Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Under the hood of The Blockchain: Forensic Analysis, Obfuscation Vectors, and Evolving Global Regulatory Frameworks

Mohammad Saeed Ahmed

30059693@students.southwales.ac.uk

University of South Wales

Nisha Rawindaran

University of South Wales

Richard Ward

University of South Wales

Research Article

Keywords: Blockchain Forensics, Address Clustering, Obfuscation Vectors, Crypto-Assets Regulation, Anti-Money Laundering

Posted Date: November 25th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-11549885/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Abstract

This study critically evaluates the evolving dynamic between advanced blockchain obfuscation methodologies, forensic tracking capabilities, and statutory regulatory regimes. The proliferation of pseudonymous public-ledger architectures has enabled criminal syndicates and state-sponsored adversaries to execute sophisticated capital flight and laundering operations. This paper evaluates the forensic efficacy of address-clustering heuristics, specifically multi-input co-spending and change-address identification—against modern obfuscation vectors, including peel chains, cross-chain swaps, zero-knowledge mixing protocols, and transactional history manipulation (dusting and dandruff attacks). Furthermore, the study analyses the structural impact of primary global regulatory instruments, including the European Union Markets in Crypto-Assets Regulation (Regulation (EU) 2023/1114), the United Kingdom Financial Services and Markets Act 2023 regulatory perimeter, and United States digital asset broker reporting mandates under 26 U.S. Code 6045 and Form 1099-DA. Through a structured critical review synthesising empirical benchmark literature and primary statutory instruments, this paper establishes that while heuristic address-clustering de-anonymises standard multi-input Unspent Transaction Output (UTXO) transactions, its analytical precision degrades significantly when confronted with non-standard script permutations and zero-knowledge architectures. In response, statutory compliance frameworks are systematically constraining adversarial off-ramps by targeting fiat conversion gateways.

1 Introduction

Public blockchain architectures embody an inherent operational tension between decentralised financial autonomy and cryptographic traceability (Narayanan et al., 2016). Designed to operate in the absence of central clearinghouses, distributed ledgers deploy public-key cryptography and consensus mechanisms to enforce transaction immutability and eliminate double-spending without intermediary trust anchors (Nakamoto, 2008). However, the pseudonymous architecture of public ledgers has established them as an attractive conduit for illicit capital flight, ransomware extortion, and adversarial financing (Furneaux, 2018; CISA, 2020).

To rigorously assess the operational limits of blockchain de-anonymisation and compliance enforcement, this research addresses three primary research questions:

- **RQ1**: What is the forensic precision, boundary limitation, and empirical false-positive rate of address-clustering heuristics when deployed against advanced obfuscation vectors, including peel chains, CoinJoin protocols, and zero-knowledge mixing systems? (Meiklejohn et al., 2016; Zhang, Wang and Luo, 2020).
- **RQ2**: How do adversarial actors deploy transactional obfuscation vectors, specifically peel chains, cross-chain bridge hopping, zero-knowledge tumblers, and transaction-history where spoofing is used to evade detection and subvert forensic graphs? (Mikhaylov et al., 2025; The MITRE Corporation, 2025).

- **RQ3**: In what ways do primary statutory frameworks, specifically the European Union Markets in Crypto-Assets Regulation (MiCA), the UK Financial Conduct Authority (FCA) regulatory perimeter under FSMA 2023, and US Department of the Treasury broker reporting mandates under 26 U.S.C. § 6045 constrain adversarial evasion strategies and alter global compliance dynamics? (European Parliament and Council of the European Union, 2023; Great Britain. Parliament, 2023a; US Department of the Treasury and Internal Revenue Service, 2024).

To address these questions, this paper employs a structured critical review methodology informed by University of South Wales research principles, synthesising peer-reviewed empirical forensic evaluations with primary statutory texts and supervisory policy frameworks. The subsequent sections establish foundational ledger mechanics, evaluate forensic clustering limitations, contrast statutory enforcement against adversarial countermeasures, and synthesise the findings within an integrated analytical typology.

2 Literature Review

The architectural foundation of distributed ledgers stems from Satoshi Nakamoto's proposal for a peer-to-peer electronic cash system designed to resolve the double-spending problem without sovereign central clearinghouses or trusted third parties (Nakamoto, 2008; Furneaux, 2018; Hill et al., 2018):

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. — Satoshi Nakamoto (2008)

Traditional electronic settlement systems rely on multi-tier financial intermediaries acting as clearinghouses. As illustrated in Fig. 1, credit and debit card transactions traverse multi-party settlement chains encompassing cardholders, merchants, acquirers, card networks, and issuing institutions (Hill et al., 2018, p. 41). This framework introduces counterparty risk, inter-bank settlement delays, and centralised points of institutional vulnerability (Hill et al., 2018).

In contrast to sovereign fiat currencies, which derive authority from legal tender designations, public cryptocurrency ledgers rely on cryptographic verification and distributed consensus algorithms (Hill et al., 2018). Forensic analysis of these systems relies upon systemic ledger traceability (Meiklejohn et al., 2016). To evaluate this systematically, core privacy concepts must be formally distinguished (Meiklejohn et al., 2016; Narayanan et al., 2016; Hill et al., 2018):

- Pseudonymity: Transacting via cryptographic public-key hashes rather than authenticated real-world identities (Hill et al., 2018).
- Anonymity: The complete absence of identity association or network linkage to a physical entity (Furneaux, 2018).

- Confidentiality: The state where transaction amounts, sender/receiver states, and balance data are encrypted or mathematically obscured from public audit (Narayanan et al., 2016).
- Unlinkability: The inability of an observer to correlate multiple distinct transactions or addresses as belonging to the same controlling entity (Meiklejohn et al., 2016).

3 Methodology

This study adopts a structured critical review methodology adhering to University of South Wales research standards to assess empirical forensic literature and binding statutory frameworks. To resolve the methodological tension between technical benchmarking literature and legislative policy texts, the protocol implements an explicit dual-tier corpus strategy.

3.1 Search Strategy and Database Querying

The literature retrieval was executed between 5 January 2026 and 20 January 2026, sampling records published between January 2016 and January 2026 to capture the operational transition from single-chain heuristics to cross-chain, zero-knowledge, and modern statutory compliance regimes. Four primary bibliographic databases were systematically queried: IEEE Xplore, ACM Digital Library, Scopus, and Web of Science (WoS).

The search protocol deployed Boolean search expressions adapted for database-specific indexing syntax:

("blockchain forensics" OR "address clustering" OR "de-anonymisation") AND ("obfuscation" OR "CoinJoin" OR "mixing protocol" OR "cross-chain") AND ("MiCA" OR "FCA" OR "IRS Form 1099-DA" OR "AML/CTF").

Database-specific query adaptations included parsing strings to abstract and keyword fields in Scopus (TITLE-ABS-KEY) and Web of Science (TS), while targeting publication titles and abstracts within IEEE Xplore and the ACM Digital Library.

3.2 Corpus Screening, Eligibility Criteria, and Quality Appraisal

The search protocol identified 342 records across the four databases. Following deduplication (yielding 289 unique records), titles and abstracts were screened against predefined eligibility criteria. Studies were excluded if they: (a) evaluated closed consortium ledgers without public off-ramps; (b) consisted of promotional industry blog posts, vendor marketing, or informal forums; or (c) lacked verifiable empirical experimental data or primary legal documentation.

The resulting corpus of 31 sources was partitioned into two distinct analytical tiers:

- **Tier 1**: Peer-Reviewed Academic Corpus ($n = 18$): Empirical benchmark studies, address-clustering algorithms, and cryptographic proofs published in indexed journals or peer-reviewed proceedings. Quality appraisal was conducted using a structured technical evaluation rubric assessing benchmark reproducibility, dataset size, clarity of ground-truth validation, and methodological disclosure of error rates.
- **Tier 2**: Primary Statutory and Supervisory Corpus ($n = 13$): Direct legislative instruments, official government regulations, and supervisory policy roadmaps issued by competent authorities (e.g. European Parliament, HM Treasury, US Federal Register, FCA, EBA, CISA). Quality appraisal required formal confirmation of statutory enactment, jurisdictional enforceability, and direct institutional authorship, strictly excluding unverified commercial digests.

4 Results/Findings/Analysis

4.1 Ledger Mechanics and Obfuscation Architecture

Public distributed ledgers function as append-only state machines secured cryptographically through sequential block hashing (Hill et al., 2018). In Proof-of-Work (PoW) networks such as Bitcoin, transactions are batched into blocks anchored by Block 0 (the Genesis Block) (Hill et al., 2018). Distributed consensus requires solving a computationally asymmetric puzzle: discovering an arbitrary integer—the Nonce—which, when combined with the block header data and hashed via SHA-256, produces an output below the network difficulty target (Narayanan et al., 2016).

Ledger tracking depends directly on the accounting model deployed at the base protocol layer (Chakravarty et al., 2020; Melo et al., 2024):

- Account-Based Architecture (e.g. Ethereum): Maintains global state as a key-value mapping of persistent balances, where transactions mutate state balances directly (Jamwal et al., 2024). Forensic tracing follows directed acyclic graphs (DAGs) between explicit account addresses (Jamwal et al., 2024).
- Unspent Transaction Output (UTXO) Architecture (e.g. Bitcoin): Balances are not tracked as static variables; instead, transactions consume pre-existing UTXOs entirely as inputs and instantiate new outputs (Chakravarty et al., 2020; Melo et al., 2024). When the combined value of input UTXOs exceeds the required payment, the remaining balance must be redirected to a freshly generated change address controlled by the sender (Melo et al., 2024; Wang et al., 2024).

Standard Bitcoin transactions employ Pay-to-Public-Key-Hash (P2PKH) scripts, where public keys undergo SHA-256 and RIPEMD-160 hashing before Base58Check encoding (Walker, 2025). Unlocking the UTXO requires providing the public key and a valid cryptographic signature satisfying the script condition (Hill et al., 2018).

Adversarial syndicates exploit these ledger structures through specific evasion pipelines (Furneaux, 2018; Kim et al., 2025):

- **Peel Chains**: A sequential layering process where large balances are systematically split across a prolonged chain of transactions, peeling minor sums to intermediate un-hosted wallets while directing the dominant remainder to fresh change addresses (Lantz, 2021; Mikhaylov et al., 2025). This technique elongates transaction graphs to disrupt heuristic tracing tools.
- **Cross-Chain Swaps (Chain Hopping)**: The rapid migration of assets across disparate ledgers via automated market makers (AMMs) and bridging protocols (The MITRE Corporation, 2025). Moving from transparent UTXO chains to smart contract networks or privacy assets exploits visibility boundaries between isolated consensus ledgers, fracturing forensic timelines (The MITRE Corporation, 2025).

4.2 Forensic Address Clustering: Heuristics, Error Rates, and Protocol Countermeasures

Digital forensics investigators utilise address-clustering heuristics to de-anonymise wallet clusters and associate pseudonymous public addresses with single controlling entities (Caringella et al., 2024). In UTXO-based blockchains, clustering relies primarily on two fundamental heuristics (Meiklejohn et al., 2016; Zhang, Wang and Luo, 2020):

1. Multi-Input Co-Spending Heuristic: Posits that if a single transaction consumes multiple UTXOs as inputs, all corresponding input addresses are controlled by the same entity holding the private keys necessary to sign the transaction (Meiklejohn et al., 2016; Ermilov, Panov and Yanovich, 2017).
2. Change Address Identification Heuristic: Analyses transaction outputs to detect newly generated return addresses controlled by the sender by evaluating deterministic features, including address script types, value decimal structures, and output ordering (Meiklejohn et al., 2016; Wang et al., 2024).

4.2.1 Empirical Accuracy and Failure Rates

While effective under standard conditions, these heuristics face significant analytical boundaries (Zhang, Wang and Luo, 2020). In their seminal empirical benchmark, Meiklejohn et al. (2016) evaluated the change-address identification heuristic across a dataset containing over 3.3 million clustered addresses validated against ground-truth service transactions. They demonstrated that without introducing temporal delay constraints (such as observing unspent outputs over a seven-day window), unrefined change-identification heuristics yield a false-positive attribution error rate of 17.1%. When wallet clients deploy randomised output indexing or transactions generate multiple change destinations, false-positive error rates frequently exceed 20% (Meiklejohn et al., 2016; Ermilov, Panov and Yanovich, 2017; Zhang, Wang and Luo, 2020).

Modern evasion vectors degrade this precision further:

Coi

• nJoin Subversion: Multi-party mixing protocols combine inputs from multiple independent participants into a unified atomic transaction with uniform output denominations (Meiklejohn et al., 2016). This deliberately subverts H1: tracking algorithms erroneously conclude that all input addresses belong to a single entity, inducing severe super-clustering errors that corrupt forensic graphs (Meiklejohn et al., 2016)

- zk-SNARK Mixers: Privacy architectures such as Tornado Cash server ledger linkability entirely using Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge (zk-SNARKs) (Chainalysis Team, 2022b; Thürkauf, 2023). Users deposit fixed denominations into a pooled smart contract, receiving a private commitment note (Thürkauf, 2023). Cryptographic proofs permit withdrawal to an unlinked address without exposing the deposit transaction hash (Chainalysis Team, 2022a; Thürkauf, 2023). Forensic re-identification is impossible on-chain and depends entirely on user Operational Security (OpSec) errors: temporal correlation, identical gas fees, or relayer attribution via KYC-regulated gateways (Thürkauf, 2023).
- Transaction History Manipulation (Dusting vs Dandruff Attacks): It is critical to distinguish transaction history contamination from capital flight (Mikhaylov et al., 2025). Dusting attacks distribute unsolicited micro-token amounts to public addresses; when a victim inadvertently spends this dust as an input in a future transaction, H1 is triggered, unmasking previously unlinked addresses (Mikhaylov et al., 2023). Conversely, 'dandruff' attacks inject zero-value transfer event logs into account-based EVM networks, spoofing transaction history records to trick users into copying look-alike addresses (Mikhaylov et al., 2023). Dandruff attacks function strictly as deceptive reconnaissance vectors; actual laundering requires downstream capital flight through bridges and liquidity pools (Mikhaylov et al., 2025; The MITRE Corporation, 2025).

Table 1
Critical Typology of Obfuscation Vectors and Forensic Countermeasures

Obfuscation Vector	Operational Mechanism	Forensic Tracking Mechanism	Empirical Limitations & Failure Modes
Peel Chains	Sequential low-value transfers peeling funds into intermediate un-hosted wallets.	Change address heuristics, graph analysis, and volume profiling.	Subverted by non-standard script formats and randomised change indices.
CoinJoin Protocols	Multi-party transaction merging with uniform output amounts.	Subgraph analysis, timing correlation, and transaction fee contribution auditing.	Forces false-positive multi-input co-spending assumptions.
zk-SNARK Mixers	Cryptographic zero-knowledge proofs breaking on-chain input-output linkability.	OpSec auditing: gas price patterns, temporal correlation, relayer KYC tracing.	Zero mathematical linkage on-chain; relies entirely on external user OpSec errors.
Cross-Chain Swaps	Asset migration across heterogeneous chains via bridges and AMM pools.	Cross-ledger liquidity bridge monitoring, lock-and-mint event pairing.	Forensic blind spots across un-indexed Layer-1/Layer-2 bridges.
Dandruff / Dusting	Unsolicited distribution of micro-tokens or zero-value transfer log injection.	UTXO taint tracking, visual graph filtering, event log signature parsing.	Can generate forensic noise and contaminate address-clustering datasets.

Table 1 establishes an integrated analytical typology demonstrating that while individual on-chain heuristics exhibit defined technical failure modes, contemporary compliance regimes operate as a compound defence model. Where cryptographic mixing severs mathematical links on-chain, statutory frameworks eliminate the financial utility of obfuscation by closing off-ramps into the fiat economy.

4.3 Evolving Statutory and Regulatory Regimes

Table 1 establishes an integrated analytical typology demonstrating that while individual on-chain heuristics exhibit defined technical failure modes, contemporary compliance regimes operate as a compound defence model. Where cryptographic mixing severs mathematical links on-chain, statutory frameworks eliminate the financial utility of obfuscation by closing off-ramps into the fiat economy.

4.3.1 United States Statutory Broker Rules

In the United States, digital assets are classified as property under Internal Revenue Service Notice 2014-21. To eliminate reporting loopholes historically exploited via unhosted peel chains, the US Department of the Treasury finalised binding regulations under 26 U.S. Code § 6045, introducing IRS Form 1099-DA (US Department of the Treasury and Internal Revenue Service, 2024).

Under 26 CFR Part 1 (TD 10000), custodial digital asset brokers, centralized trading platforms, and hosted wallet providers must report gross proceeds and adjusted cost-basis information for customer

transactions (US Department of the Treasury and Internal Revenue Service, 2024). This statutory chokepoint neutralises the core objective of peel chains: while an adversary can move assets through intermediate hops on-chain, converting those assets to fiat or real-world goods requires identity verification and taxable reporting at compliant broker endpoints (US Department of the Treasury and Internal Revenue Service, 2024). At the federal legislative level, initiatives such as the Financial Innovation and Technology for the 21st Century Act (FIT21) seek to delineate jurisdictional boundaries between the CFTC and SEC based on statutory decentralisation thresholds.

4.3.2 European Union: Markets in Crypto-Assets (MiCA)

The European Union established a comprehensive, harmonised statutory regime through Regulation (EU) 2023/1114 on Markets in Crypto-assets (MiCA) (European Parliament and Council of the European Union, 2023). MiCA eliminates internal regulatory arbitrage by establishing uniform licensing requirements for Crypto-Asset Service Providers (CASPs) across the EU Single Market (European Parliament and Council of the European Union, 2023).

Under MiCA Title V, CASPs must obtain formal authorisation from their National Competent Authority (NCA) and comply with the EU Transfer of Funds Regulation (Regulation (EU) 2023/1113) (European Parliament and Council of the European Union, 2023). CASPs must verify the originating identity of transfers from un-hosted wallets, constraining the utility of mixing services: non-compliant, pooled, or anonymised funds face immediate transaction blocking or enhanced due diligence upon reaching European regulated gateways (European Parliament and Council of the European Union, 2023). Furthermore, Title VI establishes explicit prohibitions against market manipulation, insider dealing, and misleading social promotions, establishing criminal and administrative liability for influencer-led rug pulls (European Parliament and Council of the European Union, 2023).

4.3.3 United Kingdom Statutory Framework

In the United Kingdom, statutory oversight operates under the Financial Services and Markets Act 2000 (FSMA), as amended by the Financial Services and Markets Act 2023 (Great Britain. Parliament, 2023a). Section 69 of FSMA 2023 brought cryptoassets within the scope of regulated financial activities, granting the Financial Conduct Authority (FCA) direct supervisory authority over stablecoins, exchange operators, and custody activities (Great Britain. Parliament, 2023a; Financial Conduct Authority, 2024).

The UK statutory framework integrates anti-money laundering controls under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 with the statutory Financial Promotions Regime enacted in October 2023 (Financial Conduct Authority, 2024). This regime prohibits unauthorised firms from marketing digital assets to UK consumers without explicit regulatory approval, constraining speculative recruitment pipelines. In parallel, the statutory 'Failure to Prevent Fraud' offence under the Economic Crime and Corporate Transparency Act 2023 establishes corporate liability for financial institutions that fail to implement reasonable fraud prevention procedures, compelling UK banks and exchanges to deploy automated clustering and taint-analysis filters (Great Britain. Parliament, 2023b).

4.3.4 International Initiatives and Geopolitical Cyber Warfare

Beyond Western jurisdictions, national governments are deploying sovereign blockchain initiatives alongside strict regulatory controls. Concurrently, state-level actors engage in geopolitical cyber activities, using dedicated units to exploit protocols for sovereign financing and sanction evasion, highlighting the dual-use nature of distributed ledger technologies (CISA, 2020). Because cryptographic mixing can defeat purely mathematical heuristics, law enforcement agencies increasingly rely on cross-border regulatory alignment, fiat gateway chokepoints (KYC/AML regulated exchanges), operational security errors, and seized server infrastructure to attribute identity and recover stolen assets (Furneaux, 2018; Crown Prosecution Service, 2025).

5 Limitations

This critical review has several analytical limitations. First, the literature corpus is restricted to English-language academic indexing services and Western regulatory frameworks, which may omit proprietary tracking techniques developed by private analytics firms or legislative frameworks in Asian jurisdictions. Second, the empirical evaluation of heuristic failure rates relies on historical benchmark datasets; as wallet software adopts custom coin-selection algorithms and Layer-2 rollups, heuristic precision may vary. Third, regulatory enforcement remains uneven across international boundaries, allowing adversarial actors to exploit non-compliant off-shore jurisdictions for fiat liquidation. Finally, the accelerating pace of zero-knowledge developments and legislative reforms means that compliance standards must be continuously reassessed.

6 Conclusion

This research evaluated the complex interaction between public ledger mechanics, forensic address clustering, adversarial obfuscation, and emerging statutory regimes. While distributed ledgers provide immutable transparency, their pseudonymous architecture enables an ongoing arms race between illicit syndicates and forensic investigators.

Forensic address clustering based on multi-input co-spending and change-address heuristics provides reliable tracing across standard UTXO ledgers (Zhang, Wang and Luo, 2020). However, its analytical precision degrades significantly when encountering multi-party CoinJoin transactions, zero-knowledge mixing protocols, and cross-chain bridge hopping (Thürkauf, 2023). In response, statutory regulatory frameworks, notably the EU MiCA Regulation, UK FSMA 2023 perimeter expansions, and US Treasury broker reporting rules under 26 U.S.C. 6045—are establishing enforceable compliance choke-points at fiat off-ramps. Ultimately, mitigating illicit blockchain activity requires pairing technical on-chain heuristics with international statutory alignment, ensuring that cryptographic obfuscation cannot easily convert illicit digital assets into the sovereign fiat economy.

Declarations

Author Contribution

M.S.A. conceived the study, conducted the literature retrieval and corpus screening, performed the technical and statutory analyses, and wrote the main manuscript text. N.R. and R.W. supervised the research, contributed to the conceptual framework and methodology, and critically revised the manuscript for important intellectual content. All authors reviewed and approved the final manuscript.

References

1. Caringella, M., Violante, F., Lucci, F.D., Galantucci, S. and Costantini, M. (2024) 'BACH: a tool for analyzing blockchain transactions using address clustering heuristics', *Information*, 15(10), p. 589. Available at: https://doi.org/10.3390/info15100589.
2. *Chainalysis Team* (2022a) *Crypto mixers and AML compliance*. Available at: https://www.chainalysis.com/blog/crypto-mixers/ (Accessed: 13 March 2026).
3. *Chainalysis Team* (2022b) *Understanding Tornado Cash, its sanctions implications, and key compliance questions*. Available at: https://www.chainalysis.com/blog/tornado-cash-sanctions-challenges/ (Accessed: 25 March 2026).
4. Chakravarty, M.M.T., Chapman, J., MacKenzie, K., Melkonian, O., Peyton Jones, M. and Wadler, P. (2020) 'The extended UTXO model', in Bernhard, M., Bracciali, A., Gudgeon, L., Haines, T., Klages-Mundt, A., Matsuo, S., Perez, D., Sala, M. and Werner, S. (eds) *Financial cryptography and data security*. Cham: Springer, pp. 525–539. Available at: https://doi.org/10.1007/978-3-030-54455-3_37.
5. *CISA* (2020) *Guidance on the North Korean cyber threat*. Available at: https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-106a (Accessed: 4 March 2026).
6. *Crown Prosecution Service* (2025) *Ex-NCA officer jailed for theft of 50 Bitcoin now worth £4.4m during investigation into crime on dark web*. Available at: https://www.cps.gov.uk/cps/news/ex-nca-officer-jailed-theft-50-bitcoin-now-worth-ps44m-during-investigation-crime-dark-web (Accessed: 2 January 2026).
7. Ermilov, D., Panov, M. *and* Yanovich, Y. (2017) 'Automatic Bitcoin address clustering', in *2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA)*. Cancun, Mexico, 18–21 December 2017. Piscataway: IEEE, pp. 461–466. Available at: https://doi.org/10.1109/ICMLA.2017.0-118.
8. *European Banking Authority* (2024) *Regulatory Technical Standards on the information to be provided in an application for authorisation as a crypto-asset service provider under Regulation (EU) 2023/1114*. Paris: European Banking Authority.
9. *European Parliament and Council of the European Union* (2023) *Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU)*

2019/1937. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1114 (Accessed: 15 January 2026).

10. Financial Conduct *Authority* (2024) *FCA crypto roadmap*. London: Financial Conduct Authority.
11. Financial Conduct Authority (2025) *Information for firms looking to offer crypto exchange traded notes*. Available at: https://www.fca.org.uk/news/statements/information-firms-offer-crypto-exchange-traded-notes (Accessed: 2 January 2026).
12. *Financial Crimes Enforcement Network* (2023) *Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern*, 31 CFR Part 1010. *Federal Register*, 88(214), pp. 76796–76813.
13. Furneaux, N. (2018) *Investigating cryptocurrencies: understanding, extracting, and analyzing blockchain evidence*. Indianapolis: John Wiley & Sons.
14. Great Britain. *Parliament* (2017) *The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017*, SI 2017/692. London: The Stationery Office.
15. *Great Britain. Parliament* (2023a) *Financial Services and Markets Act 2023*, c. 29. London: The Stationery Office.
16. *Great Britain. Parliament* (2023b) *Economic Crime and Corporate Transparency Act 2023*, c. 56. London: The Stationery Office.
17. Hill, B., Chopra, S., Valencourt, P. and Prusty, N. (2018) *Blockchain developer's guide*. Birmingham: Packt Publishing.
18. *Internal Revenue Service* (2014) *IRS Virtual Currency Guidance*, Notice 2014-21. Washington, D.C.: Internal Revenue Service.
19. Jamwal, S., Cano, J., Lee, G.M., Tran, N.H. and Truong, N. (2024) 'A survey on Ethereum pseudonymity: techniques, challenges, and future directions', *Journal of Network and Computer Applications*, 232, p. 104019. Available at: https://doi.org/10.1016/j.jnca.2024.104019.
20. Kim, K., Lee, S., Ramachandran, S. and Alzahrani, I. (2025) 'Cryptocurrency-driven ransomware syndicates operating on the darknet: a focused examination of the Arab world', *Egyptian Informatics Journal*, 30, p. 100665. Available at: https://doi.org/10.1016/j.eij.2025.100665.
21. Lantz, L. (2021) *Mastering blockchain: unlocking the power of cryptocurrencies, smart contracts, and decentralized applications*. Sebastopol: O'Reilly Media.
22. Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M. and Savage, *S.* (2016) 'A fistful of Bitcoins: characterizing payments among men with no names', *Communications of the ACM*, 59(4), pp. 86–93. Available at: https://doi.org/10.1145/2896384.
23. Melo, D., Pomares-Hernández, S.E., Rodríguez-Henríquez, L.M.X. and Pérez-Sansalvador, J.C. (2024) 'Unlocking blockchain UTXO transactional patterns and their effect on storage and throughput trade-offs', *Computers*, 13(6), p. 146. Available at: https://doi.org/10.3390/computers13060146.
24. Mikhaylov, D., Kutin, A., Anderson, J. *and* Falaleev, M. (2023) 'Analysis of the "dandruff attack" on the Tron network: risks, damage assessment, and solutions', *Journal of Information Security and*

Cybercrimes Research, 6(1), pp. 1–11. Available at: https://doi.org/10.26735/KQGU9199.

25. Mikhaylov, D., Kutin, A., Anderson, J., Falaleev, M., Sandzhiev, D. and Emam, H. (2025) 'Cryptocurrency fund appropriation techniques: analysis of strategies for "laundering" and withdrawing stolen digital assets', *Journal of Information Security and Cybercrimes Research*, 8(1), pp. 93–110. Available at: https://doi.org/10.26735/CZJK4881.
26. Nakamoto, S. (2008) *Bitcoin: a peer-to-peer electronic cash system*. Available at: https://bitcoin.org/bitcoin.pdf (Accessed: 28 February 2026).
27. Narayanan, A., Bonneau, J., Felten, E., Miller, A. and Goldfeder, *S.* (2016) *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton: Princeton University Press.
28. The MITRE Corporation (2025) *Cross-chain swaps (hopping) | MITRE AADAPT™*. Available at: https://aadapt.mitre.org/techniques/ADT3005/ (Accessed: 10 March 2026).
29. Thürkauf, D. (2023) 'Address clustering heuristics for account-based blockchain networks: an analysis based on a Decentraland user set', *SSRN Electronic Journal*. Available at: https://doi.org/10.2139/ssrn.4589925.
30. *US Department of the Treasury and Internal Revenue Service* (2024) *Gross proceeds and basis reporting by brokers and determination of realized gain or loss for specified digital asset transactions*, 26 CFR Part 1, TD 10000. *Federal Register*, 89(132), pp. 56410–56512.
31. Walker, G. (2025) *P2PKH | Pay to Public Key Hash*. Available at: https://learnmeabitcoin.com/technical/script/p2pkh/ (Accessed: 6 March 2026).
32. Wang, K., Cheng, Y., Tong, M.W., Niu, Z., Pang, J. *and* Han, W. (2024) 'Exploring unconfirmed transactions for effective Bitcoin address clustering', in *Proceedings of the ACM Web Conference 2024 (WWW '24)*. Singapore, 13–17 May 2024. New York: ACM, pp. 1880–1891. Available at: https://doi.org/10.1145/3589334.3645684.
33. Zhang, Y., Wang, J. *and* Luo, J. (2020) 'Heuristic-based address clustering in Bitcoin', *IEEE Access*, 8, pp. 210582–210591. Available at: https://doi.org/10.1109/ACCESS.2020.3039570.

Figures

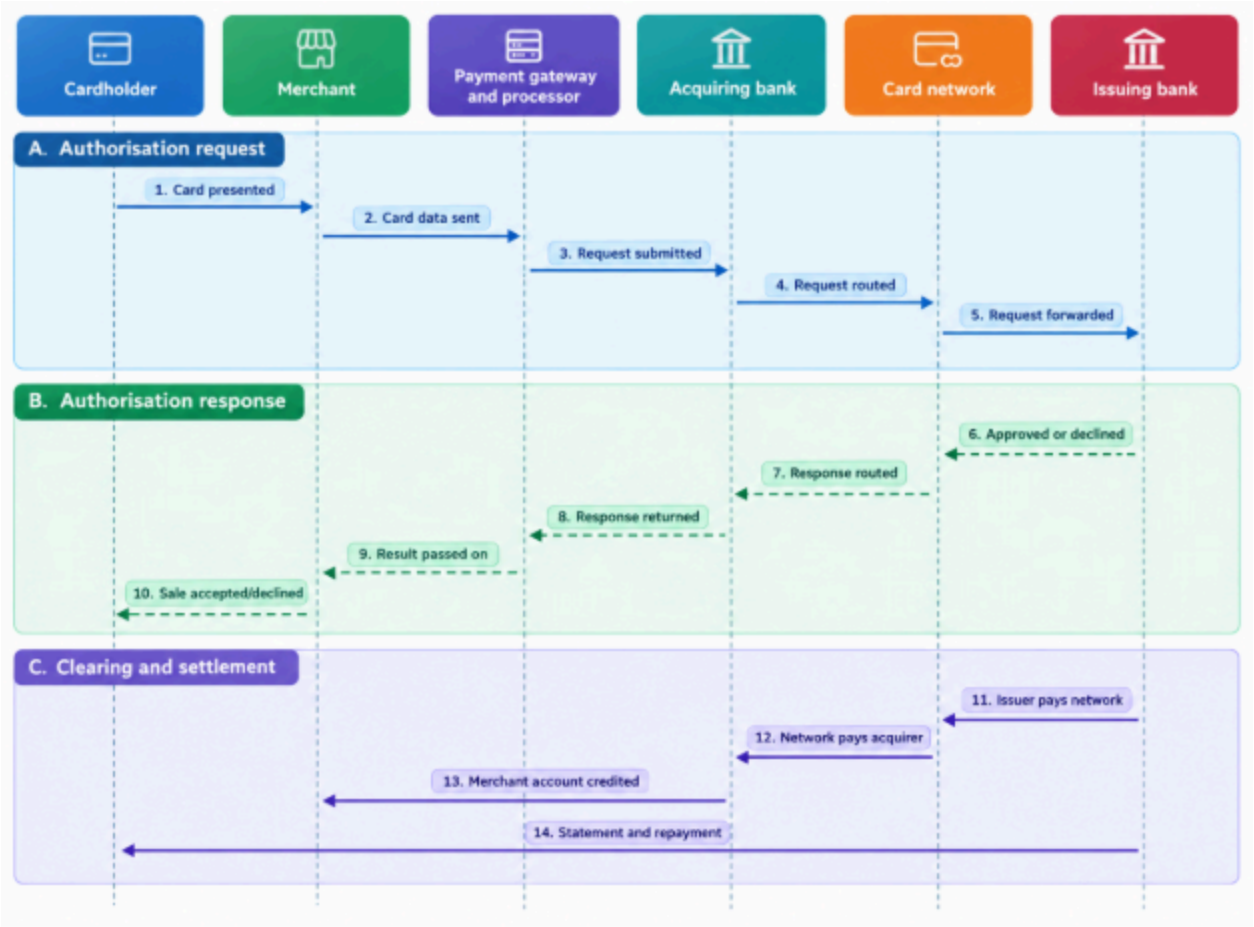


Figure 1

Debit/Credit-Based Trust System (Adapted from Hill et al., 2018, p.41)

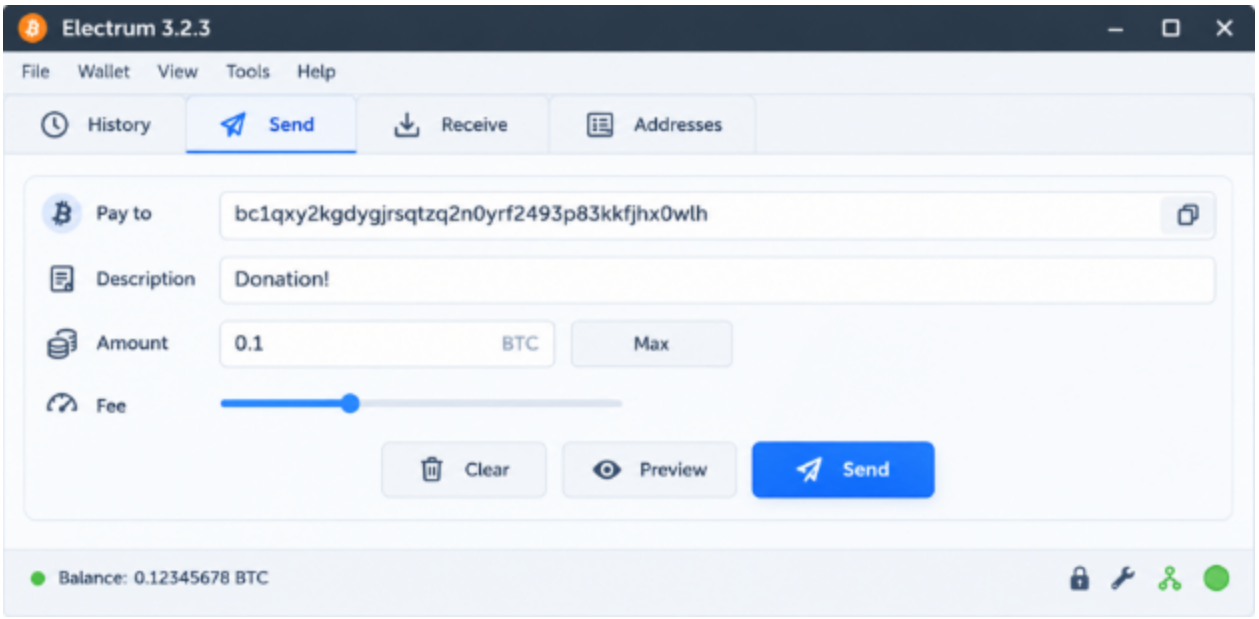


Figure 2

P2PKH Address (Adapted from Walker, 2025)



Figure 3

FCA Crypto Roadmap(Financial Conduct Authority, 2024)