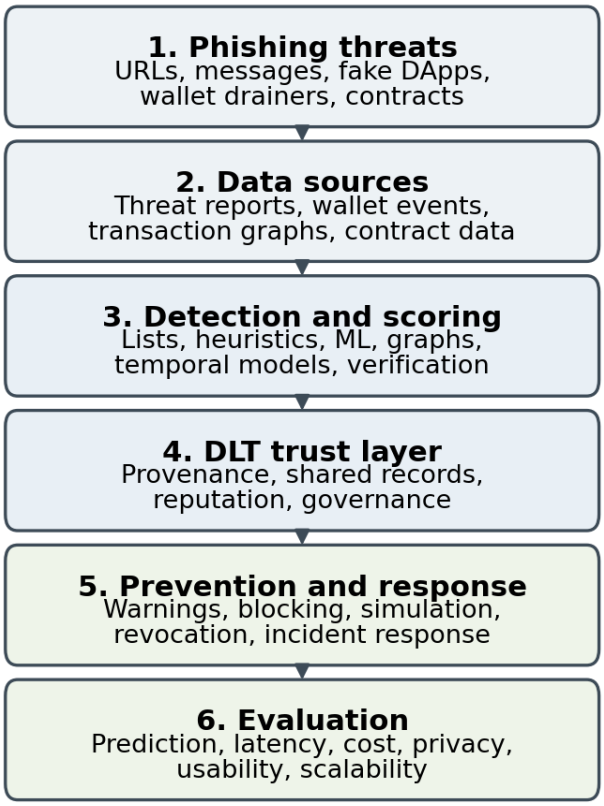



**Figure 1.** DLT anti-phishing evidence framework (authors' synthesis of the reviewed literature).

The framework starts with threats and observable data, and then separates analytical scoring from the DLT trust layer. Functions of the ledger involve provenance and shared records, as well as reputation and governance. Prevention encompasses warning, blocking, and simulation, as well as revoking or removing trusted components, or taking incident-response actions. Evaluation must therefore take both predictive measures and operational measures including, for example, latency, cost, privacy, scalability, explainability, usability and correction of mislabeling.

## 3 Materials and methods

The study used a systematic literature review methodology. Based on the PRISMA 2020 guidelines [48], we reported on the identification, screening, eligibility assessment and inclusion of articles. Searches were undertaken on Scopus, Web of Science, IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink, MDPI, and Google Scholar. Search strings comprised three concept groups, i.e. Blockchain/DLT, Phishing/related Web3 deception, and detection/prevention/mitigation/blacklisting/reputation/threat Intelligence/machine learning/graph neural networks/fraud detection. Backward and forward citation searching were also undertaken.

Papers relevant to blockchain/DLT and Web3 protection (including phishing), published in English in 2020-2026 were included. The sample included journal articles, conference articles, book chapters, standards, reviews and preprints. Other materials, including marketing literature, unsupported commentary, and fraud studies that did not contain phishing (or other Web3 protection related) research were excluded. The final sample consisted of 45 papers and included primary/empirical papers, as well as review and other papers. When interpreting the papers, we discriminated between paper types, i.e. review vs. primary/empirical papers. The objectives of the review and the corresponding methods are matched in Table 1.

**Table 1.** Objective-to-method matching.

| Objective | Review method | Expected output |
|---|---|---|
| 1 | Map years, contexts, and dominant themes | Publication and theme profile |
| 2 | Classify detection, prevention, DLT, and Web3 roles | Approach taxonomy |
| 3 | Extract data, features, platforms, validation, and metrics | Comparability profile |
| 4 | Synthesise strengths, deployment issues, and gaps | Evidence-based research agenda |

In the selection process, 168 records were found, 33 duplicates were removed, 135 titles and abstracts were screened, 72 records were excluded, 63 full texts were assessed, and 18 full texts were excluded, leaving 45 publications. The totals are depicted in Figure 2. Completed study level appraisal scores, the final search date, and record-by-record decisions for exclusion were not available, so the flow diagram should be interpreted as PRISMA-informed process reporting, not as an audit trail.

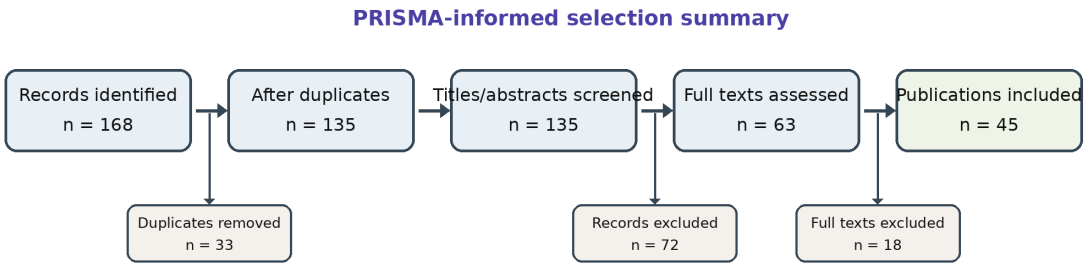



**Figure 2.** PRISMA-informed study-selection flow.

A structured extraction framework captured bibliographic details, study focus, blockchain platform, phishing vector, method, dataset, features, labels, validation, performance metrics, findings, limitations, and reported gaps. Descriptive synthesis captured years and primary themes. Thematic

synthesis explored comparisons of the technical contributions and deployment concerns. A statistical meta-analysis was not conducted due to the studies using heterogeneous tasks, datasets, labels, validation designs, and outcome measures. The review has differentiated between predictive detection and demonstrated prevention. Furthermore, its conceptual framework has been treated as an organizing lens rather than as a system architecture.

## 4 Results

### 4.1 Publication trends and research contexts

The 45 publications were distributed by year as follows (Figure 3): four in 2020, five in 2021, four in 2022, ten in 2023, eleven in 2024, nine in 2025, and two in 2026. The sample studied here is focused on 2023-2025. This is likely due to the increased interest in learning about graph construction and modeling with respect to time, contrastive learning, adapting across chains, analysis of payloads, and inspection of smart contracts. The low number in 2026 should not be read as a decline because the review does not provide a complete picture of this particular year.

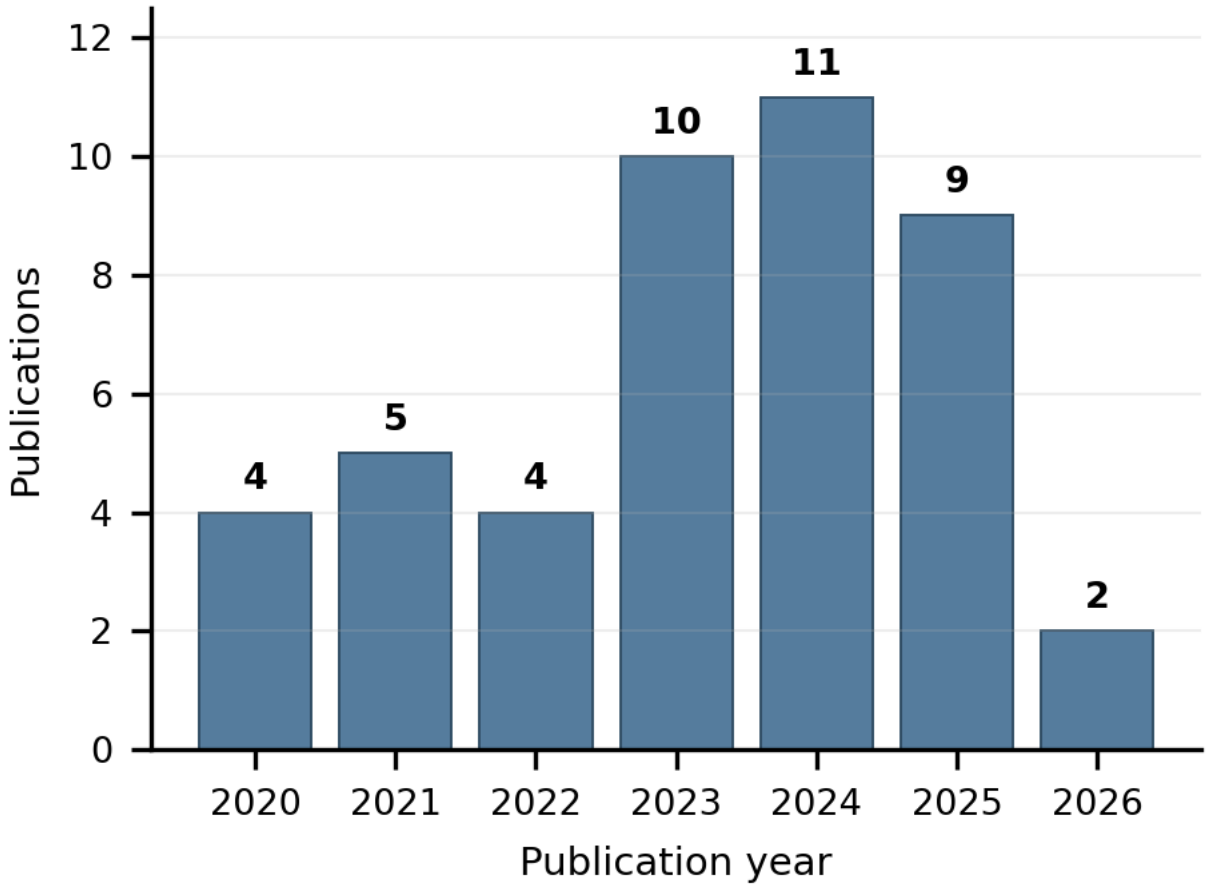



**Figure 3.** Distribution of the reviewed publications by year.

### 4.2 Research themes and technical approaches

Primary-theme coding placed nine publications in general phishing and authentication contexts, four in blockchain foundations, wider fraud and threat-intelligence contexts, three in DLT anti-phishing infrastructure contexts, twenty-six in on-chain account detection and graph or machine-learning contexts, and three in Web3 transaction or smart-contract contexts. This shows the evidence is

strongest for analytical detection of suspicious blockchain accounts, particularly in the context of Ethereum, and comparatively less for ledger-based intelligence and end-to-end user protection.

The literature encompasses five major technical families. Decentralized intelligence systems, record reports and make decisions and/or assign a reputation score. URLs and web sites are classified using textual, host, or content-based features, with the ledger sometimes serving only as an audit layer. Account and transaction models capture interaction structure using neighbor and frequency over time, as well as interface structure and behavioral changes over time. Graph models capture interaction structure over time. Transaction and contract models capture the action that produces a harmful signature or contract call. These approaches are compared in Table 2.

**Table 2.** Technical approaches, principal contributions and limitations.

| Approach | Principal contribution | Main limitation |
|---|---|---|
| DLT intelligence and blacklisting | Provenance, shared reporting, and auditable decisions | Governance, Sybil risk, privacy, correction, and cost |
| URL and website machine learning | Fast classification using lexical, host, content, or visual features | Concept drift and weak transfer to transaction settings |
| On-chain feature and graph models | Behavioural and relational detection of suspicious accounts | Label scarcity, imbalance, and Ethereum concentration |
| Temporal, streaming, and cross-chain learning | Changing behaviour, timeliness, and transfer across chains | External validation, latency, and maintenance |
| Payload and smart-contract analysis | Risk signals close to signing or contract execution | Rule evolution and limited wallet or user studies |

### 4.3 Data, platforms, and evaluation

These studies have analyzed URLs, domains, page content, labeled wallet addresses, transaction histories, token approvals, contract interactions, transaction payloads, opcodes and constructed graphs. Ethereum is prominent as it provides public data and has a programmable-contract environment to analyze accounts, tokens, and contracts while cross-chain analyses also include Bitcoin and EOSIO [17], [30]. Differences in account models, transaction semantics and contract execution across platforms pose limitations to direct model transfer. The availability of features at the time of decision is also crucial. Retrospective graph evidence might identify a scam after the funds are moved but scam prevention requires prediction and a signal before the funds are released or moved.

Predictive metrics like accuracy, precision, recall, F1 score, area under the curve and false positive rates dominate. Other metrics like latency and scalability are also discussed. However, operational measures like understanding of warnings, revocation of permissions, transaction cancellations, disputes, and analysts' workload are not evaluated. Precision and recall are always considered together and missed attacks, false alarms and unwarranted accusations must be interpreted together. Because datasets, labels, time splits and baselines are not comparable across studies, confident ranking is not possible..

# 5 Discussion

## 5.1 Strengths and deployment constraints

A primary strength of DLT-based proposals is the ability to provide explicit provenance. Participants can view who provided what information, who performed what verification, and how a particular decision was changed. On the other hand, on-chain analytics can provide relational and/or temporal evidence that may be missing in isolated blacklists. In the end, tamper evidence does not equal truth. In the absence of systems to provide accountable verification, reputation, and/or superseding decisions and due process, durably incorrect or malicious reports can not be differentiated from truth. Public ledgers can reveal victims and sensitive information, and/or be used to identify individuals under protection, so hybrid systems can benefit from explicit evaluation of privacy and costs.

Analytical limitation may take the form of small, unbalanced, or biased datasets, selective sampling, data leakage, temporal validation, platform-specific evaluation, explainability, and evidence of live deployment [12], [13], [24], [39]. Models may learn dataset artifacts and may not generalize beyond the dataset. Dynamic and self-supervised learning can help address these problems, but they introduce other considerations around compute, monitoring, and governance. A publishable evaluation should detail these considerations.

## 5.2 Detection versus demonstrated prevention

The central interpretive finding is that a ledger, a detector, and a preventive control are distinct elements. A blockchain may preserve the provenance of a risk label without improving the classifier that produced it. A high performing model may identify a suspicious account without preventing a deceptive signature. End-to-end protection requires the risk signal to be timely, appropriately integrated into an end-user workflow (e.g. browser, wallet, exchange, registrar, etc.) and understandable. Thus, future work should consider performing realistic temporal and cross-chain validation in conjunction with user-centred warning research, transaction simulation, intelligence-sharing, correction and/or prevention, and measuring the outcome of prevention.

## 5.3 Limitations of the review

The conclusions are qualified because of the mixed evidence base, and incomplete audit trail of the review. The 45-entry matrix encompasses primary and secondary studies, standards, and other contextual sources. Exact histories of searches, rationale for record-level screening, completed quality assessments for studies, and a final search date, were not fully documented. Therefore, the review does not allow for statistical pooling. It does however, support qualitative synthesis and descriptive mapping. Causal claims concerning prevention of potential losses, and definitive ranking of competing detection models, cannot be made based on this review.

# 6 Conclusion

This review integrates DLT-based anti-phishing technology in phishing detection in blockchain and Web3 ecosystems. The evidence shows that ledgers can support provenance, accountability, and shared verification of threat intelligence, and machine learning can complement detection. The evidence shows that blockchain is not a complete solution, decentralization does not necessarily improve security, and high classification scores do not always prevent financial loss.

Further research should explore how practically valuable such protection systems can be with reliable off-chain data, explicit governance, privacy controls, and correction and dispute mechanisms. Researchers should publish auditable records of their searches and extractions. There is potential to evaluate hybrid on-chain and off-chain architectures against centralized systems. This research offers an evidence-based framework to evaluate the impact of warning systems on operational outcomes, including a reduction in loss, cancellation of transactions, and false alarms, among others.

Practical and scientific value of this framework will be evaluated through research focused on (a) the design of trust frameworks to incorporate protection systems that influence trust actions, (b) user understanding of warnings, (c) balancing false alarms, (d) reducing loss, and (e) transaction cancellation. The author proposes a framework based on six components to evaluate research, design and implement systems that integrate PHC in trust frameworks.

## References


[1] Alabdan R. Phishing attacks survey: Types, vectors, and technical approaches. *Future Internet*. 2020;12(10):168. https://doi.org/10.3390/fi12100168

[2] Alkhalil Z, Hewage C, Nawaf L, Khan I. Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*. 2021;3:563060. https://doi.org/10.3389/fcomp.2021.563060

[3] Anti-Phishing Working Group. *Phishing activity trends report: 4th quarter 2025*. APWG; 2026. Available from: https://docs.apwg.org/reports/apwg_trends_report_q4_2025.pdf

[4] Scam Sniffer. *Scam Sniffer 2025: Crypto phishing losses fall 83% to $84 million*. Jan 3. 2026. https://drops.scamsniffer.io/scam-sniffer-2025-crypto-phishing-losses-fall-83-to-84-million/

[5] Bhutta MNM, et al. A survey on blockchain technology: Evolution, architecture and security. *IEEE Access*. 2021;9:61048–61073. https://doi.org/10.1109/ACCESS.2021.3072849

[6] Edirimannage S, Nabeel M, Elvitigala C, Keppitiyagama C. PhishChain: A decentralized and transparent system to blacklist phishing URLs. *arXiv*:2202.07882. 2022. https://doi.org/10.48550/arXiv.2202.07882

[7] Trad F, Semaan-Nasr E, Chehab A. MLPhishChain: A machine learning-based blockchain framework for reducing phishing threats. *Frontiers in Blockchain*. 2024;7:1484894. https://doi.org/10.3389/fbloc.2024.1484894

[8] He B, et al. TxPhishScope: Towards detecting and understanding transaction-based phishing on Ethereum. In: *Proc*. ACM SIGSAC Conf. Computer and Communications Security; 2023. p. 120–134. https://doi.org/10.1145/3576915.3623210

[9] Chen Z, Hu Y, He B, Luo D, Wu L, Zhou Y. Dissecting payload-based transaction phishing on Ethereum. *arXiv*:2409.02386. 2024.

[10] Naqvi B, Perova K, Farooq A, Makhdoom I, Oyedeji S, Porras J. Mitigation strategies against the phishing attacks: A systematic literature review. *Computers & Security*. 2023;132:103387. https://doi.org/10.1016/j.cose.2023.103387

[11] Safi A, Singh S. A systematic literature review on phishing website detection techniques. *Journal of King Saud University - Computer and Information Sciences*. 2023;35(2):590–611. https://doi.org/10.1016/j.jksuci.2023.01.004

[12] Ghosh M, Halder R, Chandra J. *A systematic review on Ethereum phishing scam detection: Challenges, empirical insights, and future directions*. Blockchain: Research and Applications. 2025. https://doi.org/10.1016/j.bcra.2025.100424

[13] Ghnemat R, Mosa H. Blockchain-based fraud detection: A systematic review of Ethereum network applications. *Cluster Computing*. 2025;28:1080. https://doi.org/10.1007/s10586-025-05797-w

[14] Chen W, Guo X, Chen Z, Zheng Z, Lu Y. Phishing scam detection on Ethereum: Towards financial security for blockchain ecosystem. In: *Proc*. 29th Int. Joint Conf. Artificial Intelligence; 2020. p. 4506–4512. https://doi.org/10.24963/ijcai.2020/621

[15] Yuan Q, Huang B, Zhang J, Wu J, Zhang H, Zhang X. Detecting phishing scams on Ethereum based on transaction records. In: *Proc*. IEEE Int. Symp. Circuits and Systems; 2020. p. 1–5. https://doi.org/10.1109/ISCAS45731.2020.9180815

[16] Zhang D, Chen J. Blockchain phishing scam detection via multi-channel graph classification. In: *Blockchain and Trustworthy Systems*; 2021. p. 241–256. https://doi.org/10.1007/978-981-16-7993-3_19

[17] Chaudhari D, Agarwal R, Shukla SK. Towards malicious address identification in Bitcoin. *arXiv*:2112.11721. 2021.

[18] Kabla AHH, Anbar M, Manickam S, Karuppayah S. Eth-PSD: A machine learning-based phishing scam detection approach in Ethereum. *IEEE Access*. 2022;10:118043–118057. https://doi.org/10.1109/ACCESS.2022.3220780

[19] Li P, Xie Y, Xu X, Zhou J, Xuan Q. Phishing fraud detection on Ethereum using graph neural network. *arXiv*:2204.08194. 2022. https://doi.org/10.48550/arXiv.2204.08194

[20] Li S, Gou G, Liu C, Hou C, Li Z, Xiong G. TTAGN: Temporal transaction aggregation graph network for Ethereum phishing scams detection. In: *Proc*. ACM Web Conf; 2022. p. 661–669. https://doi.org/10.1145/3485447.3512226

[21] Karthika RN, Valliyammai C, Naveena M. Phish Block: A blockchain framework for phish detection in cloud. *Computer Systems Science and Engineering*. 2023;44(1):777–795. https://doi.org/10.32604/csse.2023.024086

[22] Asiri S, Xiao Y, Alzahrani S, Li S, Li T. A survey of intelligent detection designs of HTML URL phishing attacks. *IEEE Access*. 2023;11:6421–6443. https://doi.org/10.1109/ACCESS.2023.3237798

[23] Joshi K, et al. Machine-learning techniques for predicting phishing attacks in blockchain networks: A comparative study. *Algorithms*. 2023;16(8):366. https://doi.org/10.3390/a16080366

[24] Kim J, Lee S, Kim Y, Ahn S, Cho S. Graph learning-based blockchain phishing account detection with a heterogeneous transaction graph. *Sensors*. 2023;23(1):463. https://doi.org/10.3390/s23010463

[25] Li S, Wang R, Wu H, Zhong S, Xu F. SIEGE: Self-supervised incremental deep graph learning for Ethereum phishing scam detection. In: *Proc*. 31st ACM Int. Conf. Multimedia; 2023. https://doi.org/10.1145/3581783.3612461

[26] Zhang Y, Su Y. Ethereum phishing detection based on graph structure and transaction sequence features fusion. In: *Service Science*; 2023. p. 247–262. https://doi.org/10.1007/978-981-99-4402-6_18

[27] Li S, et al. TGC: Transaction graph contrast network for Ethereum phishing scam detection. In: *Proc*. Annual Computer Security Applications Conf; 2023. p. 352–365. https://doi.org/10.1145/3627106.3627109

[28] Ratra S, Ghosh M, Baliyan N, Mohan JR, Singh S. Graph neural network based phishing account detection in Ethereum. *The Computer Journal*. 2024;67(12):3160–3168. https://doi.org/10.1093/comjnl/bxae079

[29] Yu W, et al. Phishing fraud detection based on the streaming graph algorithm. In: *Blockchain Transaction Data Analytics*; 2024. p. 125–147. https://doi.org/10.1007/978-981-97-4430-5_6

[30] Yan C, Han X, Zhu Y, Du D, Lu Z, Liu Y. Phishing behavior detection on different blockchains via adversarial domain adaptation. *Cybersecurity*. 2024;7:45. https://doi.org/10.1186/s42400-024-00237-5

[31] Chen Z, Huang J, Liu S, Long H. Multiscale feature fusion and graph convolutional network for detecting Ethereum phishing scams. *Electronics*. 2024;13(6):1012. https://doi.org/10.3390/electronics13061012

[32] Chen Z, Liu SZ, Huang J, Xiu YH, Zhang H, Long HX. Ethereum phishing scam detection based on data augmentation method and hybrid graph neural network model. *Sensors*. 2024;24(12):4022. https://doi.org/10.3390/s24124022

[33] Huang H, et al. PEAE-GNN: Phishing detection on Ethereum via augmentation ego-graph based on graph neural network. *IEEE Transactions on Computational Social Systems*. 2024;11(3):4326–4339. https://doi.org/10.1109/TCSS.2023.3349071

[34] Liu SZ, et al. Detection of Ethereum phishing fraud nodes based on feature enhancement strategy and GBM. *Electronics*. 2024;13(24):5060. https://doi.org/10.3390/electronics13245060

[35] Zhang J, Sui H, Sun X, Ge C, Zhou L, Susilo W. GrabPhisher: Phishing scams detection in Ethereum via temporally evolving GNNs. *IEEE Transactions on Services Computing*. 2024;17(6):3727–3741. https://doi.org/10.1109/TSC.2024.3411449

[36] Li C, Liu R, Zhang Y, Xie N, Zeng Q. Who will be hooked?: A phishing fraud detection model based on dynamic graph temporal feature coding in Ethereum. In: *Proc*. Int. Conf. Blockchain and Web3.0 Technology Innovation and Application Exchange; 2025. p. 130–141. https://doi.org/10.1007/978-981-97-9412-6_12

[37] Kavya S, Sumathi D. Staying ahead of phishers: A review of recent advances and emerging methodologies in phishing detection. *Artificial Intelligence Review*. 2024. https://doi.org/10.1007/s10462-024-11055-z

[38] Banerjee J, Ghosh M. In hot pursuit of phishers: Phishing detection in blockchain at a glance. In: *Proc*. Int. Conf. Innovative Computing and Communications; 2025. p. 293–307. https://doi.org/10.1007/978-981-96-7523-4_21

[39] Sui H, Zhang J, Chen B, Wu D, Sun X, Palaiahnakote S. EPAD: Ethereum phishing scam detection via graph contrastive learning. *Expert Systems with Applications*. 2025. https://doi.org/10.1016/j.eswa.2025.128227

[40] Alghuried A, Alghamdi A, Alkinoon A, Choi S, Mohaisen M, Mohaisen D. Fishing for phishers: Learning-based phishing detection in Ethereum transactions. *arXiv*:2504.17953. 2025.

[41] De Rosa P, Queyrut S, Bromberg YD, Felber P, Schiavoni V. PhishingHook: Catching phishing Ethereum smart contracts leveraging EVM opcodes. *arXiv*:2506.19480. 2025.

[42] Tolah A. BlockIntelChain: A blockchain-based cyber threat intelligence sharing architecture. *Scientific Reports*. 2025. https://doi.org/10.1038/s41598-025-29152-6

[43] Chen M, Liu R, Song Q, Song G, Li C, Zeng Q. HSTA: Ethereum phishing fraud detection model based on dynamic graph hybrid spatio-temporal attention mechanism. In: *Proc*. Int. Conf. Blockchain and Web3.0 Technology Innovation and Application Exchange; 2026. p. 50–61. https://doi.org/10.1007/978-981-95-4142-3_5

[44] Wu C, Chen J, Lin S, Li H, Zhao Z. Phishing detection in Ethereum via temporal graph contrastive learning. *arXiv*:2605.01207. 2026.

[45] Basit A, Zafar M, Liu X, Javed AR, Jalil Z, Kifayat K. A comprehensive survey of AI-enabled phishing attacks detection techniques. *Telecommunication Systems*. 2021;76(1):139–154. https://doi.org/10.1007/s11235-020-00733-2

[46] Murugesan S, Murugesan S, Ganesan R, Alhalabi W. Web phishing detection techniques: A survey on the state-of-the-art, taxonomy and future directions. *IET Networks*. 2020;9(5):235–246. https://doi.org/10.1049/iet-net.2020.0078

[47] Temoshok D, et al. *Digital identity guidelines: authentication and authenticator management*. NIST Special Publication 800-63B-4. Gaithersburg (MD): National Institute of Standards and Technology; 2025. https://doi.org/10.6028/NIST.SP.800-63B-4

[48] Page MJ, et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*. 2021;372:n71. https://doi.org/10.1136/bmj.n71