WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Cryptocurrency Transactions, Decentralized Finance, and Emerging Money Laundering Risks within Contemporary Digital Financial Ecosystems

Victoria Anderson

University of South Wales, UK

ABSTRACT :

Digital financial innovation is reshaping how value is transferred, stored and exchanged, creating opportunities for inclusion while challenging approaches to financial crime prevention. This article examines cryptocurrency transactions, decentralized finance and emerging money laundering risks within contemporary digital financial ecosystems. It develops a conceptual framework linking transaction characteristics, platform governance and regulatory interfaces to potential vulnerabilities across the laundering process. Particular attention is given to pseudonymous participation, cross-chain transfers, decentralized exchanges, liquidity pools, privacy-enhancing services and interactions between custodial and noncustodial systems. The analysis distinguishes legitimate privacy and technological innovation from misuse, recognising that risk varies across assets, protocols, intermediaries and jurisdictions. It considers how transaction tracing, behavioural analytics, customer due diligence and coordinated supervision may support detection while identifying limitations involving attribution, data quality, interoperability and accountability. Rather than treating decentralization as inherently illicit, the article evaluates how fragmented responsibilities and inconsistent controls can complicate investigation and intervention. Its contribution is an integrated perspective on technological, institutional and governance dimensions, supporting proportionate responses that address laundering exposure while preserving legitimate financial participation, privacy and innovation across evolving digital markets.

Keywords: Cryptocurrency transactions; Decentralized finance; Money laundering; Financial crime prevention; Blockchain analytics; Digital financial ecosystems.

1. INTRODUCTION: DIGITAL FINANCIAL INNOVATION AND THE LAUNDERING CHALLENGE

1.1 Transformation of Contemporary Financial Ecosystems

Contemporary finance increasingly combines institution-centred payment arrangements with interconnected digital services, programmable assets and distributed infrastructures. Tokenisation can represent financial claims on shared platforms and support transaction execution, although its benefits depend on implementation and governance [1]. Cryptocurrency transactions provide another means of transferring digital value, while decentralised protocols organise activities such as exchange, lending and liquidity provision through smart contracts [2].

These developments support legitimate payments, investment and experimentation with financial participation. However, claimed efficiencies should be evaluated alongside operational vulnerabilities, consumer protection and financial integrity. International policy analysis therefore considers both potential benefits and risks rather than technology adoption alone [3].

Cryptocurrency use is not evidence of criminality. Asset design, transaction purpose, service practices and institutional context vary substantially. A balanced assessment must recognise lawful activity while examining opportunities for misuse. Risk-based guidance similarly requires attention to activities and circumstances rather than indiscriminate treatment of the sector [4].

1.2 The Money Laundering Problem Across Digital Interfaces

Identifying criminal proceeds within legitimate digital activity requires evidence linking transactions to unlawful sources or purposes. Public ledgers may reveal transaction histories, but addresses do not necessarily identify their controllers. Pseudonymity describes participation through identifiers that are not inherently verified identities; it should not be equated with anonymity. Research demonstrates possibilities for linking some Bitcoin activity to identifiable services, while highlighting limits to attribution [5].

Transfers across platforms, blockchains and jurisdictions can fragment evidence and complicate responsibility. DeFi also connects with centralised trading, lending and fiat-conversion services rather than operating as an isolated system [6]. These interfaces create different opportunities for identification, monitoring and investigation.

Technological characteristics alone do not determine laundering risk. Governance arrangements, effective control, service functions and implementation

weaknesses require examination. Treasury's DeFi assessment identifies illicit-finance vulnerabilities without implying that all DeFi activity is unlawful [7]. FATF's 2026 update likewise examines remaining implementation gaps [8]. Assessment must therefore distinguish technical exposure, suspicious patterns and substantiated laundering, while considering supervision, institutional cooperation and the quality of available evidence.

1.3 Article Aim, Questions and Contribution

This article examines how cryptocurrency transactions and DeFi characteristics interact with laundering vulnerabilities and institutional responses. It asks where exposure concentrates, which evidence supports those assessments and how proportionate responses can address weaknesses without excluding legitimate activity.

The contribution is an integrated framework connecting technological features, governance structures and institutional interfaces. It will compare transaction visibility with attribution limitations, and formal responsibilities with operational control. FATF's targeted review initiative underscores the continuing importance of implementation and cross-border coordination [9].

The article will not estimate laundering prevalence without suitable empirical data or treat enforcement cases as representative of the entire ecosystem. Instead, it will distinguish documented misuse from plausible vulnerabilities and unresolved uncertainty. The next section establishes conceptual definitions and an explicit evidence-selection approach before evaluating specific risks and potential responses.

2. CONCEPTUAL FOUNDATIONS AND EVIDENCE-REVIEW APPROACH

2.1 Cryptocurrency Transactions and DeFi Architecture

Cryptocurrency transactions are transfers or other ledger-recorded operations involving cryptographically represented assets. Assets are the objects transferred; blockchains maintain records; protocols specify operating rules; interfaces provide access; and service providers perform particular functions. These layers should not be treated as interchangeable institutions.

DeFi describes financial activities organised through blockchain-based protocols and smart contracts rather than exclusively through conventional intermediaries. The Financial Stability Board identifies exchange, lending and related activities while emphasising connections with centralised services [6]. Wallets manage keys or transaction access, smart contracts execute specified instructions, and decentralised exchanges facilitate asset exchange. Liquidity arrangements supply assets against which transactions or borrowing can occur.

Custody concerns control over assets or the means of accessing them. Protocol administration concerns powers such as upgrades, permissions or operational changes. An actor may influence administration without holding every user's assets. Treasury's assessment highlights the importance of examining services and vulnerabilities rather than relying on a decentralisation label [7].

Decentralisation therefore varies across validation, ownership, governance and interface operation. Assessments will identify these dimensions separately instead of assigning identical characteristics or responsibilities to every application.

2.2 Money Laundering, Predicate Offences and Related Financial Crimes

This article adopts the United Nations Convention against Transnational Organized Crime as an institutional starting point. Its laundering provisions address specified dealings with criminal proceeds, including conversion, transfer and concealment, subject to knowledge, purpose and domestic-law qualifications [10]. A predicate offence is the underlying criminal activity generating those proceeds.

Fraud and theft may generate assets subsequently laundered, but the original offence and laundering remain distinct questions. Sanctions evasion concerns prohibited dealings under applicable restrictions and is not automatically synonymous with laundering. Activities may overlap, yet legal classification requires evidence and jurisdictional analysis.

Placement, layering and integration provide useful categories for organising discussion of entry, concealment and apparent legitimisation [11]. However, digitally generated proceeds may already exist within financial networks, and activities need not follow three clearly separated stages. The categories will therefore guide interpretation without being imposed as a universal transaction sequence.

Technical complexity, repeated transfers or privacy features will not independently establish unlawful purpose. Attribution, provenance and corroborating information must support conclusions, with uncertainty retained where evidence remains incomplete.

2.3 Source Selection, Evidence Quality and Analytical Boundaries

The proposed review will cover January 2009 to October 2026, retaining earlier foundational legal and methodological sources where necessary. The intended search cutoff is 31 October 2026; the manuscript will report the final search date after searches are completed. This is a planned critical review, not a completed systematic search.

Academic searches will use Scopus, Web of Science and relevant computing databases. Official publications, primary enforcement documents and technical documentation will supplement scholarship. Inclusion will require relevance, identifiable provenance and sufficient methodological or contextual detail. Duplicates, unsupported promotional claims and inaccessible assertions will be excluded. Review design should align with the question and transparently explain selection decisions [12].

Industry analytics will be assessed for address attribution, coverage, denominators, revisions and commercial limitations. Observed transfers will remain distinguishable from inferred ownership or illicit purpose. Allegations, admissions, judicial findings and analytical estimates will receive separate evidential labels.

Each source will retain its jurisdiction, publication date and relevant observation period. Superseded rules will be identified rather than presented as current obligations. PRISMA supports transparent reporting of systematic reviews but does not itself establish methodological quality [14]. These boundaries will underpin examination of how transaction characteristics create, constrain or redistribute exposure across different contexts.

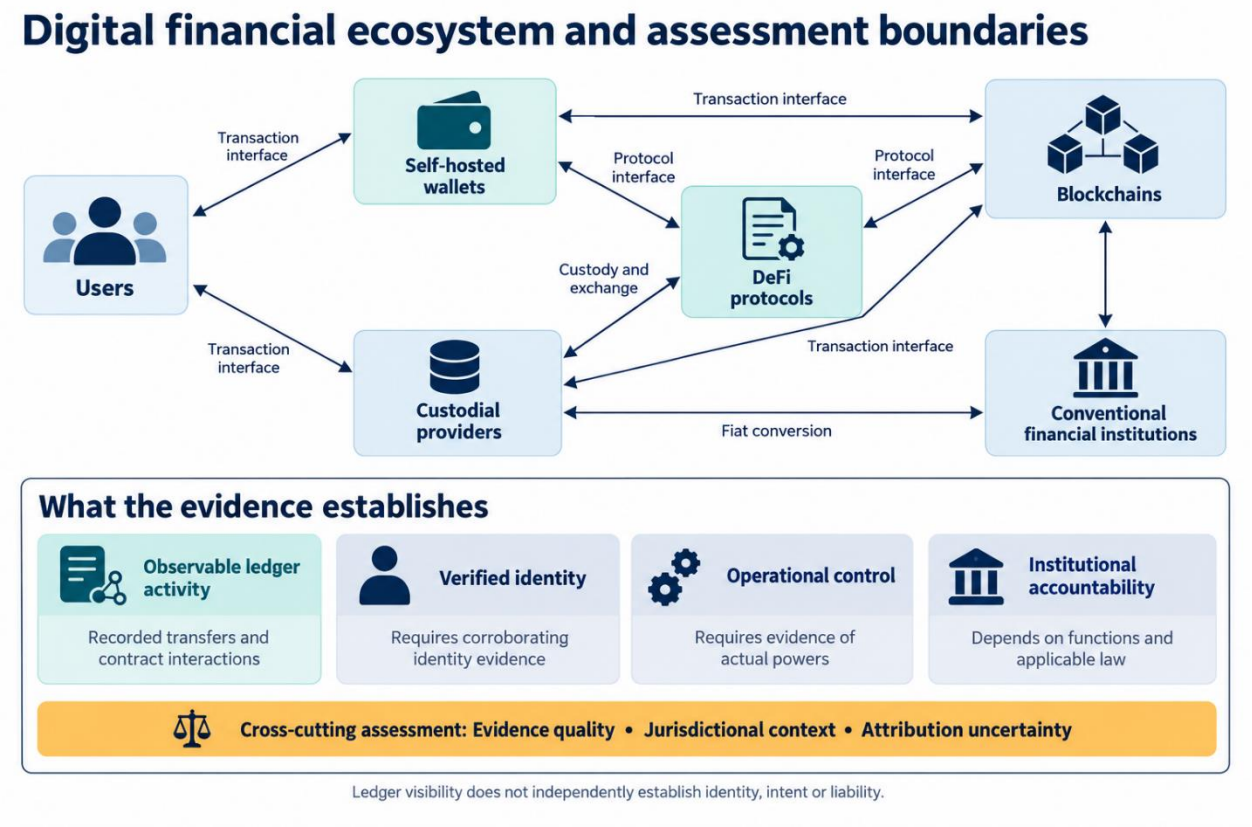


Figure 1. Digital financial ecosystem and laundering-risk assessment boundaries.

3. TRANSACTION CHARACTERISTICS AND SOURCES OF LAUNDERING EXPOSURE

3.1 Pseudonymity, Identity Attribution and Public-Ledger Visibility

Public blockchains expose transaction addresses and recorded transfers, but an address is not a verified individual or beneficial owner. One person may control several addresses, while custodial infrastructure may represent numerous customers [16]. Consequently, address activity requires contextual interpretation rather than direct translation into identities.

Public transaction histories nevertheless provide evidence for tracing recorded movements and examining relationships between transactions. Their usefulness depends on network characteristics, data completeness and the reliability of attribution methods [16]. Address labels and inferred clusters should therefore carry documented provenance, confidence levels and limitations rather than being presented as established facts.

Shared services, changing address use and intermediary arrangements can complicate attribution. Transaction proximity does not necessarily establish common ownership, and an association with an investigated address does not independently establish criminal participation [15]. Investigative conclusions require corroboration from appropriate records and other lawful evidence.

Visibility consequently differs from knowledge of ownership, purpose or criminal provenance. Legitimate financial privacy must remain distinguishable from deliberate concealment of criminal proceeds when interpreting otherwise ambiguous transaction patterns [15].

3.2 Transaction Speed, Interoperability and Cross-Chain Complexity

Rapid transaction processing can shorten the interval available for identifying suspicious activity, coordinating inquiries and requesting preservation of relevant records. However, settlement speed, confirmation requirements and finality differ between networks and services [16]. Speed therefore modifies investigative conditions without independently establishing unlawful activity.

Interoperability enables interactions between blockchain environments. Bridges support transfers of assets or related messages across networks, although their mechanisms, trust assumptions and security arrangements vary [17]. A cross-network movement may serve legitimate investment, payment or application needs and should not automatically receive a criminal interpretation.

Reconstruction becomes more demanding when records are distributed across different ledgers, service databases and jurisdictions. Inconsistent

identifiers, network architectures and attribution practices may prevent straightforward comparison. Analysts must distinguish verified transaction links from relationships inferred through timing, amounts or service labels [16].

A defensible reconstruction may consequently combine ledger records, protocol documentation, provider information and other obtained evidence. Evidential gaps and alternative interpretations should remain explicit, particularly where technical correspondence is uncertain or legal access to supporting records differs between jurisdictions [18].

3.3 Custodial, Noncustodial and Fiat-Conversion Interfaces

Custodial services typically exercise control over customers' private keys or the means of transferring assets, whereas self-hosted wallets allow users to retain that control. These arrangements influence where relevant records exist and which parties can implement controls, but custody alone does not determine overall risk [18].

Entry, exchange and withdrawal interfaces connect digital assets with other assets, services and conventional finance. Where applicable obligations attach to providers, these interfaces offer opportunities for customer identification, recordkeeping and transaction monitoring. Their effectiveness depends on implementation, supervisory oversight and access to sufficiently reliable information [18].

A self-hosted wallet is not inherently suspicious. Assessment should consider the surrounding transaction context and available evidence rather than treating the absence of a custodial intermediary as proof of criminal intent [15]. Equally, identification at one service does not establish the legitimacy of every subsequent transaction.

Weak records, ineffective monitoring or inconsistent cooperation at one interface can impair understanding of the wider chain. Assessments should therefore examine connections between services, alongside each provider's responsibilities and implemented controls [19].

3.4 Contextual Factors That Modify Risk

Risk varies with asset liquidity, service accessibility, transaction purpose and jurisdictional conditions. These characteristics affect potential exposure, but their significance depends on the activities involved and the quality of supporting evidence [19]. Market size or technological novelty alone cannot establish laundering prevalence.

Governance, accountability and control implementation modify exposure. Inherent vulnerability concerns susceptibility before relevant controls; residual risk reflects what remains after considering their effectiveness. Documented procedures should not be assumed effective without evidence of implementation and oversight [20].

Incomplete ownership, source-of-funds or transaction-purpose information introduces uncertainty rather than automatically confirming misconduct. Assessors should distinguish missing evidence from adverse evidence and explain how uncertainty affects conclusions [15]. Context-specific assessments should therefore consider technical arrangements, institutional capabilities and jurisdictional conditions together. These distinctions provide the basis for examining how particular DeFi governance structures and service arrangements redistribute responsibilities and vulnerabilities [20].

4. DEFI-SPECIFIC VULNERABILITIES AND ACCOUNTABILITY GAPS

4.1 Decentralised Exchanges and Liquidity Arrangements

Decentralised exchanges facilitate asset exchange through arrangements that may rely on smart contracts rather than an account-based intermediary. Liquidity can be supplied by participants to shared pools or organised through other trading mechanisms, with execution governed by protocol-specific rules [23]. These arrangements support legitimate price discovery, portfolio adjustment and access to digital markets.

Identification challenges arise when publicly visible addresses interact without verified identity information. However, the absence of identity data within a protocol does not establish that every participant is unidentified elsewhere. Relevant information may exist with interfaces, custodians or other connected services [18].

Protocol execution must also be distinguished from services offered through websites, applications and commercial arrangements. Interface operators may influence access or presentation even where underlying contracts remain publicly accessible [21]. Responsibilities therefore require functional assessment rather than assumptions based on branding.

Documented vulnerabilities include inconsistent controls, uncertain accountability and fragmented supervision [25]. Assessment should examine actual service arrangements, transaction context and available evidence. Trading volume, liquidity provision or permissionless access alone cannot establish laundering, criminal intent or the proportion of illicit activity within a market.

4.2 Smart Contracts, Composability and Automated Transactions

Smart contracts enable operations to execute when specified conditions are met. Composability allows applications to combine programmable components, supporting legitimate financial functions while creating dependencies between protocols and services [23]. Several recorded actions may therefore represent one economic arrangement.

Automation can complicate interpretation because execution traces do not necessarily explain the initiating party's purpose or the responsibilities of every participant. Assessment requires attention to transaction context, contract functions and the actors controlling decisions [21]. Public code can improve technical visibility without resolving identity or intent.

Software exploits must remain analytically distinct from laundering vulnerabilities. A programming defect or compromised control may enable theft,

whereas laundering concerns subsequent dealings with criminal proceeds. The events can be connected, but identifying a security failure does not independently demonstrate how stolen assets were handled [25].

Automated execution also does not eliminate human influence. Developers, administrators and service operators may retain powers affecting implementation or access [22]. Accountability should consequently follow demonstrated functions and applicable legal criteria rather than the mere presence of executable code.

4.3 Privacy-Enhancing Services and Evidential Ambiguity

Financial privacy can protect security, commercially sensitive activity and confidentiality. Public transaction histories may otherwise expose information beyond what users disclose in conventional payment settings. Official policy discussion recognises that privacy-enhancing tools can have lawful uses alongside potential criminal misuse [24].

Some services reduce straightforward linkage between recorded transfers, complicating attribution and evidential reconstruction. Nevertheless, technology use alone does not establish criminal provenance or unlawful purpose. Assessments require contextual evidence and a distinction between observed transactions, inferred relationships and verified ownership [20].

Contamination assumptions warrant caution. Interaction with a shared service does not automatically demonstrate that every user controlled, benefited from or knowingly handled criminal proceeds. Analytical conclusions should identify their assumptions and avoid converting uncertain associations into definitive accusations.

Overbroad classifications can exclude legitimate users from services and weaken confidence in monitoring decisions. Proportionate responses should therefore combine documented risk indicators, corroboration and opportunities to review disputed attribution, while recognising that incomplete visibility can leave investigative uncertainty unresolved [25].

4.4 Governance Concentration and the Meaning of Decentralisation

Decentralisation describes several dimensions rather than one organisational condition. Open transaction access or published code can coexist with concentrated authority over upgrades, interfaces or strategic decisions [22]. Technical openness therefore does not establish distributed practical control. Administrators, development teams, governance participants and interface operators may exercise different forms of influence. Assessment should identify who can propose, approve or implement changes, restrict particular services and respond to operational incidents [21]. Formal documentation should be compared with observed practices rather than accepted as a complete account.

Governance-token ownership can indicate potential participation, but holdings alone do not establish effective decision-making power or legal responsibility. Delegation, participation patterns, contractual arrangements and implementation authority may alter the significance of voting rights [22]. Responsibility consequently requires examination of actual functions, control and applicable jurisdictional rules [25]. Identifying influential actors supports accountability without assuming that every developer, token holder or participant performs the same regulated activity or bears equivalent obligations within a particular decentralised financial arrangement.

4.5 Interactions Between DeFi and Centralised Services

DeFi activity connects with custodial exchanges, wallet services and conventional payment channels. Users may depend on these interfaces for access, conversion and settlement, meaning apparently separate systems can share operational dependencies [23]. Risk assessment must therefore examine relationships across the transaction lifecycle.

Information may be distributed among protocol records, custodial accounts and financial institutions. Differences in identification practices, retention arrangements and jurisdictional access can obstruct timely reconstruction or coordinated review [18]. A strong control at one institution cannot compensate automatically for every weakness elsewhere.

Ecosystem-level assessment links these dependencies with governance and implemented safeguards [19]. It distinguishes technical exposure from evidenced misconduct while identifying where cooperation could improve understanding. Having identified vulnerabilities, the analysis can now assess the capabilities and limitations of detection, investigation and supervision across interconnected financial services.

Table 1. Cryptocurrency and DeFi risk-assessment matrix.

Ecosystem feature or interface	Legitimate function	Potential laundering vulnerability	Evidence needed	Relevant control opportunity	Main uncertainty
Public-ledger addresses	Recording and verifying transfers	Uncertain attribution to individuals or entities	Transaction records, corroborated address labels and ownership evidence	Documented attribution methods and confidence assessment	An address may represent several users or only part of one user's activity
Decentralised exchanges and liquidity arrangements	Asset exchange, liquidity provision and price discovery	Fragmented identification and unclear allocation of monitoring responsibilities	Protocol documentation, interface arrangements and contextual transaction evidence	Functional assessment of service roles and applicable controls	Protocol participation does not establish criminal purpose
Smart contracts and composability	Programmable execution and integration of financial	Complex dependencies can obscure transaction purpose and responsibility	Execution records, contract functions and evidence of initiating or controlling	Technical analysis combined with contextual investigation	Recorded execution may not reveal economic intent

Ecosystem feature or interface	Legitimate function	Potential laundering vulnerability	Evidence needed	Relevant control opportunity	Main uncertainty
	applications		actors		
Privacy-enhancing services	Financial confidentiality and protection against unwanted disclosure	Reduced straightforward linkage between transfers	Corroborated transaction evidence and explicit attribution assumptions	Proportionate investigation and review of disputed classifications	Privacy use alone does not establish illicit provenance
Governance and upgrade controls	Protocol maintenance, development and incident response	Concentrated influence may coexist with unclear accountability	Administrative permissions, governance records and implementation practices	Identification of actual control and documented responsibilities	Formal voting rights may differ from practical influence
Custodial and fiat-conversion interfaces	Asset custody, exchange and connection to conventional finance	Weak identification, recordkeeping or cooperation can interrupt evidential continuity	Customer records, transaction histories and documented control implementation	Applicable identification, monitoring and lawful information sharing	Relevant evidence may be dispersed across jurisdictions

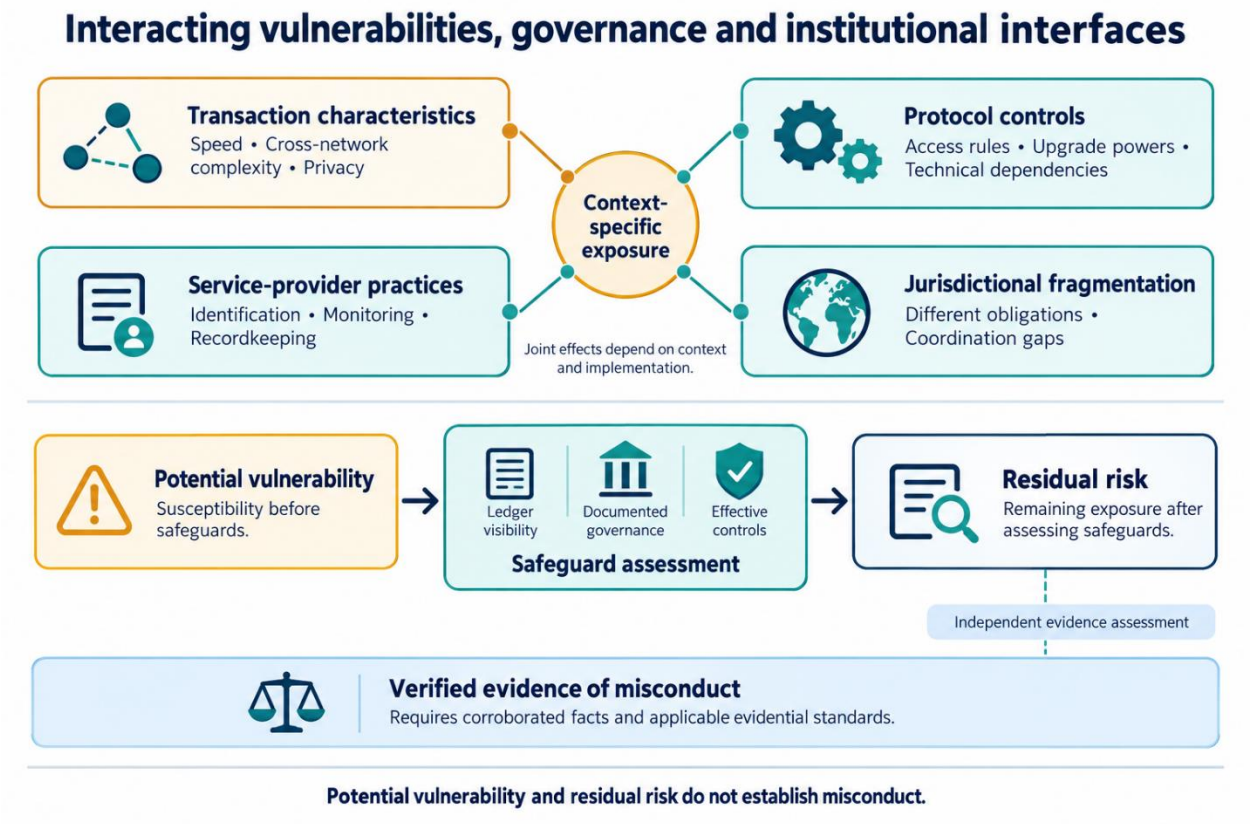


Figure 2. Interaction of technological vulnerabilities, governance arrangements and institutional interfaces.

5. DETECTION, INVESTIGATION AND GOVERNANCE RESPONSES

5.1 Blockchain Analytics and Transaction Monitoring

Blockchain analytics can reconstruct transfers, examine connections between addresses and identify patterns requiring review. Network analysis considers relationships among transactions or entities, while behavioural monitoring compares activity with contextual expectations [23]. These techniques organise evidence; they do not independently determine whether funds represent criminal proceeds.

Interpretation requires corroboration through service records, verified attribution and relevant investigative information. Address clustering and labels remain dependent on their underlying methods and evidence. Research evaluating attribution demonstrates that coverage and accuracy must be assessed within the services and datasets examined [26].

Incomplete network coverage, shared infrastructure and outdated labels can produce misleading associations. Accordingly, monitoring systems should

document data provenance, confidence and known limitations. Alerts indicate matters for assessment rather than conclusions about ownership, intent or criminal conduct [25].

Human review should examine plausible legitimate explanations and the consequences of false positives. Effectiveness assessment should include substantiated findings, missed risks, review workload and correction of attribution errors. High alert volumes alone do not demonstrate successful detection, and performance established for one network or service cannot automatically be generalised across the digital financial ecosystem [26].

5.2 Identity, Due Diligence and Information Exchange

Identity verification, customer due diligence and recordkeeping can connect otherwise pseudonymous activity with accountable service relationships. Where applicable, controls should establish customer information, assess risk and maintain records suitable for subsequent review [27]. Identity verification nevertheless does not establish the legitimacy of every transaction.

Information exchange can support continuity across participating services and competent authorities. European Union transfer requirements and associated supervisory guidance illustrate jurisdiction-specific arrangements for accompanying information and handling incomplete records [28,29]. These provisions should not be described as universally applicable.

Data quality, compatible formats and secure transmission influence whether exchanged information is useful. Incorrect identifiers can propagate errors, while unnecessary disclosure creates confidentiality risks [30]. Recipients should therefore evaluate information reliability rather than assume that transmission guarantees accuracy.

Controls face limits where participants, responsible providers or relevant records cannot readily be identified [25]. Analysis must specify the jurisdiction, effective period and actors covered, distinguishing obligations already applicable from proposed rules, international expectations and voluntary implementation practices [27].

5.3 Regulatory Perimeters and Supervisory Coordination

Regulatory assessment should examine performed functions rather than rely exclusively on descriptions such as “decentralised.” Protocol operation, interface provision and administrative influence can involve different activities and responsibilities [25]. Technical architecture informs this assessment but does not independently determine the legal perimeter.

International standards establish expectations for national implementation; domestic legislation and supervisory arrangements determine applicable obligations. Voluntary industry practices occupy a separate category and should not be presented as binding requirements [27]. Each claim therefore requires a jurisdictional and temporal boundary.

Cross-border coordination becomes difficult when connected services face inconsistent definitions, identification practices or enforcement capabilities. Cooperation can improve evidence access and supervisory understanding, but institutional mandates and confidentiality requirements constrain information exchange [28,30]. Coordination should preserve accountability rather than diffuse responsibility between authorities.

Formal registration or published procedures also do not establish effective operational compliance. Assessment should examine implemented controls, supervisory capacity and responses to identified deficiencies [25]. Responsibility must follow evidenced activities and control under applicable law, without assuming that one jurisdiction’s interpretation governs every participant globally.

5.4 Privacy, Proportionality and Legitimate Financial Participation

Excessive surveillance and unreliable attribution can expose sensitive information, restrict legitimate participation and undermine confidence in financial services. Broad exclusion may shift activity beyond supervised channels without addressing the underlying risks [31]. Controls should therefore respond proportionately to substantiated concerns.

Lawful access, data minimisation, restricted permissions and appropriate retention arrangements provide safeguards for personal information. Blockchain-related processing requires attention to persistent records and the responsibilities of actors determining processing purposes [30]. Technical availability does not itself justify unrestricted reuse.

Individuals, small providers and cross-border users may face different compliance burdens or barriers to correcting errors. Review procedures should consider these consequences alongside investigative needs [31]. Proportionality supports effectiveness and public trust by directing resources towards evidenced priorities. The following framework therefore integrates vulnerabilities, controls and evidential uncertainty without treating either extensive surveillance or limited visibility as conclusive proof of effectiveness.

Table 2. Response options, evidence requirements and implementation limitations.

Response mechanism	Intended purpose	Responsible actor where applicable	Evidence or data required	Effectiveness measure	Privacy or implementation limitation
Transaction tracing and network analysis	Reconstruct recorded movements and assess transaction relationships	Investigators, financial intelligence units and qualified analysts	Ledger records, network documentation and corroborated attribution	Reconstruction accuracy, coverage and independently supported findings	Incomplete coverage and uncertain address ownership
Behavioural transaction monitoring	Identify activity requiring contextual review	Obligated service providers and compliance teams	Transaction histories, customer context and documented indicators	Substantiated findings, false-positive burden and review timeliness	Alerts can misclassify legitimate activity; missed risks remain difficult to quantify

Response mechanism	Intended purpose	Responsible actor where applicable	Evidence or data required	Effectiveness measure	Privacy or implementation limitation
Identity verification and customer due diligence	Establish service relationships and assess customer-specific risk	Providers subject to applicable obligations	Reliable identity information and relevant supporting records	Verification quality, unresolved discrepancies and risk-appropriate review	Identity fraud, inaccessible documentation and exclusion risks
Transfer-information exchange	Preserve relevant information across covered transfers	Participating providers under applicable requirements	Required originator and beneficiary information	Completeness, accuracy and timely resolution of missing information	Incompatible systems, inaccurate records and confidentiality constraints
Supervisory cooperation	Coordinate oversight across connected activities and jurisdictions	Competent supervisors and other authorised bodies	Service-function mapping, inspection findings and lawful information-sharing arrangements	Timely assistance and evidenced remediation of deficiencies	Different mandates, legal restrictions and implementation capacity
Human review and attribution correction	Evaluate alerts and remedy unsupported associations	Trained reviewers and accountable decision-makers	Underlying evidence, confidence assessments and contextual explanations	Review quality, correction timeliness and consistency	Resource constraints and limited access to independent corroboration
Privacy and proportionality safeguards	Limit unnecessary processing and protect legitimate participation	Relevant data controllers, providers and oversight bodies	Processing purposes, access records and documented risk assessments	Data minimisation, justified access and effective complaint handling	Persistent records, unclear responsibilities and cross-border enforcement difficulties

6. INTEGRATED ASSESSMENT, LIMITATIONS AND RESEARCH PRIORITIES

6.1 A Layered Framework for Ecosystem Risk Assessment

The proposed framework combines transaction characteristics, service arrangements, governance structures and jurisdictional conditions within one assessment process. Transaction analysis examines observable movements and evidential gaps; service assessment considers operational interfaces; governance assessment identifies control; jurisdictional assessment establishes applicable responsibilities [29]. These dimensions should inform each other rather than generate disconnected judgements.

Each concern should carry an evidence statement identifying its source, date, coverage and reliability. Potential exposure describes susceptibility, documented misuse identifies supported incidents, and proven laundering requires an appropriate evidential and legal basis. These categories must not be collapsed into a single numerical risk label.

The next stage maps implemented controls, remaining vulnerabilities and responsible actors where ascertainable. Assessment should distinguish the existence of procedures from evidence that they operate effectively. Evaluation of outcomes is therefore necessary alongside examination of formal compliance [34]. fatf-gafi.org

No individual feature, including privacy technology, rapid execution or permissionless access, should determine the overall conclusion. The framework instead proposes a structured record of interacting conditions, contradictory evidence and unresolved assumptions. Its contribution is analytical organisation, not a validated risk score. Comparative application, reviewer agreement and usefulness for proportionate decisions require evaluation before claims of effectiveness or widespread suitability can responsibly follow from its adoption [35].

6.2 Interpreting the Evidence and Comparing Competing Perspectives

Claims that cryptocurrency facilitates concealment and claims that public ledgers assist investigation need not be mutually exclusive. Visibility can support reconstruction of recorded transfers while identity, economic purpose and off-chain relationships remain uncertain. Investigative value therefore depends on the network, service arrangements and corroborating information available [32].

Privacy-enhancing features and fragmented service records can restrict attribution. Conversely, persistent transaction records may allow activity to be revisited when new evidence emerges. Neither possibility establishes that all transactions are traceable or that technological complexity necessarily defeats investigation.

Case studies demonstrate mechanisms, institutional weaknesses or investigative capabilities. They do not provide representative denominators for estimating ecosystem-wide laundering prevalence. Official assessments acknowledge uncertainty about the proportion of cryptoasset activity associated with illicit conduct [33]. GOV.UK

Commercial estimates require examination of coverage, labelling practices, excluded activity and revisions. Enforcement samples disproportionately reflect detected conduct and institutional priorities, while successful cases may receive publicity. Interpretation should therefore compare competing explanations, report uncertainty and avoid treating isolated investigative successes as proof of universal control effectiveness. Evidence of criminal adaptation also requires contextual interpretation across ecosystems and periods [37].

6.3 Methodological and Practical Limitations

The review faces incomplete attribution, inaccessible provider records and inconsistent terminology. Definitions of services, decentralisation and illicit activity vary, limiting comparison across reports. Unverified labels and uncertain ownership can weaken conclusions even when transaction records themselves are accurate [32].

Publication bias may favour prominent incidents and successful investigations. Detected or prosecuted cases consequently represent a selected subset of activity rather than the entire ecosystem. Their evidential value should be preserved without extrapolating directly to population prevalence [33].

Protocols, interfaces and governance arrangements change rapidly. Findings from one period may not describe later operational conditions, while jurisdictional differences affect available records and institutional powers [29]. Generalisation across assets and service models therefore requires justification.

The framework cannot independently determine legal liability, identify every responsible participant or quantify total laundering. Its classifications depend on assumptions about evidence quality, control effectiveness and assessment boundaries. These assumptions should remain explicit, with unresolved questions recorded for investigation rather than concealed through apparently precise scoring. Formal policy adoption likewise cannot substitute for demonstrated practical effectiveness [34].

6.4 Future Research and Responsible Policy Development

Future research should compare services, networks and jurisdictions using clearly defined assessment boundaries and compatible terminology. Studies should disclose data coverage, validate attribution labels and distinguish independently confirmed findings from analytical inference. Where automated monitoring is used, testing should address validity, reliability and consequences of errors [35]. AIRC

Control evaluation should examine substantiated findings, missed risks, false-positive burdens and privacy effects. Policy adoption, registration totals and alert volumes provide implementation information but cannot independently establish reduced laundering. Supervisory evaluation should connect interventions with outcomes and documented remediation [36].

Technical specialists, legal scholars and financial-crime practitioners should collaborate with affected users to assess feasibility and proportionality [30,31]. Repeated assessment is necessary as services and criminal practices evolve [37]. Such research can test whether the proposed framework improves consistent reasoning and accountable decisions. Responsible policy development should therefore remain iterative, evidence-led and open to revision when findings challenge existing assumptions or priorities [34].



Figure 3. Risk-assessment and continuous-review framework.

7. CONCLUSION

7.1 Integrated Contribution and Principal Conclusions

Digital financial innovation creates legitimate opportunities while changing the conditions under which criminal proceeds may be transferred, investigated and controlled. The reviewed evidence indicates that laundering exposure depends on interactions between transaction characteristics, governance arrangements and institutional interfaces. Public ledgers can support investigation, but visibility does not independently establish identity, intent or criminal provenance. Equally, privacy features, self-hosted wallets and decentralised protocols do not inherently demonstrate misconduct. Risks vary across technologies, services and jurisdictions, requiring contextual assessment rather than universal classifications. The article's proposed framework connects these dimensions while distinguishing potential vulnerabilities from documented misuse and proven laundering. It does not establish ecosystem-wide prevalence or demonstrate that particular controls are effective.

7.2 Conditions for Responsible Application

Responsible application requires reliable evidence, identifiable responsibilities and interpretation sensitive to jurisdictional and temporal boundaries. Analytical methods require validation, documented uncertainty and human review, particularly when attribution affects access to financial services. Privacy, data minimisation and proportionality should guide information collection and institutional responses. Technical visibility and formal obligations alone cannot guarantee effective prevention; implemented controls require continuing evaluation against meaningful outcomes. Coordinated, evidence-based responses can strengthen financial integrity while preserving legitimate innovation, provided that policy decisions remain open to reassessment as technologies, institutional practices and available evidence change over time.

REFERENCE

1. Bjelajac Z, Bajac MB. Blockchain technology and money laundering. Law Theory & Prac.. 2022;39:21.
2. Desmond DB, Lacey D, Salmon P. Evaluating cryptocurrency laundering as a complex socio-technical system: A systematic literature review. Journal of Money Laundering Control. 2019 Jul 2;22(3):480-97.
3. Chukwunweike J. Coordinating PLC-based load shedding and variable-speed drives to prevent transformer overloading during industrial production peaks. Int J Electr Data Commun. 2025;6(2 Pt B):118-135. doi:10.22271/27083969.2025.v6.i2b.109.
4. 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. 2024 Jan 10;32(1):80-97.
5. Kumari M, Goyal NK. Artificial intelligence in the cryptocurrency ecosystem: Crime mechanisms, detection strategies, and legal perspectives. InInnovations in cryptocrime and financial fraud 2026 (pp. 245-282). IGI Global Scientific Publishing.
6. Ogan RK. Machine-learning-based API failure prediction and root-cause analytics for improving reliability of enterprise banking integration architectures at scale. Int J Comput Artif Intell. 2021;2(2):142-153. DOI:10.33545/27076571.2021.v2.i2a.378.
7. Bok K. Decentralizing finance: How DeFi, digital assets, and distributed ledger technology are transforming finance. John Wiley & Sons; 2023 Dec 18.
8. Akartuna EA, Johnson SD, Thornton AE. The money laundering and terrorist financing risks of new and disruptive technologies: a futures-oriented scoping review: EA Akartuna et al. Security Journal. 2023 Dec;36(4):615-50.
9. Bhandari, Ambika Baniya. 2026. "Bridging the Public Health–Cloud Security Divide: Workforce Implications of the HIPAA Security Rule Modernization for Public Health Informatics". *Current Journal of Applied Science and Technology* 45 (8):33-44. https://doi.org/10.9734/cjast/2026/v45i84730.
10. Rejeb A, Rejeb K, Keogh JG. Cryptocurrencies in modern finance: a literature review. Etikonomi. 2021 Feb 22;20(1):93-118.
11. Kayani U, Hasan F. Unveiling cryptocurrency impact on financial markets and traditional banking systems: Lessons for sustainable blockchain and interdisciplinary collaborations. Journal of Risk and Financial Management. 2024 Feb 1;17(2):58.
12. Bhandari, Ambika Baniya. 2026. "Quality Control Frameworks for Electronic Health Record Data Workflows in Resource-Constrained Settings: A Structured Review With Implications for Global Health Information Management". *Current Journal of Applied Science and Technology* 45 (8):1-16. https://doi.org/10.9734/cjast/2026/v45i84728.
13. Liang W, Mary BJ, Hamzah F, Taofeek A, Mattew B, Blessing M, John B, Oluwaferanmi A. Next-Gen AML Technologies and Financial Crime: The Role of AI and Blockchain in Regulating Cryptocurrency Markets. Next-Gen AML Technologies and Financial Crime: The Role of AI and Blockchain in Regulating Cryptocurrency Markets. 2025 Jun 4.
14. Muralidhar A, Lakkanna M. Regulating cryptocurrency and decentralized finance for an inclusive economy. arXiv preprint arXiv:2407.01532. 2024 Feb 15.
15. Iyanuoluwa Oluwafemi. (2024). ENVIRONMENTAL MONITORING STRATEGIES INTEGRATING MOLECULAR DETECTION TECHNOLOGIES TO ENHANCE AGRICULTURAL BIOSECURITY AND SUSTAINABLE CROP PRODUCTION SYSTEMS. International Journal Of Engineering Technology Research & Management (IJETRM), 10(12), 757–772. https://doi.org/10.5281/zenodo.21152414
16. Zhuk A. From cypherpunks to decentralized finance: How crypto-anarchy is redefining legal and economic systems. Markets, Globalization & Development Review. 2025;9(3).
17. Mergaliyeva LI, Primbetova SC. Sustaining innovation and regulation: The eco-system of decentralized and centralized finance. Economy: strategy and practice. 2025 Jan 14;19(4):20-37.

18. Bhetwal S, Bastakoti R, Acharya N, Gupta GK, Bhandari AB. Benchmarking Local LLMs for Natural-Language-to-SQL Querying in Biopharmaceutical Manufacturing: An Empirical Benchmark on Consumer-Grade Hardware. arXiv preprint arXiv:2606.01338. 2026 May 31.

19. Makarov I, Schoar A. Cryptocurrencies and decentralized finance (DeFi). Brookings papers on economic activity. 2022;2022(1):141-215.

20. Dote-Pardo J, Espinosa-Jaramillo MT. Money laundering risks of cryptocurrencies: Towards coordinated regulatory and technological strategies. Latin American Journal of Central Banking. 2025 Oct 27:100194.

21. Gaffari MA. Explainable machine learning for predicting depression risk using sleep patterns, self-esteem, and psychosocial factors. International Journal of Computer Applications Technology and Research. 2026;15(11):26–37. doi:10.7753/IJCATR1511.1003.

22. Ibrahim SA. Decrypting the Risks of Cryptocurrency: Money Laundering, Terrorism Financing, and Proliferation Financing. Pakistan Horizon. 2021 Jan 1;74(1):73-89.

23. Johnson C. Decentralized finance (DeFi): Opportunities and risks in the global financial ecosystem. Business, Marketing, and Finance Open. 2024 Mar 1;1(2):53-64.

24. Moza B. Decentralized Money: A Comprehensive Review on Cryptocurrencies. Foundation of Computer Applications. 2023 Jan 1.

25. Sandra Darkwa. Transformer-Driven Strategic Communication Analytics for Identifying Synthetic Media Manipulation and Coordinated Narrative Amplification Networks Digitally. Int J Literacy Educ 2024;4(2):333-346. DOI: 10.22271/27891607.2024.v4.i2d.434

26. Adaramola O. The dark arts of crypto laundering and the Nigerian financial ecosystem: Examining regulatory perspectives of virtual assets and virtual asset providers in mitigating money laundering risks in Nigeria. Journal of Economic Criminology. 2025 Mar 1;7:100117.

27. Arnone G, Bivona E, Visconti C. Cryptocurrencies and Illicit Finance: How Criminal Networks Undermine Sustainable Financial Markets. European Journal of Law and Technology. 2026 Sep 29;17(2).

28. Malik GM, Rashid W, Liaqat A, Jahangeer A, Sarjeet SO. Global governance and technological disruption: addressing money laundering and terrorism financing in a digital age. Remittances Review. 2022;7(2):243-58.

29. Manna M, Cesarotto I, Silvestrini A. Crypto-assets and the risk of money laundering. Digital Finance. 2026 Sep;8(3):44.

30. Dupuis D, Gleason K. Money laundering with cryptocurrency: open doors and the regulatory dialectic. Journal of Financial Crime. 2021 Mar 25;28(1):60-74.

31. Arnone G. The future of cryptocurrencies and digital currencies. InNavigating the world of cryptocurrencies: Technology, economics, regulations, and future trends 2024 Oct 5 (pp. 103-111). Cham: Springer Nature Switzerland.

32. Rysin V, Rysin M. The money laundering risk and regulatory challenges for cryptocurrency markets. Restructuring management models-changes-development. 2020:187-201.

33. Wronka C. Financial crime in the decentralized finance ecosystem: new challenges for compliance. Journal of Financial Crime. 2023 Jan 2;30(1):97-113.

34. Spyra M, Balina R, Idasz-Balina M, Zając A, Różyński F. Cryptocurrencies as a tool for money laundering: Risk assessment and perception of threats based on empirical research. Risks. 2025 Oct 2;13(10):189.

35. Campbell-Verduyn M. Bitcoin, crypto-coins, and global anti-money laundering governance. Crime, Law and Social Change. 2018 Mar;69(2):283-305.

36. Alamsyah A, Kusuma GN, Ramadhani DP. A review on decentralized finance ecosystems. Future Internet. 2024 Feb 26;16(3):76.

37. Bongini PA, Mattassoglio F, Pedrazzoli A, Vismara S. Crypto ecosystem: Navigating the past, present, and future of decentralized finance. The Journal of Technology Transfer. 2025 Oct;50(5):2054-75.