POLITICS & SECURITY
ISSN 2815-3324 Online, ISSN 2535-0358 Print

DECENTRALIZED FINANCE (DEFI) AND SANCTIONS EVASION: A RISK ANALYSIS OF MIXERS AND PRIVACY COINS IN FINANCING NATIONAL SECURITY THREATS

Andrii Svintsytskyi
Scientific Research Center Of Independent Forensic
Ministry of justice of Ukraine
Kyiv, Ukraine
https://orcid.org/0000-0002-9801-0535
svintsytskyi8143@acuedu.cc

Abstract. *The expansion of Decentralized Finance (DeFi) and Anonymity-Enhancing Technologies (AETs) has complicated the tracking of illicit financial flows. This article analyzes three distinct AETs—Tornado Cash, Monero, and Zcash—to assess how specific protocol mechanisms degrade transaction-graph attribution and obstruct compliance. Synthesizing technical literature, AML/CFT frameworks, and recent judicial documentation, the study traces how design choices translate into investigative challenges. The analysis yields three key findings. First, "decentralization" rarely eliminates control; instead, it shifts choke points to infrastructure layers such as bridges and RPC providers. Second, while AETs significantly raise attribution costs, their effectiveness is often conditional and dependent on usage patterns. Third, the Tornado Cash enforcement saga illustrates the limitations of applying traditional sanctions to autonomous code. The paper concludes by proposing a mitigation agenda focused on measurable risk reduction at entry/exit points without compromising legitimate privacy.*

Keywords: DeFi; sanctions evasion; money laundering; Tornado Cash; Monero; Zcash; FATF; OFAC; blockchain forensics.

1. INTRODUCTION

DeFi is commonly described as an "open" financial stack: smart contracts replace portions of the intermediation performed by banks, brokers, and exchanges, and composability allows protocols to interconnect in ways that compress settlement time and increase transactional velocity. In parallel, DeFi reduces or fragments traditional compliance points. In custodial finance, regulated entities can be compelled to implement KYC, transaction monitoring, and sanctions screening. In DeFi, value transfer can occur through autonomous code, with governance and user interaction distributed across protocols, web front ends, relayers, and a range of infrastructure providers. This structural shift creates a persistent governance and enforcement problem for AML/CFT and sanctions regimes. (Schär, 2021; Aramonte, Huang, & Schrimpf, 2021).

A particularly acute variant of the problem involves anonymization-enhancing technologies (AETs). For the purpose of this article, AETs are tools or protocols that materially reduce the ability of investigators and compliance teams to link inputs and outputs, associate addresses with users, or recover meaningful transaction context. AETs are not intrinsically illicit: privacy can be a legitimate security feature (e.g., protecting donors, dissidents, journalists, or corporate treasury operations). However, AETs can also be operationalized as a laundering layer for cybercrime proceeds and as a sanctions-evasion capability for state-linked threat actors. (FATF, 2024; FinCEN, 2019b).

This article focuses on three AET exemplars that represent different privacy architectures and different enforcement constraints:

• Tornado Cash (Ethereum): a non-custodial smart-contract mixer that pools deposits and allows withdrawals to new addresses via cryptographic proofs.

• Monero: a privacy coin with mandatory privacy, using ring signatures, stealth addressing, and confidential amounts.

• Zcash: a privacy-capable cryptocurrency with an optional shielded pool; users may transact transparently, privately, or in mixed modes.

The research problem is not whether these systems can be used for illicit finance—they can—but how, and under which conditions, that use becomes operationally meaningful for sanctions evasion and national-security financing. Accordingly, the paper asks four questions:

- RQ1. How do Tornado Cash, Monero, and Zcash frustrate common blockchain forensic techniques in practice?
- RQ2. What evidence links the use of these tools to laundering flows connected to sanctioned or state-linked actors?
- RQ3. What does the Tornado Cash enforcement episode (designation, litigation, and delisting) reveal about the limits of current sanctions and AML architectures when the object of control is autonomous code?
- RQ4. Which mitigation measures plausibly reduce risk without collapsing legitimate privacy and security use cases?

Additional conceptual clarifications are necessary. First, 'sanctions evasion' is used here in an operational sense: actions designed to frustrate the identification, blocking, or interdiction of transactions that involve sanctioned persons, entities, or jurisdictions. In crypto-asset contexts, evasion can occur without a direct relationship to a sanctioned entity if the intent is to obscure provenance so that counterparties and compliance systems cannot identify sanctioned involvement. Second, 'national-security financing' includes both direct financing (e.g., proceeds directed to sanctioned programs) and enabling activity (e.g., laundering stolen assets that sustain state-linked operations). These definitions keep the analysis focused on controllable mechanisms rather than on rhetorical claims about DeFi as inherently illicit. (FATF, 2024).

2. METHODS AND ANALYTICAL FRAMEWORK

This study uses a structured qualitative synthesis that links technical mechanisms to investigative and regulatory outcomes. A purely legal or purely technical account is insufficient: enforcement feasibility depends on protocol design and usage, while technical risk becomes policy-relevant only when mapped to observable attack and laundering patterns. The analytical frame therefore treats "risk" as the interaction of (i) protocol capability, (ii) attacker practice, and (iii) the regulatory perimeter. (Aramonte et al., 2021; Schär, 2021).

Sources were assembled using three criteria. First, primary authority: official publications from regulators and enforcement bodies (FATF, FinCEN, U.S. Treasury/OFAC), court documents, and peer-reviewed technical research. Second, reproducibility: sources must be publicly accessible with stable identifiers (DOI, official report number, or court PDF) to avoid invented references. Third, topical relevance: sources must speak directly to at least one of the three focal AETs or to the AML/sanctions treatment of DeFi and mixing. (FATF, 2024).

To reduce over-reliance on any single narrative, the paper triangulates key empirical claims across at least two independent source types where feasible—for example, combining an OFAC press release with a technical paper or a typology report. References were audited so that every in-text citation resolves to an existing item, each DOI/URL is functional at the time of editing, and the reference list matches the citations used in the manuscript.

The analysis proceeds in three steps. Step 1 characterizes the privacy mechanism and the expected forensic failure modes for each AET, drawing on technical literature. Step 2 examines exploitation patterns and enforcement responses using official documents and credible threat assessments. Step 3 evaluates mitigation options by separating measures that target protocol code (often constrained by immutability and jurisdiction) from measures that target interfaces and infrastructure (front ends, relayers, RPC endpoints, bridges, centralized exchanges, and fiat off-ramps).

This article does not estimate the total illicit share of DeFi activity, which is sensitive to definitional choices and to the visibility limits created by privacy tools. Observed laundering patterns may also reflect liquidity and usability constraints rather than inherent "superiority" of one AET. The discussion therefore distinguishes protocol capability from attacker adoption and treats "effectiveness" as conditional rather than absolute.

Material was coded along four dimensions: (i) privacy mechanism (what is hidden and how), (ii) enforcement surface (which actors or infrastructure can be influenced), (iii) empirical evidence type (on-chain measurement, enforcement allegation, court finding, or typology report), and (iv) uncertainty level (high/medium/low confidence). Arguments are constructed so that high-confidence claims rely on primary sources (court documents, official reports, peer-reviewed research), while lower-confidence claims are explicitly labeled and not used as sole support for conclusions.

3. RESULTS AND ANALYSIS

3.1 Technology-driven forensic friction: how privacy mechanisms change observability

3.1.1 Tornado Cash (smart-contract mixing)

Smart-contract mixers weaken transaction-graph attribution by breaking the visible linkage between deposits and withdrawals. In Tornado Cash, users deposit into a pool and later withdraw to a different address, presenting a cryptographic proof that authorizes withdrawal without revealing which deposit is being spent. The practical effect is not "invisibility" but loss of deterministic linkability: investigators can often still estimate probabilities, but direct graph tracing becomes substantially harder when withdrawals are delayed and the pool is liquid. (Brownworth, Durfee, Lee, & Martin, 2024).

Two design features matter for enforcement. First, non-custodial execution: there is no operator holding user funds in the traditional sense, which reduces the utility of licensing, record-keeping, and supervisory levers used for custodial services. Second, immutability: once deployed, the smart contracts cannot easily be modified, and governance may be minimal or dispersed. These features complicate sanctioning or regulating the protocol "as such," and they help explain why enforcement strategies often shift toward interfaces (web front ends), relayers, and centralized off-ramps.

3.1.2 Monero (mandatory privacy)

Monero is engineered to make privacy the default. It uses stealth addressing to conceal recipients, ring signatures with decoys to obscure which input is being spent, and Ring Confidential Transactions (RingCT) to hide amounts. Ledger-level analysis therefore has limited visibility into value flow compared to transparent chains. However, technical research demonstrates that anonymity is not binary: traceability depends on parameter choices and on how users behave. (Noether et al., 2016).

Empirical analysis of Monero traceability documents weaknesses that can enable probabilistic deanonymization under certain conditions—particularly when decoy selection or usage distributions create identifiable patterns. These findings do not eliminate Monero's privacy advantage, but they clarify that "untraceable" is an over-statement; investigative friction rises, but does not become infinite.

3.1.3 Zcash (optional privacy)

Zcash provides both transparent and shielded transaction types. Users may transact entirely transparently, entirely within the shielded pool, or through mixed interactions. The optional model creates an ecosystem-level risk: if only a minority of users use shielded transactions, the anonymity set may be small, and structured usage patterns can shrink it further. Empirical work on Zcash shows that identifiable patterns of interaction between transparent and shielded pools can allow heuristics that reduce effective anonymity for many users. (Kappos, Yousaf, Maller, & Meiklejohn, 2018).

Taken together, the three AETs illustrate a key point for sanctions and AML: the relevant question is rarely whether privacy exists, but how often it is used, at what liquidity levels, and how privacy interacts with interfaces and off-ramps.

- Implementation details that matter for investigations

Tornado Cash pools were historically structured around fixed denominations (e.g., discrete deposit sizes in ETH or ERC-20 equivalents). Fixed denominations can support privacy by ensuring that many deposits are indistinguishable in amount, but they can also provide investigators with constraints: if only a small number of deposits occur in a period, or if withdrawals cluster after specific events, investigators can combine timing, exchange-interaction data, and off-chain intelligence to generate narrowed suspect sets. The presence of relayers—third parties that submit withdrawal transactions and pay gas fees in exchange for a fee—adds another layer: relayers can improve usability, but they also create service points that can be monitored, regulated, or denied access by infrastructure providers.

From a compliance perspective, the most consequential observation is that the mixer's on-chain code does not exist in isolation. Typical user journeys include web interfaces, wallet software, RPC providers, and centralized exchanges used before or after mixing. In sanctions settings, authorities can influence risk by shaping these adjacent layers even when the contracts themselves remain immutable.

- Traceability research and what it implies (without over-claiming)

Peer-reviewed work on Monero traceability identifies concrete weaknesses in historical decoy selection strategies and the resulting age distribution of "mixins." In practical terms, if decoys are sampled in a way that makes the real input systematically "newer" than decoys, an analyst can apply a newest-output heuristic to guess the likely real spend with non-trivial accuracy. A related effect is 'chain-reaction' analysis: once some outputs are identified as real spends, other transactions can become vulnerable by elimination. These findings have led Monero to change parameters over time; the key takeaway is not that Monero is easily traceable, but that privacy performance is an empirical question that depends on design, wallet behavior, and ecosystem practices.

- Optional privacy and the anonymity-set problem

Zcash's design allows multiple transaction patterns: transparent-to-transparent (t→t), transparent-to-shielded (t→z), shielded-to-transparent (z→t), and shielded-to-shielded (z→z). When the shielded pool is sparsely used, t→z and z→t transactions can create identifiable funnels, especially when users repeatedly shield and deshield similar amounts or when exchanges implement structured workflows. Empirical analysis shows that even when shielded transactions are cryptographically strong, ecosystem-level behavior can shrink effective anonymity through clustering and pattern matching.

3.1.4 Why 'AET effectiveness' is conditional

Across the three AETs, effectiveness depends on three practical variables that are often missing from generalized, AI-like discussions of "privacy."

(a) Liquidity and crowd size. Mixers rely on pooling: the larger the pool and the more heterogeneous the user base, the harder attribution becomes. Conversely, thin liquidity, fixed denominations, or short time windows can yield informative signals.

(b) Interaction with compliant infrastructure. Even if on-chain traces are weak, cash-out typically requires interaction with regulated exchanges, stablecoin issuers, or fiat gateways. When those actors enforce sanctions screening and freeze authority, they can re-introduce control points that AETs do not remove.

(c) User behavior and default settings. Zcash illustrates how optional privacy can underperform when users do not adopt shielded transfers consistently. Monero illustrates how protocol defaults can strengthen privacy, but also how parameter choices and decoy sampling matter.

Accordingly, the policy question is best framed as: which combinations of tools, liquidity conditions, and off-ramp environments yield meaningful sanctions-evasion capability?

3.1.5 Investigative responses: what still works when on-chain linkability is weak

AETs reduce the value of purely on-chain tracing, but investigations rarely rely on chain data alone. Common approaches include: (i) exploiting interface data (web logs, wallet telemetry, relayer records where available), (ii) subpoenas and information requests to centralized exchanges and custodians, (iii) attribution through reuse of infrastructure (developer repos, IP patterns, hosting), and (iv) probabilistic and clustering methods that combine timing, denomination, and behavioral fingerprints. The practical

effect of AETs is therefore to shift investigations toward higher-cost, multi-source intelligence rather than to render investigations impossible. This shift matters for policy because it changes which institutions have comparative advantage (FIUs, cyber units, intelligence services) and how resource-intensive routine compliance becomes.

Table 1. Mechanisms, security objectives, and investigative implications of selected AETs

Technology	Security objective	Core mechanism	Limits & investigative implications (summary)	Representative sources
Tornado Cash (Ethereum mixer)	Break deposit→withdrawal linkage on-chain	Pool-based mixing with ZK proofs; non-custodial smart contracts	Raises attribution cost; effectiveness depends on pool liquidity, timing, and off-ramp controls; enforcement often targets interfaces/infrastructure	U.S. Treasury/OFAC (2022); Brownworth et al. (2024)
Monero (privacy coin)	Hide sender, receiver, and amount by default	Stealth addresses, ring signatures (decoys), RingCT (confidential amounts)	Ledger has low observability; empirical work shows probabilistic weaknesses under certain parameter/usage regimes	Noether et al. (2016); Möser et al. (2018)
Zcash (privacy-capable coin)	Enable private transfers via shielded pool	Optional shielded transactions (zk-SNARKs) and transparent transactions	Optionality shrinks anonymity set when adoption is low; heuristics can link t↔z usage patterns	Kappos et al. (2018)

3.2. Exploitation for sanctions evasion and national-security financing

3.2.1 Illicit finance pathways in DeFi: a practical decomposition

Sanctions evasion and laundering through DeFi typically follow a modular pipeline: (i) acquisition (theft, fraud, ransomware, or state-sponsored cyber operations), (ii) conversion and fragmentation (swapping assets, splitting outputs, moving across chains via bridges), (iii) obfuscation (mixing or privacy coins), and (iv) integration (cash-out via centralized exchanges, OTC brokers, or conversion into spendable assets). AETs primarily serve the obfuscation stage but can also be used to reduce attribution risk during conversion and integration.

Official U.S. Treasury analysis emphasizes that DeFi protocols may be exploited in multiple stages, particularly where compliance controls are weak, governance is diffuse, or interfaces enable anonymous access. The FATF has similarly highlighted gaps where decentralized architectures blur the identification of "responsible persons" for AML obligations. The resulting enforcement problem is not only technical, but institutional: existing AML frameworks assume regulated intermediaries that can be compelled to collect identity data and implement controls. (U.S. Department of the Treasury, 2023; FATF, 2024).

3.2.2 Tornado Cash: enforcement signal and evidentiary posture

In August 2022, OFAC designated Tornado Cash in connection with laundering proceeds of cybercrime and specifically referenced laundering associated with North Korea-linked Lazarus Group. Whatever one's view of the breadth of the designation, the action demonstrates that U.S. authorities considered a non-custodial mixer to be materially relevant for national-security risk. Importantly, OFAC's narrative did not require the claim that Tornado Cash alone enables laundering; rather, it treated the mixer as a high-risk component in broader laundering pipelines. (U.S. Department of the Treasury, Office of Foreign Assets Control [OFAC], 2022).

Subsequent empirical analysis examined the impacts and behavioral responses to the sanctions. The literature on sanctioning autonomous protocols is still developing, but the evidence suggests substitution effects: when one tool becomes costly or risky to use (due to sanctions exposure or compliance controls at

interfaces), illicit actors may shift to other AETs, other bridges, or less-compliant venues. This implies that enforcement is a risk-shaping intervention rather than a complete technical solution.

3.2.3 Privacy coins in sanctions context: capability versus adoption

From a capability standpoint, privacy coins can provide stronger on-chain privacy than mixers because they reduce observability at the base-layer protocol level. However, whether they are used for sanctions evasion depends on liquidity, exchange support, and the availability of off-ramps. Jurisdictions and exchanges vary in their tolerance of privacy coins, and delistings or restricted support can impose practical constraints. As a result, privacy coins can be attractive for certain threat models but may be less convenient at scale than mixing combined with cross-chain swaps and centralized exchange cash-out.

Zcash's optional privacy model illustrates a related trade-off: it can be used privately, but if shielded usage is rare and interactions are patterned, anonymity can degrade. Monero offers mandatory privacy, but its integration into regulated off-ramps is often constrained. These frictions help explain why illicit actors commonly use a hybrid approach—mixing on highly liquid chains, rapid cross-chain movement, and strategic use of venues with weak compliance—rather than relying exclusively on a single privacy coin.

3.2.4 Bridges, stablecoins, and 'composability laundering'

DeFi's composability enables a laundering strategy that can be described as 'composability laundering': an actor chains together swaps, bridges, mixers, and centralized off-ramps in a sequence that is individually commonplace but collectively opaque. Bridges are particularly consequential because they convert assets between chains, often breaking investigative continuity when different ledgers have different observability and different compliance ecosystems. Stablecoins can also function as a risk-transfer instrument: if a stablecoin issuer has freeze authority and enforces sanctions, the stablecoin may be a control point; if illicit proceeds remain in non-freezable assets or move across chains before stablecoin conversion, the window for intervention can be narrow.

From a policy perspective, this suggests that focusing only on one AET (e.g., mixers) may miss the broader laundering architecture. The objective is therefore to identify the minimal set of chokepoints that consistently appear across pipelines—often centralized off-ramps and key infrastructure—while recognizing that attackers can re-compose pipelines when a chokepoint tightens.

3.2.5 What the evidence base can and cannot establish

Public reporting on AET use for illicit finance is uneven. Official documents (e.g., U.S. Treasury risk assessments and OFAC press releases) can provide credible signals about observed laundering typologies, but they often omit methodological details for operational reasons. Law enforcement and FIU reporting may also be episodic, focusing on prominent cases. In parallel, technical research can measure protocol properties and traceability limits, but it cannot always connect those properties to real-world sanction-evasion outcomes.

To manage these limitations, this paper treats official enforcement narratives as evidence of policy salience and observed typologies, not as exhaustive measurement. For broader threat context, Europol's IOCTA reporting and similar assessments are used to frame the evolving role of crypto assets in organized crime and cyber-enabled laundering, while recognizing that such reports aggregate diverse national inputs and do not isolate DeFi mechanisms with precision. These constraints reinforce the value of a mechanism-based approach: even when totals are uncertain, the causal pathway from privacy mechanism to reduced observability can be analyzed with technical clarity. (Europol, 2024).

3.2.6 Security incidents, MEV, and laundering opportunities

Large-scale cyber theft is a primary upstream driver of laundering demand. In DeFi, exploits can occur through smart-contract vulnerabilities, governance failures, key compromise, or bridge design weaknesses. These incidents interact with AETs in two ways. First, attackers need rapid conversion and obfuscation pathways to reduce interdiction risk immediately after an exploit. Second, the same ecosystem features that enable MEV and adversarial transaction ordering—documented in the literature on

frontrunning and miner/maximal extractable value (MEV)—also illustrate how transaction execution is strategic rather than neutral in DeFi, complicating monitoring and incident response. (Daian et al., 2019).

While MEV research is not primarily an illicit-finance literature, it supports a broader claim: DeFi is a security-sensitive environment where adversaries adapt rapidly and where protocol-level incentives can produce behavior that undermines fairness and predictability. For sanctions and AML, this means that 'static' rule sets will be outpaced unless enforcement is adaptive and focused on durable chokepoints. (Daian et al., 2019).

3.3. Enforcement architecture under stress: Tornado Cash as a legal and policy case study

3.3.1 The Fifth Circuit decision and the 'autonomous code' problem

The Fifth Circuit's decision in Van Loon v. Department of the Treasury directly addressed whether immutable smart contracts associated with Tornado Cash could be treated as "property" subject to blocking under IEEPA-based sanctions authorities. The court's reasoning (whatever one's normative view) is significant for policy design: it underscores that sanctions frameworks built around persons, entities, and property may not map cleanly onto autonomous software that lacks a traditional owner/operator relationship. (Van Loon v. Department of the Treasury, 2024).

3.3.2 Delisting and its implications for future tools

In March 2025, OFAC removed Tornado Cash from the SDN List. The delisting does not imply that laundering risk disappeared; rather, it reflects a re-alignment between enforcement posture and the legal/institutional constraints clarified by litigation and related policy considerations. For compliance practitioners, the key implication is that enforcement strategies may increasingly focus on controllable layers: hosted services, identifiable operators, relayers that provide transaction services, centralized exchanges, stablecoin issuers, and other infrastructure that can implement screening and blocking. (U.S. Department of the Treasury, 2025; OFAC, 2025).

3.3.3 What sanctions can and cannot do in DeFi

Sanctions remain a powerful tool for shaping risk at interfaces and off-ramps. However, sanctions are not a substitute for technical or governance measures that reduce the ability of illicit actors to exploit protocol design. The Tornado Cash episode suggests a need for more discriminating interventions—targeting identifiable service provision (e.g., relayers or hosted front ends) and downstream integration points—rather than attempting to treat autonomous code as a conventional sanctions target.

3.3.4 The compliance lesson: code is hard to 'block,' services are easier

A practical compliance lesson from the Tornado Cash episode is that sanctions enforcement scales more reliably against services and infrastructure than against immutable contracts. Front ends can be taken down or geoblocked; relayers and hosting providers can be compelled or can voluntarily restrict service; exchanges can refuse deposits linked to high-risk contracts; and issuers of centralized stablecoins can freeze funds. These interventions do not eliminate privacy tools but they reshape the risk surface: they reduce the convenience of laundering and increase the probability that illicit actors must touch a regulated perimeter at some point.

At the same time, an overly broad approach can create false positives and collateral damage. For example, autonomous contracts can be used by legitimate users for privacy and security reasons; indiscriminate screening may lead to 'taint' concerns that trap innocent users. A mature compliance posture therefore requires more granular risk indicators—combining typologies, timing, interaction patterns, and known threat-actor infrastructure—rather than simple address blocking.

3.3.5 Substitution, displacement, and the risk of policy whack-a-mole

A recurrent enforcement risk is displacement: restricting one tool may push illicit actors toward alternatives rather than eliminating laundering. Mixers can be substituted by other mixers, by cross-chain swaps that fragment tracing, or by privacy coins where off-ramps exist. Likewise, if exchanges tighten

controls, actors can shift to OTC brokers or to jurisdictions with weaker enforcement. This is not an argument against enforcement; it is an argument for defining success realistically. The measurable objective is often to increase friction, reduce scalability of laundering pipelines, and create actionable intelligence at conversion points.

3.4. Regulatory baseline: FATF and U.S. financial-crime authorities

3.4.1 FATF standards and the 'DeFi gap'

The FATF framework remains the primary international baseline for AML/CFT treatment of virtual assets. In its guidance and targeted updates, FATF has consistently pushed for (i) extending AML/CFT obligations to virtual asset service providers (VASPs), (ii) implementing the 'travel rule' for relevant transfers, and (iii) closing gaps created by decentralization narratives that obscure responsible persons. A recurring theme in FATF updates is that decentralization does not automatically remove accountability: where a natural or legal person has 'sufficient influence' or provides services that enable transfers (e.g., operating an exchange interface or exercising control over a protocol), that actor may fall within AML obligations. At the same time, FATF acknowledges that some arrangements may lack clear intermediaries, creating supervision and enforcement challenges. (FATF, 2024; FATF, 2025).

These standards become practically relevant in DeFi because compliance is frequently fragmented: token issuance may be centralized while trading is decentralized; stablecoins may have a centralized issuer while liquidity provision is decentralized; bridges may be operated by identifiable validator sets while user access is permissionless. The result is regulatory arbitrage potential. Sophisticated illicit actors exploit the seams between these layers, moving value across protocols that are each only partially within the regulatory perimeter. (FATF, 2025).

3.4.2 FinCEN: mixers as a money-laundering concern

In the United States, FinCEN has treated mixing as a recurrent money-laundering typology and has issued guidance and advisories clarifying how Bank Secrecy Act obligations apply to certain virtual currency business models. FinCEN has also pursued rulemaking that frames 'convertible virtual currency mixing' as a class of transactions of primary money-laundering concern, signaling a willingness to use strong regulatory levers against mixing activity. While the precise scope and final form of these measures depend on legal process and implementation, the policy direction is clear: U.S. financial-crime authorities view mixing as a high-risk function regardless of whether it is provided by a custodial service or via decentralized infrastructure. (FinCEN, 2019a, 2019b, 2023).

4.DISCUSSION: MITIGATION OPTIONS AND TRADE-OFFS

Mitigation approaches fall into four categories. (U.S. Department of the Treasury, 2023).

(1) Entry and exit controls. The most consistently feasible controls remain at centralized exchanges, custodians, stablecoin issuers, and fiat gateways. Improved sanctions screening, transaction monitoring informed by typologies, and coordinated information sharing can meaningfully reduce integration opportunities for illicit proceeds. These measures do not eliminate mixing or privacy coins, but they raise the cost of cash-out.

(2) Infrastructure-layer interventions. In DeFi, many user interactions occur through web front ends, API providers, RPC endpoints, relayers, and bridge operators. These actors can implement risk controls (blocking sanctioned addresses, refusing to relay transactions, or limiting exposure to high-risk contracts) even when the underlying contracts are immutable. The limitation is evasion: users can self-host interfaces or route through alternative infrastructure. Nevertheless, infrastructure interventions can reduce scale and convenience.

(3) Protocol-level design choices. Some protocols can incorporate compliance-enabling features without surrendering non-custodial design—for example, optional compliance modules, circuit-breaker controls for known exploit patterns, or disclosure-selective privacy mechanisms. These approaches are

unevenly applicable, and they can conflict with the ideological and competitive pressures in DeFi. Still, they are more durable than purely external controls when adopted.

(4) Legal clarity and accountability. Where there are identifiable developers, operators, or service providers, legal accountability can complement technical controls. The challenge is to distinguish legitimate privacy engineering from intentional facilitation of money laundering. Overbroad liability could chill security research and legitimate privacy use. A workable regime therefore needs definitional precision and safe harbors for good-faith development and security work.

The trade-off is not privacy versus security in the abstract, but which forms of privacy and which threat models are being prioritized. Some privacy uses (protecting donors or vulnerable users) are socially valuable; other uses (laundering sanctioned proceeds) are socially harmful. Policy responses that treat all privacy as suspect risk both ineffectiveness (driving activity to less visible venues) and collateral damage (weakening digital security and civil liberties). The mitigation agenda should therefore be anchored in measurable risk reduction and in targeted interventions where control is feasible.

(5) Privacy-preserving compliance concepts

A growing research and policy conversation explores whether privacy and compliance can co-exist through selective disclosure. Examples include 'view keys' or audit keys (allowing a user to disclose transaction details to a regulator or counterparty under defined conditions), zero-knowledge 'proof-of-innocence' concepts (proving funds are not derived from a sanctioned set without revealing full history), and regulated disclosure at conversion points (e.g., requiring enhanced due diligence for shielded or mixed funds when entering a custodial platform). These ideas are not yet uniform in implementation, but they matter because they shift the debate from a binary 'privacy versus enforcement' frame to an engineering-and-governance frame. (FATF, 2024).

Any privacy-preserving compliance design must be evaluated against attacker adaptation. If disclosure mechanisms can be bypassed by avoiding the regulated perimeter, they become relevant primarily at off-ramps. But even then, they can raise the expected cost of illicit finance while preserving legitimate privacy for low-risk users.

5.CONCLUSION

This article analyzed how three AET exemplars—Tornado Cash, Monero, and Zcash—create forensic friction that can be operationalized for sanctions evasion and the financing of national-security threats. The central claim is mechanism-based: privacy tools change observability and attribution, which in turn changes the cost and feasibility of enforcement. Yet the analysis also shows that AET effectiveness is conditional. Mixers depend on liquidity and timing; Zcash privacy depends on shielded-pool adoption; Monero privacy is strong but not absolute and is constrained by off-ramp availability.

The Tornado Cash enforcement episode illustrates a second conclusion: sanctions and AML frameworks built around intermediaries struggle when the target is autonomous code. The policy response that scales is therefore likely to be layered—entry/exit controls, infrastructure-layer risk management, selective protocol design choices, and clearer legal boundaries—rather than a single "ban" or a single compliance fix. For journal publication, these conclusions imply that scholarship should move beyond generic claims about DeFi "risk" and instead specify which mechanisms, which choke points, and which institutional constraints are decisive.

Answering the research questions explicitly: RQ1 is addressed by showing that each AET undermines deterministic attribution through distinct mechanisms, with conditional effectiveness. RQ2 is addressed by synthesizing official enforcement and risk-assessment materials that link AETs—especially mixing—to laundering typologies used by state-linked actors, while acknowledging measurement limits. RQ3 is addressed through the Tornado Cash case, illustrating both the reach and the constraints of sanctions when applied to autonomous code. RQ4 is addressed by a layered mitigation portfolio that prioritizes interfaces, off-ramps, infrastructure, and privacy-preserving compliance design rather than expecting protocol-level prohibition to succeed.

REFERENCES

Aramonte, S., Huang, W., & Schrimpf, A. (2021). DeFi risks and the decentralisation illusion. BIS Quarterly Review (December 2021). Bank for International Settlements. Retrieved from: https://www.bis.org/publ/qtrpdf/r_qt2112b.pdf

Brownworth, D., Durfee, Z., Lee, M., & Martin, A. (2024). Regulating decentralized systems: Evidence from sanctions on Tornado Cash (Staff Report No. 1112). Federal Reserve Bank of New York. https://doi.org/10.59576/sr.1112

Chainalysis. (2024). The 2024 Crypto Crime Report. Chainalysis. Retrieved from: https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/

Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L., & Juels, A. (2019). Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges. *ArXiv, abs/1904.05234*.

European Union Agency for Law Enforcement Cooperation (Europol). (2025). Internet Organised Crime Threat Assessment (IOCTA) 2025. Europol. Retrieved from: https://www.europol.europa.eu/publications-events/main-reports/iocta-report

FATF (2024), Targeted Upate on Implementation of the FATF Standards on Virtual Assets/VASPs, FATF, Paris, France, https://www.fatf-gafi.org/

FATF (2025), Targeted Upate on Implementation of the FATF Standards on Virtual Assets/VASPs, FATF, Paris, France, https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/targeted-update-virtualassets-vasps-2025.html

Financial Crimes Enforcement Network. (2019a). Application of FinCEN's regulations to certain business models involving convertible virtual currencies (FIN-2019-G001). U.S. Department of the Treasury. Retrieved from: https://www.fincen.gov/system/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf

Financial Crimes Enforcement Network. (2019b). Advisory on illicit activity involving convertible virtual currency mixers (FIN-2019-A003). U.S. Department of the Treasury. Retrieved from: https://www.fincen.gov/system/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf

Financial Crimes Enforcement Network. (2023). Proposal of special measure regarding convertible virtual currency mixing as a class of transactions of primary money laundering concern (FINCEN-2023-0016) (Notice of proposed rulemaking). U.S. Department of the Treasury. Retrieved from: https://www.federalregister.gov/documents/2023/10/23/2023-23449/proposal-of-special-measure-regarding-convertible-virtual-currency-mixing-as-a-class-of-transactions

Kappos, G., Yousaf, H., Maller, M., & Meiklejohn, S. (2018). An empirical analysis of anonymity in Zcash. In Proceedings of the 27th USENIX Security Symposium (pp. 463–477). USENIX Association. Retrieved from: https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-kappos.pdf

Möser, M., Soska, K., Heilman, E., Lee, K., Heffan, H., Srivastava, S., Hogan, K., Hennessey, J., Miller, A., Narayanan, A., & Christin, N. (2018). An empirical analysis of traceability in the Monero blockchain. Proceedings on Privacy Enhancing Technologies, 2018(3), 143–163. https://doi.org/10.1515/popets-2018-0025

Noether, S., & Mackenzie, A. (2016). Ring confidential transactions. Ledger, 1, 1–18. https://doi.org/10.5195/LEDGER.2016.34

Schär, F. (2021). Decentralized finance: On blockchain- and smart contract-based financial markets. Federal Reserve Bank of St. Louis Review, 103(2), 153–174. https://doi.org/10.20955/r.103.153-74

U.S. Department of the Treasury, Office of Foreign Assets Control. (2022). U.S. Treasury sanctions notorious virtual currency mixer Tornado Cash. U.S. Department of the Treasury. Retrieved from: https://home.treasury.gov/news/press-releases/jy0916

U.S. Department of the Treasury, Office of Foreign Assets Control. (2025). Cyber-related designation removal: Tornado Cash. U.S. Department of the Treasury.

U.S. Department of the Treasury. (2023). Illicit finance risk assessment of decentralized finance. U.S. Department of the Treasury. Retrieved from: https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf

U.S. Department of the Treasury. (2025). Treasury delists Tornado Cash. U.S. Department of the Treasury. Retrieved from: https://home.treasury.gov/news/press-releases/sb0057

Van Loon v. Department of the Treasury, No. 23-50669 (5th Cir. 2024). Retrieved from: https://law.justia.com/cases/federal/appellate-courts/ca5/23-50669/23-50669-2024-11-26.html