Cureus Journal of Computer Science
https://doi.org/10.7759/s44389-026-00097-9

Review Article

Evaluating the Effectiveness of Blockchain Analytics Tools in Detecting Money Laundering Across Stablecoins

Kehinde Hamed [1], Moshood Sorinola [2]

1. *Financial Crime and Compliance Management, Utica, USA*
2. *Business Analytics, Georgia State University, Georgia, USA*

Received: April 18, 2026 | Review began: April 27, 2026 | Review ended: May 12, 2026 | Published: June 03, 2026

Abstract

Stablecoins carried most illicit virtual-asset transaction value in 2025, while many blockchain anti-money laundering (AML) tools still reflect design assumptions inherited from Bitcoin's unspent transaction output graph. Evidence from peer-reviewed studies, preprints, industry reports, and regulatory sources published from 2019 to early 2026 was reviewed to assess how far those assumptions carry into USDT and USDC environments. Commercial platforms support attribution, wallet-risk scoring, exchange screening, and investigations, but cross-chain routing weakens continuous tracing; Elliptic estimated $21.8 billion in illicit and high-risk flows through cross-chain methods in 2025. Bitcoin classifiers report accuracies above 97% on Elliptic-family benchmarks, although class imbalance and limited precision-at-recall reporting make operational value difficult to judge. StableAML, the only USDT/USDC-specific classifier identified, found stronger signal in behavioral wallet features than in topology-heavy Bitcoin-derived approaches. Regulation and issuer freezes add intervention points, but slow response cycles, scarce stablecoin labels, and closed vendor thresholds limit independent evaluation. Stablecoin AML evaluation depends on public labeled datasets, precision-at-recall metrics, latency measures, and independent audits of commercial tools.

Categories: Forensic Analysis, Blockchain and Cryptocurrency, Machine Learning (ML)

Keywords: blockchain analytics, anti-money laundering, stablecoins, graph neural networks, cryptocurrency compliance, usdt, usdc, fatf travel rule

Introduction And Background

Approximately $51 billion in cryptocurrency was laundered in 2024, about 0.14% of the $9 trillion in on-chain volume that year [1]. Stablecoins, dollar-pegged tokens now carrying the majority of illicit crypto value, displaced Bitcoin in that role between 2023 and 2025 [1].

Chainalysis, Elliptic, TRM Labs, and the academic classifiers trained on the Elliptic Bitcoin dataset all assume an unspent transaction output (UTXO) model in which subgraph tracing follows continuous chains of inputs and outputs [2]. Stablecoins on Ethereum and TRON operate on account-based ledgers. Token transfers fragment the transaction graph. Programmable mechanics (swaps, bridging, and smart contract interactions) sever the continuous chains these tools depend on (Figure *1*). Issuers can freeze wallets, an enforcement mechanism without an equivalent in Bitcoin [3]. Classifier accuracies above 97% on the Elliptic benchmark collapse under real-world class imbalance: one model achieved 99% accuracy by labeling every transaction as legitimate [4]. MiCA, the GENIUS Act, Financial Action Task Force (FATF) Travel Rule updates, and separate stablecoin frameworks in Singapore and Hong Kong impose different compliance obligations on different actors at different thresholds [5].

This review contributes a stablecoin-specific transferability framework for evaluating whether blockchain analytics tools designed around Bitcoin transaction topology can support anti-money laundering detection in account-based stablecoin ecosystems. The analysis does not introduce a new classifier. Instead, it separates detection approaches by ledger assumption, data substrate, detection method, operational output, and failure mode. That framing clarifies why high-performing Bitcoin classifiers do not necessarily translate to USDT and USDC networks, where swaps, bridges, issuer freezes, and off-chain attribution reshape the detection problem.

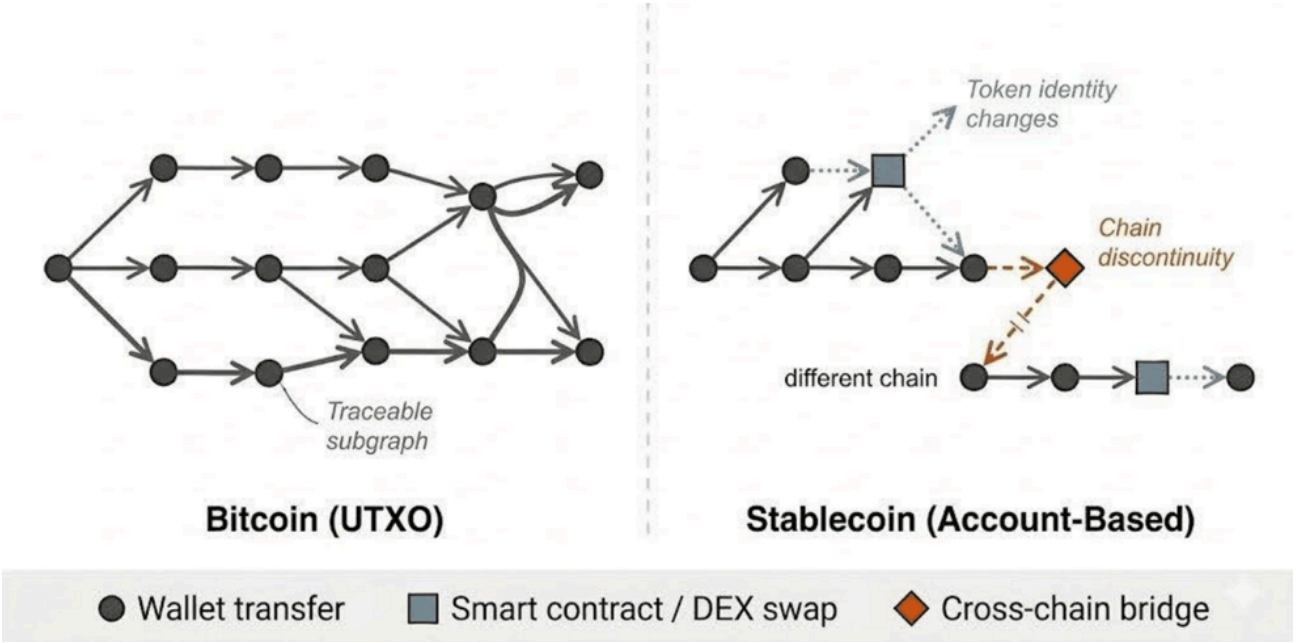

FIGURE 1: Bitcoin UTXO versus stablecoin transaction graph structures.

Source: Author's creation.
Schematic transaction graph structures for Bitcoin UTXO chains (left) and Ethereum stablecoin transfers (right). Node shapes distinguish transaction types; dashed edges indicate tracing discontinuities at bridge interfaces and smart contract interactions.
DEX, Decentralized exchange; UTXO, Unspent transaction output

Review

Methodology

Database searches were conducted across Institute of Electrical and Electronics Engineers (IEEE) Xplore, Association for Computing Machinery (ACM) Digital Library, Springer Link, ScienceDirect, PubMed Central, and arXiv between January and March 2026. Search terms combined three concept groups using Boolean operators: Group A (blockchain analytics OR blockchain forensics OR on-chain analysis), Group B (anti-money laundering OR illicit transaction detection OR suspicious activity report), and Group C (stablecoin OR USDT OR USDC OR Tether OR Circle). Queries paired A AND B to capture blockchain anti-money laundering (AML) research broadly, then A AND B AND C to isolate stablecoin-specific work. Publications from 2019 onward were included, with the lower bound set by the release of the Elliptic Bitcoin transaction dataset, the earliest publicly available benchmark enabling empirical AML evaluation on blockchain data. No upper date limit was applied; the most recent source included was published in February 2026.

Studies were included if they met at least one of four criteria: (a) technical evaluation of a blockchain analytics tool or platform for AML purposes, (b) application of a machine learning or graph-based classifier to cryptocurrency transaction data with reported performance metrics, (c) empirical analysis of stablecoin-specific laundering typologies or obfuscation techniques, or (d) comparative analysis of regulatory frameworks governing virtual asset service provider compliance

How to cite this article:
Hamed K, Sorinola M (June 03, 2026) Evaluating the Effectiveness of Blockchain Analytics Tools in Detecting Money Laundering Across Stablecoins. Cureus J Comput Sci 3 : es44389-026-00097-9. DOI https://doi.org/10.7759/s44389-026-00097-9

obligations. Exclusions applied to work that focused exclusively on privacy coins without reference to stablecoins or general-purpose blockchain analytics, proposed theoretical models without empirical evaluation on transaction data, or were published in languages other than English. Titles and abstracts were screened first; studies meeting at least one inclusion criterion advanced to full-text review. Industry reports from Chainalysis, Elliptic, TRM Labs, the Financial Action Task Force, and the United Nations Office on Drugs and Crime were included where they provided quantitative data on illicit transaction volumes, enforcement actions, or tool capabilities not available in peer-reviewed sources. Reference lists of all included studies were reviewed to identify additional relevant publications; this snowballing process continued until no further novel sources emerged. Initial database searches and snowball citation tracking yielded a combined pool from which 34 sources met at least one inclusion criterion and were retained for analysis.

Quality appraisal followed a narrative approach rather than a formal risk-of-bias instrument, consistent with the heterogeneous evidence base spanning peer-reviewed articles, conference proceedings, preprints, industry reports, and regulatory documents. Work reporting precision and recall at specified thresholds was weighted more heavily than those reporting only aggregate accuracy, given that extreme class imbalance in AML classification renders accuracy misleading. Vendor-published performance claims were included but flagged as lacking independent verification wherever no third-party evaluation was available.

All figures and tables presented in this review were created by the authors for this article and are not reproduced from any previously published source.

Results

Detection Approaches Clustered by Transferability Risk

Five tool families recur across the literature: commercial tracing platforms, Bitcoin benchmark classifiers, Ethereum or stablecoin-specific classifiers, issuer freeze systems, and compliance infrastructure. Each family depends on a different kind of evidence. Commercial products rely on attribution databases, address histories, and service-level intelligence. Bitcoin classifiers lean on UTXO transaction topology. Stablecoin classifiers draw more heavily on wallet behavior, token transfers, and contract interactions. Issuer controls the use of blacklist and freeze events. Compliance systems depend on identity, Travel Rule messages, suspicious activity workflows, and reporting records.

Table *1* uses those distinctions to compare the main detection approaches. The comparison matters because stablecoin laundering does not simply add another asset to the Bitcoin tracing problem. USDT and USDC move through account-based ledgers, decentralized exchanges, smart contracts, bridges, and issuer-controlled token contracts. Those features change what the tool can observe and where the trail can break.

How to cite this article:
Hamed K, Sorinola M (June 03, 2026) Evaluating the Effectiveness of Blockchain Analytics Tools in Detecting Money Laundering Across Stablecoins. Cureus J Comput Sci 3 : es44389-026-00097-9. DOI https://doi.org/10.7759/s44389-026-00097-9

Detection class	Main assumption	Evidence used	Practical role	Stablecoin gap
Commercial tracing platforms	Funds can be followed across visible paths	Address clusters, entity labels, service histories	Risk scoring; attribution; exchange screening	Bridges and DEX swaps break trails
Bitcoin ML/GNN models	UTXO topology predicts illicit activity	Elliptic-family Bitcoin labels and features	Benchmark classification	Accuracy can mask class imbalance
Stablecoin classifiers	Wallet behavior carries stronger signal	Token transfers, contract calls, wallet activity	Wallet-risk classification; alert triage	Few public labels; limited replication
Issuer freeze systems	Centralized issuers can stop tokens	Blacklists, freeze events, token contracts	Asset freezing; sanctions response	Freeze speed and displacement are unclear
Compliance infrastructure	Identity-bearing intermediaries control off-ramps	KYC, Travel Rule, SAR, tax records	Reporting; customer screening; off-ramp control	

TABLE 1: Taxonomy of anti-money laundering detection approaches across Bitcoin and stablecoin ecosystems.

AML, Anti-money laundering; DEX, Decentralized exchange; GNN, Graph neural network; KYC, Know Your Customer; ML, Machine learning; OTC, Over the counter; SAR, Suspicious activity report; UTXO, Unspent transaction output

Commercial Tracing at Cross-Chain Boundaries

Commercial blockchain analytics platforms offer scale and case-support capacity that academic classifiers usually do not have. Chainalysis had mapped more than $24 trillion in value across over one billion addresses by early 2023, and its Reactor product has supported major enforcement investigations [6]. Elliptic applies predictive risk scoring to wallet behavior and processes more than two million screenings each month across more than 100 cryptoassets [6,7]. TRM Labs screens risk across more than 100 blockchains and traces activity on 45 [6]. These systems help investigators connect wallets to known services, screen exchange deposits, monitor sanctions exposure, and reconstruct activity after a suspicious event.

Their limits appear at the points where stablecoin laundering changes venue. The major analytics platforms do not verify wallet ownership directly; exchanges and other virtual asset service providers have to pair analytics outputs with Know Your Customer records before an address can be tied to a legal identity [8]. Cross-chain routing creates a second break. Elliptic estimated that more than $21.8 billion in illicit and high-risk crypto moved through cross-chain methods in 2025 [9]. TRM Labs reported $141 billion in stablecoins received by illicit entities in 2025, with flows concentrated in activity that benefits from stablecoin liquidity and settlement speed [10]. Chainalysis also identified centralized exchanges as major off-ramps while documenting growth in bridge-mediated illicit flows [11]. The evidence therefore supports a narrower claim: commercial tools remain useful, but their strongest role in stablecoin AML lies in risk scoring, service attribution, and off-ramp triage rather than uninterrupted chain-following.

Bitcoin Benchmarks and Validation Limits

How to cite this article:
Hamed K, Sorinola M (June 03, 2026) Evaluating the Effectiveness of Blockchain Analytics Tools in Detecting Money Laundering Across Stablecoins. Cureus J Comput Sci 3 : es44389-026-00097-9. DOI https://doi.org/10.7759/s44389-026-00097-9

Academic AML classifiers still draw mainly from Bitcoin datasets. Hassan et al. [12] found that blockchain AML models commonly train within a narrow dataset family. Weber et al. [2] released the Elliptic Bitcoin dataset with roughly 200,000 transactions labeled as licit or illicit, making it the reference benchmark for graph-based cryptocurrency AML research. Elmougy and Liu [13] extended the same line of work through Elliptic++, with more than 822,000 Bitcoin address-level nodes, 56 features, and 1.27 million temporal interactions. Elliptic2 shifted the unit of analysis toward subgraphs and scaled the dataset to nearly 200 million transactions and 122,000 labeled illicit-linked subgraphs [7,14]. These datasets improved reproducibility, but they still test Bitcoin behavior.

Reported model performance is high. Alarab and Prakoonwit [15] reached 97.77% accuracy with a graph-based long short-term memory architecture and temporal convolutional layers. Lawal et al. [4] reported 98.14% accuracy, 94.23% precision, and 86.22% recall with a topology adaptive graph convolutional network. Lin et al. [16] reported 98.02% accuracy and a 0.9799 F1-score with ChronoWave-graphic neural network (GNN). Lo et al. [17] used self-supervised graph pretraining before Random Forest classification, and Inspection-L reported high precision with lower recall. These studies show that Bitcoin graph data can support strong benchmark performance.

The operational meaning of those scores is less secure. Illicit labels make up a small share of Elliptic-family data, and live AML screening usually faces even lower base rates. Accuracy can therefore reward a model that mostly predicts the majority class. Lawal et al. [4] documented this failure directly: one graph neural network trained on Elliptic data predicted every test node as licit and detected no illicit activity. Cost-sensitive learning, oversampling, graph augmentation, and temporal modeling help, but published results remain hard to compare because studies do not use a common operational protocol.

Johannessen and Jullum [18] reported the most practice-facing metric in the reviewed classifier literature. Their heterogeneous message-passing neural network, tested on production transaction data from DNB in Norway, reached 84% precision at 1% recall and 67% precision at 50% recall. That framing matches the compliance problem more closely than headline accuracy: how many generated alerts deserve investigation? Effendi and Chattopadhyay showed that XGBoost under fully homomorphic encryption could preserve high accuracy on balanced AML data and improve F1-score with graph features on imbalanced data, although computational cost limited real-time use [19]. Across the classifier evidence, the weakness is not model sophistication. It is validation fit: Bitcoin datasets, inconsistent imbalance handling, and limited reporting at recall levels that compliance teams can use.

Stablecoin-Specific Laundering Changes the Detection Substrate

Stablecoins change the object being traced. Foley et al. [20] estimated substantial illegal activity in earlier Bitcoin markets, but later illicit flows moved toward assets that offered stable pricing, deep liquidity, fast settlement, and broad exchange support. Carpentier-Desjardins et al. documented 1,036 decentralized-finance crime events from 2017 to 2022, with minimum losses of $10 billion, and identified token swaps, flash loans, and bridge exploits as recurring mechanisms [21]. Those mechanisms sit inside the stablecoin transaction environment rather than at its edge.

Ethereum and TRON stablecoin flows do not preserve the same chain structure that Bitcoin forensics rely on. Wu et al. [22] showed that token swaps and cross-chain transfers can obscure the source of funds in Ethereum heists through contract interactions rather than simple chains of custody. Liu et al. [23] proposed GTN2vec for Ethereum money laundering detection and combined structural and behavioral information, but the approach still depends on recoverable transaction relationships. Benson et al. [24] argued that decentralized exchanges and bridges often fall outside ordinary AML perimeters because they can operate without conventional identity checks and face inconsistent Travel Rule obligations. The detection task therefore moves from following a continuous path to recognizing behavior across fragmented venues.

Stablecoin-specific work points in that direction. FATF identified stablecoin use in sanctions evasion and proliferation-financing contexts [25]. United Nations Office on Drugs and Crime's reporting on TRON-based USDT fits the same pattern: low fees and fast confirmation made TRON-based USDT attractive for cyberfraud and illegal gambling networks in East and Southeast Asia [26]. Fanusie and Isabella [27] similarly linked stablecoin illicit-finance risk to low transaction costs, rapid settlement, and secondary markets without direct issuer-customer relationships. StableAML, the only purpose-built

How to cite this article:
Hamed K, Sorinola M (June 03, 2026) Evaluating the Effectiveness of Blockchain Analytics Tools in Detecting Money Laundering Across Stablecoins. Cureus J Comput Sci 3 : es44389-026-00097-9. DOI https://doi.org/10.7759/s44389-026-00097-9

framework identified for USDT and USDC on Ethereum, found that behavioral wallet features outperformed topology-heavy graph neural network approaches adapted from Bitcoin research [28]. The finding does not make topology irrelevant. It shows that stablecoin AML needs features that capture wallet behavior, contract interaction, token movement, and typology-specific activity, not only graph continuity.

Table *2* summarizes the empirical and technical studies underlying the classifier and stablecoin-specific evidence discussed above.

How to cite this article:
Hamed K, Sorinola M (June 03, 2026) Evaluating the Effectiveness of Blockchain Analytics Tools in Detecting Money Laundering Across Stablecoins. Cureus J Comput Sci 3 : es44389-026-00097-9. DOI https://doi.org/10.7759/s44389-026-00097-9

Study	Architecture	Data	Comparators	Metrics	Key results	Context	Main limitation
Weber et al. [2]	GCN vs. RF	Elliptic BTC, 200K txns, 4,545 illicit labels	RF, GCN, GCN + temporal	F1, acc	RF F1 = 0.81, GCN F1 = 0.69	Benchmark	Single-vendor labels; BTC only
Elmougy & Liu [13]	Multi-model comparison, address-level	Elliptic++ BTC, 822K address nodes, 56 features	RF, XGBoost, LR, MLP	Acc, F1, AUC	Extended address-level classification on larger node set	Benchmark	BTC only; no stablecoin data
Elliptic & MIT-IBM [7,14]	Subgraph classification	Elliptic2 BTC, 200M txns, 122K subgraphs	Subgraph vs. txn-level	Subgraph illicit rate	Smurfing, nested services as dominant typologies	Benchmark	BTC only; single-vendor labels
Alarab & Prakoonwit [15]	Graph-LSTM	Elliptic BTC	GCN, GAT, ML baselines	Acc	97.77% acc	Benchmark	No prec/recall; no stablecoin data
Lawal et al. [4]	TAGCN + SHAP	Elliptic BTC	GCN, GAT, GraphSAGE	Acc, prec, recall, F1, MCC	98.14% acc, F1 = 0.90, MCC=0.89	Benchmark	Majority-class collapse: zero illicit detection
Lin Z et al. [16]	ChronoWave-GNN, wavelet-temporal	Elliptic BTC	GCN, GAT, EvolveGCN	Acc, F1	98.02% acc, F1 = 0.9799	Benchmark	BTC UTXO only; no stablecoin eval
Lo et al. [17]	Inspection-L, self-supervised GNN	Elliptic BTC	GCN, RF, supervised GNN	Prec, recall	Prec = 0.972, Recall = 0.721	Benchmark	BTC only; not tested on stablecoins
Johannessen & Jullum [18]	HMPNN, heterogeneous GNN	DNB Norway, 5M nodes, 10M edges, SAR labels	XGBoost, LR, GraphSAGE	PR AUC, prec@recall	Prec = 84% at 1% recall, Prec = 67% at 50% recall	Deployment	Single bank; not crypto-specific
Effendi & Chattopadhyay [19]	XGBoost under FHE	IBM AML synthetic, balanced + imbalanced	Unencrypted XGBoost	Acc, F1, prec, recall	>99% all metrics, +8% F1 w/ graph features	Synthetic	Synthetic data; real-time infeasible

How to cite this article:
Hamed K, Sorinola M (June 03, 2026) Evaluating the Effectiveness of Blockchain Analytics Tools in Detecting Money Laundering Across Stablecoins. Cureus J Comput Sci 3 : es44389-026-00097-9. DOI https://doi.org/10.7759/s44389-026-00097-9

Wu et al. [22]	EthereumHeist, address classification	ETH hack/scam addresses, custom labels	Traditional ML	Classification acc	Swaps + cross-chain = primary obfuscation	Benchmark	ETH native only; no stablecoin isolation
Liu et al. [23]	GTN2vec, graph embedding	ETH native txns, constructed labels	Node2Vec, DeepWalk	Detection rate	Gas/timestamp features improved detection	Benchmark	Continuous-chain assumption; breaks on stablecoin swaps
Juvinski & Brini [28]	StableAML, tree-ensemble + behavioral	ETH USDT+USDC, 2017-2025, custom labels	GNN (Elliptic benchmarks)	Macro-F1	Stablecoin features > topological GNN	Benchmark (stablecoin)	Single study; labels unverified; no TRON data

TABLE 2: Characteristics of studies evaluating machine learning and blockchain analytics tools for anti-money laundering classification.

Source: Author's compilation.
acc, Accuracy; AUC, Area under the curve; BTC, Bitcoin; ETH, Ethereum; F1, F1-score; FHE, Fully homomorphic encryption; GAT, Graph attention network; GCN, Graph convolutional network; GNN, Graph neural network; HMPNN, Heterogeneous message-passing neural network; LR, Logistic regression; LSTM, Long short-term memory; MCC, Matthews correlation coefficient; MLP, Multi-layer perceptron; PR AUC, Precision-recall area under the curve; prec, Precision; RF, Random forest; SAR, Suspicious activity report; SHAP, Shapley additive explanations; TAGCN, Topology adaptive graph convolutional network; txns, Transactions; UTXO, Unspent transaction output

Compliance, Freezes, and Latency

Regulation has widened the set of actors expected to monitor stablecoin activity. FATF updated Recommendation 16 and reported that 85 of 117 surveyed jurisdictions had passed Travel Rule legislation by 2025, up from 65 in 2024 [29]. Elliptic counted 99 jurisdictions with some version of Travel Rule implementation by the end of 2025 [5]. The European Union Transfer of Funds Regulation applies to cryptoasset transfers from December 2024 and sets no minimum threshold for covered crypto transfers [30]. MiCA adds issuer licensing, reserve, and redemption obligations across the European Union [31]. The GENIUS Act created the first federal U.S. stablecoin framework in July 2025, with implementing regulations due in 2026 [32]. AMLBot reports freeze data for both Tether and Circle [3], while Tether's own disclosures separately document enforcement-related freezes [33]. Organization for Economic Co-operation and Development's (OECD) Crypto-Asset Reporting Framework adds tax-reporting obligations for cross-border crypto-asset activity [34].

Issuer records create a separate stablecoin-specific evidence stream. AMLBot reported high-risk exposure across USDT and USDC, with USDT carrying larger absolute exposure and TRON representing a major share of frozen activity [3]. Freezing gives stablecoin issuers an enforcement lever that Bitcoin does not provide. It also creates measurable questions that the current literature has barely tested: how long does a freeze take, how much value moves before the freeze activates, and where does activity shift afterward?

Coverage is not the same as detection capability. Thresholds differ across jurisdictions. Issuer duties differ from virtual asset service provider (VASP) duties. Decentralized exchanges, peer-to-peer transfers, unlicensed over the counter (OTC) brokers, and bridge protocols can sit outside identity-bearing compliance systems or touch them only briefly [24]. Issuer

freezes can stop value after detection, but the reviewed literature did not identify a standard measure for freeze speed against laundering speed. The unresolved operational question is simple: can detection, escalation, legal review, and freeze execution happen before funds disperse through swaps, bridges, OTC desks, or fiat off-ramps?

Cross-Evidence Synthesis: Where the Evidence Breaks

Blockchain analytics has not failed for lack of technical sophistication. The weak point appears when benchmark success is carried into stablecoin deployment. Bitcoin studies model UTXO transaction topology, but USDT and USDC laundering often passes through account-based transfers, contract calls, swaps, bridges, and short-lived service interfaces. A model can score well on Elliptic-family data and still miss the behavior that matters in stablecoin flows.

Metrics create another blind spot. Accuracy, F1-score, and benchmark rank say little about alert quality when illicit activity has a very low base rate. Compliance teams need to know how many alerts remain useful at an investigation-feasible recall. Johannessen and Jullum's precision-at-recall reporting moves closer to that question than most cryptocurrency classifier studies, but comparable stablecoin evidence is still absent.

The data problem is harder to work around. The Elliptic family made Bitcoin AML research reproducible; no equivalent benchmark exists for USDT or USDC across Ethereum and TRON. Commercial platforms fill part of that gap, but their labels, thresholds, and false-positive rates remain largely closed to independent scrutiny. Stablecoin AML research can already show why Bitcoin-era assumptions weaken. It cannot yet compare detection tools under shared operational conditions.

Discussion

Bitcoin-trained analytics tools still have a place in stablecoin AML work. Their strongest uses, however, sit closer to attribution, risk scoring, and off-ramp triage than to complete transaction-path reconstruction. A tool can identify a risky wallet, link an address to a known service, or support an exchange investigation without solving the harder stablecoin problem: tracing value through contract calls, token swaps, bridge interfaces, OTC brokers, and issuer-controlled freeze mechanisms.

StableAML's behavioral result gives the clearest technical signal in the reviewed literature [28]. Stablecoin laundering does not only alter the asset denomination; it changes the features that carry detection value. UTXO-based tracing rewards continuity. Stablecoin flows often break continuity by design. Account-based ledgers record token balances and contract interactions, while decentralized exchanges and bridges create short, functional handoffs rather than simple ownership chains. Under those conditions, wallet behavior, timing, token choice, interaction with known services, and repeated contract-use patterns may carry more detection value than graph topology alone.

Bitcoin graph methods still matter for benchmarking and for parts of investigative analysis. Commercial tools also retain practical value because exchanges, custodians, sanctions lists, and known illicit services create anchor points. The problem is evidentiary transfer. Accuracy above 97% on Elliptic-family data may show benchmark progress, but it does not show whether an AML team can review the generated alerts, whether the model survives class imbalance, or whether the same features detect USDT and USDC laundering on Ethereum or TRON.

The evaluation problem is as important as the modeling problem. Johannessen and Jullum's precision-at-recall reporting comes closer to AML operations because compliance teams work under alert-volume constraints [18]. A model that detects more suspicious transactions only helps if the alert stream stays reviewable. Most cryptocurrency AML studies still report accuracy, F1-score, or benchmark ranking without showing how many useful alerts remain at investigation-feasible recall. Stablecoin studies need that operational framing even more because illicit activity can move quickly across bridges, decentralized exchanges, and off-ramp services.

Regulation and issuer controls add a separate layer, not a substitute for detection. Travel Rule implementation, MiCA, the GENIUS Act, and the OECD Crypto-Asset Reporting Framework widen the number of actors with monitoring or reporting duties [5,29-34]. Tether and Circle freezes show that stablecoin issuers can intervene after suspicious activity is identified [3,33]. Those powers are valuable, but they act after detection. The unresolved issue is latency. Figure *2* places the latency

How to cite this article:
Hamed K, Sorinola M (June 03, 2026) Evaluating the Effectiveness of Blockchain Analytics Tools in Detecting Money Laundering Across Stablecoins. Cureus J Comput Sci 3 : es44389-026-00097-9. DOI https://doi.org/10.7759/s44389-026-00097-9

problem in operational terms by contrasting the speed of stablecoin laundering with the slower sequence of detection, escalation, legal review, and enforcement response. If funds pass through swaps, bridges, OTC brokers, or fiat off-ramps before escalation and freeze execution, the existence of a freeze function may record enforcement capacity without preventing laundering. Stablecoin AML research needs timing measures: detection delay, escalation delay, legal review delay, freeze execution, pre-freeze value movement, and post-freeze displacement.

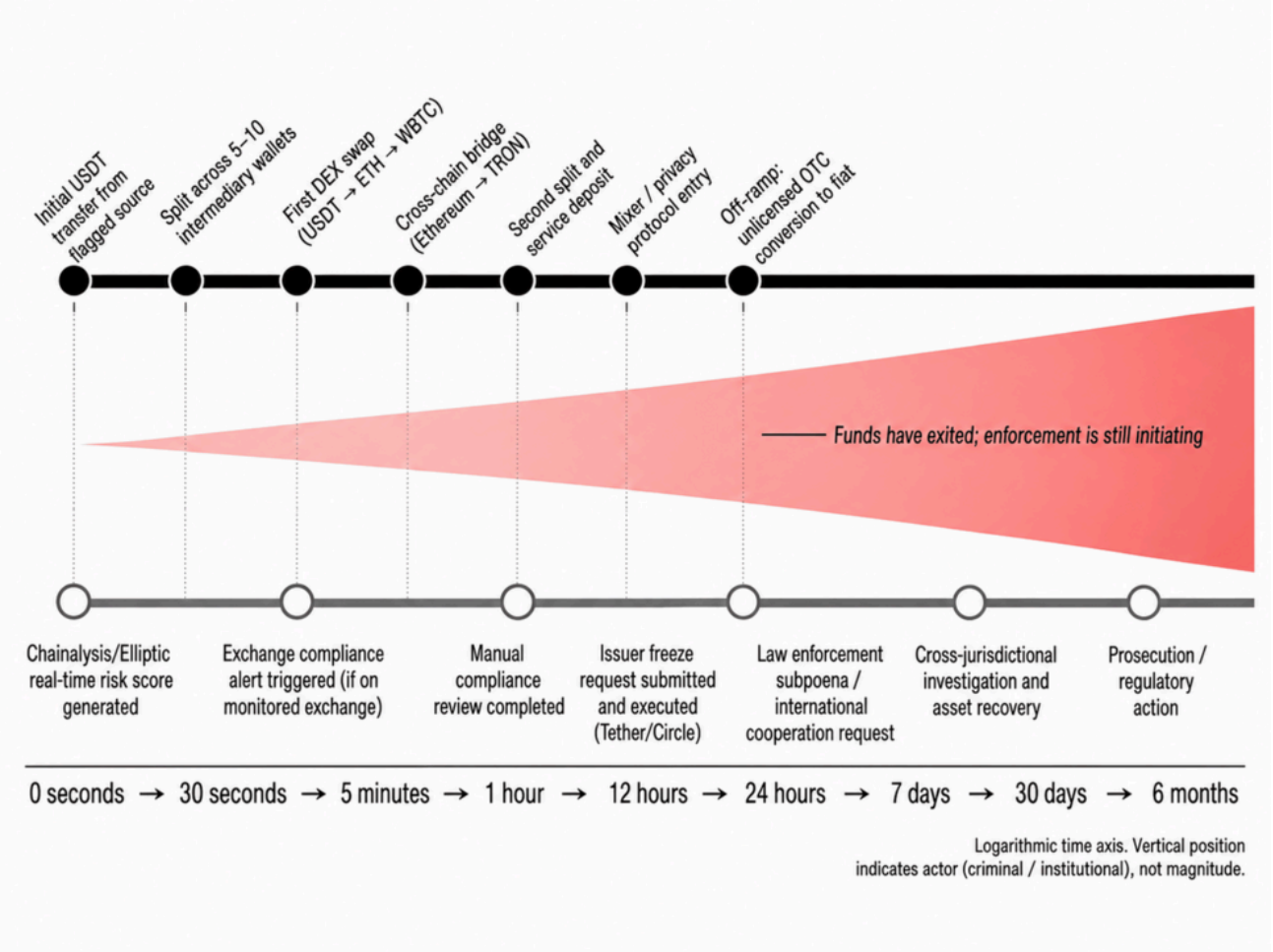

FIGURE 2: Stablecoin laundering velocity versus detection response latency.

Source: Author's creation.
Timeline comparison of stablecoin laundering stages (top) and enforcement response stages (bottom) on a logarithmic time axis. Criminal operations complete within minutes to hours; institutional enforcement responses span hours to months. Vertical position indicates actor type (criminal or institutional), not magnitude.

The practical implication is that stablecoin AML should be evaluated as a joint system. Classifiers, commercial analytics platforms, issuer controls, and compliance rules solve different parts of the workflow. A classifier may rank wallets. A vendor platform may attach service intelligence. A VASP may connect a wallet to an identity. An issuer may freeze tokens. Regulators may require reporting. Treating any one component as the solution hides the weakest handoff between them. The evidence reviewed here points to those handoffs as the places where stablecoin laundering remains hardest to interrupt.

How to cite this article:
Hamed K, Sorinola M (June 03, 2026) Evaluating the Effectiveness of Blockchain Analytics Tools in Detecting Money Laundering Across Stablecoins. Cureus J Comput Sci 3 : es44389-026-00097-9. DOI https://doi.org/10.7759/s44389-026-00097-9

Several limits affect the synthesis. This review did not identify any study that benchmarked commercial platforms and academic classifiers side by side on live stablecoin transaction data. Stablecoin-specific labeled datasets remain scarce, so the evidence depends partly on preprints, industry reports, issuer disclosures, regulatory documents, and vendor documentation. Commercial platforms generally disclose limited information about labeling methods, alert thresholds, false-positive rates, and model updating. These gaps restrict independent comparison and explain why stablecoin AML detection cannot yet be evaluated with the transparency available for Bitcoin benchmark models.

A useful next benchmark would include USDT and USDC activity across Ethereum and TRON, labels derived from enforcement records and issuer freeze lists, and time-stamped events that permit latency analysis. Evaluation would need to report precision at operational recall levels, false-positive burden, detection delay, and displacement after freezes. Vendor audits should test cross-chain tracing, bridge handoffs, decentralized exchange swaps, OTC exposure, and issuer-freeze response under realistic laundering sequences. Those measures would give regulators and compliance teams evidence that maps more closely to stablecoin laundering workflows.

Conclusions

Bitcoin-oriented analytics remain useful for wallet attribution, risk scoring, and exchange investigations. Bitcoin benchmark performance, however, does not establish stablecoin deployment readiness. USDT and USDC laundering often moves through account-based ledgers, contract calls, swaps, bridges, OTC routes, issuer controls, and compliance handoffs that UTXO-centered models were not built to evaluate. Stablecoin AML research needs public labeled datasets, precision-at-recall reporting, latency measures, and independent vendor audits. Without that infrastructure, detection tools will continue to look stronger in benchmark settings than in the operational environments where stablecoin laundering occurs.

Additional Information

Author Contributions

All authors have reviewed the final version to be published and agreed to be accountable for all aspects of the work.

Concept and design: Kehinde Hamed

Acquisition, analysis, or interpretation of data: Kehinde Hamed, Moshood Sorinola

Drafting of the manuscript: Kehinde Hamed, Moshood Sorinola

Critical review of the manuscript for important intellectual content: Kehinde Hamed, Moshood Sorinola

Supervision: Moshood Sorinola

Disclosures

Conflicts of interest: In compliance with the ICMJE uniform disclosure form, all authors declare the following: **Payment/services info:** All authors have declared that no financial support was received from any organization for the submitted work. **Financial relationships:** All authors have declared that they have no financial relationships at present or within the previous three years with any organizations that might have an interest in the submitted work. **Other relationships:** All authors have declared that there are no other relationships or activities that could appear to have influenced the submitted work.

Data Availability Statements

Data sharing is not applicable. This work is theoretical; no datasets were generated or analyzed.

How to cite this article:
Hamed K, Sorinola M (June 03, 2026) Evaluating the Effectiveness of Blockchain Analytics Tools in Detecting Money Laundering Across Stablecoins. Cureus J Comput Sci 3 : es44389-026-00097-9. DOI https://doi.org/10.7759/s44389-026-00097-9

References

1. Chainalysis: The 2025 Crypto Crime Report. (2025). Accessed: April 6, 2026: https://go.chainalysis.com/2025-Crypto-Crime-Report..
2. Weber M, Domeniconi G, Chen J, Weidele DKI, Bellei C, Robinson T, Leiserson CE: Anti-money laundering in bitcoin: experimenting with graph convolutional networks for financial forensics. . Association for Computing Machinery. 2019, 1-7. 10.48550/arXiv.1908.02591
3. AMLBot: Stablecoin Report: USDT and USDC Illicit Activity Study. (2024). Accessed: April 6, 2026: https://umdigital.science/wp-content/uploads/stablecoin-report-2024.pdf.
4. Lawal O, Okolie A, Obunadike C: An explainable graph neural network framework for anti-money laundering in cryptocurrency transactions using the elliptic dataset. International Journal of Network Security & Its Applications. 2025, 17:27-39. 10.5121/ijnsa.2025.17602
5. How Crypto Regulation Changed in 2025: A Global Review. (2025). Accessed: April 6, 2026: https://www.elliptic.co/blog/how-crypto-regulation-changed-in-2025.
6. Labs: Product Documentation and Platform Capabilities. (2023). Accessed: April 6, 2026: https://www.chainalysis.com/product/reactor/.
7. Elliptic: Our New Research: Enhancing Blockchain Analytics Through AI. (2024). Accessed: April 6, 2026: https://www.elliptic.co/blog/our-new-research-enhancing-blockchain-analytics-through-ai.
8. Financial Action Task Force: Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. (2025). Accessed: April 6, 2026: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/guidance-rba-virtual-assets-2021.html.
9. Elliptic: The State of Cross-Chain Crime 2025. (2025). Accessed: April 6, 2026: https://www.elliptic.co/resources/the-state-of-cross-chain-crime-2025.
10. TRM Labs: 2026 Crypto Crime Report. (2026). Accessed: April 6, 2026: https://www.trmlabs.com/reports-and-whitepapers/2026-crypto-crime-report.
11. Chainalysis: 2024 Crypto Money Laundering Report. (2024). Accessed: April 6, 2026: https://www.chainalysis.com/blog/2024-crypto-money-laundering.
12. Hassan MU, Rehmani MH, Chen J: Anomaly detection in blockchain networks: a comprehensive survey. IEEE Communications Surveys & Tutorials. 2022, 25:289-318. 10.1109/comst.2022.3205643
13. Elmougy Y, Liu L: Demystifying fraudulent transactions and illicit nodes in the bitcoin network for financial forensics. Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining. 2023, 3979-90. 10.1145/3580305.3599803
14. Bellei C, Xu M, Phillips R, et al.: The shape of money laundering: subgraph representation learning on the blockchain with the Elliptic2 dataset. KDD MLF '24: KDD Workshop on Machine Learning in Finance. KDD MLF '24: KDD Workshop on Machine Learning in Finance. 2024, 1-7. 10.48550/arXiv.2404.19109
15. Alarab I, Prakoonwit S: Graph-based LSTM for anti-money laundering: experimenting temporal graph convolutional network with bitcoin data. Neural Processing Letters. 2022, 55:689-707. 10.1007/s11063-022-10904-8
16. Lin Z, Luo Q, Wu D, Shen J, Li L, Nong X, Qin Z: Detecting illicit transactions in bitcoin: a wavelet-temporal graph transformer approach for anti-money laundering. Scientific Reports. 2026, 16:1-17. 10.1038/s41598-025-23901-3
17. Lo WW, Kulatilleke GK, Sarhan M, Layeghy S, Portmann M: Inspection-L: self-supervised GNN node embeddings for money laundering detection in bitcoin. Applied Intelligence. 2023, 53:19406-19417. 10.1007/s10489-023-04504-9
18. Johannessen F, Jullum M: Finding money launderers using heterogeneous graph neural networks. The Journal of Finance and Data Science. 2025, 11:100273. 10.1016/j.jfds.2025.100175
19. Effendi F, Chattopadhyay A: Privacy-preserving graph-based machine learning with fully homomorphic encryption for collaborative anti-money laundering. Security, Privacy, and Applied Cryptography Engineering. Knechtel, J. (ed): Springer, Cham; 2025. 15351:80-105. 10.1007/978-3-031-80408-3_6
20. Foley S, Karlsen JR, Putniņš TJ: Sex, drugs, and bitcoin: how much illegal activity is financed through cryptocurrencies?. The Review of Financial Studies. 2019, 32:1798-1853. 10.1093/rfs/hhz015

How to cite this article:
Hamed K, Sorinola M (June 03, 2026) Evaluating the Effectiveness of Blockchain Analytics Tools in Detecting Money Laundering Across Stablecoins. Cureus J Comput Sci 3 : es44389-026-00097-9. DOI https://doi.org/10.7759/s44389-026-00097-9

21. Carpentier-Desjardins C, Paquet-Clouston M, Kitzler S, Haslhofer B: Mapping the DeFi crime landscape: an evidence-based picture. Journal of Cybersecurity. 2025, 11:1-19. 10.1093/cybsec/tyae029

22. Wu J, Lin D, Fu Q, Yang S, Chen T, Zheng Z, Song B: Toward understanding asset flows in crypto money laundering through the lenses of ethereum heists. IEEE Transactions on Information Forensics and Security. 2023, 19:1994-2009. 10.1109/tifs.2023.3346276

23. Liu J, Yin C, Wang H, Wu X, Lan D, Zhou L, Ge C: Graph embedding-based money laundering detection for ethereum. Electronics. 2023, 12:1-14. 10.3390/electronics12143180

24. Benson V, Turksen U, Adamyk B: Dark side of decentralised finance: a call for enhanced AML regulation based on use cases of illicit activities. Journal of Financial Regulation and Compliance. 2023, 32:80-97. 10.1108/jfrc-04-2023-0065

25. Financial Action Task Force: Targeted Report on Stablecoins and Unhosted Wallets - Peer-to-Peer Transactions. (2026). Accessed: April 6, 2026: https://www.fatf-gafi.org/en/publications/Virtualassets/targeted-report-stablecoins-unhosted-wallets.html.

26. United Nations Office on Drugs and Crime: Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia. (2024). Accessed: April 6, 2026: https://www.unodc.org/roseap/uploads/documents/Publications/2024/Casino_Underground_Banking_Report_2024.pdf.

27. Fanusie YJ, Isabella T: Stablecoin markets and mitigating illicit finance. Georgetown University Center for Financial Markets and Policy. 2025, 1-14.

28. Juvinski L, Brini A: StableAML: machine learning for behavioral wallet detection in stablecoin anti-money laundering on ethereum. arXiv. 2026, 1-27. 10.48550/arXiv.2602.17842

29. Financial Action Task Force: Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers. (2025). Accessed: April 6, 2026: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2025.html.

30. European Union: Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets (Transfer of Funds Regulation). (2023). Accessed: April 6, 2026: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1113.

31. European Parliament and Council of the European Union: Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA. (2023). Accessed: April 6, 2026: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1114.

32. Guiding and Establishing National Innovation for U.S. Stablecoins (GENIUS) Act. (2025). Accessed: April 8, 2026: https://www.congress.gov/bill/119th-congress/senate-bill/1582.

33. International Compliance Association: Stablecoins: The New Epicentre of Crypto Fraud. (2025). Accessed: April 8, 2026: https://www.int-comp.org/insight/stablecoins-the-new-epicentre-of-crypto-fraud/.

34. Organisation for Economic Co-operation and Development: International Standards for Automatic Exchange of Information in Tax Matters: Crypto-Asset Reporting Framework and 2023 update to the Common Reporting Standard. OECD Publishing. 2023, 1-139. 10.1787/896d79d1-en

How to cite this article:
Hamed K, Sorinola M (June 03, 2026) Evaluating the Effectiveness of Blockchain Analytics Tools in Detecting Money Laundering Across Stablecoins. Cureus J Comput Sci 3 : es44389-026-00097-9. DOI https://doi.org/10.7759/s44389-026-00097-9