Inside the Crypto Laundering Machine: A Taxonomic Study of Crypto Money Laundering Schemes and Countermeasures

by

Hesam Sarkhosh

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Mathematics
in
Computer Science

Waterloo, Ontario, Canada, 2026

© Hesam Sarkhosh 2026

Author's Declaration

This thesis consists of material all of which I authored or co-authored: see Statement of Contributions included in the thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Statement of Contributions

A substantial portion of this thesis is based on my previously published conference paper [240] (H. Sarkhosh, U. Maroof, and D. Barradas, "The Dark Art of Financial Disguise in Web3: Money Laundering Schemes and Countermeasures," in Proceedings of the 20th Annual APWG Symposium on Electronic Crime Research (eCrime), 2025), for which I am the first author. All of the content and sections of that paper constitute my original research contribution and are reused in this thesis. In adapting this work for a master's thesis, I have elaborated on several sections to provide additional detail and context, and I have refined the proposed taxonomy of money laundering schemes in Web3—expanding it with new content and updating it to reflect the current state of the field.

Abstract

The rise of *Web3* and *Decentralized Finance (DeFi)* has enabled borderless access to financial services empowered by smart contracts and blockchain technology. However, the ecosystem's trustless, permissionless, and borderless nature presents substantial regulatory challenges. The absence of centralized oversight and the technical complexity create fertile ground for financial crimes. Among these, *money laundering* is particularly concerning, as in the event of successful scams, code exploits, and market manipulations, it facilitates covert movement of illicit gains. Beyond this, there is a growing concern that cryptocurrencies can be leveraged to launder proceeds from drug trafficking, or to transfer funds linked to terrorism financing.

Crypto money laundering remains diverse and insufficiently systematized, with prior work fragmented, dated, or limited to individual vectors. We address this through a systematic, interdisciplinary review of academic, regulatory, and industry sources. We first establish the necessary background: how the classical placement, layering and integration stages of laundering adapt to Web3, the pseudonymity that underpins these schemes, and the fact that tracing cryptocurrency transactions requires access to data traces that come in varied forms. Building on this foundation, we consolidate known schemes into a taxonomy of money laundering in Web3, organizing laundering into a set of high-level obfuscation strategies and the intermediary mechanisms through which they are realized, while also identifying emerging schemes not previously documented. We systematize these intermediary mechanisms along several dimensions, including the intent behind their design and whether they are purpose-built privacy tools or exploited infrastructure, their custodial or non-custodial nature, their deployment layer, and their underlying privacy techniques.

We then turn to the countermeasures raised against these schemes, spanning both detection, which uncovers illicit activity after it occurs, and prevention, which limits the opportunity for laundering in the first place, as pursued across academia, regulation, and industry. From this synthesis we draw out the open challenges that remain, and chart future research directions toward a more transparent Web3 financial ecosystem, offering insights for researchers, policymakers, and practitioners.

Acknowledgements

I am deeply grateful to my supervisor, Professor Diogo Barradas, whose guidance, patience, and genuine care consistently went beyond what his role required. His mentorship shaped not only this thesis but also my growth as a researcher, and for that I am sincerely thankful.

I would also like to thank everyone who supported and accompanied me along this path and throughout my academic journey. Your encouragement, in ways both large and small, made this work possible.

This work was supported by Canada's National Cybersecurity Consortium and Mastercard Technologies Canada ULC.

Table of Contents

Author's Declaration ii

Statement of Contributions iii

Abstract iv

Acknowledgements v

List of Figures ix

List of Tables x

1 Introduction 1

2 Foundations of Web3 and DeFi 3

2.1 Blockchains and consensus 3

2.2 Smart contracts 4

2.3 Crypto assets 5

2.4 Cryptocurrency wallets 6

3 Survey Methodology 8

3.1 Research Questions 8

3.2 Review Methodology 9

3.3 Search Strategy and Sources . . . 9
3.4 Inclusion and Exclusion Criteria . . . 10
3.5 Study Selection . . . 10
3.6 Incorporating Grey and Industry Literature . . . 11
3.7 Taxonomy Construction . . . 12
3.8 Scope, Boundaries, and Threats to Validity . . . 13

4 Primer on Crypto Money Laundering **15**
4.1 Deanonymization in Web3 . . . 16
4.2 Typologies of Data for Web3 AML Forensics . . . 17

5 Taxonomy of Crypto Money Laundering **19**
5.1 General Strategies . . . 19
5.1.1 Transaction Flow Obfuscation (TFO) . . . 20
5.1.2 Commingling . . . 22
5.1.3 Chain-hopping . . . 23
5.1.4 Disconnected fund flow (DFF) . . . 23
5.1.5 Exploit Subjective Valuations . . . 25
5.1.6 Exploit Regulatory Gaps . . . 26
5.2 Intermediary Mechanisms . . . 27
5.2.1 Privacy-enhancing Technologies (PETs) . . . 28
5.2.1.1 PETs: Custodial Services . . . 34
5.2.1.2 PETs: Layer-1 Solutions . . . 35
5.2.1.3 PETs: Chain Extensions . . . 36
5.2.1.4 PETs: Layer-2 Privacy Rollups . . . 37
5.2.1.5 PETs: Application-Layer Solutions . . . 37
5.2.1.6 PETs: Off-Chain Coordinator Overlay . . . 39
5.2.2 Exploited Infrastructures . . . 40

5.2.2.1 Cryptocurrency Exchanges . . . 40
5.2.2.2 Cross-chain Bridges . . . 42
5.2.2.3 DeFi Mechanisms . . . 42
5.2.2.4 Non-Fungible Tokens (NFTs) . . . 45
5.2.2.5 Cryptocurrency ATMs . . . 47
5.2.2.6 Card-Based Instruments . . . 47
5.2.2.7 Online Gambling Platforms . . . 50
5.2.2.8 Initial Coin Offerings (ICOs) . . . 51
5.2.2.9 Consensus Protocols . . . 52
5.2.2.10 Payment Channel Networks (PCNs) . . . 53

6 Crypto Money Laundering Countermeasures 55
6.1 Detection Measures . . . 55
6.2 Prevention Measures . . . 56

7 Open Challenges and Future Directions 59

8 Conclusion 61

References 63

Appendix A: Literature Comparison 93

List of Figures

3.1 Study selection process. 11

5.1 Transaction flow obfuscation (TFO) patterns. 20
5.2 Disjoint reciprocal transfers (DRT). 24
5.3 Taxonomy of crypto money laundering schemes. 27

List of Tables

A.1 Cryptocurrency laundering schemes coverage across existing surveys. . . . 94

Chapter 1

Introduction

Blockchains emerged as a transformative technology aimed at decentralization, transparency, and trustless transactions. This vision materialized in 2009 with the launch of *Bitcoin* [205], the first decentralized digital currency enabling peer-to-peer (P2P) transfers without intermediaries. Bitcoin marked a paradigm shift, replacing institutional trust with cryptographic proof [21]. The second major milestone was Ethereum [37], which introduced smart contracts, expanding blockchains into programmable platforms for decentralized applications (*dApps*) [21]. As adoption grew, so did the broader idea of decentralized systems, culminating in the concept of *Web3*, coined in 2014, to describe a decentralized alternative to the traditional internet [80]. Web3's emergence catalyzed the rise of *decentralized finance (DeFi)*—a blockchain-based, P2P financial system offering alternatives to traditional mechanisms such as lending and investment [300]. As of July 2025, the global cryptocurrency market cap reached $3.8 trillion, with DeFi accounting for $135 billion in total value locked (TVL), demonstrating DeFi's expanding global impact [58, 72].

Critics have long warned that the unregulated nature of Web3 facilitates illicit activity [300], including fraud, scams, wash trading, and code exploits [306]. The presence of high-value assets continues to attract cybercriminals; in 2024 alone, $2.2 billion was stolen from Web3 platforms [266], followed by the recent $1.5 billion *Bybit* hack in February 2025—considered the largest crypto theft to date [142]. A key driver behind such crimes is the ability to obscure the origin of illicit assets and integrate them into the legitimate economy—a process known as *money laundering* [211]. Because this ability is what ultimately lets criminals profit from stolen funds, it acts as a core incentive for financial crime; conversely, disrupting it undermines that incentive and helps deter such activity more broadly. Frequently associated with drug trafficking and terrorism financing, money laun-

dering is increasingly leveraging Web3 [306, 157, 63]; between 2019 and 2023, an estimated $93 billion was laundered via cryptocurrencies [265].

Despite growing concern, crypto money laundering schemes remain highly diverse and insufficiently systematized. While works such as Sneck [252], Comolli and Korver [63], and Almeida et al. [6] provide partial overviews, they often lack depth, breadth, or up-to-date coverage. Foundational studies like Möser et al. [204], though influential, are now outdated and omit recent developments. Even more recent contributions, such as Lin et al. [176], fall short of offering a comprehensive taxonomy of laundering schemes. A parallel body of work examines only specific laundering vectors—such as *mixing services* [248, 10, 234, 67], *initial coin offerings* (ICOs) [17], *cross-chain bridges* [143], and *non-fungible tokens* (NFTs) [306, 199]. While informative, these studies remain fragmented and lack synthesis across the broader laundering landscape.

For addressing the above gap, this work delivers a survey that consolidates known cryptocurrency-based money laundering approaches identified in academic and regulatory sources. We categorize these approaches by their overarching strategies and the tools or intermediaries employed, and map them to the respective stages of the laundering process. Recognizing the role of data in anti-money laundering efforts, we also examine the types and sources of data relevant to each approach. We provide a comparison with previous surveys in Appendix A.

We begin by outlining the foundations of Web3 and DeFi (§2) and describing our methodology for data collection and analysis (§3). We then examine how traditional laundering stages adapt to Web3 and the challenges of deanonymization in this emerging ecosystem (§4). Next, we present our taxonomy of laundering schemes (§5), including general obfuscation strategies (§5.1) and intermediary mechanisms exploited throughout the laundering process to implement these strategies (§5.2). We conclude with a survey of countermeasures from academia, regulators, and industry (§6), and outline open challenges and future research directions (§7).

Chapter 2

Foundations of Web3 and DeFi

This section outlines foundational concepts essential for understanding Web3 and DeFi. Key topics include the underlying blockchain infrastructures, classification of digital assets, and the role of crypto wallets in asset management. Understanding how value is created, stored, and moved in this ecosystem is critical for assessing its susceptibility to money laundering.

2.1 Blockchains and consensus

A blockchain is a decentralized, cryptographically linked ledger maintained across a P2P network [310, 163]. Such networks are either *permissionless*, where anyone may join, transact, and validate, or *permissioned*, where only vetted participants hold these rights [21]. To ensure consistency and *Byzantine Fault Tolerance* (BFT)—resilience to malicious parties—blockchains rely on consensus protocols [310]. Bitcoin introduced the *Nakamoto consensus* [205], using *proof of work (PoW)* to achieve consensus by requiring nodes to solve computational puzzles; the longest valid chain is treated as authoritative [310, 163]. In comparison, Proof of Stake (PoS) protocols select block proposers based on the amount of possessed and locked assets (stake), reducing energy use by eliminating intensive computations. Both models incentivize participation through transaction fees and block rewards, and aim to maintain integrity and immutability.

Blockchains also differ in how they record state. The *unspent transaction output* (UTXO) model used by Bitcoin treats coins as discrete outputs consumed and recreated by each transaction [205], whereas account-based chains such as Ethereum keep running

balances updated through state transitions [304, 311]. This shapes forensic tracing: UTXO co-spending exposes multi-input heuristics that cluster addresses spent together [189], while the account model invites interaction-based and behaviour-based clustering of reused addresses [293].

Public blockchains are at once *transparent*, since every transaction is permanently and openly recorded, and *pseudonymous*, as addresses are not inherently tied to real identities [7]. This is double-edged. Immutability and visibility enable forensic reconstruction of fund flows, yet pseudonymity is exactly what launderers exploit, framing a central privacy–transparency trade-off [75]. Sustaining decentralization and security at scale further strains throughput, so base blockchain networks, also known as *Layer-1* blockchains, often sacrifice performance [311]. *Layer-2* solutions improve blockchain scalability by moving computation and execution off the main chain, settling back on Layer-1 only periodically to cut cost and latency [132, 224], but at a price. Off-chain activity can weaken Layer-1's immutability, security, and on-chain traceability while, by design, either strengthening privacy or adding new trust assumptions [132].

2.2 Smart contracts

Conceptualized by Szabo in the 1990s [261], smart contracts are self-executing programs that enforce predefined rules without intermediaries [306]. Unlike traditional contracts, enforcement is automatic and encoded within the contract logic [31, 300]. Ethereum [37] extended blockchains into programmable state machines, enabling Turing-complete logic via smart contracts [172]. These contracts execute atomically—either fully completing or reverting without side effects [300]. By providing this programmable application layer, smart contracts form the foundation of Web3 and underpin the development of decentralized applications (*dApps*) [4, 306, 300].

Contract codes run inside a deterministic virtual machine; the *Ethereum Virtual Machine* (EVM) is the de facto standard, and *EVM-compatible* chains such as BNB Smart Chain [23] reuse its bytecode and tooling, whereas *non-EVM* platforms such as Solana [166] adopt different execution models [304, 311]. This programmability turns blockchains into application deployment platforms. Contracts mint fungible and non-fungible tokens via standards such as ERC-20 and ERC-721 [114, 86], empower cross-chain bridges that lock and mint assets [169], and compose with one another into complex protocols [300]. Since on-chain code cannot natively reach external data, services called *oracles* feed off-chain information such as asset prices into contracts [300]. Calls execute atomically and can bundle many operations into one all-or-nothing transaction. *Flash loans*, for example, exploit this

feature. They lend funds through a chain of operations that borrow and repay within a single transaction, valid only if fully settled by its end [300]. Although deployed bytecode is immutable, contracts can still be made *upgradeable*, introducing administrative control that can itself be exploited [300]. These powers carry inherent limits. Execution must stay deterministic, contract state and logic are publicly visible, every operation consumes *gas*, and code cannot reach off-chain resources unaided. These constraints shape how contracts are both built and abused [304, 300].

2.3 Crypto assets

We adopt the term *crypto assets* as a unified descriptor for blockchain-based, exchangeable digital assets [111, 309], where "crypto" denotes cryptocurrency. While alternative terms such as "digital assets" and "crypto-coins (CCs)" are also prevalent [300, 42], we use *crypto assets* throughout for consistency. This category includes:

Coins and gas tokens. Blockchains such as Bitcoin [205], Monero [289], and Ripple [145] support a single native cryptocurrency—BTC, XMR, and XRP—commonly referred to as "coins," used as digital currency and for paying transaction or mining fees [196, 310]. In contrast, smart contract platforms like Ethereum [37], Solana [166], and Binance Smart Chain [23] use native "gas tokens"—ETH, SOL, and BNB— to cover transaction costs and smart contract execution [311]. The term "coin" is often used to describe the native currency of a blockchain including gas tokens, while gas tokens are specific to platforms that support smart contracts.

Utility and community tokens. Blockchains with smart contract support enable the creation of secondary tokens via standards such as ERC-20 [114] in Ethereum and BEP-20 [22] in Binance Smart Chain. These tokens may serve functional roles (e.g., governance, staking) or may lack explicit utility [1, 317].

Wrapped tokens. A wrapped token is a tokenized representation of another asset, minted to make that asset usable in contexts where its original form cannot operate. One common use is cross-chain interoperability. Since assets cannot move directly between blockchains due to isolated state machines, bridges lock the original asset on the source chain and mint an equivalent token on the destination chain [212, 169]. For instance, locking BTC yields wBTC for use in Ethereum-based protocols [169]. Such bridges generally consist of three parts, a *custodian* that locks the asset, a *communicator* that transmits confirmations, and a *debt issuer* that mints or burns the wrapped token [169]. Wrapping also serves other purposes. WETH is the ERC-20 version of ETH, letting the native gas token interact with

smart contracts that expect the ERC-20 interface [301, 114], while yield-bearing wrappers such as weETH represent the staked token eETH and accrue its staking rewards through price appreciation rather than a growing balance [88].

Stablecoins. Stablecoins are digital assets pegged to external references (typically fiat, e.g., USD) [197, 199]. Unlike volatile cryptocurrencies like Bitcoin, they aim to serve as stable stores of value [197]. Stablecoins are classified by [197]: peg type (fiat, commodities [55]), collateral type (fiat, crypto, commodities, algorithmic), collateral amount (full, over-collateralized, partial, or none), and stabilization mechanisms. Their stability depends on collateral volatility, reserves, macroeconomic conditions, and user incentives [164, 134].

Non-fungible tokens (NFTs). Web3 tokens are broadly classified as *fungible* or *non-fungible* [306]. Fungible tokens are interchangeable and divisible, with each unit holding equal value. In contrast, NFTs are unique, indivisible assets that function as digital certificates of ownership [199]. Each NFT is identified by an ID and linked to off-chain metadata (e.g., media files) via a URL [313]. NFTs serve as foundational components of Web3 metaverse ecosystems by facilitating verifiable, transferable ownership of virtual assets [199, 302, 306]. Unlike fungible tokens with market-driven pricing, NFT values are subjective [282], often exchanged through auctions on platforms like OpenSea [302].

2.4 Cryptocurrency wallets

Cryptocurrency wallets are essential tools for storing, managing, and transferring digital assets within virtual economies [199]. A wallet enables users to initiate transactions by signing them with a private key, and broadcasts it to the blockchain for validation [141]. Wallets vary by design and provider [199], and are typically classified along two dimensions [141, 199]: (a) network connectivity, where hot wallets (e.g., web, mobile) are internet-connected, and cold wallets (e.g., hardware, paper) are offline to reduce exposure to cyber threats; and (b) key management, where custodial wallets entrust private keys to third parties, while non-custodial wallets give users full control and responsibility. Cryptocurrency wallets are typically initialized using a 12- or 24-word mnemonic phrase drawn from a standardized 2048-word list [215, 141]. These phrases encode entropy and act as human-readable seeds for private key generation, enabling secure recovery [215, 141]. Most wallets implement the hierarchical deterministic (HD) model defined in BIP-32 [308], allowing a single master seed to produce a tree of key pairs [65]. Protocol-specific derivation paths [235] yield distinct addresses, and the one-way nature of key derivation makes seed reconstruction or cross-chain address inference cryptographically infeasible. The ease of

wallet generation facilitates abuse, allowing malicious parties to create large numbers of wallets [199]. Some networks, such as Ripple [145], disincentivize mass wallet generation by imposing a reserve balance requirement.

Beyond key-controlled wallets, *smart contract wallets* or *smart accounts* are a specific kind of cryptocurrency wallet governed by on-chain smart contract code rather than a single private key, in contrast to *externally owned accounts* (EOAs), the key-pair wallets discussed earlier, whose authority derives solely from a keypair [39]. Because their authorization logic is programmable, these wallets can enforce arbitrary spending conditions—most notably *multi-signature* schemes that require approvals from m of n designated owners before a transaction executes. *Safe* [237], formerly Gnosis Safe, is one of the most widely adopted examples, securing assets for individuals, decentralized autonomous organizations (DAOs), and institutional treasuries through configurable owner thresholds and modular extensions. Such wallets can also batch several operations into a single atomic transaction, delegate restricted permissions to modules, and—under *account abstraction* (ERC-4337)—sponsor gas fees or accept alternative authentication methods [39, 237]. Critically, a smart contract wallet can pool funds under shared, programmable control, while account-abstraction factories let a single operator cheaply deploy and coordinate many distinct addresses [39, 237].

Chapter 3

Survey Methodology

This chapter explains how we chose the sources behind this survey. It states the research questions we set out to answer, describes the review methodology we follow, lists our search strategy and sources, and sets out the criteria for including and excluding a source.

3.1 Research Questions

The survey is organized around six research questions (RQs), answered in the order the chapters that follow present them.

RQ1. How do the classical placement, layering, and integration (PLI) stages of money laundering apply to Web3, and where do they fall short? (§4)

RQ2. How does pseudonymity underpin these schemes, and what tiers of anonymity does it afford? (§4.1)

RQ3. What on-chain, off-chain, and cross-chain data underpin the forensic investigation of these schemes? (§4.2)

RQ4. What overarching strategies do actors employ to obscure the origin, flow, and ownership of illicit assets in Web3? (§5.1)

RQ5. Through which intermediary mechanisms and enablers are these strategies realized in practice? (§5.2)

RQ6. What detection and prevention countermeasures exist across academia, regulation, and industry, and what gaps remain? (§6, §7)

3.2 Review Methodology

Our review is *informed by* the PRISMA 2020 reporting guidelines [214] and by established guidance for systematic literature reviews [155], structured around the stages of identification, screening, eligibility assessment, and inclusion. We adopt these frameworks to bring transparency and repeatability to source selection rather than to claim full conformance: as a systematization-of-knowledge effort spanning several disciplines, our goal is breadth of synthesis rather than the narrow, hypothesis-testing focus for which PRISMA was originally devised. Because authoritative evidence in this domain frequently originates outside peer-reviewed venues, we further adopt a multivocal approach that deliberately incorporates grey literature, following the guidance of Garousi et al. [119] (see §3.6).

3.3 Search Strategy and Sources

In our survey, we primarily used Google Scholar to gather research from venues in cybersecurity, blockchain, and financial crime. Given the rapid evolution of DeFi, academic literature alone is insufficient for capturing emerging laundering tactics. To supplement scholarly work, we included regulatory reports, preprints, books, and theses, spanning the intersection of topics between finance and computer security. We also drew on curated SoK resources [173, 267] and contextualized real-world incidents via reputable news sources and blogs.

We queried Google Scholar using keyword sets such as *"Cryptocurrency money laundering," "AML in Web3," "crypto laundering," "DeFi money laundering," "mixing services,"* and related terms. These searches yielded over 50 published academic papers and preprints. Key articles were selected based on relevance, citation count, and venue, and forward citation analysis was used to identify additional sources. Given our work's interdisciplinary scope, we expanded our search to finance literature via our university's library, guided by a subject librarian. This resulted in the finding of additional studies, expanding our reference pool to over 200 sources. We shortlisted articles based on titles, followed by screening abstracts and introductions. Final selections were made after reviewing core technical sections. Many of these works cited non-peer-reviewed sources, including publications from industry, financial watchdogs (e.g., FinCEN, Interpol), and annual reports from forensic firms such as Chainalysis [48], Elliptic [83], Mandiant [185], and Merkle Science [191].

3.4 Inclusion and Exclusion Criteria

To make our selection decisions explicit and repeatable, we applied a consistent set of criteria, and a source had to satisfy all of them to be included. It had to be topically relevant, addressing cryptocurrency- or Web3-enabled money laundering, anti-money laundering (AML), or a closely related aspect such as laundering strategies, intermediaries, deanonymization, forensic data, or countermeasures. It also had to come from a credible source, meaning either peer-reviewed work or authoritative grey literature such as regulatory, governmental, or established forensic-firm reporting that supplies current evidence the academic record lacks. Beyond this, we kept only sources written in English, and only those within our temporal window, which spans foundational works from 2013 onward [204] through mid-2025, with priority given to recent contributions while retaining seminal studies.

We excluded a source when it met any of the opposite conditions. Off-topic works were dropped, such as those dealing solely with price prediction or trading strategies, which bear no substantive relation to laundering or AML. We also set aside sources that lacked analytical or technical substance relevant to our research questions, along with duplicates and versions superseded by a later, more complete work. Finally, we removed promotional or otherwise non-credible grey literature whose claims we could not confirm.

3.5 Study Selection

Figure 3.1 summarizes the selection process. Identification combined keyword searches on Google Scholar, subject-librarian-guided searches of the finance literature through our university's library, and authoritative grey literature. We screened records by title against the scope above, then assessed abstracts and introductions, and finally appraised the core technical sections of the remaining candidates for eligibility. Throughout, we applied forward and backward snowballing—following both citations and cited-by links from retained works—to surface sources the keyword searches missed. The studies that survived this process form the corpus synthesized in the remainder of the thesis.

[1]The numbers shown come from our recorded search. We describe how many sources were dropped at each stage in words rather than giving exact counts.

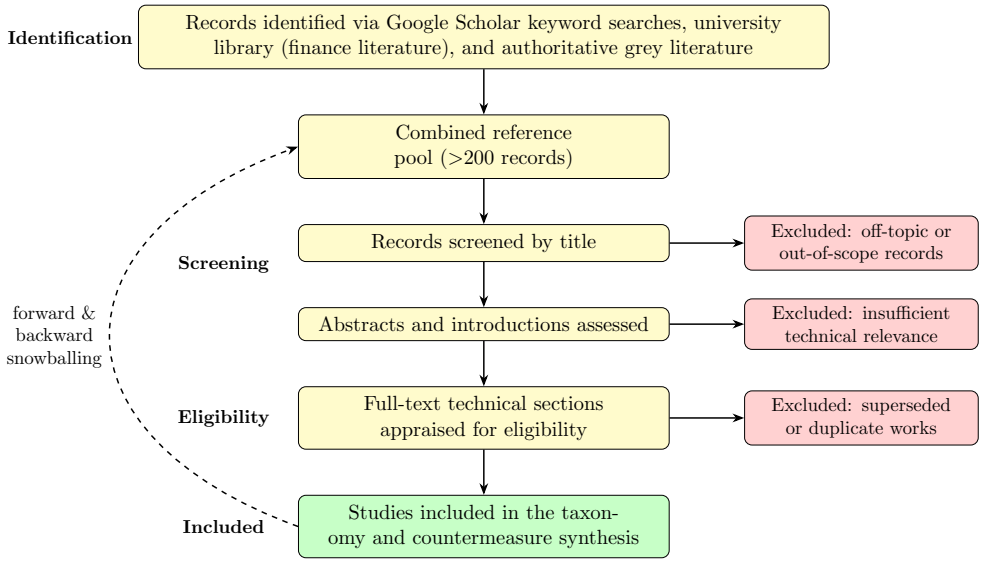


Figure 3.1: PRISMA-informed overview of the study selection process.[1]

3.6 Incorporating Grey and Industry Literature

In this field, much of the most current evidence first appears in grey literature rather than in peer-reviewed venues. This includes new laundering techniques, who was behind particular incidents, and estimates of how much illicit value is moving. Forensic firms such as Chainalysis [48], Elliptic [83], Mandiant [185], and Merkle Science [191], along with regulators and financial watchdogs (e.g., FinCEN, Interpol), publish findings well before academic work catches up. Leaving these sources out would make the survey miss the most recent developments, but using them without care would risk picking up commercial spin or claims we cannot check. We therefore treated grey literature as allowed but secondary evidence. We preferred peer-reviewed sources for analytical claims, confirmed grey-literature claims across several independent sources where we could, and used industry and regulatory reporting mainly for timeliness, such as current statistics, emerging tactics, and real-world incidents, rather than as the only basis for a claim. This approach follows established guidance for including grey literature in systematic reviews [119].

3.7 Taxonomy Construction

To construct our taxonomy, we began by listing all laundering approaches identified in the literature, supplementing each with domain-specific sources to enhance coverage and accuracy. Working bottom-up, we coded each approach by the technique it employs, the intermediary or enabler it relies on, and the laundering stage it serves, then grouped recurring patterns into higher-level themes. From this, we derived a top-down model that organizes laundering into six overarching strategies and the intermediary mechanisms through which those strategies are carried out: ten exploited-infrastructure mechanisms, each mapped directly to the strategies and stages it serves, and a body of privacy-enhancing technologies that we organize by deployment form and the blueprints they combine rather than as a flat list (see Figure 5.3).

We divided the intermediary mechanisms into two categories by the intention behind their design. Privacy-enhancing technologies (PETs) are tools built on purpose to protect privacy; exploited infrastructures are ordinary Web3 services, such as exchanges and bridges, that were built for legitimate use but can be repurposed for financial secrecy and money laundering. For the PETs we found that the labels the field relies on, such as *mixer*, *tumbler*, *shielded pool*, and *anonymity-enhanced cryptocurrency* (or *privacy coin*), do not form a usable categorization. These labels overlap heavily, are not mutually exclusive on any specific attribute or factor, and often lack a solid definition, so real-world implementations usually fit under several of them at once, and some fit none cleanly. A tool commonly called a mixer may equally be a shielded pool, and a privacy coin often embeds a mixer-like module, so trying to assign each tool to a single such label breaks down, as we justify in the PETs section (§5.2.1). The one axis on which every PET does have exactly one value is its *deployment* form, so we make that the mutually exclusive backbone of the taxonomy, ranging from custodial services through the protocol-native layers to application-layer contracts and off-chain coordinators. Alongside it we record a second axis that captures what a tool actually does: the set of underlying privacy *blueprints* it combines, a dozen primitives such as pooling, ring signatures, zero-knowledge proofs, and trusted execution environments, each tagged with a chip coloured by the laundering strategy it serves. Together the two axes let a reader see both where a tool operates and what it is made of, without forcing it into a single overlapping label.

We also placed every strategy and mechanism within the placement, layering, and integration (PLI) model adapted to Web3 (§4), tagging each with the stages it touches, and we mapped each intermediary to the strategies it can carry out. The structure was refined step by step, and as new sources were added we revisited the category boundaries to keep them consistent and aligned with the PLI model. To ensure completeness, we

extended our investigation beyond academic literature, identifying emerging techniques not previously documented (see Appendix A). We further cross-checked the taxonomy's coverage against prior surveys, confirming that it covers the vectors they treat in isolation while also including techniques they omit. We also synthesized countermeasures from academic, regulatory, and industry sources, classifying prevention and detection strategies by approach and scope to complement our analysis and provide an overview of defenses aimed at tackling crypto money laundering.

3.8 Scope, Boundaries, and Threats to Validity

This survey is scoped to money laundering in the Web3 and DeFi setting, encompassing the obfuscation strategies, intermediary mechanisms, supporting data, and countermeasures associated with it. Several adjacent topics fall outside our scope: we treat predicate crimes such as fraud, theft, and scams only insofar as they generate illicit proceeds to be laundered, not as objects of study in their own right; we invoke traditional fiat-currency laundering only as a comparative baseline; and we do not undertake a jurisdiction-by-jurisdiction legal analysis or implement and benchmark detection tooling.

A further boundary concerns the privacy-enhancing technologies (§5.2.1). The tools we name under each deployment form are illustrative examples, meant to show what a given form and its blueprints look like in practice, not an attempt to gather and list every privacy tool in the ecosystem, which would fall outside our scope and date quickly. Our contribution there is the two-axis scheme itself, deployment form and blueprints, as a way to categorise such tools. The scheme is deliberately open-ended, so new deployment forms and new blueprints can be added as they emerge without disturbing its structure.

Several threats to the validity of this methodology warrant acknowledgment. First, reliance on indexed venues and English-language sources introduces a risk of selection and publication bias; we mitigated this through snowballing and the deliberate inclusion of grey literature, but cannot rule out the omission of relevant non-indexed or non-English work. Second, the field moves quickly: with a review horizon ending in mid-2025, techniques emerging after this point are necessarily absent. Third, our use of industry reporting carries the limitations discussed in §3.6, namely the potential for commercial framing and limited verifiability, which we offset through cross-corroboration. Finally, taxonomy construction involves interpretive judgment in drawing category boundaries; we reduced this subjectivity through iterative refinement and cross-validation against the placement–layering–integration model and prior surveys. These methodological threats are distinct

from the substantive open challenges of AML in Web3—such as the scarcity of labeled data and the dual-use tension of privacy technologies—which we examine in §7.

Chapter 4

Primer on Crypto Money Laundering

Money laundering is the process of concealing the illicit origins of criminal proceeds to make them appear legitimate [306, 63]. By obscuring financial trails, money laundering enables offenders to integrate unlawful gains into the legal economy while concealing the underlying crimes and perpetrators [211, 258]. This often involves transforming assets, transferring them across jurisdictions, or layering transactions [63]. A big concern with Web3 is its exploitation for money laundering [252]. The pseudonymity of cryptocurrency transactions hampers regulatory and law enforcement efforts by obscuring the origin/destination of funds. Criminals often favor decentralized services over centralized ones with AML controls [211]. Crypto money laundering is also used to integrate proceeds from Web3-native crimes such as scams and hacks [63, 306].

Money laundering stages. The money laundering process is traditionally divided into three primary stages: placement, layering, and integration (PLI) [63, 252, 157, 199, 31].

Placement. This initial stage introduces illicit funds into the financial system. Offenders often convert cash into legitimate-looking assets to avoid suspicion, using techniques like "smurfing"—breaking large sums into smaller, less conspicuous transactions [252, 199]. As the first point of contact with regulated systems, placement is both critical and risky [268, 199]. In Web3, placement generally involves converting illicit fiat into crypto assets (§2.3), often via loosely regulated *centralized exchanges* (CEXs) to evade detection [252, 63].

Layering. This stage follows placement and involves fabricating transaction records to conceal the origin of illicit funds [199], typically through a series of complex transactions designed to distance the assets from their source [252]. In Web3, this often involves employing obfuscation strategies (discussed in §5.1) that reduce funds' traceability.

Integration. This final stage returns the laundered funds to the legitimate economy, where they appear as legitimate wealth and can be used freely without arousing suspicion [252, 63, 281]. It usually means holding the proceeds as assets with a lawful-looking origin, such as real estate, luxury goods, or artwork [252].[1]

While some scholars have noted limitations of the classical PLI framework in the context of emerging financial technologies (e.g., mapping specific behaviors to distinct PLI stages can be challenging with cryptocurrencies) [122, 44], it continues to serve as a foundational model in money laundering research [63]. We thus structure our taxonomy on crypto-enabled money laundering around the PLI model, while accounting for domain-specific particularities. For instance, in certain Web3-native crimes such as fraud, theft, or scams, the placement phase may be less distinct or entirely bypassed, as illicit proceeds originate within the crypto ecosystem [130, 306]. In such cases, laundering often begins with layering and proceeds to integration via off-ramping or asset conversion [265].

The next section examines the pseudonymous nature of the Web3 ecosystem and its role in laundering, outlines tiers of anonymity, and highlights a core challenge to deanonymization: limited access to data traces that hampers AML efforts.

4.1 Deanonymization in Web3

Anonymity in cryptocurrencies is mainly assessed along two dimensions: preventing transaction *linkage* and concealing user *identities* [7]. Alsalami et al.[7] outline four anonymity tiers: (a) *Pseudonymity*, where users are identified by blockchain addresses that are not inherently tied to real-world identities; (b) *Set anonymity*, which conceals a user's identity by embedding them within a broader group—called "anonymity set"—such that the sender is indistinguishable from others in the set, typically through mechanisms like ring signatures (e.g., Monero [289]); (c) *Full anonymity*, which extends beyond set anonymity by cryptographically hiding both the sender's identity and transaction path, using techniques such as zero-knowledge proofs and commitment schemes (e.g., Zcash [318]); and (d)

[1] In the Web3 literature, integration is often presented in a way that blurs it with "off-ramping". Several sources treat converting crypto back into fiat, or buying assets such as NFTs, as integration in itself [117, 199]. Strictly, off-ramping completes integration only when the funds come to rest as legitimate-looking wealth, giving the launderer a credible origin story for the money if anyone asks where it came from [281, 63]. On its own, moving or converting value is closer to layering. For example, a house bought with illicit funds can later be presented as property that was simply owned and sold, so it comes to read as legitimate wealth, whereas an NFT bought the same way is not yet accepted in this manner and its purchase stays closer to layering. Because this looser reading is so common across the sources, we follow it in our taxonomy and treat off-ramping as integration.

Confidential transactions, which expands full anonymity by obscuring transaction amounts to ensure value privacy (e.g., Monero's Bulletproofs).

Law enforcement has increasingly turned to blockchain forensics [75], engaging firms such as Chainalysis [48], TRM Labs [278] and Elliptic [83] to assist in tracing cryptocurrency flows. Deanonymization often relies on correlating on-chain activity with off-chain data, particularly from gatekeepers such as CEXs that enforce *know your customer* (KYC) policies designed to associate customers with prosecutable real-world identities [63]. When illicit assets interact with these services, investigators can link wallet addresses to real-world identities. On-chain graph analysis supports this process [7, 43]. Deanonymization and AML detection measures are often data-driven (§6). Understanding data nature, scope, and accessibility is key for post-incident tracing and proactive measures. Next, we outline the typology of data used for data-driven money laundering countermeasures.

4.2 Typologies of Data for Web3 AML Forensics

The data used for tracing illicit activity in Web3 can be broadly categorized into two types:

On-chain data. This data type refers to information immutably recorded on public blockchains [63, 291], including transaction histories, addresses, amounts, fees, and timestamps [75]. Blockchains based on the *unspent transaction output* (UTXO) model (e.g., Bitcoin [205]) record UTXOs' ownership changes, while smart contract platforms (e.g., Ethereum [37]) log state transitions, events, and token transfers [300, 304]. On-chain data is publicly accessible through APIs or explorers like Etherscan [98], Bitquery [29], and The Graph [271]. However, privacy-focused blockchains (e.g., Monero [289], Zcash [318]) deliberately restrict transparency [75]. Crucially, public availability does not guarantee traceability; some on-chain data is deliberately constructed such that, despite being fully public, it remains insufficient to reconstruct the underlying transaction flow [248]. We discuss such privacy-enhancing designs in §5.2.1.

Off-chain data. This data type originates outside blockchains, and is stored by centralized entities [291]. Sources include CEXs and custodial wallets, which often comply with KYC/AML regulations [63]. These entities collect data such as names, IDs, IPs, device fingerprints, and activity logs [159, 137, 130] that are accessible to investigators through legal processes. Additional sources include messaging platforms (e.g., Telegram, Discord), dark web listings, and communication logs [130, 99], which provide context on laundering coordination. Analytics firms and regulators also maintain databases of flagged addresses and known scam networks [137]. While fragmented and variable in quality, off-chain data

is essential for linking blockchain activity to real-world actors [199]. Off-chain data also arises from *Layer-2* scaling solutions (§2.1). By moving execution off the main chain and settling on Layer-1 only periodically, many retain transaction-level data off-chain, such as payment or state channels, where only channel opening and closing settle on-chain, so the on-chain record alone may be insufficient to trace individual transfers [132, 224]. This off-chain locality can also be reinforced cryptographically. For instance, *zk-rollups* execute transactions off-chain and post only succinct validity proofs and state commitments on-chain, keeping detailed transaction data off the base layer [273], while TEE-based designs (e.g., Ekiden [52]) execute contracts confidentially inside trusted hardware enclaves [172], so sensitive transaction data need not be exposed even off-chain. We return to these cryptographic techniques as the privacy blueprints behind PETs (§5.2.1).

Notably, *cross-chain transactional traces* are vital for detecting asset movement between blockchains—a process known as *chain-hopping* (see §5.1.3)[176]. These traces are not separate from on-chain or off-chain data but may consist of either—or both—depending on the method used. For example, on-chain smart contract logs from decentralized bridges (e.g., Wormhole [115], Multichain [203]) reflect token locking, minting, or burning [212, 117], while atomic swaps using *hashed timelock contracts* (HTLCs) [63, 132] or interoperability protocols like LayerZero [165] and Axelar [206] produce traceable on-chain interactions [212]. In contrast, chain-hopping via centralized services leaves only basic on-chain deposit and withdrawal traces, with most linkage data held off-chain in custodial databases [193]. Finally, some methods—such as those in §5.1.4—generate no cross-chain traces at all.

Tracing illicit asset flows—especially across obfuscation layers—requires correlating on-chain and off-chain data from different sources. Each source offers a partial view; only by combining them can investigators fully reconstruct laundering paths. Sophisticated actors exploit gaps in data, jurisdiction, and privacy tools to evade detection [63].

Chapter 5

Taxonomy of Crypto Money Laundering

The previous chapter laid out how laundering unfolds across the placement, layering, and integration (PLI) stages (§4), the tiers of anonymity a launderer may attain (§4.1), and the types data traces these activities leave behind (§4.2). Building on that foundation, this chapter presents our taxonomy in two parts. We first systematize the high-level *strategies* launderers rely on to obscure the origin, flow, and ownership of illicit assets across the PLI stages (§5.1). We then turn to the *intermediary mechanisms* that realize these strategies in practice (§5.2). Some are privacy-enhancing technologies (PETs), purpose-built to protect user privacy (§5.2.1). Others are ordinary Web3 infrastructure, designed with entirely different use cases in mind but repurposed by launderers to evade financial transparency (§5.2.2). As Fig. 5.3 shows, a single intermediary often implements one or more of these strategies.

5.1 General Strategies

Consider a launderer who has just brought illicit value into the Web3 ecosystem and now wants to hide where that value came from and where it is going. At a high level, only a handful of distinct goals are available to them, and the strategies in this section map onto those goals. They may simply *add noise* to the trail, dispersing assets across self-controlled addresses and transactions until the path is too tangled to follow. We call this *transaction flow obfuscation* (§5.1.1). They may *blend* their funds with those

of unwitting third parties, dissolving individual ownership into a shared pool. This is *commingling* (§5.1.2). They may try to *sever* the trail outright, leaving no observable link between source and destination, a strategy we call *disconnected fund flow* (§5.1.4). Unlike most others, it applies not only during layering but across placement and integration as well. They may move the assets *across blockchains*, forcing investigators to stitch together heterogeneous and often incompatible ledgers, a tactic known as *chain-hopping* (§5.1.3). Beyond manipulating the transaction graph, launderers also borrow a classic technique from the traditional economy, exploiting the subjective, opaque valuation of unique assets such as art [242, 113], now inherited in Web3 through NFTs (§5.1.5) [199]. And underlying every stage is the standing opportunity to *exploit regulatory gaps*, the uneven and often lax oversight across jurisdictions and services [42, 63] (§5.1.6). We group these strategies into six categories. In practice, implementations often combine or blur them, making it difficult to assign a scheme to a single tactic; still, this classification provides a systematic lens for understanding laundering patterns.

5.1.1 Transaction Flow Obfuscation (TFO)

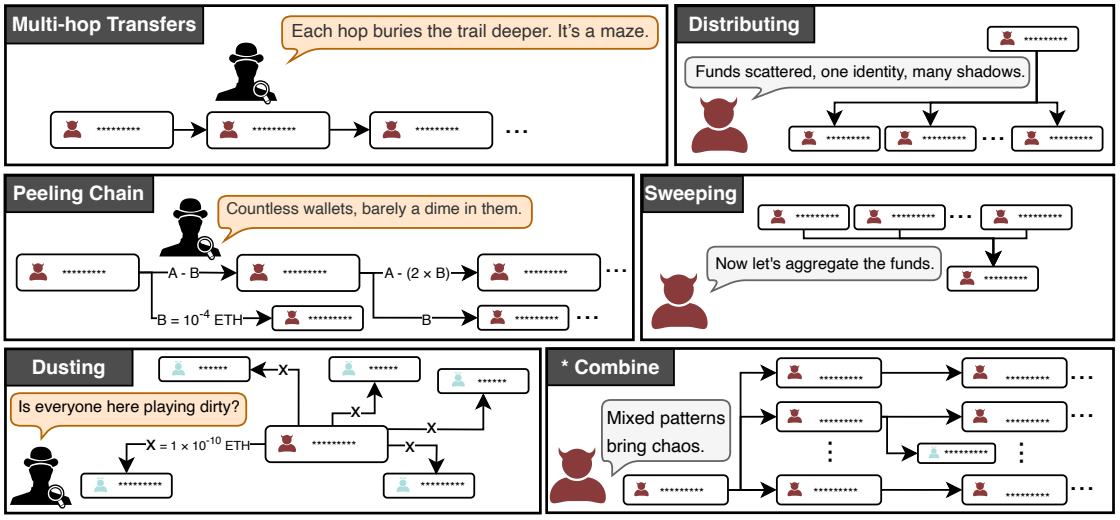


Figure 5.1: Transaction flow obfuscation (TFO) patterns.

Transaction graph analysis as a means to detect illicit transactions is inherently error-prone, often yielding false positives due to the structural complexity of blockchain transactions [43, 31]. *Transaction flow obfuscation* (TFO) refers to techniques that deliberately

increase the complexity of blockchain transaction patterns, often by moving assets between wallets controlled by the same actor, mimicking usual transactional patterns [50, 249]. As noted in §2.4, the ability of rapid, low-cost creation of new addresses is often exploited to obfuscate illicit fund flows [31, 199]. Dispersing assets across many wallets increases transaction graph complexity and hinders forensic methods like address clustering [43, 243, 176]. Below, we outline common TFO patterns (see Fig. 5.1).

Multi-hop transfers. Chainalysis reports that over 80% of illicit value flows involve routing funds through intermediary wallets—distinct addresses placed between the illicit source and the final conversion service—to increase obfuscation [47]. Each intermediary "hop" represents a transfer between addresses [183, 157]. Multi-hop transfers often form long chains of "relay transactions" [50], complicating manual tracing, e.g., when using public block explorers.

Peeling chain. A *peeling chain* is a transaction pattern commonly used by mixing services (§5.2.1) to obfuscate the origin of large cryptocurrency holdings through incremental transfers [43]. It consists of a sequence of "peel transactions"—each with one input and two outputs [50, 10]. Starting from a high-balance address, a small amount is sent to an external address while the remainder returns to a sender-controlled address [43]. This process recurses until the balance is fully dispersed, often ending with conversion at exchanges into fiat or other assets [43, 243, 250]. These patterns can generate false positives, as they resemble Bitcoin's "change address" behavior. Under Bitcoin's UTXO model, outputs must be fully spent, and excess funds are typically returned to a newly generated change address [43, 50]. This similarity complicates distinguishing illicit from legitimate transactions [43, 50].

Distributing and sweeping. "Distributing transactions" typically involve any number of inputs and more than three outputs and are used to split large sums into smaller outputs [249, 50]. They are often associated with a single entity sending funds to multiple recipients, as seen in gambling payouts or pooled mining rewards. These patterns, like peeling chains, relate to smurfing—the practice of breaking large amounts into smaller units to avoid detection [199]. In contrast, "sweep transactions" consolidate multiple inputs into a single output [50]. Commonly used by organizations for audit transparency or fund management, they are also employed to aggregate stolen assets from compromised wallets [249, 50].

Dusting. Dusting term originally refers to the practice of sending negligible amounts of cryptocurrency—called "dust"—to multiple wallets to trace and de-anonymize users by monitoring subsequent UTXO spending [298, 56, 277]. It is employed by malicious actors for extortion, by law enforcement for investigations, and by analytics firms for research [56].

In account-based systems like Ethereum, dusting has evolved into a phishing technique, where adversaries send counterfeit tokens embedded with malicious smart contracts. Interacting with these tokens—for example, through swaps or approvals—can lead to wallet compromise [277]. Dusting is also used for "address poisoning", a phishing scheme in which attackers send small transactions from addresses resembling a victim's address (e.g., with matching initial and final characters) [192]. These addresses appear in transaction histories, increasing the chance of accidental reuse and misdirected funds.

Although not categorized as an explicit obfuscation attempt, in October 2018, the BestMixer.io mixer sent small Bitcoin amounts to numerous addresses—ostensibly for advertising [67]. However, this act is widely interpreted as an attempt to disrupt AML systems by contaminating clean addresses, expanding the anonymity set and generating false positives in taint analysis (see §6.2) [67, 7].

5.1.2 Commingling

In financial and legal contexts, *commingling* denotes the intentional mixing of funds from multiple sources to obscure their origin and hinder traceability [170, 63, 44]. It was central to 1990s warehouse banking schemes, where pooled client deposits masked individual ownership, facilitating tax evasion and money laundering [63]. In Web3, commingling commonly occurs during layering, where assets from multiple parties are merged within a shared transactional or custodial structure. Unlike TFO (§5.1.1), where a single actor moves funds across self-controlled addresses or dusting recipients without their participation, commingling requires multiple parties. This shifts pseudonymity to set anonymity, thus probabilistically assigning fund origins to a group [7].

The terms *commingling*, *mixing*, *tumbling*, and *swapping* are closely related in cryptocurrency literature and often lead to confusion [63, 262]. To clarify, in this paper we use *commingling* as an umbrella term referring to the "pooling" of assets from distinct parties to obscure their provenance [170]. *Swapping*, by contrast, involves shuffling transaction destinations to achieve unlinkability [307, 248, 10] (§5.1.4). *Mixing* is often used as a broader term in the literature, encompassing various actions employed in *mixers* (§5.2.1), including TFO (§5.1.1), swapping (§5.1.4), and commingling [307, 63]. Although the terms *mixing* and *tumbling* are often used interchangeably, some sources distinguish them. Tumbling refers to fragmenting transactions into smaller parts to obscure transaction trails [130, 59], placing it under the TFO category and close to patterns such as peeling chains and distribution. These terms are easier to tell apart once we define the underlying primitives as *blueprints* in the PETs section (§5.2.1), where pooling, tumbling, and swapping are each treated in their own right.

5.1.3 Chain-hopping

Chain-hopping is an advanced obfuscation technique involving the deliberate transfer of assets across multiple blockchain networks to disrupt traceability [10, 63]. It poses significant challenges for investigators, who must aggregate and correlate transactional data from heterogeneous platforms—using cross-chain traces with on-chain or off-chain origins (§4.2)—to attempt path reconstruction for inferring ownership and track illicit flows [157]. Anonymity-enhanced blockchains (§5.2.1) further complicate forensic analysis [63].

Chain-hopping may occur via CEXs, where custodial platforms convert assets across chains [6, 63], or via DEXs using liquidity pools and atomic swaps [139], enabling peer-to-peer cross-chain transfers without intermediaries [300, 63](§5.2.2.1). Cross-chain bridges[143], which lock assets on one chain and release equivalents on another, are also key enablers of chain-hopping (§5.2.2.2). All such chain-hopping enablers are detailed in §5.2.2.

5.1.4 Disconnected fund flow (DFF)

While previously discussed tactics often leave residual data traces that can support partial linkage between source and destination account, a distinct class of techniques—referred to as *disconnected fund flow* (DFF) [10, 248]—aims to eliminate any traceable connection between illicit origins and final destinations. And while earlier tactics typically offer set anonymity [7]—providing limited resistance to deanonymization—DFF can approach full anonymity [7] (see §4.1). Finally, unlike prior layering-specific strategies, DFF techniques are also applicable during placement and integration. Below, we explore these tactics.

Disjoint reciprocal transfers (DRTs). A representative example of DFF is a process we refer to as *disjoint reciprocal transfers* (DRTs), after its structural characteristics—two reciprocal P2P transactions intentionally designed to appear unrelated (see Fig. 5.2). These transactions lack observable links, rendering their connection untraceable or extremely difficult to reconstruct, even with advanced forensic tools [234, 6, 63].

Placement via DRTs. In the placement phase, launderers introduce illicit funds—often in the form of physical cash—into the cryptocurrency ecosystem via P2P asset swaps with third parties [6, 63]. These exchanges typically occur through informal channels such as online forums, encrypted messaging apps, or social media. The actor transfers tainted funds to a counterparty, who returns an equivalent amount of clean cryptocurrency. With minimal contact through safe communication channels, these exchanges must be protected against deanonymization. Given the placement stage's inherent risk [268, 199,

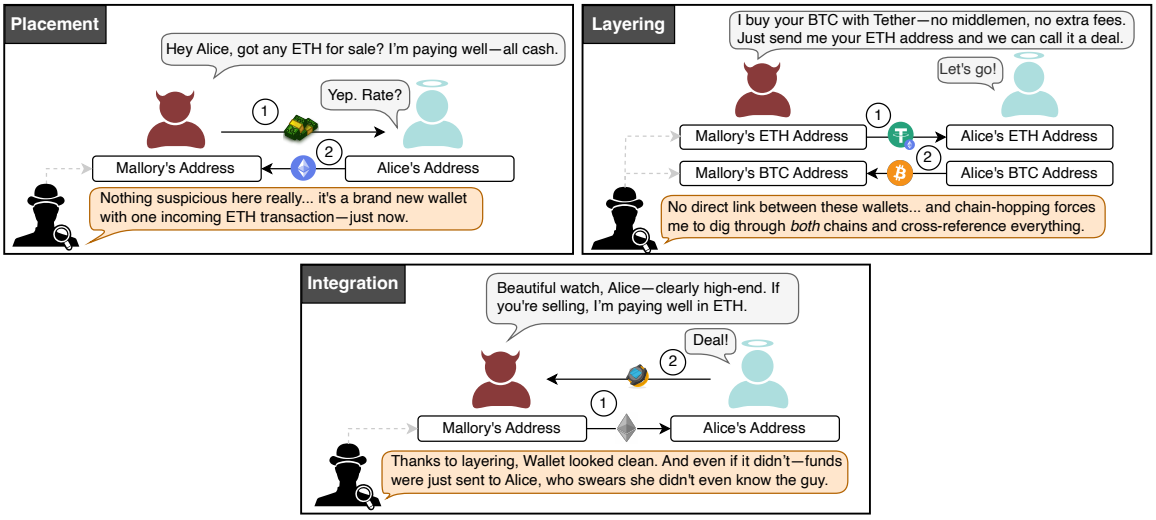


Figure 5.2: Disjoint reciprocal transfers (DRT).

252], launderers exercise caution by avoiding traceable interactions and leverage *privacy-enhancing technologies* (PETs) such as *Tor*[77] to obscure personal identifiers and conceal network-level metadata[204].

Layering via DRTs. Layering can leverage DRTs, enabling a malicious actor (Mallory) to exchange tainted cryptocurrency for ostensibly clean assets from a third party (Alice) without leaving discernible links. When both transaction happen on the same blockchain, both parties must use distinct addresses for sending and receiving ($\text{Mallory}_0 \rightarrow \text{Alice}_0$, $\text{Alice}_1 \rightarrow \text{Mallory}_1$), since reusing any address exposes linkages. Related work on stealth address schemes similarly seeks to preserve recipient anonymity by rendering repeated payments unlinkable [65]. Furthermore, DRTs can facilitate chain-hopping (§5.1.3). While requesting address changes may raise suspicion in single-chain transfers, it appears natural when assets are exchanged across blockchains—e.g., Bitcoin for USDT. As discussed in §2.4, addresses on different blockchains, particularly those derived from hierarchical deterministic (HD) wallets [235], are structurally unrelated. This address discontinuity breaks implicit links.

Integration via DRTs. DRTs can also serve as conduits for reintroducing laundered assets into the legitimate economy [6]. Adversaries may employ layered crypto assets to acquire high-value goods—such as real estate, vehicles, luxury commodities, or high-end NFTs—through transactions with legitimate third parties, thereby completing the laundering cycle.

Related to DRTs are over-the-counter (OTC) and P2P trades [63, 252], often facilitated by CEXs, such as KuCoin's P2P interface for USD–USDT swaps [160]. Here, the platform acts as an intermediary, connecting laundering actors with third parties. However, CEXs involvement introduces a degree of transparency that can undermine the disjoint nature of the transaction. While CEXs retain transactional records and are subject to KYC and AML regulations [63], malicious actors often exploit regulatory gaps to avoid identification (§5.1.6).

Swapping. Swapping is also a DFF technique that shuffles transaction destinations to achieve unlinkability by decoupling user inputs and outputs, thereby preserving address anonymity [307, 248, 10]. For instance, a swap can map transactions as follows:

$$\text{(Intended)}\ \ \mathrm{A} \xrightarrow{20} \mathrm{D},\ \mathrm{B} \xrightarrow{10} \mathrm{E},\ \mathrm{C} \xrightarrow{10} \mathrm{F}$$

$$\text{(Final)}\ \ \mathrm{A} \xrightarrow{10} \mathrm{E},\ \mathrm{A} \xrightarrow{10} \mathrm{F},\ \mathrm{B} \xrightarrow{10} \mathrm{D},\ \mathrm{C} \xrightarrow{10} \mathrm{D}$$

We make this swapping mechanism concrete later, when we cover *atomic swaps* among the PET blueprints (§5.2.1), the trustless realisation of exchanging one's coins for another's so that incoming and outgoing value cannot be linked. Atomic swaps rest on hash-time-locked contracts (HTLCs), the same primitive behind payment channel networks (§5.2.2.10), where a swap is in effect a one-hop channel.

5.1.5 Exploit Subjective Valuations

Consider colluding malicious actors, *Mallory* and *Darth*. To obscure a $50,000 illicit payment, Mallory initially acquires a low-value artwork (e.g., $50) and orchestrates its resale through collusive bidding to artificially inflate its price. Darth subsequently purchases the piece for $50,050, legitimizing the transaction by attributing the overpayment to sentimental value. Mallory, in turn, justifies the windfall as a capital gain, thereby laundering the funds under the guise of a legitimate art sale. The subjective nature of art valuation shields both parties from direct legal scrutiny [108, 242]. FATF's 2023 report underscores how the art market's opacity and lax regulation enable such exploitation [113]. Unlike fungible assets (e.g., fiat, gold), which are uniformly priced, non-fungible assets are unique, with volatile and opaque valuations. NFTs (§5.2.2.4) brought subjective valuation into the digital realm, enabling laundering [199, 190, 321]. A prominent example is *The Merge*, which sold for $91.8 million [299].

5.1.6 Exploit Regulatory Gaps

Exploiting regulatory gaps is a core strategy in crypto money laundering [42]. Launderers leverage inconsistent AML enforcement across jurisdictions, exploiting regulatory fragmentation to move illicit funds [63, 42]. KYC regulations are central to AML compliance, requiring service providers and exchanges to verify identities, monitor transactions, and report suspicious activity [63, 199, 251]. However, many offshore or non-compliant cryptocurrency services lack KYC controls, enabling anonymous transactions and regulatory evasion [63]. *Regulatory arbitrage* is a tactic where launderers shift operations to jurisdictions with lax AML oversight, exploiting systemic gaps and hindering international enforcement [63, 251]. The global expansion of decentralized financial ecosystems and VASPs in regions with inconsistent regulation, such as parts of Asia-Pacific and Latin America, amplifies these risks [251].

As enforcement tightens, launderers increasingly focus on defeating the onboarding check itself rather than hunting for services without one. Many VASPs now outsource this check to third-party verification providers such as Sumsub, which run document, biometric, and liveness checks for exchanges and other regulated firms [260]. To clear such checks, launderers turn to identities that are stolen, forged, or bought outright. Accounts are opened with misused or stolen personal details [99], and stolen identity information is sold openly by dark web vendors [63]. Operators who comply on paper often pass the due-diligence stage using false documents or money mules [117].

Two further methods have made this easier and harder to detect. The first is synthetic. Fraud-as-a-service tools now produce forged documents and deepfake selfies, and rising deepfake volumes have made such content cheap to obtain [259]. A two-month investigation by MIT Technology Review found 22 public Telegram channels selling virtual-camera software, stolen biometric templates, and deepfake generators to defeat the liveness checks of firms such as Binance and Revolut [154]. The second uses real people. Kaspersky describes an underground store that pays volunteers in disadvantaged countries small sums, around $5 to $20, for photos and videos of themselves holding blank cards that are later swapped for forged IDs [274]. A plausible extension of this model, not yet documented, is to recruit the same people to complete the live check on demand, so an account is opened with a real person, real documents, and a genuine liveness pass, all purchased. Much of this trade happens openly on Telegram and Discord rather than the dark web, where the market for pre-verified accounts stays comparatively small [45]. However they are obtained, these identities let a launderer open many accounts at once and feed small amounts through each to stay under monitoring thresholds (§5.2.2.6).

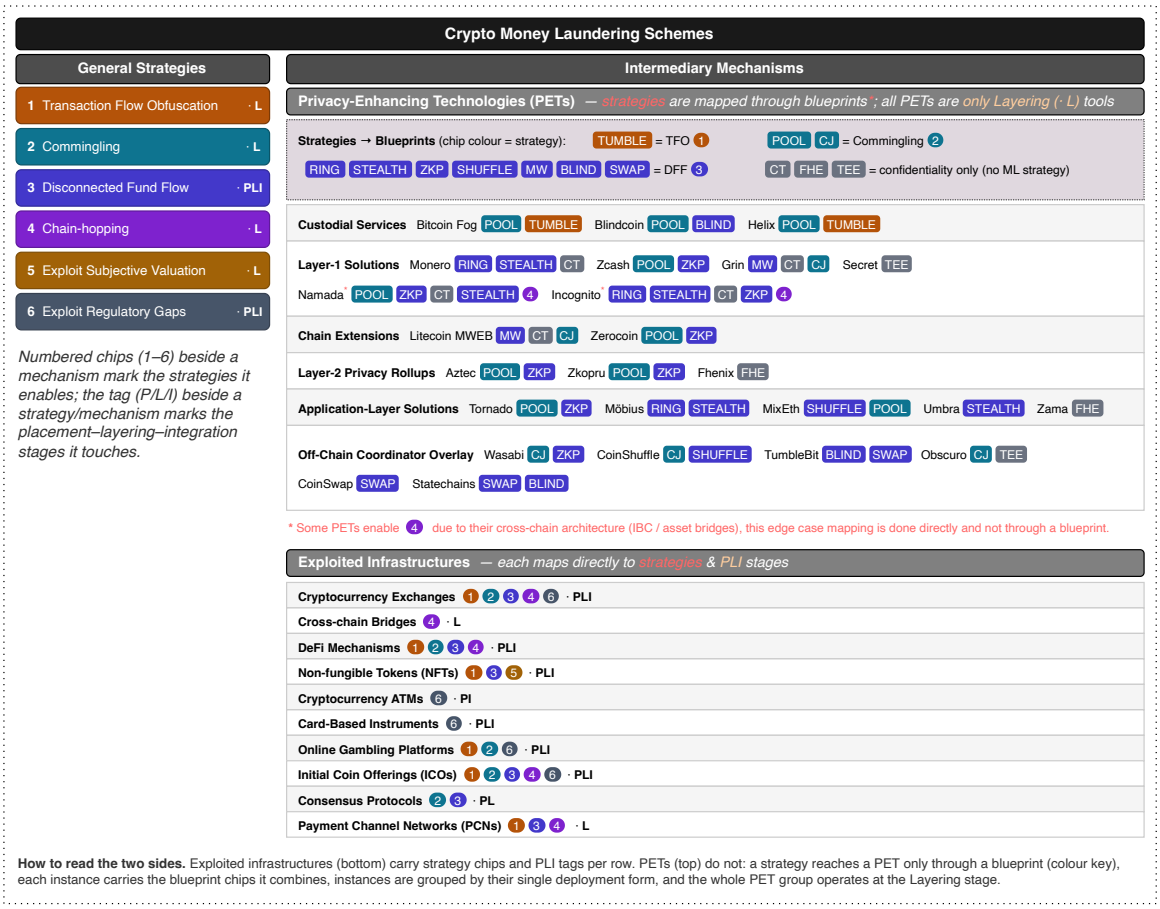


Figure 5.3: Taxonomy of crypto money laundering schemes.

5.2 Intermediary Mechanisms

If §5.1 describes *what* launderers try to achieve, this section examines *how* they achieve it. Strategies do not execute themselves; they are realized through concrete intermediary mechanisms that sit between an illicit source and its eventual destination. These intermediaries fall into two broad kinds, which structure the two parts below. Some are *privacy-enhancing technologies* (PETs), tools purpose-built to improve user privacy, such as mixers and anonymity-enhanced cryptocurrencies and protocols, whose very design frustrates traceability (§5.2.1). Others are ordinary components of the Web3 ecosystem, such as exchanges (§5.2.2.1), bridges (§5.2.2.2), DeFi protocols (§5.2.2.3), and NFT market-

places (§5.2.2.4), built with entirely legitimate use cases in mind but opportunistically repurposed to evade financial transparency (§5.2.2). In what follows, we examine the principal intermediary mechanisms exploited in crypto money laundering, and show how each enacts one or more of the strategies above across the placement, layering, and integration stages.

5.2.1 Privacy-enhancing Technologies (PETs)

The privacy-enhancing technologies gathered here are tools built on purpose to protect the privacy of on-chain financial activity, the record of who paid whom and how much that a public ledger would otherwise expose. They act on the transaction graph and the coins themselves. This sets them apart from network-layer anonymity tools such as Tor or a VPN, which hide the IP address behind a transaction but leave its on-chain trail intact [7]. Our concern throughout is this financial, on-chain privacy. Work in this area is usually framed around a small set of broad labels, most often *mixers* and *anonymity-enhanced cryptocurrencies*, and we keep both to connect our taxonomy to that work. A *mixer* (or *tumbler*) is usually described as the primary transaction-anonymity tool in Web3, a service that pools funds from many users and redistributes them to break the link between a coin's source and its destination [123, 67, 63]. In practice, though, "mixer" is a broad umbrella (§5.1.2). The same word is used for a custodial operator that holds and shuffles deposits, for a non-custodial coordinator that only arranges a joint CoinJoin, and even for a smart-contract shielded pool [307, 248]. In the map we build for the PETs in our taxonomy, these fall across three different deployment forms—custodial, off-chain coordinator overlay, and the application layer.

Anonymity-enhanced cryptocurrencies (AECs), also called *privacy coins*, are blockchains whose design hides the sender, the receiver, the amount, or all three at once, going beyond the ordinary pseudonymity of a transparent ledger [63, 7]. Most sit at the protocol-native layers, Layer-1, extension blocks, and Layer-2 [63, 7, 36, 13]. The same privacy is increasingly offered higher up, as application-layer confidential tokens [158, 34], which some would also place under the AEC umbrella. Many AECs are built from the very mechanisms the literature calls mixing [63]. Dash applies CoinJoin [70, 63], and Zcash's shielded pool [241, 318] is the same construction that underlies a smart-contract mixer such as Tornado Cash [217]. Treating "mixer" and "AEC" as two self-contained categories therefore hides more than it reveals. Our framework instead describes each tool along two axes that do not blur. The first is the *blueprints* it is assembled from and the second is the single *deployment form* in which every tool runs, which organises these tools in subsections that follow.

The primer (§4) set out how anonymity is graded in blockchain systems (§4.1) and what data traces a transaction leaves behind (§4.2). Before turning to the PETs themselves, we describe the two axes along which each is characterised, the cryptographic or hardware *blueprints* it is built from and the single *deployment* form in which it runs. Deployment organises the subsections that follow, one per form; the blueprints are tagged with a compact chip, ZKP or POOL, say, that reappears beside every tool, so a reader can see at a glance which primitives a PET combines. Blueprint chips are coloured by the laundering strategy each primitive serves (§5.1). Tumbling-style noise (TUMBLE) feeds *transaction flow obfuscation*, pooling and CoinJoin (POOL, CJ) feed *commingling*, and the linkage-breakers (ZKP, STEALTH, MW, and the rest) feed *disconnected fund flow*, approaching the full anonymity of §4.1. A fourth, greyed group serves no laundering strategy at all. Confidential transactions and the confidential-computation engines (CT, FHE, TEE) hide only an amount or a contract's state, leaving the on-chain graph of who paid whom fully visible.[1] Like the anonymity tiers themselves, these mechanisms are inherently dual-use, protecting legitimate financial privacy and, equally, frustrating the tracing of illicit flows.

Blueprints. The following primitives are the building blocks from which the PETs in this section are assembled. They are Lego parts, not a menu of one-to-one choices, because a single tool usually fuses several at once. A shielded pool, for instance, uses pooling to commingle funds while a zero-knowledge proof or a trusted enclave hides who owns what inside it. Each blueprint on its own maps to a single laundering strategy, or to none for the confidentiality-only group, as its chip colour marks (see Figure 5.3) and its definition states. A tool that combines several blueprints then inherits the strategies of all of them.

CT *Confidential transactions.* *Confidential transactions* conceal the *amount* transferred while still allowing the network to verify that a transaction is valid, meaning its inputs and outputs balance and no new coins are created [289, 7]. This is achieved with cryptographic *commitments* that hide the value yet remain additively verifiable, paired with *range proofs* (e.g., Bulletproofs [35]) that guarantee the hidden amount is non-negative. Crucially, only the amount is concealed. The sending and receiving addresses, and hence the path along which value moves, remain visible on-chain. Confidential transactions thus add *value privacy* (the fourth anonymity tier of §4.1) without, on their own, breaking the traceability of fund flow.

[1] These provide *confidentiality*, not anonymity. Unlike every other blueprint here, they break no link between a payment's source and destination, so on their own they enact none of the strategies of §5.1; the distinction is what they hide, the value or state rather than the who-paid-whom that the linkage-breakers conceal.

RING *Ring signatures and decoy signers.* A *ring signature* lets a member of a group sign a message such that a verifier is convinced the signer belongs to the group but cannot tell which member produced it [289]. Applied to payments, the true input is combined with a set of unrelated outputs (*decoys*, drawn from other users), so that every member of the resulting "ring" appears an equally plausible source of the funds. On each spend the real input is hidden behind these decoy signers, and no single transaction reveals which participant actually moved the money. Unlike confidential transactions, no on-chain field is concealed here; rather, the genuine trace is *obscured*, the movement path *fractured*, and *noise* added, so that the real path becomes hard to isolate. In the terms of §4.1, this raises the default *pseudonymity* of a transparent ledger to *set anonymity* by drawing other parties into the anonymity set [7].

STEALTH *Stealth addresses.* Where ring signatures hide the sender, *stealth addresses* hide the recipient. For each payment the sender derives a fresh, one-time address on the receiver's behalf, so the receiver's published address never appears on-chain and successive payments to the same party cannot be linked [65]. In practice they are paired with sender-hiding techniques such as ring signatures, so that both ends of a payment are obscured at once. By concealing the receiving side as well, stealth addresses push set anonymity toward the *full anonymity* of §4.1 [7].

CJ *CoinJoin. CoinJoin* obscures which party paid whom by merging several users' payments into a single joint transaction that pools all of their inputs and outputs [187, 31]. Because every input and output shares the one transaction, an observer cannot reliably match a given input to its output; yet each participant still pays their own intended recipient, and no one surrenders custody of their funds [248, 307]. Like a ring signature, CoinJoin hides the real trace within a crowd rather than concealing or removing it, raising pseudonymity to the *set anonymity* of §4.1, which grows with each added participant [7]. It is the primitive underlying many mixing services (§5.2.1).[2]

POOL *Pooling. Pooling* gathers funds from many users into one shared reserve or standing pool and pays out from the common pot, so a withdrawal cannot be tied back to the deposit that funded it. Where CoinJoin merges several payments inside a single transaction, a pool persists over time and its anonymity set grows with every deposit it still holds. On its own, pooling rests on trusting whoever controls the reserve; combined with a concealment

[2]This is why we tag CoinJoin with commingling but ring signatures with disconnected fund flow, even though both hide the sender in a crowd. Commingling is the pooling of many parties' assets in one place so that ownership of the funds becomes unclear (§5.1.2), which is exactly what CoinJoin does by merging everyone's inputs and outputs into a single transaction. A ring signature pools no assets at all. Each party's coins stay their own, and only the identity of the true spender is obscured by the decoy signers, which breaks the sender-to-receiver link rather than blending ownership (§5.1.4).

blueprint such as a zero-knowledge proof or a trusted enclave, it becomes a cryptographic *shielded pool* in which not even the operator can link deposits to withdrawals [307]. Pooling is the direct on-chain realisation of *commingling* (§5.1.2), raising pseudonymity to the set anonymity of §4.1.

TUMBLE *Tumbling. Tumbling* breaks a trail into noise rather than hiding any single field. A service splits funds into many smaller outputs, spreads them across fresh addresses, and staggers them with randomised delays and fees, so timing and amount heuristics can no longer line an input up with its output [130, 59]. It is the classical mechanism of the earliest mixers and the on-chain realisation of *transaction flow obfuscation* (§5.1.1); on its own it adds noise but severs no link, so it is usually layered on top of pooling.

ZKP *Zero-knowledge proofs (ZKPs).* A *zero-knowledge proof* lets one party convince another that some statement is true while revealing nothing beyond the fact that it holds [126, 106]. For instance, you can prove you know an account's password without ever sending the password, or prove your balance is above a limit without disclosing the balance itself. Most cryptocurrency systems use a compact, non-interactive variant called a *zk-SNARK*, whose proofs are small and quick to verify [241]. ZKPs play more than one role in the PETs here. Their signature use is the *shielded* transaction or pool, where a proof confirms a transfer is valid while hiding sender, receiver, and amount, and lets a note be spent without revealing which deposit it came from. This gives transaction unlinkability and, in the terms of §4.1, full anonymity, a direct form of disconnected fund flow (§5.1.4) [241, 7]. The same primitive also serves narrower ends. A *range proof* shows that a hidden amount is non-negative, which is how confidential transactions keep a balance verifiable while it stays concealed. A *zk-rollup* posts only a succinct validity proof to the base chain, moving the detailed record off it (§4.2) [273]. The same capability even underpins selective disclosure for compliance, attesting that "this address is not linked to sanctioned or illicit clusters" [200] while withholding everything else. The property is thus double-edged. It enables privacy-preserving compliance, yet equally lets launderers minimise the data they expose.

FHE *Fully homomorphic encryption (FHE). Fully homomorphic encryption* allows computation to be performed directly on encrypted data, producing an encrypted result, without ever decrypting the inputs [121]. Long sought as a theoretical goal, it was first realized by Gentry in 2009 [121]. In a blockchain setting, FHE enables *confidential smart contracts* in which account balances and transaction inputs can remain encrypted on-chain while the network still executes contract logic over them, so sensitive values are never exposed in the clear yet remain fully usable [254]. Its guarantee rests purely on the hardness of

the underlying mathematics, though at a heavy performance cost that today confines it to high-value, narrow workloads [254].

SHUFFLE *Shuffle / DC-net.* A *shuffle* lets a group of participants jointly permute a set of outputs so that no one, not even a coordinator, can tell which input maps to which output, severing the link between them. In cryptocurrency mixing this is built with *secure multi-party computation* (MPC). A *DC-net* (dining-cryptographers network) or a *verifiable shuffle* lets the participants' own wallets agree on the permuted set without revealing the mapping [234, 314]. MPC is a general technique (it also underpins *threshold* wallets that split a private key across several machines so that no one holds it alone [120]), but the blueprint we track here is this participant-run shuffle, which serves *disconnected fund flow* (§5.1.4) by breaking the tie between sender and receiver. We label the chip by this use rather than by MPC itself, since the same general engine also serves confidentiality elsewhere.

BLIND *Blind signatures.* A *blind signature* lets a party obtain a valid signature on a message without the signer ever seeing its contents. In a mixer it lets a coordinator authorise each user's withdrawal while remaining unable to link that withdrawal to the deposit that paid for it, so the coordinator can arrange the mix yet never learns who paid whom [10]. It is the primitive behind the classic Chaumian mixing designs and the blinded coordinators of several CoinJoin services. Like the other coordination primitives here, blind signatures serve *disconnected fund flow* (§5.1.4) by severing the observable link between a payment's source and destination.

SWAP *Atomic swaps.* An *atomic swap* exchanges one party's coins for another's of equal value so that both transfers succeed together or neither does, enforced by a hash-time-locked contract (HTLC) that releases the funds only against a shared secret [20]. Because the two legs are separate, ordinary-looking transactions with no direct link between them, the swap breaks the on-chain trail between a coin's source and destination without pooling or joining. This is the *swapping* paradigm that mixing surveys set against obfuscation [307, 26], and it realises *disconnected fund flow* (§5.1.4). The same HTLC primitive underlies payment-channel routing, so an atomic swap is in effect a one-hop version of what a payment channel network does (§5.2.2.10).

TEE *Trusted execution environments (TEEs).* A *trusted execution environment* takes a hardware rather than a mathematical route to privacy [172]. It is an isolated "enclave" inside the processor that runs code and data shielded from the operating system, the machine's operator, and even an attacker with physical access; *remote attestation* then lets an outside party verify exactly which code is running inside the enclave before entrusting it with secrets [172, 52]. Because the enclave operates on plaintext at near-native speed,

TEEs can deliver confidential smart contracts [172, 52] far more easily and efficiently than the cryptographic methods above. That convenience carries a different kind of assumption, however. Unlike ZKPs, FHE, and MPC, whose guarantees reduce to mathematical hardness, a TEE's privacy rests on *trust in the hardware vendor* and its attestation infrastructure [172]. This trust has repeatedly proven fragile. Enclaves have been broken by side-channel and fault-injection attacks, and the prospect of vendor backdoors means the isolation is not absolute [172]. For an adversary seeking robust, provable privacy, solutions resting on hardware trust are therefore a weaker guarantee than the mathematics-based alternatives.

MW *MimbleWimble.* *MimbleWimble* illustrates how these primitives combine into a complete privacy design. Introduced anonymously in 2016 and later given a formal security treatment [221, 116], it abandons addresses and scripts entirely and rests on three ideas: confidential transactions hide every amount [35]; a built-in *CoinJoin* [187] aggregates transactions within a block so that individual inputs and outputs cannot be paired; and *cut-through* deletes intermediate outputs that are created and later spent, discarding much of the transaction history rather than merely hiding it. The result is a lean chain with no addresses and hidden values [116]. Its amount-hiding is robust, but, as its formal analysis makes clear, the guarantees are strongest against inflation and theft, while transaction-graph privacy is more limited and depends on how transactions are aggregated [116]. Like the other full-anonymity techniques above, MimbleWimble severs the link between a payment's source and destination, and so also functions as a disconnected-fund-flow technique (§5.1.4).

Deployment forms. A PET is defined not only by its blueprints but by where it runs and who operates it, and this second axis is how we organise the survey that follows. Deployment is the one axis on which every tool has exactly one value, so it structures the subsections below, and we define each form as its subsection opens. There are six. The *custodial* form is where an operator holds the funds. Three *protocol-native* kinds, Layer-1, extension, and Layer-2, build privacy into a chain of its own. The *application layer* is an ordinary smart contract added to a transparent chain. The *off-chain coordinator overlay* is where a non-custodial coordinator arranges a joint transaction that then settles on-chain. A single blueprint can appear at several of these; pooling, for instance, surfaces as a custodial mixer, a Layer-1 shielded coin, an application-layer contract, and a Layer-2 rollup, so each tool is best read by its blueprints and its deployment together.

5.2.1.1 PETs: Custodial Services

A *custodial* tool is one where an operator takes control of the user's coins. The user sends funds to the service, which holds them, pools them with everyone else's deposits, and later pays back different coins from its own reserve [307]. Because the operator sits between source and destination and already sees the whole picture, cryptography adds little here; privacy reduces to POOL pooling, usually layered with TUMBLE tumbling, the randomised delays, fees, and output splitting that break timing and amount correlations. Two things follow from custody. The operator can abscond with the reserve, the standing exit-scam risk, and holding customer funds makes it a regulated money transmitter under anti-money-laundering law [109]. That legal exposure is why custodial mixers are the ones most often seized and prosecuted, and custody is the single feature that sets them apart from the non-custodial off-chain coordinators of §5.2.1.6, which arrange the same kind of mix but never hold the funds.

The earliest mixers were all of this kind. *BitLaundry* and *Bitcoin Fog* (POOL TUMBLE) appeared soon after Bitcoin: a user deposited to a hosted wallet and the service dispersed the funds across many outputs over hours or days to hide the source [204, 127, 9]. In practice their anonymity was often weak, as a small pool of users could leave some deposits directly linkable to withdrawals [204]. A short academic line then tried to make custody *accountable*: *Mixcoin* (POOL TUMBLE) added a signed warranty so that theft by the mix would be publicly provable [32], and *Blindcoin* (POOL BLIND) went further, using Chaumian blind signatures so the operator could not even link a deposit to its matching withdrawal [288]. Both stayed custodial, though; a warranty deters theft, it does not prevent it.

Custody did not stop the model from scaling to enormous volumes. *Helix* (POOL TUMBLE) laundered more than $300 million for darknet users before its operator pleaded guilty [283]; *ChipMixer* (POOL), which swapped deposits for pre-funded fixed-value "chips" drawn from its reserve, processed over $3 billion before a 2023 takedown [284, 307]; and *Blender.io* (POOL TUMBLE) and *Bestmixer.io* (POOL TUMBLE) were sanctioned or seized for laundering, Blender being the first virtual-currency mixer ever designated by the U.S. Treasury [285, 100]. In the terms of our strategies, a custodial mixer performs *commingling* (§5.1.2) and, through its delays and splitting, *transaction flow obfuscation* (§5.1.1). Most stop there and never cut the trail cryptographically, since the operator holds the full mapping. Tools such as *Blindcoin* are exceptions, using blind signatures so that not even the operator can link a deposit to its withdrawal, which adds *disconnected fund flow* (§5.1.4) despite custody, and there may well be others beyond the ones we cover here.

5.2.1.2 PETs: Layer-1 Solutions

A *Layer-1* PET builds privacy into a blockchain's own base protocol, so that every transaction the chain processes can inherit the guarantee (§4.2). Here privacy is a property of the money itself: a user adopts a dedicated privacy coin, or a federated privacy sidechain pegged to a parent chain, rather than routing mainstream funds through an external tool. Because the design is native, a Layer-1 PET can make privacy the default on every transfer, and, by the deployment rule of this section, any tool operating at this layer is a coin or chain in its own right, never a mixer or a pool bolted onto a transparent ledger.

The best-known privacy coins hide the three parts of a payment with dedicated primitives. *Monero* (RING STEALTH CT) makes privacy mandatory, combining ring signatures to hide the sender among decoys, stealth addresses to hide the receiver, and confidential transactions to hide the amount [289, 7]. *Zcash* (POOL ZKP), building on the Zerocash design [241, 318], instead keeps a single *shielded pool*: a zk-SNARK proves a transfer valid while hiding sender, receiver, and amount, and a note can be spent without revealing which deposit it came from. Zcash privacy is opt-in, so shielded funds share an anonymity set only with other shielded users. *Iron Fish* (POOL ZKP CT STEALTH) reuses Zcash's shielded-pool design, known as *Sapling*, but turns it on by default for every account [149].

Some of these chains go further and are cross-chain by design. *Namada* runs a multi-asset shielded pool derived from the same Sapling design (POOL ZKP CT STEALTH) [8], while *Incognito* takes the ring-signature route of Monero, shielding assets brought in from other chains and transacting them with ring signatures, hidden amounts, and one-time addresses (RING STEALTH CT ZKP) [148]. Because both move shielded value across chains, they can also serve *chain-hopping* (§5.1.3), which here follows from their cross-chain architecture rather than from any blueprint, and our taxonomy marks this with a chain-hopping tag beside each (Figure 5.3).[3]

A second family follows the *MimbleWimble* design, which drops addresses entirely and aggregates a block's transactions into one so that individual inputs and outputs cannot be paired (§4.2). *Grin* (MW CT CJ) is the minimal implementation [128, 221], while *Beam* (MW CT ZKP POOL) adds *LelantusMW*, a one-out-of-many shielded pool that lifts the anonymity set into the tens of thousands [18, 19, 150]. *Dash* (CJ) sits apart: it is a transparent chain with an optional *PrivateSend* feature that mixes three users' coins through

[3]This is an edge case in our scheme. A strategy normally reaches a PET through its blueprints, but Namada's and Incognito's chain-hopping comes from their interoperable design (IBC and asset bridges), not from a chip; their chips still map them to disconnected fund flow and, through Namada's pool, commingling in the usual way.

a masternode-coordinated CoinJoin [70].[4] *Liquid* (CT), a federated Bitcoin sidechain, hides only the amount and asset type of a transfer through confidential transactions and assets [76].

A newer family delivers privacy not by hiding a coin's trail but by running *confidential smart contracts*, in which account balances and contract state stay encrypted on-chain. *Secret Network* (TEE) and *Oasis Sapphire* (TEE) execute contracts inside hardware enclaves so node operators never see the plaintext [245, 210], an approach whose academic anchor is *Ekiden* (TEE) [52]. *Inco* (FHE TEE) pursues the same goal with fully homomorphic encryption, computing directly on ciphertext [146].[5] As noted for the confidentiality blueprints, these hide values and state rather than the transaction graph, so on their own they provide confidentiality rather than the linkage-breaking anonymity of the coins above; their laundering relevance appears mainly when a pooling contract is deployed on top of them.

5.2.1.3 PETs: Chain Extensions

An *extension* adds privacy to an existing transparent chain through a protocol change, typically a soft fork that introduces an opt-in confidential ledger alongside the main one, rather than launching a separate coin [36]. Users move funds into the extension to gain privacy and back out to return to the transparent chain. Because the change lives in the base protocol, an extension is a native design by the deployment rule, never an external overlay; what marks it out is that the privacy is added to a chain that began transparent, and is used only by those who opt in. *Litecoin MWEB* (MW CT CJ) is the clearest example: a 2022 soft fork added MimbleWimble *extension blocks* to Litecoin, letting users peg coins into a confidential aggregate where amounts are hidden and transactions are joined, then peg them back out [36]. *Zerocoin* (POOL ZKP) was an earlier proposal in the same spirit, extending Bitcoin with a cryptographic accumulator into which fixed-denomination coins are minted and later spent through a zero-knowledge proof, breaking the link between mint and spend [195]; it was never activated on Bitcoin and instead shipped as its own coin, Firo. A recurring limit of the form is that the peg-in and peg-out remain visible on the transparent chain, so only activity *inside* the extension is shielded.

[4] Mechanically PrivateSend is an off-chain-coordinated mix like the overlays of §5.2.1.6; it sits here only because its coordinators are Dash's own protocol-native masternodes, so the mixing is native to the chain rather than an external overlay [70].

[5] Inco is a moving target: its 2023 form was a Layer-1 fhEVM, placed here [146], but it has since repositioned as an application-layer (§5.2.1.5) confidentiality coprocessor [147].

5.2.1.4 PETs: Layer-2 Privacy Rollups

A *Layer-2* PET executes transactions off the main chain and settles back to it, posting only succinct proofs and state commitments to the base layer (§4.2) [273]. Moving execution off-chain both scales throughput and, when the rollup is built for privacy, keeps the detailed record from ever appearing on the base chain. As with the other native layers, a privacy rollup is a chain in its own right that a user opts into, not an overlay contract on a transparent ledger.

Most privacy rollups are *zk-rollups* that carry a shielded pool off-chain. *Aztec* (POOL ZKP) is a privacy-first zk-rollup on Ethereum whose notes are encrypted so that only their owner can read them, with client-side proofs settling private state to the base chain [13].[6] *Zkopru* (POOL ZKP) combines an *optimistic rollup* for data availability—one that assumes its off-chain transactions are valid by default and relies on fraud proofs during a challenge window to catch bad ones [273]—with zk-SNARK proofs for privacy, giving private transfers and swaps of ETH and tokens [175]. *Nightfall v3* (POOL ZKP CT), from EY's blockchain team and Polygon [102], is an optimistic zk-rollup that batches confidential ERC-20 transfers to cut their cost.[7] A different route runs a confidential-compute rollup: *Fhenix* (FHE) was designed as an FHE rollup that computes over encrypted state [322], though, like the confidential-compute chains of §5.2.1.2, its guarantee is confidentiality rather than linkage-breaking.

5.2.1.5 PETs: Application-Layer Solutions

An *application-layer* PET is an ordinary smart contract deployed on a general-purpose transparent chain, adding privacy without touching the base protocol (§4.2). It is the most accessible form to build and the one a launderer can reach with mainstream assets such as ETH or an ERC-20, but it is bounded by what the host chain permits. This layer is also where the old "mixer" and "AEC" labels blur most: a shielded pool, a confidential token,

[6] The original *AZTEC protocol* (2018) was an application-layer design of on-chain confidential-token contracts, built on a custom range proof rather than a zk-SNARK, and it appears in §5.2.1.5 [303]. The same team later rebuilt it as the privacy-first Layer-2 zk-rollup described here [13], so the name denotes two distinct generations at different layers.

[7] Nightfall is an evolving family from EY, and its versions sit at different deployment layers. The original *Nightfall v1* (2019) was a set of on-chain smart contracts for private ERC-20 and ERC-721 transfers, an application-layer design that reappears in §5.2.1.5 [158]. The *v3* shown here is the later EY and Polygon rewrite that moved the same idea onto a Layer-2 optimistic rollup to cut gas costs [102], and a later *Nightfall v4* (2025) replaced the optimistic rollup with a pure zk-rollup for near-instant finality [101]. This tool thus spans two of our deployment forms in different versions.

and a stealth-payment overlay all live here as contracts, so the mechanism, not the layer, tells them apart.

The most familiar are *shielded pools*, which take in a mainstream asset and let a user withdraw their own value later behind a zero-knowledge proof. *Tornado Cash* (POOL ZKP) is the canonical case: fixed-denomination deposits share a pool, and a withdrawal to a fresh address proves ownership of an unspent note without revealing which [217]. *Railgun* (POOL ZKP) generalises this to arbitrary tokens held in a private balance [226]. *Privacy Pools* (POOL ZKP)—a specific protocol from Ethereum co-founder Vitalik Buterin and colleagues—adds a compliance twist to the shielded-pool idea [38]. It begins like Tornado Cash. Users deposit into a shared pool and later withdraw to a fresh address[8], proving with a zero-knowledge proof that they own one of the pool's deposits without revealing which, so a withdrawal cannot be tied to any single deposit. The twist comes at withdrawal, where the user gives a second zero-knowledge proof that their deposit belongs to a chosen subset of the pool called an *association set*. They can prove membership in a set (in effect, "my funds come from one of these deposits") or exclusion from one ("my funds come from none of these deposits"), and they build the set to include reputable deposits while leaving out any tied to known theft or sanctions. An honest user can therefore distance their money from illicit deposits in public, while their exact deposit stays hidden among the rest of the set. Criminals, unable to place their funds in a clean set, are separated out, which the authors frame as a separating equilibrium between compliant and non-compliant users [38].

Other contracts realise a mix without a persistent pool. *Möbius* (RING STEALTH) is a self-described ring-signature tumbler.[9] Senders pay into a contract addressed to recipients' one-time keys, and each recipient withdraws by signing on behalf of the whole group [188]. *MixEth* (SHUFFLE POOL) instead has the participants run a verifiable shuffle over the deposited keys, so that no party or coordinator learns the mapping [247].

A third group makes privacy native to a *token* rather than a pool. Confidential-token contracts such as EY's *Nightfall v1* (POOL ZKP CT) [158], *Zether* (ZKP CT) [34], and the 2018 *AZTEC* protocol (CT ZKP) [303] hide the amounts, and in some cases the parties, of transfers in an otherwise ordinary ERC-20; *Zama*'s fhEVM (FHE) does the same with

[8] Withdrawing to a fresh address is not the stealth-address blueprint. Here the withdrawer simply sends to another address they already control, which any user can do by hand. A stealth address instead has the *sender* derive a one-time address on the *recipient's* behalf for every payment, so that repeated payments to the same party cannot be linked [65]. Privacy Pools does not do this, so it earns no STEALTH chip.

[9] The name reflects loose usage. As we noted earlier (§5.1.2) and again at the start of this section (§5.2.1), some writers reserve *tumbling* for the specific split-and-stagger noise technique we adopt as the TUMBLE blueprint, while others use *tumbling* interchangeably with *mixing*, and *tumbler* with *mixer*. Möbius is one of the latter. It splits and staggers nothing, so despite the name it earns no TUMBLE chip.

fully homomorphic encryption over encrypted balances [69], and *smartFHE* (FHE ZKP) is an academic construction pairing FHE with correctness proofs [254]. Finally, *Umbra* (STEALTH) brings stealth addresses to Ethereum through the ERC-5564 standard, so that a recipient receives each payment at a fresh one-time address that cannot be linked to their public identity [297, 253, 65].[10]

5.2.1.6 PETs: Off-Chain Coordinator Overlay

An *off-chain coordinator overlay* arranges a joint transaction among many users off the chain, then settles it as a single ordinary transaction on-chain. Nothing here changes the base protocol, and no operator ever takes custody. The participants co-sign, so their keys never leave their wallets (§5.2.1). Custody is the one line that separates these tools from the custodial mixers of §5.2.1.1. A custodial operator holds the reserve, can exit-scam, and is a regulated money transmitter, whereas a coordinator here cannot touch user funds. Its legal status therefore stays contested even while custodial mixers are seized.

Most of these are *CoinJoin* coordinators, which merge many users' inputs and outputs into one transaction so that no input can be matched to an output. They differ mainly in how the coordination is run. *Wasabi* (CJ ZKP) uses a central but untrusted coordinator whose WabiSabi protocol issues zero-knowledge credentials, so it can assemble the join without learning the mapping [104]. *Samourai*'s Whirlpool (CJ BLIND) runs a similar blinded coordinator built on Chaumian blind signatures [105], while *JoinMarket* (CJ) replaces the server with a fee market in which "makers" offer liquidity to "takers" who assemble the join [151]. A more decentralised line removes the coordinator entirely: *CoinShuffle* and its successor *DiceMix* (CJ SHUFFLE) have the participants themselves run a peer shuffle, and *ValueShuffle* (CJ CT STEALTH SHUFFLE) extends this to hide amounts and receivers as well [233, 234, 232].

Some overlays reach unlinkability without a plain CoinJoin. *TumbleBit* (BLIND SWAP) is an untrusted payment hub: through off-chain puzzle-solving and blind signatures, value moves from payer to payee without the hub learning the pairing or being able to steal [138]. *Obscuro* (CJ TEE) builds its CoinJoin inside a hardware enclave, so the operator holds the mixing keys only within the enclave and can neither take custody nor learn the permutation [276].

A distinct family *swaps* coins rather than joining or pooling them. *CoinSwap* (SWAP) has two users atomically exchange equal-value coins through hash-time-locked contracts, so

[10] The 2018 AZTEC protocol hides amounts with a custom range proof but leaves note owners as identifiable addresses, so its set-anonymity is weak; it is confidential more than anonymous.

no link is written between input and output on-chain and the swap looks like an ordinary payment rather than a recognisable mix [20]. *Statechains*, as used by Mercury, move coins off-chain and let users swap equal-value statecoins in *blinded* groups run by a conductor that cannot learn who swapped with whom (SWAP BLIND) [255, 60].

5.2.2 Exploited Infrastructures

Unlike the PETs above, the mechanisms that follow were never built to hide anything. They are ordinary parts of the Web3 economy, the exchanges, bridges, lending protocols, and marketplaces that millions of honest users rely on every day. What draws a launderer to them is not a privacy feature but their reach and their gaps. These services move value at scale, often across chains or between crypto and the traditional financial system, and many operate with weak or uneven identity checks [63]. Because they carry no privacy design, we describe them differently from the PETs. There are no blueprints to list and no single deployment form to pin down, so instead we map each mechanism directly to the laundering strategies it can serve and to the placement, layering, and integration stages it touches, as our taxonomy figure records (Figure 5.3).

We examine these exploited tools and infrastructures across ten different categories, namely cryptocurrency exchanges, cross-chain bridges, DeFi mechanisms and protocols, NFTs, crypto ATMs, card-based instruments, online gambling platforms, initial coin offerings (ICOs), consensus protocols, and payment channel networks (PCNs), each exploited to facilitate laundering in its own way.

5.2.2.1 Cryptocurrency Exchanges

Cryptocurrency exchanges are pivotal in the Web3 ecosystem, enabling conversions between fiat and various crypto assets [63]. Their central role makes them exploitable across all money laundering stages: placement, layering, and integration [63, 199].

Centralized exchanges (CEXs). CEXs act as intermediaries for asset trading [63], managing users' assets via internal custodial wallets [199] funded with fiat or cryptocurrencies. Beyond simple conversion, major CEXs offer a broad set of trading and investment products, including spot, margin, and futures trading, staking and yield products, and automated trading bots [49]. Their yield and lending products are a custodial version of the DeFi mechanisms discussed earlier (§5.2.2.3), with the exchange holding the assets and running the strategy for the user. This broad product range gives launderers more ways to move, mix, and disguise value within a single platform.

Placement via CEXs. As crypto ecosystem gatekeepers, CEXs are frequently exploited for placement in weak regulation settings (§5.1.6) [63]. Criminals leverage offshore and no-KYC exchanges to convert illicit fiat into crypto, often using smurfs or money mules (multiple accounts depositing smaller amounts to avoid suspicion) [63, 117]. Integrated P2P and OTC services within CEXs [160] facilitate DRTs, enabling fiat-to-crypto conversions (§5.1.4) that disconnect fund flows by exploiting regulatory gaps [117, 47].

Layering via CEXs. Many CEXs support off-chain internal transfers between user accounts [40, 162, 25, 27, 57], typically free, functioning as simple database operations. These enable off-chain fund movements, with no on-chain traces. In lax compliance settings where KYC measures are absent, such movements evade both on-chain and off-chain tracing, contributing to DFF (§5.1.4). CEXs also facilitate *chain-hopping* (§5.1.3) by allowing users to deposit assets on one blockchain and withdraw on another [117]. Finally, while most reputable exchanges now assign unique deposit addresses to each user powered by HD wallets, there have been instances where exchanges have reused addresses across multiple users [293, 213]. This contributes to obfuscating transaction flows (§5.1.1) when conducting taint analysis [293], as well as aggregating funds from multiple users in one place, inherently contributing to *commingling* (§5.1.2).

Integration via CEXs. CEXs may serve as off-ramps for converting laundered crypto-assets into fiat, reintroducing them into the traditional economy [199, 47, 176]. In jurisdictions with KYC/compliance gaps, OTC brokers offer launderers low-risk fiat exit points [47].

Decentralized exchanges (DEXs). DEXs operate autonomously via smart contracts, without centralized intermediaries [309, 63]. They automatically match users trading virtual assets. Beyond individual DEXs, aggregators synchronize with multiple platforms, pulling order book data to automate trades and offer best pricing [63]. As DEXs do not interface with fiat, their laundering utility is mostly limited to layering.

Layering via DEXs. Launderers employ *TFO* by exchanging tainted assets across liquidity pools [176, 286]. Atomic cross-chain swaps [139, 183] enable *chain-hopping* (§5.1.3), allowing assets to traverse multiple blockchains with minimal traceability [286, 117, 63].

DEXs have mostly offered a decentralized form of spot trading, but decentralized versions of other CEX products have since emerged, most notably futures trading.

Layering via decentralized perpetuals. The clearest example of this shift is HyperLiquid, a decentralized exchange for perpetual futures, a leveraged derivative with no expiry date [144]. Unlike typical DEXs that settle through liquidity pools, it runs a fully on-chain order book and records every order, trade, and liquidation on-chain [144]. Matching the speed of a centralized venue was not feasible on a general-purpose chain, so its team built

a dedicated Layer-1 with a custom HyperBFT consensus that gives sub-second finality and very high throughput [144]. For a launderer, on-chain derivatives are one more place to add noise. Positions can be opened, closed, and offset between accounts under common control, so value shifts through a series of trades rather than plain transfers, which deepens TFO (§5.1.1) [63]. Because this activity sits on a separate Layer-1, following it also means tracing across another chain (§5.1.3).

5.2.2.2 Cross-chain Bridges

These bridges enable interoperability between isolated blockchains, transferring assets, data, and messages [143, 319]. They typically use (a) *lock-and-mint/burn-and-release* or (b) *liquidity-pool-based models* to manage cross-chain flows [169, 319]. In the former, tokens are locked (reversible) or burned (irreversible) on the source chain, while equivalent wrapped tokens (see §2.3) are minted on the destination [169]. Liquidity-pool-based bridges bypass wrapped tokens, executing swaps using pools of original assets.

Bridging also applies to non-fungible tokens [136]. *Bridged NFTs* are NFTs transferred across chains via a similar lock-and-mint logic as described above.

Layering via bridges. Bridges enable *layering* by facilitating chain-hopping (§5.1.3) [176, 286], allowing launderers to move assets across blockchains and sever direct provenance links [143], thus making it more difficult to trace these assets [319, 201]. Past studies reveal that a substantial portion of cross-chain fund flows reaches exchanges, highlighting the operational integration of bridge-based chain-hopping into broader laundering pipelines [143]. Since NFT bridges facilitate the transfer of NFTs between blockchain networks [136], they might also be used to facilitate chain-hopping (§5.1.3).

5.2.2.3 DeFi Mechanisms

DeFi is built from building blocks such as lending platforms, yield aggregators, liquid staking, and stablecoins, many of which can be exploited to add an extra layer of obfuscation to transaction flows [63, 300]. Although DeFi's decentralized nature and lack of fiat interaction limit its role in placement and integration, custodial stablecoin issuers extend DeFi's reach to these stages [197].

Loan providers. Decentralized lending protocols facilitate permissionless borrowing through two primary mechanisms, over-collateralized loans and flash loans [300, 133]. Aave, a leading decentralized lending protocol, runs a two-sided market where suppliers deposit

assets to earn yield and borrowers draw funds against collateral worth more than the loan [2]. Over-collateralized loans resemble traditional debt arrangements, requiring users to lock assets exceeding the loan value [300]. In contrast, flash loans allow users to borrow assets without collateral, under the condition that the borrowed amount is repaid within the same blockchain transaction. If the repayment condition is not met, the transaction is reverted, ensuring no risk to the lender.

Layering via over-collateralized loans. Illicit assets can be pledged as collateral to obtain clean loaned funds [300]. Furthermore, by extending loans to third parties and receiving repayments, launderers facilitate commingling (§5.1.2) of illicit and legitimate assets. Borrowing a different asset than the one pledged also swaps the token on the surface, adding to transaction-flow obfuscation (§5.1.1). Cross-chain lending further supports obfuscation via chain-hopping (§5.1.3) [319]. Because these protocols run on several chains, a launderer can pledge collateral on one chain and draw the loan on another, so the flow splits across separate ledgers that investigators must then trace with different explorers. *Layering via flash loans.* Launderers can acquire flash loans and execute complex transactions within a single block, including wash trading (fake trades used as cover) and cycling assets before repaying the loan [133, 63]. Flash loans can also facilitate collateral swapping or the repayment of loans with different assets. These activities can result in TFO (§5.1.1) and the commingling of illicit funds with loaned assets (§5.1.2).

Yield farming and liquidity pools. Yield farming refers to the practice of providing capital to DeFi protocols in exchange for financial rewards, typically in the form of governance or utility tokens [309, 300]. A key mechanism for this is liquidity provisioning to Automated Market Makers (AMMs), which replace traditional order books by enabling token swaps in DEXs through algorithmically managed liquidity pools [66]. Users who supply assets to these pools earn a share of the transaction fees and may also receive protocol incentives. Yield farming can happen in both decentralized and custodial forms (e.g., through CEXs).

Layering via yield farming. Launderers invest tainted assets into yield farming to earn rewards, commingling (§5.1.2) illicit funds with clean proceeds [176, 286].

Layering via liquidity pools. Launderers begin by creating fake tokens [176], which they pair with legitimate assets such as ETH within DEXs. This pairing involves supplying both assets to a new liquidity pool, enabling the counterfeit token to appear tradeable. By conducting wash trades between accounts they control, launderers simulate organic market activity and inflate the token's perceived legitimacy. This tactic commingles (§5.1.2) illicit funds with on-chain liquidity while masking their origin. Ultimately, launderers extract clean ETH from the pool, disguised as ordinary DEX trading.

Liquid staking and yield vaults. Running a solo validator on Ethereum requires locking 32 ETH, which is out of reach for many users [125]. Liquid staking protocols remove this barrier by pooling deposits of any size and returning a *liquid staking token* (LST) that stands for the staked funds and their accruing rewards, such as Lido's stETH or ether.fi's eETH [125, 174, 88]. Unlike locked stake, an LST stays tradable and can be reused across DeFi, and yield-bearing wrappers like weETH fold the rewards into the token's price rather than a growing balance (§2.3) [88]. Staking as an exploited consensus infrastructure is covered separately (§5.2.2.9). The forms here are institutionalized and composable with other protocols, which is why we place them among DeFi mechanisms. A close relative is the automated yield vault, or yield aggregator, such as ether.fi's Liquid vaults, which take a deposit and spread it across a basket of DeFi protocols to raise returns, handing back a vault token that records the depositor's share [94, 93].

Commingling via pooled deposits. Staking pools and vaults hold the funds of many users in one shared contract, so illicit deposits mix with everyone else's (§5.1.2), and the LST or vault token returned carries no visible tie to the original tainted coins [286, 63]. Pooled and custodial staking commingles funds in the same way (§5.2.2.9).

Layering via under-watched tokens. An LST or vault token still holds and moves the value of its underlying deposit, yet it is less familiar than a base asset like ETH and can draw less attention in review. A launderer can shift value by moving these tokens while scrutiny stays on better-known coins, adding steps and noise to the trail and contributing to TFO (§5.1.1) [63]. Because LSTs are also accepted as collateral in lending markets [125], tainted value can be parked as collateral and borrowed against, placing more distance between the funds and their later use. As these tokens and vaults span several chains, the same moves can extend into other ledgers, feeding the chain-hopping described above (§5.1.3).

Layering via staking loops. Beyond a single borrow, the composability of these tokens lets a launderer build a repeating loop. They can stake ETH to get weETH, post the weETH as collateral in a lending market like Aave to borrow USDC, buy more ETH, and stake that too, then run the cycle again [125, 2]. Restaking, introduced by EigenLayer [81], pushes this further. It lets the same staked ETH or an LST be opted in to help secure additional services built on Ethereum, known as *actively validated services* (AVSs) such as bridges and oracles, in exchange for extra rewards, and a *liquid restaking token* (LRT) keeps the restaked position tradable so it can re-enter the loop [125]. Each turn folds another round of swaps, loans, staking, and restaking into the position, so a compact-looking holding unwinds into a long, tangled trail when investigators later reconstruct it, adding noise and deepening TFO (§5.1.1) [63].

Stablecoins. Stablecoins, especially fiat-backed variants, serve as gateways between fiat economies and DeFi [164]. As introduced earlier (§2.3), they are pegged to a fiat currency and hold a steady value, unlike volatile coins like ETH [197]. That stability is also what draws launderers, who can park or move value without exposure to price swings, and stablecoins now make up the majority of all illicit cryptocurrency transaction volume [47].

Placement and integration via fiat-backed stablecoins. Fiat-backed issuers such as Circle [54] and Tether [269] mint tokens against reserves when a customer deposits fiat, and burn them on redemption [197]. This primary channel runs through regulated, KYC-checked accounts, so minting clean stablecoins straight from illicit cash is difficult [199]. Launderers instead acquire stablecoins on secondary markets, through exchanges, DEXs, or over-the-counter and peer-to-peer trades where identity checks are weak or absent, or by clearing KYC with fake or purchased identities (§5.1.6). Once held, the tokens move freely on-chain and can be spent or cashed out, which completes placement and integration [63]. One risk stays with the launderer. Fiat-backed issuers can freeze or blacklist flagged addresses, so they tend to move quickly or fall back on decentralized alternatives [47].

Layering via crypto-collateralized stablecoins. Crypto-collateralized stablecoins such as Dai [182] take a different route. They are minted by locking crypto as over-collateral rather than by depositing fiat, so there is no fiat on-ramp or issuer KYC to clear [197]. A launderer can pledge illicit crypto to mint fresh Dai, which is exploitable during layering, and because no central issuer controls the token, the minted Dai is not directly freezable the way USDC or USDT are [63, 47]. That resistance is not absolute. Much of Dai's own collateral has at times been centralized stablecoins, with USDC alone making up about a third, so a freeze on USDC can still reach Dai indirectly, as the Tornado Cash sanctions in 2022 made clear [270].

5.2.2.4 Non-Fungible Tokens (NFTs)

Non-fungible tokens were first implemented on Ethereum via EIP-721 [86] and later became available on Bitcoin through "Ordinals," which inscribe arbitrary data onto serialized satoshis [231]. In Web3, NFTs serve as digital ownership certificates, enabling verifiable scarcity [199, 135]. NFTs are tightly coupled with Web3 metaverses. The term "metaverse," coined in *Snow Crash* [257], has evolved into a vision of immersive, networked 3D environments. Inspired by MMO games [199], Web3 metaverses include platforms such as Decentraland [71] and The Sandbox [272], where NFTs represent avatars, skins, and virtual land parcels. Here, NFTs underpin digital property rights and enable economic

transactions [199]. Acquiring metaverse properties often requires only a wallet, bypassing KYC checks [306].

NFTs have been examined as laundering vectors across all PLI stages [252, 199, 306]. Metaverse platforms, where NFT trading is prevalent, offer fertile ground for laundering due to liquidity and ease of transfer of digital collectibles [199].

Placement via NFTs. As described in §5.1.4, illicit fiat can be funneled into NFTs via disjoint reciprocal transfers, introducing tainted funds into the crypto ecosystem. One route is to pay an artist or current owner in cash for an NFT that has genuine resale demand, then place that money into crypto by reselling or auctioning the NFT to other buyers who pay in cryptocurrency.

Layering via NFTs. As discussed in §5.1.5, NFT trading with subjective pricing contributes to layering, since colluding wallets can trade the same token at inflated prices to move value and mask its origin, while bridged NFTs also facilitate chain-hopping (§5.2.2.2).

Integration via NFTs. As discussed in §4 and §5.1.4, NFTs can act as value stores or speculative assets [252], and be sold to reintroduce cleaned funds into the legal economy. Selling the NFT on a public marketplace then returns the proceeds as what looks like ordinary art or collectible income.

NFTs do not always carry subjective prices. Some hold objective value because they represent a claim on assets or a position in a protocol. A Uniswap v3 liquidity position, for instance, is issued as an ERC-721 NFT that represents the provider's deposited liquidity and the fees it earns [3], and liquid staking protocols such as ether.fi (§5.2.2.3) mint a withdrawal-request NFT when a user unstakes, which the holder later burns to claim the underlying ETH [89]. These tokens can be transferred between wallets like any other NFT, so a single transfer can carry a sizeable and objective amount of value.

Layering via value-bearing NFTs. Value-bearing NFTs open a further route. Because they hold objective value yet trade on the same rails as art and collectibles, they can move funds between wallets while drawing little attention. Detection tools that follow fungible-coin flows, or that treat NFTs as low-value curiosities, can overlook a transfer that actually carries a large claim, much like the under-watched tokens seen in DeFi (§5.2.2.3). Routing value through them adds steps and noise to the trail, deepening TFO (§5.1.1) [63]. This holds only when the token works like cash or a bearer cheque, where whoever holds the NFT can redeem the value it represents. If instead a protocol ties redemption to the wallet and key that first received the NFT, much like a cheque made out to a name, transferring the token does not transfer the claim, so the value cannot be turned back into money by anyone else and the NFT loses its use for laundering.

5.2.2.5 Cryptocurrency ATMs

Cryptocurrency ATMs, also known as "Bitcoin ATMs (BTMs)" [209], enable access to crypto without online exchanges and can be found in stores or gas stations [63, 209]. To deposit cash and purchase crypto, users provide minimal ID (e.g., a phone number) and scan a receiver address via QR code [63, 209]; some BTMs generate paper wallets if no address is given [209]. For withdrawals, crypto is sent to a designated address and cash is dispensed. Machines come in two forms: one-way BTMs that only sell crypto for cash, and two-way BTMs that also buy crypto back and pay out cash. Only two-way machines offer a cash-out route [63, 209].

BTMs have drawn scrutiny for illicit use [63, 252]. TRM Labs reported that the cash-to-crypto sector, largely driven by BTMs, processed at least $160M in illicit funds since 2019 [167]. BTMs are frequently used by dark web vendors to cash out illicit proceeds [63], prompting regulatory concern [167]. Despite existing safeguards, inconsistent regulations and weak KYC measures allow launderers to exploit BTMs to inject illicit funds into the financial system or retrieve them as seemingly legitimate assets [63, 252]. Because the level of identification is usually tied to the transaction size, launderers split larger sums into smaller deposits across several machines and sessions to stay below the thresholds that trigger an ID check or a report [63, 252].

In laundering terms, BTMs serve two stages. They support *placement* when cash is fed in and turned into crypto, moving illicit banknotes into the digital economy, and *integration* when crypto is sold back for cash that looks like a normal withdrawal. A BTM is not a layering tool on its own. For example, the crypto bought at a machine can be moved later through an exchange to hide its trail; in this process, it is the exchange that carries out the layering (§5.2.2.1).

5.2.2.6 Card-Based Instruments

Several card-based instruments can be exploited for laundering. These range from ordinary retailer gift cards bought with crypto, through pre-funded crypto gift-cards and vouchers, to crypto-backed payment cards run as custodial or non-custodial programs.

Gift-card shops. Platforms like Bitrefill [30] sell ordinary retailer gift cards that can be paid for with crypto, often without strong KYC policies. A launderer pays in illicit crypto and receives a gift card for a mainstream retailer or service, such as a large online store or a food-delivery app. The card works much like a bearer instrument. It holds a fixed value, carries no record of who funded it, and can be spent, gifted, or passed on to someone else.

Criminals have long used gift cards to conceal illicit flows and move value quietly [63], and cards bought with crypto inherit the same appeal.

Integration via gift-card resale. The launderer converts illicit crypto into gift cards and resells them to third parties, often at a discount through informal markets, receiving cash or another asset that carries no obvious link back to the original funds [63].

Layering via gift-card-to-crypto swaps. The same cards can also sever the trail. Where a marketplace accepts gift cards as payment for cryptocurrency, a launderer can buy cards with illicit crypto and then use them to buy fresh coins elsewhere. The new crypto arrives with no on-chain link to the illicit source, so the gift card acts as an off-chain hop that disconnects the flow of funds (§5.1.4).

Pre-funded crypto gift-cards and vouchers. Sold in fiat, these products are pre-loaded with fixed crypto amounts and redeemed via embedded private keys or claim codes. *Ballet* steel cards [236, 16], *Tangem Notes* [263, 292], *Casascius/Denarium* coins [41, 74], and digital vouchers from *CryptoVoucher*, *Bitnovo*, and *Azteco* [68, 28, 78, 14] are notable examples. Although many providers have discontinued pre-loaded options, likely in response to rising regulatory scrutiny, such mechanisms remain accessible in some markets and are considered high-risk instruments [110].

Placement via bulk purchase. Acquirable in bulk, they can be exploited for illicit fiat placement, particularly in weak-KYC jurisdictions (§5.1.6).

Custodial crypto-backed card programs. Crypto-linked cards (e.g., Visa [295], Mastercard [186]) enable users to spend crypto directly, with issuers converting it to fiat at purchase time so merchants receive traditional currency [63]. These cards, also offered by exchanges and payment processors, function like fiat-funded debit cards, enabling online/in-person payments and ATM withdrawals [294, 61]. In this custodial model the exchange or issuer holds the customer's assets and settles the conversion, so the user never controls the underlying keys. Major exchanges such as KuCoin [161] and Binance [24] have run card programs of this kind. However, they pose laundering risks akin to traditional financial tools [63].

Integration via card spending. Launderers spend converted crypto through these cards, turning it into ordinary purchases and cash withdrawals and integrating it into the fiat economy.

Non-custodial crypto-backed card programs. A newer class of card programs keeps custody of the underlying assets with the user rather than the issuer. These are offered mostly by *DeFi neobanks* such as Ether.fi [90], Kast [152], by decentralized payment networks such as Gnosis Pay [124], and by self-custody wallet providers such as Tangem [263]

and Trust Wallet [279]. What they usually share is that the money stays in a wallet the user controls, often a smart contract wallet of the kind described earlier (§2.4). Ether.fi and Gnosis Pay, for instance, both build on a Safe smart contract account [95, 124].

A DeFi neobank offers the everyday parts of a normal neobank, a spending card, a balance, and transfers, but it does not take custody of the customer's money. A normal neobank holds deposits on the customer's behalf. A DeFi neobank instead leaves the assets in a smart contract wallet that the customer controls, and account settings such as the card spend limit are enforced on-chain by that contract rather than by the operator [95]. Ether.fi works this way. Each user gets their own Safe vault, and the company cannot move or spend the assets without the user's approval [95]. These services have grown quickly as smart contract wallets and account abstraction have matured.

Such neobanks rarely connect to the card networks on their own. They run the card program through a card provider such as Rain [227] or Reap [228], which sits between the neobank and Visa or Mastercard. A provider or program that reaches sufficient scale can instead become a network principal member and issue directly, without a third-party sponsor, as Reap has done with Visa [228].

Providers like Rain and Reap have made it far easier for virtual asset service providers to launch their own cards, and many have done so in recent years; Tangem, for example, pairs its self-custody wallet with its own card program [263]. Some prefer a co-branded card with an established neobank over building a program directly. MEXC took this route in early 2026, launching a co-branded card with Ether.fi while letting users keep on-chain custody of their assets [194].

Integration via account spending. The barrier to entry is low. A user opens an account, clears a light KYC check, moves crypto into the neobank, and can spend it straight away wherever the card is accepted. This lets illicit funds be integrated by buying assets that hold their value and can be resold, such as real estate in some jurisdictions or luxury watches and jewellery. Once resold, the proceeds carry a legitimate-looking origin, the sale of property or goods, often in a different country from where the funds first entered.

Placement via bank rails. Several of these platforms also connect to ordinary bank rails. Ether.fi, for example, lets users move fiat into and out of their wallets through ACH and Fedwire [91], SWIFT [92], SEPA [97], and Pix in Brazil [96]. Providers such as Avenia [12] and bridge.xyz [33] supply this kind of stablecoin bank rail. This gives each account a virtual bank presence that can receive wires and convert between stablecoins and fiat. Illicit fiat can then be placed by opening many accounts and feeding small amounts into each, a form of smurfing, using fake or purchased identities to clear KYC (§5.1.6). Keeping

each deposit small helps the activity stay under the thresholds of monitoring tools such as Sardine [239] (§6.1).

Layering via account hops. The same accounts work as layering hops in two ways at once. As a crypto wallet, the neobank's vault is one more address in a chain of transfers. As a virtual bank account, it can take in a wire and send the funds on to another account, or pass value between the crypto and banking systems. Moving money to a third party through the virtual account extends the trail into the traditional banking layer.

5.2.2.7 Online Gambling Platforms

Online gambling platforms are key vectors for financial obfuscation and money laundering [252, 242]. What makes them useful is not the game but the payout. Money taken out of a casino or betting site looks like "winnings," which gives dirty money a believable story about where it came from. The launderer does not even have to really gamble to get that story [242, 63]. While most accept fiat and crypto, many crypto-native implementations operate with minimal regulation [252], exposing laundering vectors across all PLI stages [110]. What separates safer sites from risky ones is regulation. Licensed sites must check who their customers are and report suspicious activity. In the United States, any casino earning over $1 million a year has to follow the Bank Secrecy Act's identity-check rules [63], so launderers avoid these sites and turn to unlicensed, offshore, or crypto-only ones where the checks are weak or missing [6]. This is not a small problem. One UNODC survey found more than 340 licensed and unlicensed casinos being used for laundering across Southeast Asia [252].

Placement via gambling deposits. Illicit fiat or crypto is deposited into gambling accounts as wagers [252]. To stay unnoticed, launderers rarely move all the money at once. They split it across many accounts, either their own or "mule" accounts opened in other people's names, and put in small amounts each time. That way every account looks like just another ordinary, small-stakes player [252, 110].

Layering via gambling activity. Fragmented bets and intra-platform transfers create transaction graphs that mimic legitimate behavior (§5.1.1) [6, 252]. Illicit funds mix with real winnings (§5.1.2) [252]. Another method barely gambles at all. By betting on both sides of an even bet, such as red and black at roulette, the player is almost sure to get most of the money back as "winnings," without really trying to win [107]. The small amount lost to the house is just treated as a cost of doing business, the price of turning dirty money into clean money [242]. Games where players bet against each other open another door. Two players working together can play against one another and let one lose on purpose,

which moves the money across as if it were a normal game. In poker this is known as "chip dumping" [107, 110]. Anti-laundering checks usually only watch bets made against the casino itself, so money passed between players can slip by unnoticed [168].

Integration via withdrawals. Remaining balances, now masked as gambling proceeds, are withdrawn to wallets or bank accounts and misrepresented as legitimate income [63].

Prediction markets. A newer kind of site turns betting into trading. On a *prediction market*, people buy and sell shares in the outcome of a real event, such as an election or a sports final. Each share costs between $0 and $1, and the price shows how likely the market thinks the outcome is. A "Yes" share at $0.60 means about a sixty percent chance [223]. *Polymarket*, launched in 2020 and running on the Polygon blockchain with trades paid in stablecoins, is the biggest example [112, 223]. There is no house. Each market is a smart contract, buyers and sellers are matched directly, and when the event is over the result is decided by a decentralized "optimistic oracle" that anyone can take part in, rather than by a company [223, 180]. These traits make prediction markets an easy fit for laundering. The same deposit, trade, and withdraw pattern still works. Crypto goes in, bets are placed, and the money comes out looking like trading profit. Because players trade directly with each other, the deliberate-loss trick works here too, since two wallets can take opposite sides of the same market to move money between them. No company sits in the middle checking identities either, so the money moves with little to stop it [6]. This is not a rare or small activity. More than $3 billion was traded on Polymarket's 2024 U.S. election markets [225], and regulators have taken notice. Polymarket paid a $1.4 million fine to the U.S. CFTC in 2022 for running an unregistered market [62].

5.2.2.8 Initial Coin Offerings (ICOs)

ICOs are blockchain-based fundraising mechanisms where ventures issue digital tokens in exchange for crypto or fiat [73, 17]. Unlike traditional channels, they use white papers instead of regulated prospectuses and rely on online promotion rather than underwriting, offering global investor access with minimal legal barriers [73, 17]. Issued tokens generally fall into three categories: currency (payment), utility (platform access), and investment (profit participation), though many are hybrids [156]. The absence of shareholder rights and governance structures deprives token holders of oversight and heightens fraud risks [73]. The decentralized nature and regulatory gaps (§5.1.6) make ICOs exploitable across PLI stages:

Placement via ICOs. Placement is feasible when ICOs accept fiat. Criminals can convert illicit cash into digital tokens. Weak KYC during early ICO phases [73] facilitated such entry, though fiat acceptance remains less common than crypto.

Layering via ICOs. More commonly, ICOs accept cryptocurrencies like BTC or ETH. In that case, illegal crypto funds are invested into ICOs, where they appear as legitimate contributions to a cryptocurrency project [17]. If the project succeeds, the funds are returned as profits, now disguised as lawful investment gains. Essentially, malicious actors invest tainted funds—commingling them with clean assets of other participants (§5.1.2)—and receive new tokens (§5.1.1). If the ICO sends tokens to a different address than the payer's, it introduces DFF (§5.1.4). Accepting payments on one network (eg., Bitcoin) but issuing tokens on another (e.g., Ethereum) also enables *chain-hopping* (§5.1.3). A more advanced mirroring tactic (§5.2.2.3) is to create a counterfeit ICO, where actor A hosts the ICO, and B buys worthless tokens using illicit crypto. The transaction appears as a speculative loss but facilitates value transfer, exploiting justifiable price volatility.

Integration via ICOs. If a counterfeit ICO accepts fiat, the scheme extends into integration. For instance, if B invests in an ICO launched by A and the token later loses value, B's crypto is "lost" while A obtains legitimate fiat proceeds, successfully off-ramping the crypto assets. Projects where developers abandon the protocol without making false promises are "soft rug-pulls" and may not be considered criminal [171].

5.2.2.9 Consensus Protocols

Recent studies reveal that consensus protocols, particularly Proof of Work (PoW) and Proof of Stake (PoS), can be exploited for money laundering and sanctions evasion [264, 137, 184].

Placement via PoW. Illicit fiat can be channeled into mining by investing on hardware, electricity, and hosting, generating fresh crypto that appears clean on-chain, a method reportedly used by the Iranian government to bypass sanctions [46]. This approach converts fiat into blockchain-native assets, forming an unlinkable flow (§5.1.4). Iran shows how this works at state scale. After recognizing crypto mining in 2019, it set up a licensing regime where miners use heavily subsidized electricity, much of it from the country's oil and gas, and must sell their mined bitcoin to the central bank [82]. The bank then spends that bitcoin with overseas suppliers to pay for imports, turning energy reserves into a cross-border asset that moves outside the SWIFT banking system Iran is cut off from [82]. Because the coins are freshly mined, they carry no earlier on-chain history to trace. Another Chainalysis report identified mining pool addresses receiving both ransomware proceeds and legitimate earnings [264], evidencing ongoing *commingling* activity (§5.1.2). Here the

pool works much like a mixer, blending a launderer's illicit deposits with genuine miners' rewards so the payout looks like ordinary mining income.

Layering via PoW. Mandiant discovered that a North Korean group it tracks as *APT43* launders stolen funds through cloud mining and hash rental services to acquire fresh, untainted assets [184], constituting a disconnection in fund flow (§5.1.4). The scheme runs in a few steps. The group pays a hash rental or cloud mining service with crypto stolen in earlier hacks. The service then points its hash power at a wallet the group controls and mines new coins into it. Those coins are block rewards with no on-chain link to the stolen payment, so the group is left with clean, freshly mined crypto while the trail back to the theft is broken [184].

Layering via PoS. Launderers may stake illicit funds to generate fresh rewards. Liquid staking and its tokens, such as stETH [174], were discussed in the DeFi mechanisms section (§5.2.2.3), which explains how they keep staked value liquid and make tracing harder. Staking via custodial or pooled DeFi services also facilitates commingling (§5.1.2) of illicit funds [286]. Launderers may also withdraw rewards to new wallets, re-stake them, or apply additional layers using other mentioned techniques.

5.2.2.10 Payment Channel Networks (PCNs)

Payment Channel Networks (PCNs) are off-chain protocols developed to improve blockchain scalability and efficiency [224, 207, 79]. They enable users to route payments through intermediaries without direct channels. For example, if Alice is connected to Bob and Bob to Charlie, Alice can pay Charlie via Bob using hashed timelock contracts (HTLCs) [157]. Instead of recording each transaction on-chain, two parties open a bi-directional channel by locking funds in a multi-signature address, exchange rapid off-chain micro-transactions, and settle the net balance on-chain when the channel closes [157, 248]. These networks rest on the same hash-time-locked contracts introduced with atomic swaps (§5.2.1). An atomic swap is in effect a one-hop channel, while a PCN chains many such hops into a routed path, each hop paying out only against a shared secret.

Layering via PCNs. Originally developed for scalability, PCNs have also emerged as effective obfuscation tools in the layering phase of money laundering. By fragmenting illicit funds and routing them through multiple off-chain paths, often via dormant or low-liquidity links, criminals can obscure transaction trails and complicate attribution [157]. This tactic embodies both TFO and DFF (§5.1.1, §5.1.4). Tainted funds may be split across multiple paths and settled in different currencies, hindering flow reconstruction even when endpoints

are observed [157]. Each extra hop adds more noise to the trail, making flow reconstruction harder still. PCNs further enhance anonymity by recording only channel openings and closures on-chain; intermediate transfers remain off-ledger [248]. While most PCNs are confined to a single blockchain, such as the *Lightning Network* on Bitcoin [224] or the *Raiden Network* on Ethereum [207], their use of HTLCs and atomic swaps enables experimental cross-chain capabilities that facilitate chain-hopping (§5.1.3). Notably, frameworks like the *Perun Network* propose support for cross-chain atomic swaps [218].

Chapter 6

Crypto Money Laundering Countermeasures

In response to increasingly sophisticated crypto money laundering schemes, anti-money laundering (AML) measures have evolved along two paradigms: (a) detection measures, which aim to uncover laundering activity (§6.1); and (b) prevention measures, which seek to obstruct laundering before it occurs or prevent its recurrence (§6.2).

6.1 Detection Measures

Detection measures monitor and analyze transactional data to identify suspicious behavioral patterns across the blockchain ecosystem. Systematically, they fall into the following groups:

Rule-based detection. AML detection has traditionally relied on rule-based systems, which use predefined thresholds and expert-crafted conditions to flag suspicious activity [290, 219]. Conditions such as transaction limits, unusual patterns, or specific event triggers can be used to generate alerts for investigation [290]. An advantage of rule-based frameworks is their interpretability and alignment with regulatory expectations, as institutions must justify flagged activity. Lin et al. [176] used rule-based methods on Ethereum to trace laundering paths, while clustering techniques link addresses based on heuristics like multi-input usage [129, 189]. Firms such as Elliptic [83], Chainalysis [48], and CipherTrace [53] apply these rules across chains for real-time AML risk assessment. However, rule-based systems are afflicted by high false positives, static rules that demand expert

maintenance, and limited adaptability to evolving laundering tactics, making them less scalable without continuous expert updates [51, 290].

Data-driven detection. Machine learning techniques are used to inspect complex and evolving patterns in transactional data [290]. These automate detection, reducing manual rule reliance and enable adapting to evolving laundering tactics. Several approaches aim to classify licit and illicit transactions or entities [290], often employing transaction graph analysis and addressing class imbalance challenges [290]. Other graph-based approaches [316, 177, 256, 179] model entities (e.g., users or wallets) as nodes, and relationships or flows as edges, based on the premise that laundering accounts form distinct structural patterns compared to legitimate ones. Another line of work [220, 198] frames money laundering as an outlier detection problem, using clustering techniques to isolate anomalous users and transactions. Gu et al. [131] focused on anomalous transaction amounts to flag potentially malicious exchanges. Other studies [275, 118, 320] advanced illicit activity detection across services such as exchanges, mixers, darknet markets, gambling platforms, and mining entities by leveraging transaction histories, address data, and structural or behavioral features within Bitcoin and Ethereum. Further efforts analyzed account-level transaction histories to detect illicit addresses [103, 178], and combined transaction and account-level insights [84] to enhance fraud detection.

In practice, much of this monitoring is not built in-house. Most VASPs integrate commercial fraud and AML platforms instead, so they are worth noting here. Sardine [239] is one widely used example. It runs real-time transaction monitoring that combines a configurable rules engine with machine-learning models trained on large volumes of device, behavioral, and transaction signals, spanning both paradigms above. Exchanges, neobanks, and crypto card programs (§5.2.2.6) rely on it to flag fraudulent patterns, of which money laundering is only one, and the same controls help them meet KYC and transaction-reporting duties [239]. Comparable platforms such as Unit21 [280] and ComplyAdvantage [64] fill a similar role. These engines also lean on blockchain-intelligence providers that label addresses by risk. Alongside the analytics firms introduced earlier, such as Chainalysis [48], TRM Labs [278] supplies these labels, and Sardine ingests TRM's wallet-screening reason codes so on-chain risk feeds straight into its detection rules [238].

6.2 Prevention Measures

Prevention efforts focus on regulatory controls, institutional safeguards, and public engagement, aiming to deter illicit activity by enhancing transparency. These include:

Regulatory deterrents. Global regulators, led by the FATF, have extended AML guidelines to *Virtual Asset Service Providers* (VASPs)—including exchanges, stablecoin issuers, DeFi platforms, and NFT marketplaces [157]. The U.S. and the European Union (EU) have codified these into laws such as the *Bank Secrecy Act* and the *Fifth AML Directive* (5AMLD), mandating KYC, *Customer Due Diligence* (CDD), transaction monitoring, and reporting of suspicious behaviors like smurfing [290]. KYC obliges VASPs to verify identities and flag suspicious activity. U.S. enforcement bodies such as FinCEN and the SEC implement these rules, even citing market manipulation risks to reject Bitcoin ETF applications [157]. Consumer protection is also improving, with the EU's MiCA and the UK's FCA introducing safeguards, e.g., cooling-off periods for crypto purchases [229, 246].

Promoting public awareness. Crypto money laundering operates as a complex sociotechnical system that remains poorly understood by users [153]. Launderers exploit this knowledge gap through fake ICOs (§5.2.2.8), in-person crypto trades (§5.1.4), and gift card sales (§5.2.2.6), often targeting vulnerable groups such as students and the elderly [5, 6]. In response, governments, industry bodies, and academics have launched educational initiatives, including workshops and online awareness campaigns. Notable examples include programs led by the *Central Bank of Bahrain* (CBB), the *Global Blockchain Business Council* (GBBC) [315], and the *Australian Securities and Investments Commission* (ASIC) [11].

Blocklisting and sanctions. Blocklisting in cryptocurrencies involves identifying transactions linked to financial crimes and "tainting" the associated coins [157]. This is feasible in cryptocurrencies like Bitcoin, where each UTXO's publicly visible transaction history imparts a sense of uniqueness and non-fungibility. For example, the *U.S. Office of Foreign Assets Control* (OFAC) sanctioned Bitcoin addresses tied to Iranian ransomware operators in 2018 [287]. Two primary blocklisting mechanisms have been proposed [200, 157]: the *Poison* policy, which taints all coins in subsequent transactions involving a blocklisted account, and the *Haircut* policy, which limits tainting to the specific coins in the blocklisted transaction. Additionally, public "taint-lists" have been proposed to discourage engagement with tainted assets [312].

Deanonymization and legal prosecution. As noted in §4, launderers exploit the inherently pseudonymous nature of the Web3 ecosystem, which collectively embolden their use of cryptocurrencies as a primary medium for illicit financial activity [7, 63]. In response, government agencies and affiliated private organizations have invested in improving deanonymization techniques [75]. These efforts aim to unmask illicit actors, enabling subsequent legal investigation and prosecution. However, PETs such as mixers and privacy coins (§5.2.1) facilitate anonymity and financial secrecy, prompting technical [140, 307] and regulatory responses. Centralized mixers like *bestmixer.io* were dismantled by author-

ities, while decentralized ones, being non-custodial and jurisdiction-resistant, evade such actions [67]. Despite this, OFAC sanctioned the decentralized mixer *Tornado Cash* in 2022 for laundering $7B [202]. Privacy coins face similar scrutiny: Monero was delisted by Kraken across the *European Economic Area* (EEA) in 2024 [244], and will be further restricted under upcoming EU AML regulations—set to take effect by 2027— banning anonymous accounts linked to privacy coins [230].

Chapter 7

Open Challenges and Future Directions

Data accessibility. A key limitation of data-driven AML is the lack of large, reliably labeled datasets [290]. Despite curation, most labels remain approximate, degrading supervised model performance due to imbalance and limited coverage [181]. Absence of ground truth raises false positives in detection and blocklisting, risking collateral damage. Among the data types in §4, on-chain data—though public—is vast, noisy, and ever-growing. Off-chain data face compliance barriers, often lacking KYC records or imposing access restrictions [63]. Cross-chain traces inherit similar gaps or are entirely missing (e.g., DRT §5.1.4). Constructing transaction graphs entails fusing blockchain ledgers, smart contract logs, and proprietary VASP databases, complicating data correlation.

Future directions. (a) Develop semi-/self-supervised models to reduce label reliance; (b) promote benchmark datasets via joint labeling by regulators and VASPs; (c) design graph aggregation frameworks for unified, temporally-aligned, multi-source representations; (d) expand data labeling efforts, building on prior contributions such as [15, 198, 181].

Pseudonymity and decentralization. Lack of custodianship limits legal authority to freeze assets or block addresses, while pseudonymity impedes deanonymization and prosecution. PETs strengthen anonymity, and their decentralized, non-custodial design renders dismantling infeasible. For instance, in 2024, a U.S. federal appeals court overturned OFAC's sanctions on Tornado Cash, holding that its immutable, autonomous smart contracts are not sanctionable entities [216].

Future directions. (a) Promote blockchain infrastructures which are regulatory-compliant, such as *Ripple*—partnering with banks and payment providers to embed AML measures

and KYC protocols into Web3 [208]—and decentralized identity frameworks such as *Worldcoin* [305], *Ethereum Name Service* (ENS) [87] and *Polygon ID* [222], that support verifiable user and service authorization; (b) Develop legal/technical frameworks enabling accountable PET deployment and develop compliance-aware PETs with selective disclosure [296].

Regulatory arbitrage. The borderless nature of the crypto ecosystem undermines AML enforcement. VASPs based in lax regulatory environments can serve a global user base [63] and used to move assets across non-compliant jurisdictions.

Future directions. (a) Investigate cross-border enforcement mechanisms to mitigate fragmentation and propose incentive-aligned global AML standards for VASPs; (b) Smart contracts could embed logic to restrict access from addresses linked to sanctioned or non-compliant jurisdictions. This can be facilitated in dApps using *compliance oracles* that inject off-chain regulatory data (e.g., KYC status, sanctions lists, AML risk scores) into smart contracts (e.g., *Silent Data* [85]).

Legitimate privacy concerns. Deanonymization efforts further risk infringing the privacy of non-malicious users. PETs also safeguard legitimate interests—financial autonomy in authoritarian regimes, commercial confidentiality, etc. Their dual-use nature complicates regulation, as blanket bans risk infringing rights and deterring innovation.

Future directions. Privacy-preserving mechanisms such as ZKP-based compliance frameworks (e.g, Silent Data), and identity systems (e.g, Polygon ID) may enable verifiable, privacy-preserving identities and regulatory attestations, ensuring compliance while preserving user privacy.

Chapter 8

Conclusion

This survey aimed to address the absence of a systematized taxonomy of crypto money laundering schemes, by organizing existing and emerging strategies at an abstract level and examining their implementations across various mechanisms and infrastructures across the ecosystem. Earlier work tended to treat laundering as a flat list of tools, was often example-driven, and predated much of the Web3 economy, leaving no unified way to separate what a launderer tries to achieve from the means that achieve it. We set out to close that gap.

To do so, we built a two-dimensional taxonomy that separates six general *strategies*, the goals a launderer pursues, from the *mechanisms* that carry them out, and we mapped both onto the placement, layering, and integration stages and onto the on-chain, off-chain, and cross-chain traces they leave (§4). On the mechanism side, we drew a line between privacy-enhancing technologies, tools built to protect privacy, and ordinary Web3 infrastructures repurposed for secrecy (§5.2). For the former we set aside the overlapping labels the field relies on, such as *mixer* and *privacy coin*, and organized every tool instead by its deployment form and the cryptographic blueprints it combines (§5.2.1). For the latter we covered ten categories, among them channels that earlier surveys largely overlook, such as consensus participation, payment channel networks, cross-chain bridges, and crypto-backed cards. We then reviewed the countermeasures ranged against these schemes, from rule-based and data-driven detection to the commercial platforms most services now rely on, alongside preventive and regulatory measures (§6), and set our coverage against prior surveys to show what a unified account adds (Appendix A).

Several themes cut across this picture. Laundering is rarely the work of a single tool. Launderers chain strategies and mechanisms together across stages, as when staked value is wrapped, pledged as collateral, borrowed against, and staked again in a loop, or when a

crypto-backed card moves value between the on-chain and banking worlds. The center of gravity has also shifted, from the custodial mixers of the Bitcoin era toward laundering that is native to Web3, riding on composable DeFi protocols, movement across chains, and value-bearing tokens whose worth is easy to overlook. Running through all of it is the double-edged nature of a public ledger, whose transparency enables forensic reconstruction yet whose pseudonymity and privacy tooling are exactly what launderers exploit. Detection, in turn, has become an increasingly commercial and compliance-driven effort, carried out by analytics firms and monitoring platforms that most regulated services now integrate.

The taxonomy is meant to be operationally useful. Investigators can read from a scheme to the traces it is likely to leave and the stage it serves, builders of forensic tools can see where coverage is thin, particularly off-chain and across chains, and regulators can locate the gaps that laundering exploits, above all the uneven oversight between jurisdictions and services. The open problems that remain, from the scarcity of labeled data to the unresolved tension between privacy and accountability, are taken up in §7.

Despite these advances, launderers continue to adapt, casting a pressing need for scalable forensic tools and responsive policy frameworks to safeguard the integrity of the decentralized ecosystem.

References

[1] 21Shares and CoinGecko. The global crypto classification standard. https://assets.coingecko.com/reports/Research/The-Global-Crypto-Classification-Standard-21Shares-CoinGecko.pdf, 2023. Accessed: 2025-04-21.

[2] Aave. Aave — open source decentralized non-custodial liquidity protocol. https://aave.com/, 2026. Accessed: 2026-07-29.

[3] Hayden Adams, Noah Zinsmeister, Moody Salem, River Keefer, and Dan Robinson. Uniswap v3 core. https://uniswap.org/whitepaper-v3.pdf, 2021. Accessed: 2026-07-29.

[4] Bogdan Adamyk, Vladlena Benson, Oksana Adamyk, and Oksana Liashenko. Risk management in defi: Analyses of the innovative tools and platforms for tracking defi transactions. *Journal of Risk and Financial Management*, 18(1):38, 2025.

[5] Eray Arda Akartuna, Shane D Johnson, and Amy Thornton. Preventing the money laundering and terrorist financing risks of emerging technologies: An international policy delphi study. *Technological Forecasting and Social Change*, 179:121632, 2022.

[6] Hugo Almeida, Pedro Pinto, and Ana Fernández Vilas. A review on cryptocurrency transaction methods for money laundering. In *Proceedings of the 5th International Conference on Finance, Economics, Management and IT Business*, 2023.

[7] Nasser Alsalami and Bingsheng Zhang. Sok: A systematic study of anonymity in cryptocurrencies. In *Proceedings of the 3rd IEEE Conference on Dependable and Secure Computing*, pages 1–9, 2019.

[8] Anoma Foundation. Namada protocol specifications. Multi-Asset Shielded Pool (MASP) and IBC. https://specs.namada.net/. Accessed: 2026-07-25.

[9] Anonymous. BitLaundry announcement. https://bitcointalk.org/index.php?topic=963.0, 2011. Accessed: 2025-04-26.

[10] Alireza Arbabi, Ardeshir Shojaeinasab, Behnam Bahrak, and Homayoun Najjaran. Mixing solutions in bitcoin and ethereum ecosystems: A review and tutorial. *arXiv preprint arXiv:2310.04899*, 2023.

[11] ASIC. ASIC launches consumer awareness campaign – 'Don't get burnt by hype'. https://asic.gov.au/about-asic/news-centre/find-a-media-release/2023-releases/23-284mr-asic-launches-consumer-awareness-campaign-don-t-get-burnt-by-hype/, 2023. Accessed: 2025-05-14.

[12] Avenia. Avenia — borderless liquidity. https://avenia.io/, 2026. Accessed: 2026-07-17.

[13] Aztec Network. Aztec documentation: Privacy-first zkRollup. https://docs.aztec.network/. Accessed: 2026-07-25.

[14] Azteco. Azteco bitcoin vouchers. https://azte.co.

[15] Hyochang Baek, Junhyoung Oh, Chang Yeon Kim, and Kyungho Lee. A model for detecting cryptocurrency transactions with discernible purpose. In *Proceedings of the 11th International Conference on Ubiquitous and Future Networks*, pages 713–717, 2019.

[16] Ballet Global Inc. Secure your crypto with ballet cold storage wallet. https://www.ballet.com/, n.d. Accessed: 2025-05-18.

[17] Raffaella Barone and Donato Masciandaro. Cryptocurrency or usury? crime and alternative money laundering techniques. *European Journal of Law and Economics*, 47(101), 2019.

[18] Beam. BEAM: The scalable confidential cryptocurrency (position paper). https://docs.beam.mw/BEAM_Position_Paper_v0.2.2.pdf, 2018. Accessed: 2026-07-25.

[19] Beam. Lelantus-MW: Private transactions in Mimblewimble. https://docs.beam.mw/Lelantus-MW.pdf, 2019. Accessed: 2026-07-25.

[20] Chris Belcher. Design for a CoinSwap implementation for massively improving Bitcoin privacy and fungibility. Concept introduced by G. Maxwell (2013), 2020. https://gist.github.com/chris-belcher/9144bd57a91c194e332fb5ca371d0964. Accessed: 2026-07-25.

[21] Badr Bellaj, Aafaf Ouaddah, Emmanuel Bertin, Noel Crespi, and Abdellatif Mezrioui. Sok: A comprehensive survey on distributed ledger technologies. In *Proceedings of the 4th International Conference on Blockchain and Cryptocurrency*, pages 1–16, 2022.

[22] Binance. Bep-20 token standard. https://docs.bnbchain.org/smart-chain/developer/BEP20, 2024. Accessed: 2025-04-21.

[23] Binance. Binance smart chain documentation. https://docs.bnbchain.org/, 2024. Accessed: 2025-04-21.

[24] Binance. Binance card. https://www.binance.com/en/cards, 2026. Accessed: 2026-07-17.

[25] Binance Support. How to make an internal transfer to another binance account. https://www.binance.com/en/support/faq/detail/360037037312, 2020. Accessed: 2025-05-14.

[26] Bitcoin Optech. CoinSwap. Bitcoin Optech Topics. https://bitcoinops.org/en/topics/coinswap/. Accessed: 2026-07-25.

[27] Bitfinex Support. Internal transfer within bitfinex. https://support.bitfinex.com/hc/en-us/articles/900001925366-Internal-transfer-within-Bitfinex, 2025. Accessed: 2025-05-14.

[28] Bitnovo Global SL. Bitnovo – buy and sell cryptocurrencies easily. https://www.bitnovo.com/en/buy/cash/. Accessed: 2025-05-18.

[29] Bitquery. Blockchain api and crypto data products - bitquery. https://bitquery.io. Accessed: 2025-04-16.

[30] Bitrefill. Getting started - frequently asked questions. https://help.bitrefill.com/hc/en-us/categories/360002992880-Getting-Started, 2025. Accessed: 2025-04-27.

[31] Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll, and Edward W. Felten. Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In *Proceedings of the 36th IEEE Symposium on Security and Privacy*, pages 104–121, 2015.

[32] Joseph Bonneau, Arvind Narayanan, Andrew Miller, Jeremy Clark, Joshua A. Kroll, and Edward W. Felten. Mixcoin: Anonymity for Bitcoin with accountable mixes. In *Financial Cryptography and Data Security (FC 2014)*, volume 8437 of *LNCS*, pages 486–504. Springer, 2014.

[33] Bridge. Bridge — stablecoin infrastructure and apis for developers. https://bridge.xyz/, 2026. Accessed: 2026-07-17.

[34] Benedikt Bünz, Shashank Agrawal, Mahdi Zamani, and Dan Boneh. Zether: Towards privacy in a smart contract world. In *Financial Cryptography and Data Security (FC 2020)*. Springer, 2020. Cryptology ePrint Archive, Paper 2019/191. https://eprint.iacr.org/2019/191.

[35] Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Greg Maxwell. Bulletproofs: Short proofs for confidential transactions and more. In *Proceedings of the 39th IEEE Symposium on Security and Privacy*, pages 315–334, 2018.

[36] David Burkett. LIP-0002 and LIP-0003: MimbleWimble via extension blocks (MWEB). Litecoin Improvement Proposals, https://github.com/litecoin-project/lips, 2019. Accessed: 2026-07-15.

[37] Vitalik Buterin. A next-generation smart contract and decentralized application platform. https://cryptoverze.s3.us-east-2.amazonaws.com/wp-content/uploads/2018/11/10012235/Ethereum-ETH-whitepaper.pdf, 2014. Accessed: 2025-03-19.

[38] Vitalik Buterin, Jacob Illum, Matthias Nadler, Fabian Schär, and Ameen Soleimani. Blockchain privacy and regulatory compliance: Towards a practical equilibrium. *Blockchain: Research and Applications*, 5(1):100176, 2024.

[39] Vitalik Buterin, Yoav Weiss, Dror Tirosh, Shahaf Nacson, Alex Forshtat, Kristof Gazso, and Tjaden Hess. ERC-4337: Account abstraction using alt mempool. Ethereum Improvement Proposals, no. 4337, https://eips.ethereum.org/EIPS/eip-4337, 2021. Accessed: 2025-06-23.

[40] Bybit Help Center. How to withdraw assets via internal transfer. https://www.bybit.com/en/help-center/article/How-to-Withdraw-Assets-via-Internal-Transfer, 2024. Accessed: 2025-05-14.

[41] Mike Caldwell. Casascius physical bitcoins. https://www.casascius.com/.

[42] Malcolm Campbell-Verduyn. Bitcoin, crypto-coins, and global anti-money laundering governance. *Crime, Law and Social Change*, 69(2), 2018.

[43] Michele Caringella, Francesco Violante, Francesco De Lucci, Stefano Galantucci, Matteo Costantini, et al. Bach: A tool for analyzing blockchain transactions using address clustering heuristics. *Information*, 15(10):589, 2024.

[44] Stefan D Cassella. Toward a new model of money laundering: Is the "placement, layering, integration" model obsolete? *Journal of Money Laundering Control*, 21(4):494–497, 2018.

[45] CertiK. Kyc'd wallet sales on dark net markets. https://www.certik.com/resources/blog/3bUwDt2r8azcC7cqddl6rZ-kycd-wallet-sales-on-dark-net-markets, 2023. Accessed: 2026-07-24.

[46] Chainalysis. The 2022 crypto crime report. https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf, 2022. Accessed: 2025-04-28.

[47] Chainalysis. Money laundering and cryptocurrency: Trends and new techniques for detection and investigation. https://airant.org/wp-content/uploads/2024/07/Report_-Money_laundering_and_Cryptocurrency.pdf, 2024. Accessed: 2025-04-23.

[48] Chainalysis. Chainalysis – blockchain data platform. https://www.chainalysis.com/, 2025. Accessed: 2025-04-14.

[49] Chainalysis. What is a centralized exchange (cex)? https://www.chainalysis.com/glossary/centralized-exchange/, 2025. Accessed: 2026-07-29.

[50] Tao-Hung Chang and Davor Svetinovic. Improving bitcoin ownership identification using transaction patterns analysis. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 50(1):9–20, 2018.

[51] Zhiyuan Chen, Le Dinh Van Khoa, Ee Na Teoh, Amril Nazir, Ettikan Kandasamy Karuppiah, and Kim Sim Lam. Machine learning techniques for anti-money laundering (aml) solutions in suspicious transaction detection: A review. *Knowledge and Information Systems*, 57:245–285, 2018.

[52] Raymond Cheng, Fan Zhang, Jernej Kos, Warren He, Nicholas Hynes, Noah Johnson, Ari Juels, Andrew Miller, and Dawn Song. Ekiden: A platform for confidentiality-preserving, trustworthy, and performant smart contract execution. In *Proceedings of the 4th IEEE European Symposium on Security and Privacy*, pages 185–200. IEEE, 2019.

[53] CipherTrace. Ciphertrace - blockchain forensics team. https://cryptoslate.com/companies/ciphertrace/, 2025. Accessed: 2025-04-14.

[54] Circle. Usdc — regulated stablecoin for global opportunities. https://www.circle.com/usdc. Accessed: 2025-05-14.

[55] Coinbase. What are real world assets (rwa)? https://www.coinbase.com/en-ca/learn/crypto-glossary/what-are-real-world-assets-rwa, 2024. Accessed: 2025-04-21.

[56] Coinbase. What is a crypto dusting attack, and how to avoid it? https://www.coinbase.com/en-ca/learn/tips-and-tutorials/what-is-crypto-dusting-attack-and-how-to-avoid-it, 2025. Accessed: 2025-04-23.

[57] Coinbase Help. Withdrawing crypto assets. https://help.coinbase.com/en/prime/trading-and-funding/withdrawing-crypto-assets, 2025. Accessed: 2025-05-14.

[58] Coingecko. Global cryptocurrency market cap charts. https://www.coingecko.com/en/global-charts, 2025. Accessed: 2025-07-17.

[59] CoinMarketCap Academy. Tumbler. https://coinmarketcap.com/academy/glossary/tumbler, 2021. Accessed: 2025-04-26.

[60] CommerceBlock. Mercury CoinSwaps. https://medium.com/@commerceblock/mercury-coinswaps-a8df6637bed8, 2021. Blinded statecoin swaps via a conductor. Accessed: 2026-07-25.

[61] Ontario Securities Commission. Crypto-asset survey 2023. https://www.osc.ca/sites/default/files/2023-12/inv-research_20231129_crypto-asset-survey-2023.pdf, 2023. Accessed: 2025-04-27.

[62] Commodity Futures Trading Commission (CFTC). Cftc orders event-based binary options markets operator to pay $1.4 million penalty. Release Number 8478-22. https://www.cftc.gov/PressRoom/PressReleases/8478-22, 2022. Accessed: 2026-07-17.

[63] Alexandra D. Comolli and Michele R. Korver. Surfing the first wave of cryptocurrency money laundering. *Department of Justice Journal of Federal Law and Practice*, 69(3), 2021.

[64] ComplyAdvantage. Complyadvantage — ai-native financial crime detection platform. https://complyadvantage.com/, 2026. Accessed: 2026-07-29.

[65] Nicolas T Courtois and Rebekah Mercer. Stealth address and key management techniques in blockchain systems. In *Proceedings of the 3rd International Conference on Information Systems Security and Privacy*, pages 559–566, 2017.

[66] Simon Cousaert, Jiahua Xu, and Toshiko Matsui. Sok: Yield aggregators in defi. In *Proceedings of the 4th IEEE International Conference on Blockchain and Cryptocurrency*, 2022.

[67] Jesse Crawford and Yong Guan. Knowing your bitcoin customer: Money laundering in the bitcoin economy. In *Proceedings of the 13th International Conference on Systematic Approaches to Digital Forensic Engineering*, pages 38–45, 2020.

[68] CryptoVoucher.io. Cryptovoucher - buy crypto instantly. https://cryptovoucher.io/.

[69] Morten Dahl, Clément Danjou, Daniel Demmler, Tore Frederiksen, Petar Ivanov, Marc Joye, Dragos Rotaru, Nigel Smart, and Louis Tremblay Thibault. fhEVM: Confidential EVM smart contracts using fully homomorphic encryption, version 1.0.2. Zama, 2023. https://github.com/zama-ai/fhevm. Accessed: 2026-07-25.

[70] Dash Core Group. Dash: Digital cash. https://www.dash.org/. Accessed: 2025-04-25.

[71] Decentraland Foundation. Decentraland white paper 2.0. https://decentraland.org/whitepaper2.pdf, November 2024. Accessed: 2025-04-13.

[72] DeFiLlama. Defillama - defi dashboard. https://defillama.com/, 2025. Accessed: 2025-07-17.

[73] Angelos Delivorias. Understanding initial coin offerings: A new means of raising funds based on blockchain. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)696167, 2021.

[74] Denarium. Denarium bitcoin - physical bitcoin coins. https://denarium.com/.

[75] Dominic Deuber, Viktoria Ronge, and Christian Rückert. Sok: Assumptions underlying cryptocurrency deanonymizations. *Proceedings on Privacy Enhancing Technologies*, 2022.

[76] Johnny Dilley, Andrew Poelstra, Jonathan Wilkins, Marta Piekarska, Ben Gorlick, and Mark Friedenbach. Strong federations: An interoperable blockchain solution

to centralized third-party risks. arXiv:1612.05491, 2016. https://arxiv.org/abs/1612.05491.

[77] Roger Dingledine, Nick Mathewson, Paul F Syverson, and Others. Tor: The second-generation onion router. In *Proceedings of the 13th USENIX Security Symposium*, pages 303–320, 2004.

[78] Dundle. Buy bitnovo voucher online — instant delivery. https://dundle.com/nl/en/bitnovo/. Accessed: 2025-05-18.

[79] Stefan Dziembowski, Lisa Eckey, Sebastian Faust, and Daniel Malinowski. Perun: Virtual payment hubs over cryptocurrencies. In *Proceedings of the 40th IEEE Symposium on Security and Privacy*, pages 106–123. IEEE, 2019.

[80] Gilad Edelman. The father of web3 wants you to trust less. https://www.wired.com/story/web3-gavin-wood-interview/, 2021. Accessed: 2025-03-19.

[81] EigenLayer Team. EigenLayer: The restaking collective. https://docs.eigencloud.xyz/eigenlayer/concepts/whitepaper, 2023. Accessed: 2026-07-29.

[82] Elliptic. How iran uses bitcoin mining to evade sanctions. https://www.elliptic.co/blog/how-iran-uses-bitcoin-mining-to-evade-sanctions, 2021. Accessed: 2026-07-29.

[83] Elliptic. Elliptic – blockchain analytics and crypto compliance solutions. https://www.elliptic.co/, 2025. Accessed: 2025-04-14.

[84] Youssef Elmougy and Ling Liu. Demystifying fraudulent transactions and illicit nodes in the bitcoin network for financial forensics. In *Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining*, pages 3979–3990, 2023.

[85] Noam Elstein. Automating aml checks for token holders in smart contracts. https://www.silentdata.com/blog/automating-aml-checks-for-all-token-holders-in-smart-contracts, April 2025. Accessed:Accessed: 2025-05-25.

[86] William Entriken, Dieter Shirley, Jacob Evans, and Nastassia Sachs. Erc-721 non-fungible token standard. https://github.com/ethereum/ERCs/blob/master/ERCS/erc-721.md, 2018. Accessed: 2025-04-27.

[87] Ethereum Name Service. Ethereum Name Service (ENS). https://ens.domains/, 2025. Accessed: Accessed: 2025-05-25.

[88] ether.fi. eeth. https://etherfi.gitbook.io/etherfi/staking/eeth, 2024. Accessed: 2025-06-23.

[89] ether.fi. WithdrawRequestNFT: ether.fi protocol smart contract. https://github.com/etherfi-protocol/smart-contracts/blob/master/src/withdrawals/WithdrawRequestNFT.sol, 2025. Accessed: 2026-07-29.

[90] ether.fi. ether.fi — stake, earn, spend. do more with your crypto. https://www.ether.fi/, 2026. Accessed: 2026-07-17.

[91] ether.fi. Fedwire and ach transfers (usd) — ether.fi help center. https://help.ether.fi/en/articles/584583-fedwire-and-ach-transfers-usd, 2026. Accessed: 2026-07-17.

[92] ether.fi. Fund your vault via swift (usd) — ether.fi help center. https://help.ether.fi/en/articles/586159-fund-your-vault-via-swift-usd, 2026. Accessed: 2026-07-17.

[93] ether.fi. How liquid works — ether.fi help center. https://help.ether.fi/en/articles/517109-how-liquid-works, 2026. Accessed: 2026-07-29.

[94] ether.fi. Liquid — automated DeFi yield vaults. https://www.ether.fi/liquid, 2026. Accessed: 2026-07-29.

[95] ether.fi. Managing your card and vault limits — ether.fi help center. https://help.ether.fi/en/articles/330661-managing-your-card-and-vault-limits, 2026. Accessed: 2026-07-17.

[96] ether.fi. Pix transfers (brl) — ether.fi help center. https://help.ether.fi/en/articles/449829-pix-transfers-brl, 2026. Accessed: 2026-07-17.

[97] ether.fi. Sepa bank transfers (eur) — ether.fi help center. https://help.ether.fi/en/articles/586168-sepa-bank-transfers-eur, 2026. Accessed: 2026-07-17.

[98] Etherscan. Etherscan: Ethereum blockchain explorer. https://etherscan.io. Accessed: 2025-04-16.

[99] Europol. *Internet Organised Crime Threat Assessment (IOCTA 2017\)*. European Union Agency for Law Enforcement Cooperation (Europol), 2017.

[100] Europol. Multi-million euro cryptocurrency laundering service Bestmixer.io taken down. Europol Newsroom, 2019. https://www.europol.europa.eu/media-press/newsroom/news/multi-million-euro-cryptocurrency-laundering-service-bestmixerio-taken-down. Accessed: 2026-07-25.

[101] EY. EY upgrades Nightfall, a zero-knowledge roll-up enabling private transactions on the Ethereum blockchain. https://web.archive.org/web/20260728200952/https://www.ey.com/en_gl/newsroom/2025/04/ey-upgrades-nightfall-a-zero-knowledge-roll-up-enabling-private-transactions-on-the-ethereum-blockchain, 2025. Archived 2026-07-28; original at https://www.ey.com/en_gl/newsroom/2025/04/ey-upgrades-nightfall-a-zero-knowledge-roll-up-enabling-private-transactions-on-the-ethereum-blockchain.

[102] EY Blockchain. nightfall_3: An optimistic version of Nightfall. Polygon Nightfall, 2022. https://github.com/EYBlockchain/nightfall_3. Accessed: 2026-07-25.

[103] Steven Farrugia, Joshua Ellul, and George Azzopardi. Detection of illicit accounts over the ethereum blockchain. *Expert Systems with Applications*, 150:113318, 2020.

[104] Ádám Ficsór, Yuval Kogman, Lucas Ontivero, and István András Seres. WabiSabi: Centrally coordinated CoinJoins with variable amounts. Cryptology ePrint Archive, Paper 2021/206, 2021. https://eprint.iacr.org/2021/206.

[105] Ádám Ficsór and TDevD. ZeroLink: The Bitcoin fungibility framework. https://github.com/nopara73/ZeroLink, 2017. Specification underlying Samourai Whirlpool. Accessed: 2026-07-25.

[106] Uriel Fiege, Amos Fiat, and Adi Shamir. Zero knowledge proofs of identity. In *Proceedings of the 19th Annual ACM Symposium on Theory of Computing*, pages 210–217, 1987.

[107] Financial Action Task Force (FATF) and Asia/Pacific Group on Money Laundering (APG). Vulnerabilities of casinos and gaming sector. https://home.treasury.gov/system/files/246/vulnerabilities-casinos-gaming-sector-032009.pdf, 2009. Accessed: 2026-07-17.

[108] Financial Crime Academy. Money laundering in the art market. https://financialcrimeacademy.org/money-laundering-in-the-art-market/, 2023. Accessed: 2025-04-25.

[109] Financial Crimes Enforcement Network (FinCEN). Application of FinCEN's regulations to certain business models involving convertible virtual currencies. Guidance FIN-2019-G001, https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-certain-business-models, 2019. Accessed: 2026-07-15.

[110] Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). Special bulletin on laundering the proceeds of crime through online gambling sites. https://fintrac-canafe.canada.ca/intel/bulletins/gambling-jeu-eng, 2024. Accessed: 2025-04-27.

[111] FINRA. Crypto assets. https://www.finra.org/investors/investing/investment-products/crypto-assets, 2024. Accessed: 2025-04-21.

[112] Zachary Folk. Peter thiel invests in polymarket political betting platform—but the future of gambling on elections remains unclear. Forbes. https://www.forbes.com/sites/zacharyfolk/2024/05/14/peter-thiel-invests-in-polymarket-political-betting-platform-but-the-future-of-gambling-on-elections-remains-unclear/, 2024. Accessed: 2026-07-17.

[113] Financial Action Task Force. Money laundering and terrorist financing in the art and antiquities market, 2023.

[114] Ethereum Foundation. Erc-20 token standard. https://ethereum.org/en/developers/docs/standards/tokens/erc-20/, 2015. Accessed: 2025-04-21.

[115] Wormhole Foundation. Wormhole – a cross-chain messaging protocol. https://wormhole.com, 2023. Accessed: 2025-04-18.

[116] Georg Fuchsbauer, Michele Orrù, and Yannick Seurin. Aggregate cash systems: A cryptographic investigation of mimblewimble. In *Advances in Cryptology – EUROCRYPT 2019*, 2019.

[117] Romina Gabbiadini, Lorenzo Gobbi, and Eugenio Rubera. Money laundering and blockchain technology: Can you follow the trail of cryptocurrency transactions? Technical Report 893, Bank of Italy, 2024.

[118] Leonid Garin and Vladimir Gisin. Machine learning in classifying bitcoin addresses. *The Journal of Finance and Data Science*, 9(1):100109, 2023.

[119] Vahid Garousi, Michael Felderer, and Mika V. Mäntylä. Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. *Information and Software Technology*, 106:101–121, 2019.

[120] Rosario Gennaro and Steven Goldfeder. Fast multiparty threshold ECDSA with fast trustless setup. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 1179–1194, 2018.

[121] Craig Gentry. Fully homomorphic encryption using ideal lattices. In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing*, pages 169–178, 2009.

[122] Paul Gilmour, Brian Omondi, Hatice Feyza Alkaç, Bing Han, Abigail Carre, Dina Kapardis, and Ceri Halfpenny. *Reexamining the 'Placement-Layering-Integration' Model of Money Laundering*. The Institute of Money Laundering Prevention Officers, September 2024.

[123] Noemi Glaeser, Matteo Maffei, Giulio Malavolta, Pedro Moreno-Sanchez, Erkan Tairi, and Sri Aravinda Krishnan Thyagarajan. Foundations of coin mixing services. In *Proceedings of the 29th ACM SIGSAC Conference on Computer and Communications Security*, pages 1259–1273, 2022.

[124] Gnosis Pay. Gnosis pay — card programs. https://gnosispay.com/, 2026. Accessed: 2026-07-17.

[125] Krzysztof Gogol, Yaron Velner, Benjamin Kraner, and Claudio Tessone. SoK: Liquid staking tokens (LSTs) and emerging trends in restaking. https://arxiv.org/abs/2404.00644, 2024. arXiv:2404.00644.

[126] S Goldwasser, S Micali, and C Rackoff. The knowledge complexity of interactive proof-systems. In *Proceedings of the 17th Annual ACM Symposium on Theory of Computing*, pages 291–304, 1985.

[127] Andy Greenberg. Feds arrest an alleged $336m bitcoin-laundering kingpin. https://www.wired.com/story/bitcoin-fog-dark-web-cryptocurrency-arrest, 2021. Accessed: 2025-04-26. Subscription required.

[128] Grin Developers. Introduction to MimbleWimble and Grin. https://github.com/mimblewimble/grin/blob/master/doc/intro.md. Accessed: 2026-07-25.

[129] Reuben Grinberg. Bitcoin: An innovative alternative digital currency. *Hastings Science & Technology Law Journal*, 4:159, 2012.

[130] Blockchain Intelligence Group. Law enforcement resource guide for cryptocurrency investigations. https://blockchaingroup.io/wp-content/uploads/2025/02/Law-Enforcement-Resource-Guide-for-Cryptocurrency-Investigations-.pdf, 2025. Accessed: 2025-04-17.

[131] Zhuoming Gu, Dan Lin, and Jiajing Wu. On-chain analysis-based detection of abnormal transaction amount on cryptocurrency exchanges. *Physica A: Statistical Mechanics and Its Applications*, 604:127799, 2022.

[132] Lewis Gudgeon, Pedro Moreno-Sanchez, Stefanie Roos, Patrick McCorry, and Arthur Gervais. Sok: Off the chain transactions. *IACR Cryptol. ePrint Arch.*, 2019:360, 2019.

[133] Lewis Gudgeon, Sam Werner, Daniel Perez, and William J Knottenbelt. Defi protocols for loanable funds: Interest rates, liquidity and market efficiency. In *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*, pages 92–112, 2020.

[134] Matthias Hafner, Marco Henriques Pereira, Helmut Dietl, and Juan Beccuti. The four types of stablecoins: A comparative analysis. *arXiv preprint arXiv:2308.07041*, 2023.

[135] Badis Hammi, Sherali Zeadally, and Alfredo J Perez. Non-fungible tokens: a review. *IEEE Internet of Things Magazine*, 6(1):46–50, 2023.

[136] Christopher G Harris. Cross-chain technologies: Challenges and opportunities for blockchain interoperability. In *Proceedings of the IEEE International Conference on Omni-layer Intelligent Systems*, pages 1–6, 2023.

[137] Dani Haston. Cryptoasset realization: How cryptocurrencies are frozen, seized, and forfeited. https://www.chainalysis.com/blog/cryptoasset-realization-explained/, 2022. Accessed: 2025-04-17.

[138] Ethan Heilman, Leen Alshenibr, Foteini Baldimtsi, Alessandra Scafuro, and Sharon Goldberg. Tumblebit: An untrusted bitcoin-compatible anonymous payment hub. In *Proceedings of the 24th Network and Distributed System Security Symposium*, pages 17–30, 2017.

[139] Maurice Herlihy. Atomic cross-chain swaps. In *Proceedings of the 37th ACM Symposium on Principles of Distributed Computing*, pages 245–254, 2018.

[140] Younggee Hong, Hyunsoo Kwon, Sangtae Lee, and Junbeom Hur. Poster: De-mixing bitcoin mixing services, 2018.

[141] Sabine Houy, Philipp Schmid, and Alexandre Bartel. Security aspects of cryptocurrency wallets—a systematic literature review. *ACM Computing Surveys*, 56(1):1–31, 2023.

[142] Elizabeth Howcroft. Crypto's biggest hacks and heists after $1.5 billion theft from bybit. *Reuters*, 2025. Accessed: 2025-03-19.

[143] Xiaohui Hu, Hang Feng, Pengcheng Xia, Gareth Tyson, Lei Wu, Yajin Zhou, and Haoyu Wang. Piecing together the jigsaw puzzle of transactions on heterogeneous blockchain networks. *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, 8(3):1–27, 2024.

[144] Hyperliquid. Hyperliquid documentation. https://hyperliquid.gitbook.io/hyperliquid-docs, 2025. Accessed: 2026-07-29.

[145] Ripple Labs Inc. Xrp ledger. https://xrpl.org/. Accessed: April 21, 2025.

[146] Inco. Introducing inco: The modular confidential computing network. https://www.inco.org/blog/introducing-inco-the-modular-confidential-computing-network, 2023. Accessed: 2026-07-25.

[147] Inco. Inco lightning: Confidential smart contract library for blockchains. https://web.archive.org/web/20260728194106/https://www.inco.org/lightning, 2025. Archived 2026-07-28; original at https://www.inco.org/lightning.

[148] Incognito Team. Incognito mode for cryptonetworks. Incognito Whitepaper (archived), 2019. http://web.archive.org/web/20230209100429/https://we.incognito.org/t/incognito-whitepaper-incognito-mode-for-cryptonetworks/168. Accessed: 2026-07-25.

[149] Iron Fish. Iron fish whitepaper. https://ironfish.network/learn/whitepaper, 2021. Accessed: 2026-07-25.

[150] Aram Jivanyan. Lelantus: A new design for anonymous and confidential cryptocurrencies. Cryptology ePrint Archive, Paper 2019/373, 2019. https://eprint.iacr.org/2019/373.

[151] JoinMarket-Org. JoinMarket: CoinJoin that people will actually use. https://github.com/JoinMarket-Org/joinmarket-clientserver. Accessed: 2026-07-25.

[152] KAST. Kast — the global money app powered by stablecoins. https://www.kast.xyz/, 2026. Accessed: 2026-07-17.

[153] Vinay Kumar Kasula. *Awareness of Cryptocurrency Scams*. PhD thesis, University of the Cumberlands, 2024.

[154] Fiona Kelliher. Cyberscammers are bypassing banks' security with illicit tools sold on telegram. https://www.technologyreview.com/2026/04/15/1135898/cyberscammers-bypassing-bank-telegram/, 2026. MIT Technology Review. Accessed: 2026-07-24.

[155] Barbara Kitchenham and Stuart Charters. Guidelines for performing systematic literature reviews in software engineering. EBSE Technical Report EBSE-2007-01, Keele University and Durham University, 2007.

[156] Lars Klöhn, Nicolas Parhofer, and Daniel Resas. Initial coin offerings (icos): Economics and regulation. https://ssrn.com/abstract=3290882, 2018.

[157] Kartick Kolachala, Ecem Simsek, Mohammed Ababneh, and Roopa Vishwanathan. Sok: Money laundering in cryptocurrencies. In *Proceedings of the 16th International Conference on Availability, Reliability and Security*, pages 1–10, 2021.

[158] Chaitanya Konda, Michael Connor, Duncan Westland, Quentin Drouot, and Paul Brody. Nightfall. EY Global Blockchain R&D, 2019. https://github.com/EYBlockchain/nightfall. Accessed: 2026-07-25.

[159] Kraken. Privacy notice. https://www.kraken.com/legal/privacy, 2025. Accessed: 2025-04-17.

[160] KuCoin. Kucoin p2p fiat trade and otc platform. https://www.kucoin.com/otc/buy/USDT-USD, 2024. Accessed: 2025-05-04.

[161] KuCoin. Kucard — crypto debit card, pay with crypto anywhere. https://www.kucoin.com/kucard, 2026. Accessed: 2026-07-17.

[162] KuCoin Support. How to transfer between internal accounts on kucoin. https://www.kucoin.com/support/900006083046, 2021. Accessed: 2025-05-14.

[163] Yujin Kwon, Hyoungshick Kim, Yung Yi, and Yongdae Kim. An eye for an eye: Economics of retaliation in mining pools. In *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*, pages 169–182, 2019.

[164] Yujin Kwon, Kornrapat Pongmala, Kaihua Qin, Ariah Klages-Mundt, Philipp Jovanovic, Christine Parlour, Arthur Gervais, and Dawn Song. What drives the (in) stability of a stablecoin? *arXiv preprint arXiv:2307.11754*, 2023.

[165] LayerZero Labs. Layerzero – an omnichain interoperability protocol. https://layerzero.network, 2023. Accessed: 2025-04-18.

[166] Solana Labs. Solana documentation. https://docs.solana.com/, 2024. Accessed: 2025-04-21.

[167] TRM Labs. Illicit activity involving crypto atms is double that of overall crypto industry. https://www.trmlabs.com/post/illicit-activity-involving-crypto-atms-is-double-that-of-overall-crypto-industry, 2024. Accessed: 2025-04-27.

[168] Isys Lam and Andrew Dornbierer. Money laundering through the gambling industry. Basel Institute on Governance, Quick Guide 28. https://baselgovernance.org/sites/default/files/2022-09/QG28%20gambling.pdf, 2022. Accessed: 2026-07-17.

[169] Sung-Shine Lee, Alexandr Murashkin, Martin Derka, and Jan Gorzny. Sok: Not quite water under the bridge: Review of cross-chain bridge hacks. In *Proceedings of the 5th IEEE International Conference on Blockchain and Cryptocurrency*, pages 1–14, 2023.

[170] Legal Information Institute. Commingling. https://www.law.cornell.edu/wex/commingling, n.d. Accessed: 2025-04-24.

[171] Michelle Legge. Rug pulls: Your complete guide. https://koinly.io/blog/crypto-rug-pulls-guide/, 2024. Accessed: 2025-05-18.

[172] Rujia Li, Qin Wang, Qi Wang, David Galindo, and Mark Ryan. SoK: Tee-assisted confidential smart contract. *arXiv preprint arXiv:2203.08548*, 2022.

[173] Shujun Li. Shujun li's online bibliography of sok (systematization of knowledge) papers. https://www.hooklee.com/Research/SoK/SoK.html, 2024. Accessed: 2024-12-05.

[174] Lido. steth: The mechanics of steth. https://blog.lido.fi/steth-the-mechanics-of-steth/, 2021. Accessed: 2025-05-22.

[175] Wanseob Lim and barryWhiteHat. Zkopru (zk optimistic rollup) for private transactions. Ethereum Research, 2020. https://ethresear.ch/t/zkopru-zk-optimistic-rollup-for-private-transactions/7717. Accessed: 2026-07-25.

[176] Dan Lin, Jiajing Wu, Qishuang Fu, Yunmei Yu, Kaixin Lin, Zibin Zheng, and Shuo Yang. Towards understanding crypto money laundering in web3 through the lenses of ethereum heists. *arXiv preprint arXiv:2305.14748*, 2023.

[177] Dan Lin, Jiajing Wu, Yunmei Yu, Qishuang Fu, Zibin Zheng, and Changlin Yang. Denseflow: Spotting cryptocurrency money laundering in ethereum transaction graphs. In *Proceedings of the 33rd ACM Web Conference*, pages 4429–4438, 2024.

[178] Yu-Jing Lin, Po-Wei Wu, Cheng-Han Hsu, I-Ping Tu, and Shih-Wei Liao. An evaluation of bitcoin address classification based on transaction history summarization. In *Proceedings of the 1st IEEE International Conference on Blockchain and Cryptocurrency*, pages 302–310, 2019.

[179] Jiayi Liu, Changchun Yin, Hao Wang, Xiaofei Wu, Dongwan Lan, Lu Zhou, and Chunpeng Ge. Graph embedding-based money laundering detection for ethereum. *Electronics*, 12(14):3180, 2023.

[180] Xu Long, Yishun Wang, and Xiaoqi Li. From fomo3d to lottery DApp: Analysis of Ethereum-based gambling applications. arXiv preprint arXiv:2508.12303, 2025. Accessed: 2026-07-17.

[181] Joana Lorenz, Maria Inês Silva, David Aparício, João Tiago Ascensão, and Pedro Bizarro. Machine learning methods to detect money laundering in the bitcoin blockchain in the presence of label scarcity. In *Proceedings of the 1st ACM International Conference on AI in Finance*, pages 1–8, 2020.

[182] MakerDAO. Makerdao — an unbiased global financial system. https://makerdao.com/en/. Accessed: 2025-05-14.

[183] Giulio Malavolta, Pedro Moreno-Sanchez, Clara Schneidewind, Aniket Kate, and Matteo Maffei. Anonymous multi-hop locks for blockchain scalability and interoperability. *Cryptology ePrint Archive*, 2018.

[184] Mandiant. Apt43: North korean group uses cybercrime to fund espionage operations. https://www.mandiant.com/resources/blog/apt43-north-korea-cybercrime-espionage, 2023. Accessed: 2025-04-28.

[185] Mandiant. Mandiant: Cybersecurity services and threat intelligence. https://www.mandiant.com/, 2025. Accessed: 2025-04-28.

[186] Mastercard. Crypto card program by mastercard for enabling everyday purchases. https://www.mastercard.com/global/en/business/issuers/crypto/card-program.html, n.d. Accessed: 2025-05-18.

[187] Gregory Maxwell. Coinjoin: Bitcoin privacy for the real world. https://bitcointalk.org/index.php?topic=279249.msg2983902#msg2983902, 2013. Accessed: 2025-05-28.

[188] Sarah Meiklejohn and Rebekah Mercer. Möbius: Trustless tumbling for transaction privacy. *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2018(2):105–121, 2018. Cryptology ePrint Archive, Paper 2017/881. https://eprint.iacr.org/2017/881.

[189] Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M Voelker, and Stefan Savage. A fistful of bitcoins: Characterizing payments among men with no names. In *Proceedings of the 13th Internet Measurement Conference*, pages 127–140, 2013.

[190] Amin Mekacher, Alberto Bracci, Matthieu Nadini, Mauro Martino, Laura Alessandretti, Luca Maria Aiello, and Andrea Baronchelli. Heterogeneous rarity patterns drive price dynamics in nft collections. *Scientific reports*, 12(1):13890, 2022.

[191] Merkle Science. Ai-powered blockchain analytics & predictive risk platform. https://www.merklescience.com. Accessed: 2025-04-16.

[192] Merkle Science. Exploring the nuances of address poisoning. https://www.merklescience.com/blog/exploring-the-nuances-of-address-poisoning. Accessed: 2025-05-08.

[193] Merkle Science. Chain hopping: The future of crypto money laundering. https://www.merklescience.com/blog/chain-hopping-the-future-of-crypto-money-laundering, 2022. Accessed: 2025-04-18.

[194] MEXC. Mexc partners with ether.fi to expand ecosystem utility with a co-branded card. https://blog.mexc.com/mexc-partners-with-ether-fi-with-a-co-branded-card/, 2026. Accessed: 2026-07-17.

[195] Ian Miers, Christina Garman, Matthew Green, and Aviel D. Rubin. Zerocoin: Anonymous distributed e-cash from Bitcoin. In *2013 IEEE Symposium on Security and Privacy*, pages 397–411. IEEE, 2013.

[196] Hossein Mohit and Vess L. Johnson. Coin or token: Different motivations for investing in cryptocurrency. https://aisel.aisnet.org/treos_amcis2022/33, 2022. Accessed: 2025-05-14. AMCIS 2022 TREOs, Entry 33.

[197] Amani Moin, Kevin Sekniqi, and Emin Gun Sirer. Sok: A classification framework for stablecoin designs. In *Proceedings of the 24th International Conference on Financial Cryptography and Data Security*, pages 174–197, 2020.

[198] Patrick M Monamo, Vukosi Marivate, and Bhesipho Twala. A multifaceted approach to bitcoin fraud detection: Global and local outliers. In *Proceedings of the 15th IEEE International Conference on Machine Learning and Applications*, pages 188–194, 2016.

[199] Annelieke Mooij. *Regulating the Metaverse Economy: How to Prevent Money Laundering and the Financing of Terrorism*. Springer Nature, 2024.

[200] Malte Möser and Arvind Narayanan. Effective cryptocurrency regulation through blacklisting. https://maltemoeser.de/paper/blacklisting-regulation.pdf, 2019.

[201] Ajmal Muhammad and Jesper Kristensen. On cross-chain pathfinding and bridge selection for decentralized finance. https://www.researchgate.net/publication/374950963_On_Cross-chain_Pathfinding_and_Bridge_Selection_for_Decentralized_Finance, 2024. Accessed: 2025-03-19.

[202] Thomas Mulligan. A new u.s. crackdown has crypto users worried about their privacy. https://time.com/6205143/tornado-cash-us-crypto-ban/, 2022. Accessed: 2025-05-24.

[203] Multichain. Multichain – the ultimate router for web3. https://multichain.org, 2023. Accessed: 2025-04-18.

[204] Malte Möser, Rainer Böhme, and Dominic Breuker. An inquiry into money laundering tools in the bitcoin ecosystem. In *Proceedings of the 10th Anti-Phishing Working Group eCrime Researchers Summit*, pages 1–14, 2013.

[205] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Self-published white paper*, 2008. Accessed: 2025-03-19.

[206] Axelar Network. Axelar – secure cross-chain communication. https://axelar.network, 2023. Accessed: 2025-04-18.

[207] Raiden Network. Raiden network. https://raiden.network/, 2025. Accessed: 2025-07-26.

[208] Todayq News. Ripple unveils advanced aml monitoring for regulatory compliance. https://www.binance.com/en-IN/square/post/14684867993666, October 2024. Accessed: 2025-05-26.

[209] Franklin Noll. The controversial business of cash-to-crypto bitcoin atms. *Payments System Research Briefing*, 2023.

[210] Oasis Protocol Foundation. Sapphire ParaTime: Confidential EVM. https://docs.oasis.io/build/sapphire/. Accessed: 2026-07-25.

[211] U.S. Department of the Treasury. Money laundering. https://home.treasury.gov/policy-issues/terrorism-and-illicit-finance/money-laundering, 2024. Accessed: 2025-03-19.

[212] Wei Ou, Shiying Huang, Jingjing Zheng, Qionglu Zhang, Guang Zeng, and Wenbao Han. An overview on cross-chain: Mechanism, platforms, challenges and advances. *Computer Networks*, 218:109378, 2022.

[213] Wizard Of Ozzie. Reuse of addresses by a service ("get new address" returning funded addresses). https://bitcoin.stackexchange.com/questions/36907/reuse-of-addresses-by-a-service-get-new-address-returning-funded-addresses, 2015. Accessed: 2025-05-14.

[214] Matthew J. Page, Joanne E. McKenzie, Patrick M. Bossuyt, Isabelle Boutron, Tammy C. Hoffmann, Cynthia D. Mulrow, Larissa Shamseer, Jennifer M. Tetzlaff, Elie A. Akl, Sue E. Brennan, Roger Chou, Julie Glanville, Jeremy M. Grimshaw, Asbjørn Hróbjartsson, Manoj M. Lalu, Tianjing Li, Elizabeth W. Loder, Evan Mayo-Wilson, Steve McDonald, Luke A. McGuinness, Lesley A. Stewart, James Thomas, Andrea C. Tricco, Vivian A. Welch, Penny Whiting, and David Moher. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ*, 372:n71, 2021.

[215] Marek Palatinus, Pavol Rusnak, Aaron Voisine, and Sean Bowe. Bip 0039: Mnemonic code for generating deterministic keys. https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki, 2013. Accessed: 2025-04-21.

[216] Gina M Parlovecchio, Justin Herring, Tamer A Soliman, Adam S Hickey, Joseph A Castelluccio, and Brendan J Harrington. Federal appeals court tosses ofac sanctions on tornado cash and limits federal government's ability to police crypto transactions. https://www.mayerbrown.com/en/insights/publications/2024/12/federal-appeals-court-tosses-ofac-sanctions-on-tornado-cash-and-limits-federal-governments-ability-to-police-crypto-transactions, 2024. Accessed: 2025-05-25.

[217] Alexey Pertsev, Roman Semenov, and Roman Storm. Tornado cash privacy solution, version 1.4. Whitepaper, 2019. Archived at https://berkeley-defi.github.io/. Accessed: 2026-07-25.

[218] Perun Network. PerunX: Cross-chain atomic swaps with full decentralization and security. https://perun.network/perun-x/, 2025. Accessed: 2025-07-26.

[219] Eric Pettersson Ruiz and Jannis Angelis. Combating money laundering with machine learning—applicability of supervised-learning algorithms at cryptocurrency exchanges. *Journal of Money Laundering Control*, 25(4):766–778, 2022.

[220] Thai Pham and Steven Lee. Anomaly detection in the bitcoin system—a network perspective. *arXiv preprint arXiv:1611.03942*, 2016.

[221] Andrew Poelstra. Mimblewimble. https://download.wpsoftware.net/bitcoin/wizardry/mimblewimble.pdf, 2016. Accessed: 2026-07-15.

[222] Polygon Labs. Introducing Polygon ID: Zero-Knowledge Identity for Web3. https://polygon.technology/blog/introducing-polygon-id-zero-knowledge-own-your-identity-for-web3, 2022. Accessed: Accessed: 2025-05-25.

[223] Polymarket. Polymarket 101. https://docs.polymarket.com/polymarket-101, 2025. Accessed: 2026-07-17.

[224] Joseph Poon and Thaddeus Dryja. The bitcoin lightning network: Scalable off-chain instant payments. https://lightning.network/lightning-network-paper.pdf, 2016. Accessed: 2025-07-26.

[225] Marie Poteriaieva. Polymarket's $3.2 billion election bet shows web3 potential. Forbes. https://www.forbes.com/sites/digital-assets/2024/11/05/polymarkets-32-billion-election-bet-shows-web3-potential/, 2024. Accessed: 2026-07-17.

[226] RAILGUN Project. RAILGUN project whitepaper. https://railgun.org, 2021. Accessed: 2026-07-25.

[227] Rain. Rain — stablecoin payments platform for enterprise. https://www.rain.xyz/, 2026. Accessed: 2026-07-17.

[228] Reap. Card issuing program and api — reap. https://reap.global/products/card-issuing, 2026. Accessed: 2026-07-17.

[229] FCA Press Release. Fca introduces tough new rules for marketing cryptoassets. https://www.fca.org.uk/news/press-releases/fca-introduces-tough-new-rules-marketing-cryptoassets, 2023. Accessed: 2025-05-26.

[230] IFC Review. Eu: Eu to ban trading of privacy coins from 2027. https://www.ifcreview.com/news/2025/may/eu-eu-to-ban-trading-of-privacy-coins-from-2027, 2025. Accessed: 2025-05-24.

[231] Casey Rodarmor. Ordinal theory handbook. https://docs.ordinals.com/introduction.html.

[232] Tim Ruffing and Pedro Moreno-Sanchez. Mixing confidential transactions: Comprehensive transaction privacy for Bitcoin. Cryptology ePrint Archive, Paper 2017/238; FC 2017 BITCOIN Workshop, 2017. Describes the ValueShuffle protocol. https://eprint.iacr.org/2017/238.

[233] Tim Ruffing, Pedro Moreno-Sanchez, and Aniket Kate. CoinShuffle: Practical decentralized coin mixing for Bitcoin. In *Computer Security – ESORICS 2014*, volume 8713 of *LNCS*, pages 345–364. Springer, 2014.

[234] Tim Ruffing, Pedro Moreno-Sanchez, and Aniket Kate. P2P mixing and unlinkable bitcoin transactions. In *Proceedings of the 24th Annual Network and Distributed System Security Symposium*, 2017.

[235] Pavol Rusnak and Marek Palatinus. BIP 44: Multi-account hierarchy for deterministic wallets. https://github.com/bitcoin/bips/blob/master/bip-0044.mediawiki, 2014. Accessed: 2025-04-24.

[236] Aaron S. Ballet crypto wallet review 2025: The pros and cons. https://www.bitdegree.org/crypto/ballet-crypto-wallet-review, 2025. Accessed: 2025-05-18.

[237] Safe Ecosystem Foundation. Safe: Smart account infrastructure (formerly gnosis safe). https://docs.safe.global/, 2024. Accessed: 2025-06-23.

[238] Sardine. Sardine product capabilities — q1 2024 updates. https://www.sardine.ai/blog/product-update-q1-2024, 2024. Accessed: 2026-07-29.

[239] Sardine. Sardine — agentic financial crime platform for fraud prevention & aml. https://www.sardine.ai/, 2026. Accessed: 2026-07-17.

[240] Hesam Sarkhosh, Uzma Maroof, and Diogo Barradas. The dark art of financial disguise in Web3: Money laundering schemes and countermeasures. In *Proceedings of the 20th Annual APWG Symposium on Electronic Crime Research*, 2025.

[241] Eli Ben Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. Zerocash: Decentralized anonymous payments from bitcoin. In *Proceedings of the 35th IEEE Symposium on Security and Privacy*, pages 459–474, 2014.

[242] Stephen Schneider. Money laundering in canada: A quantitative analysis of royal canadian mounted police cases. *Journal of Financial Crime*, 11(3):282–291, 2004.

[243] Merkle Science. Money laundering in crypto: How criminals hide their tracks. https://www.merklescience.com/blog/money-laundering-in-crypto-how-criminals-hide-their-tracks, 2024. Accessed: 2025-03-19.

[244] Spectrum Search. Kraken to delist monero in the eu amid regulatory pressures. https://spectrum-search.com/europe-clamps-down-on-monero-kraken-to-delist-privacy-coin-amid-regulatory-shifts/, 2024. Accessed: 2025-05-24.

[245] Secret Network. Secret network graypaper. https://scrt.network/graypaper. Accessed: 2026-07-25.

[246] European Securities and Markets Authority (ESMA). Markets in crypto-assets regulation (mica). https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica. Accessed: 2025-05-24.

[247] István András Seres, Dániel A. Nagy, Chris Buckland, and Péter Burcsi. MixEth: Efficient, trustless coin mixing service for Ethereum. Cryptology ePrint Archive, Paper 2019/341; presented at Tokenomics 2019, 2019. https://eprint.iacr.org/2019/341.

[248] Ardeshir Shojaeinasab. *Decoding Illicit Bitcoin Transactions: A Multi-Methodological Approach for Anti-Money Laundering and Fraud Detection in Cryptocurrencies*. PhD thesis, University of Victoria, 2024. Accessed: 2025-02-07.

[249] Ardeshir Shojaeinasab, Amir Pasha Motamed, and Behnam Bahrak. Mixing detection on bitcoin transactions using statistical patterns. *IET Blockchain*, 3(3):136–148, 2023.

[250] SlowMist. Crypto compliance series — what is peel chain. https://slowmist.medium.com/crypto-compliance-series-what-is-peel-chain-7b5be0bb7214, 2023. Accessed: 2025-03-19.

[251] slowmist. 2024 blockchain security and anti-money laundering annual report. Technical report, SlowMist, 2024.

[252] Aleksi Sneck. Cryptocurrency and their use in money laundering and terrorism financing. Master's thesis, Laurea University of Applied Sciences, 2024. Accessed: 2025-03-19.

[253] Matt Solomon, Toni Wahrstätter, Ben DiFrancesco, Vitalik Buterin, and Gary Ghayrat. ERC-6538: Stealth meta-address registry. Ethereum EIP (Final), 2023. https://eips.ethereum.org/EIPS/eip-6538. Accessed: 2026-07-25.

[254] Ravital Solomon, Rick Weber, and Ghada Almashaqbeh. smartFHE: Privacy-preserving smart contracts from fully homomorphic encryption. In *Proceedings of the 8th IEEE European Symposium on Security and Privacy*, 2023.

[255] Ruben Somsen. Statechains: Non-custodial off-chain Bitcoin transfer. https://medium.com/@RubenSomsen/statechains-non-custodial-off-chain-bitcoin-transfer-1ae4845a4a39, 2019. Accessed: 2026-07-25.

[256] Kiwhan Song, Mohamed Ali Dhraief, Muhua Xu, Locke Cai, Xuhao Chen, Arvind Mithal, and Jie Chen. Identifying money laundering subgraphs on the blockchain. In *Proceedings of the 5th ACM International Conference on AI in Finance*, pages 195–203, 2024.

[257] Neal Stephenson. *Snow Crash*. Bantam Books, 1992.

[258] Steven M. D'Antuono. Combating money laundering and other forms of illicit finance. https://www.fbi.gov/news/testimony/combating-money-laundering-and-other-forms-of-illicit-finance, 2025. Accessed: 2025-03-19.

[259] Sumsub. Fraud trends for 2025: From AI-driven scams to identity theft and fraud democratization. https://sumsub.com/blog/fraud-trends-sumsub-fraud-report/, 2024. Accessed: 2026-07-24.

[260] Sumsub. Crypto KYC & identity verification platform. https://sumsub.com/crypto/, 2026. Accessed: 2026-07-24.

[261] Nick Szabo. Formalizing and securing relationships on public networks. *First Monday*, 2(9), 1997.

[262] Erkan Tairi, Pedro Moreno-Sanchez, and Matteo Maffei. A2l: Anonymous atomic locks for scalability in payment channel hubs. In *Proceedings of the 42nd IEEE Symposium on Security and Privacy*, pages 1834–1851, 2021.

[263] Tangem. Tangem — your secure crypto & hardware wallet. https://www.tangem.com/.

[264] Chainalysis Team. Cryptocurrency mining pools and crypto money laundering. https://www.chainalysis.com/blog/cryptocurrency-mining-pools-money-laundering/, 2023. Accessed: 2025-02-07.

[265] Chainalysis Team. 2024 Crypto Money Laundering Report. https://www.chainalysis.com/blog/2024-crypto-money-laundering/, February 2024. Accessed: 2025-02-07.

[266] Chainalysis Team. $2.2 billion stolen from crypto platforms in 2024, but hacked volumes stagnate toward year-end as dprk slows activity post-july. *Chainalysis Blog*, 2024. Accessed: 2025-02-28.

[267] Oakland SoK Team. Systematizing systematization of knowledge. https://oaklandsok.github.io/. Accessed: 2025-04-05.

[268] Fabian Teichmann. Recent trends in money laundering. *Crime, Law and Social Change*, 73(2), 2020.

[269] Tether. Tether (usdt). https://tether.to/en. Accessed: 2025-05-14.

[270] The Defiant. MakerDAO may execute 'emergency shutdown' if sanctions hit DAI. https://thedefiant.io/news/defi/tornado-impact-makerdao-dai, 2022. Accessed: 2026-07-29.

[271] The Graph. The graph: Decentralized protocol for indexing blockchain data. https://thegraph.com. Accessed: 2025-04-16.

[272] The Sandbox Team. The sandbox: A decentralized gaming platform. https://installers.sandbox.game/The_Sandbox_Whitepaper_2020.pdf, 2020. Accessed: 2025-04-27.

[273] Louis Tremblay Thibault, Tom Sarry, and Abdelhakim Senhaji Hafid. Blockchain scaling using rollups: A comprehensive survey. *IEEE Access*, 10:93039–93054, 2022.

[274] Alanna Titterington. How deepfakes threaten kyc. https://www.kaspersky.com/blog/how-deepfakes-threaten-kyc/51987/, 2024. Kaspersky Daily. Accessed: 2026-07-24.

[275] Kentaroh Toyoda, Tomoaki Ohtsuki, and P Takis Mathiopoulos. Multi-class bitcoin-enabled service identification based on transaction history summarization. In *Proceedings of the 6th IEEE International Congress on Cybermatics*, pages 1153–1160, 2018.

[276] Muoi Tran, Loi Luu, Min Suk Kang, Iddo Bentov, and Prateek Saxena. Obscuro: A Bitcoin mixer using trusted execution environments. In *34th Annual Computer Security Applications Conference (ACSAC 2018)*, pages 692–701. ACM, 2018.

[277] Trezor. Dusting attacks & airdrop scam tokens. https://trezor.io/support/a/dusting-attacks-airdrop-scam-tokens. Accessed: 2025-04-23.

[278] TRM Labs. Trm labs – blockchain intelligence and crypto compliance. https://www.trmlabs.com/, 2025. Accessed: 2025-04-14.

[279] Trust Wallet. Trust wallet — crypto wallet for bitcoin, ethereum & millions of assets. https://trustwallet.com/, 2026. Accessed: 2026-07-17.

[280] Unit21. Unit21 — ai platform for fraud and aml operations. https://www.unit21.ai/, 2026. Accessed: 2026-07-29.

[281] United Nations Office on Drugs and Crime (UNODC). Money laundering. https://www.unodc.org/unodc/en/money-laundering/overview.html. Accessed: 2026-07-23.

[282] Nitin Upadhyay and Shalini Upadhyay. The dark side of non-fungible tokens: Understanding risks in the nft marketplace from a fraud triangle perspective. *Financial Innovation*, 11(1):62, 2025.

[283] U.S. Department of Justice. Ohio resident pleads guilty to operating darknet-based Bitcoin "mixer" that laundered over $300 million. Office of Public Affairs press release, 2021. https://www.justice.gov/archives/opa/pr/ohio-resident-pleads-guilty-operating-darknet-based-bitcoin-mixer-laundered-over-300-million. Accessed: 2026-07-25.

[284] U.S. Department of Justice. Justice department investigation leads to takedown of darknet cryptocurrency mixer that processed over $3 billion of unlawful transactions. Office of Public Affairs press release, 2023. https://www.justice.gov/archives/opa/pr/justice-department-investigation-leads-takedown-darknet-cryptocurrency-mixer-processed-over-3. Accessed: 2026-07-25.

[285] U.S. Department of the Treasury. U.s. treasury issues first-ever sanctions on a virtual currency mixer, targets DPRK cyber threats. Press release JY0768, 2022. https://home.treasury.gov/news/press-releases/jy0768. Accessed: 2026-07-25.

[286] U.S. Department of the Treasury. Illicit finance risk assessment of decentralized finance. https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf, April 2023. Accessed: 2025-05-22.

[287] U.S. Department of the Treasury press release . Treasury designates iran-based financial facilitators of malicious cyber activity and for the first time identifies associated digital currency addresses. https://home.treasury.gov/news/press-releases/sm556, 2018. Accessed: 2025-05-22.

[288] Luke Valenta and Brendan Rowan. Blindcoin: Blinded, accountable mixes for Bitcoin. In *Financial Cryptography and Data Security 2015 Workshops (BITCOIN 2015)*, volume 8976 of *LNCS*, pages 112–126. Springer, 2015.

[289] Nicolas Van Saberhagen. Cryptonote v 2.0. https://www.getmonero.org/ru/resources/research-lab/pubs/whitepaper_annotated.pdf, 2013. Accessed: 2025-02-07.

[290] Dylan Vassallo, Vincent Vella, and Joshua Ellul. Application of gradient boosting algorithms for anti-money laundering in cryptocurrencies. *SN Computer Science*, 2(3):143, 2021.

[291] Awid Vaziry, Kaustabh Barman, and Patrick Herbke. Sok: Bridging trust into the blockchain—a systematic review on on-chain identity. In *Proceedings of the 6th Conference on Blockchain Research & Applications for Innovative Networks and Services*, pages 1–9, 2024.

[292] Victor. Tangem launches smart banknotes. https://www.altcoinbuzz.io/product-release/tangem-launches-smart-banknotes/, 2018. Accessed: 2025-05-18.

[293] Fabian Victor, Martin Lüders, George Kappos, and Arthur Gervais. Address clustering heuristics for ethereum. In *Proceedings of the 24th Financial Cryptography and Data Security International Conference*, pages 617–633, 2020.

[294] Visa. The crypto phenomenon: 2022 consumer attitudes and usage. https://usa.visa.com/content/dam/VCOM/regional/na/us/Solutions/documents/visa-cryptocurrency-a-and-u-2022-final-white-paper.pdf, 2022. Accessed: 2025-04-27.

[295] Visa Inc. The crypto phenomenon: Consumer attitudes & usage. https://usa.visa.com/content/dam/VCOM/regional/na/us/Solutions/documents/visa-cryptocurrency-a-and-u-2022-final-white-paper.pdf, 2022. Accessed: 2025-04-27.

[296] Eric Wagner, Roman Matzutt, and Martin Henze. Seldom: An anonymity network with selective deanonymization. *arXiv preprint arXiv:2412.00990*, 2024.

[297] Toni Wahrstätter, Matt Solomon, Ben DiFrancesco, and Vitalik Buterin. ERC-5564: Stealth addresses. Ethereum EIP (Final), 2022. https://eips.ethereum.org/EIPS/eip-5564. Accessed: 2026-07-25.

[298] Yunpeng Wang, Jin Yang, Tao Li, Fangdong Zhu, and Xiaojun Zhou. Anti-dust: A method for identifying and preventing blockchain's dust attacks. In *Proceedings of the 1st International Conference on Information Systems and Computer Aided Education*, pages 274–280, 2018.

[299] Ziwei Wang, Jiashi Gao, and Xuetao Wei. Do nfts' owners really possess their assets? a first look at the nft-to-asset connection fragility. In *Proceedings of the 32nd ACM Web Conference*, pages 2099–2109, 2023.

[300] Sam Werner, Daniel Perez, Lewis Gudgeon, Ariah Klages-Mundt, Dominik Harz, and William Knottenbelt. Sok: Decentralized finance (defi). In *Proceedings of the 4th ACM Conference on Advances in Financial Technologies*, pages 30–46, 2023.

[301] WETH. Wrapped ether (weth). https://weth.io/, 2017. Accessed: 2025-06-23.

[302] Bryan White, Aniket Mahanti, and Kalpdrum Passi. Characterizing the opensea nft marketplace. In *Companion Proceedings of the 32nd ACM Web Conference*, pages 488–496, 2022.

[303] Zachary J. Williamson. The AZTEC protocol, version 1.0.1. https://github.com/AztecProtocol/AZTEC/blob/master/AZTEC.pdf, 2018. Accessed: 2026-07-25.

[304] Gavin Wood. Ethereum: A secure decentralised generalised transaction ledger. Technical report, Ethereum Foundation, Ethereum Foundation, February 2025. Accessed: 2025-04-28. Formal Specification of Ethereum as of the Shanghai Upgrade.

[305] Worldcoin Foundation. Worldcoin whitepaper. https://whitepaper.world.org/, 2023. Accessed: 2025-05-26.

[306] Jiajing Wu, Kaixin Lin, Dan Lin, Ziye Zheng, Huawei Huang, and Zibin Zheng. What financial crimes are hidden in metaverse? taxonomy and countermeasures. In *From Blockchain to Web3 & Metaverse*, pages 181–214. Springer, 2023.

[307] Lei Wu, Yufeng Hu, Yajin Zhou, Haoyu Wang, Xiapu Luo, Zhi Wang, Fan Zhang, and Kui Ren. Towards understanding and demystifying bitcoin mixing services. In *Proceedings of the 30th Web Conference 2021*, pages 33–44, 2021.

[308] Pieter Wuille. Bip 32: Hierarchical deterministic wallets. https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki, 2012. Accessed: 2025-04-21.

[309] Jiahua Xu, Krzysztof Paruch, Simon Cousaert, and Yebo Feng. Sok: Decentralized exchanges (dex) with automated market maker (amm) protocols. *ACM Computing Surveys*, 55(11):1–50, 2023.

[310] Jie Xu, Cong Wang, and Xiaohua Jia. A survey of blockchain consensus protocols. *ACM Computing Surveys*, 55(13s):1–35, 2023.

[311] Minghui Xu, Yihao Guo, Chunchi Liu, Qin Hu, Dongxiao Yu, Zehui Xiong, Dusit Niyato, and Xiuzhen Cheng. Exploring blockchain technology through a modular lens: A survey. *ACM Computing Surveys*, 56(9):1–39, 2024.

[312] Feixue Yan, Sheng Wen, Yang Xiang, and Shiping Chen. Shapley-value-based explanations for cryptocurrency blacklist detection. In *Proceedings of the 23rd IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, pages 435–442, 2024.

[313] Qinglin Yang, Huawei Huang, Kaixin Lin, and Jiajing Wu. An introduction to web3 and metaverse. In *From Blockchain to Web3 & Metaverse*, pages 1–26. Springer, 2023.

[314] Andrew C. Yao. Protocols for secure computations. In *Proceedings of the 23rd Annual Symposium on Foundations of Computer Science*, pages 160–164, 1982.

[315] Oudha Yousif, Mohammed Dawood, Faiez Thanoon Jassem, and Nameer Hashim Qasim. Curbing crypto deception: evaluating risks, mitigating practices and regulatory measures for preventing fraudulent transactions in the middle east. *Encuentros: Revista de Ciencias Humanas, Teoría Social y Pensamiento Crítico*, 22(4):311–334, 2024.

[316] Yunmei Yu, Jiajing Wu, Dan Lin, and Qishuang Fu. Money laundering detection on ethereum: Applying traditional approaches to new scene. In *Proceedings of the 29th IEEE International Conference on Parallel and Distributed Systems*, pages 1759–1766, 2023.

[317] Kristina Zatonatska, Matthias Fromberger, and Klaus Hering. A taxonomy of cryptocurrency tokens: A financial instrument perspective. https://pdfs.semanticscholar.org/98b4/0f1e696b26c5c19f7a87e1abe4b0858c647f.pdf, 2022. Accessed: 2025-04-21.

[318] Zcash. Zcash: Internet money, reimagined. https://z.cash. Accessed: 2025-04-16.

[319] Mengya Zhang, Xiaokuan Zhang, Yinqian Zhang, and Zhiqiang Lin. Security of cross-chain bridges: Attack surfaces, defenses, and open problems. In *Proceedings of the 27th International Symposium on Research in Attacks, Intrusions and Defenses*, pages 298–316, 2024.

[320] Jiajun Zhou, Chenkai Hu, Jianlei Chi, Jiajing Wu, Meng Shen, and Qi Xuan. Behavior-aware account de-anonymization on ethereum interaction graph. *IEEE Transactions on Information Forensics and Security*, 17:3433–3448, 2022.

[321] Vivian Ziemke, Benjamin Estermann, Roger Wattenhofer, and Ye Wang. What determines the price of nfts? In *Proceedings of the 29th IEEE International Conference on Parallel and Distributed Systems*, pages 1562–1568, 2023.

[322] Guy Zyskind, Yonatan Erez, Tom Langer, Itzik Grossman, and Lior Bondarevsky. FHE-Rollups: Scaling confidential smart contracts on Ethereum and beyond. Fhenix, 2024. https://www.fhenix.io/. Accessed: 2026-07-25.

Appendix A

Literature Comparison

This appendix compares our systematization of laundering schemes with prior scholarly efforts that aim to classify money laundering in the cryptocurrency ecosystem. Table A.1 (see next page) presents a taxonomy-based coverage analysis, highlighting the overlap and divergence between our work and existing surveys. The mechanism columns follow the two-part structure of our taxonomy: a single column for privacy-enhancing technologies (PETs), the tools purpose-built for privacy, set apart by a rule from the ten exploited infrastructures that follow.

Kolachala et al. [157] label their work as a systematization of knowledge paper on money laundering in cryptocurrencies; however, their primary focus is on money laundering countermeasures, particularly about blocklisting and traceability. Although they provide a detailed technical analysis of laundering via PCNs and HTLCs, they do not aim to propose a structured taxonomy of laundering strategies or intermediary mechanisms.

Lin et al. [176] introduce a modified lifecycle-based taxonomy of money laundering stages in cryptocurrency systems. While this offers a broad conceptual framing, it leaves out many laundering schemes.

Shojaeinasab [248] concentrates on forensic detection using address graph analysis and machine learning. The study briefly acknowledges key laundering infrastructures such as mixers, privacy coins, exchanges, and PCNs, but does not attempt a formal categorization of laundering strategies or mechanisms. Its primary contribution lies in detection rather than systematization.

Sneck [252] presents a systematic literature review of cryptocurrency-enabled laundering and terrorist financing. The work touches on several components of our taxonomy,

Table A.1: Cryptocurrency laundering schemes coverage across existing surveys.

Surveys / Laundering Schemes	General Strategies						Intermediary Mechanisms									
	Transaction Flow Obfuscation	Commingling	Disconnected Fund Flow	Chain-hopping	Exploit Subjective Valuations	Exploit Regulatory Gaps	Privacy-enhancing Technologies (PETs)	Cryptocurrency Exchanges	Cross-chain Bridges	DeFi Mechanisms	NFTs	Cryptocurrency ATMs	Card-Based Instruments	Online Gambling	Initial Coin Offerings	Consensus Protocols	Payment Channel Networks
Kolachala et al. [157]	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓
Lin et al. [176]	✓	✗	✗	✓	✗	✗	✓	✓	✗	✓	✗	✗	✗	✗	✓	✗	✗
Shojaeinasab [248]	✓	✗	✓	✓	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓
Sneck [252]	✗	✗	✗	✓	✗	✓	✓	✓	✓	✗	✓	✓	✗	✓	✗	✗	✗
Almeida et al. [6]	✗	✗	✓	✓	✗	✓	✓	✓	✗	✗	✗	✓	✓	✓	✗	✗	✗
Comolli and Korver [63]	✗	✓	✓	✓	✗	✓	✓	✓	✗	✗	✗	✓	✓	✓	✓	✗	✗
Möser et al. [204]	✓	✗	✓	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Mooij [199]	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗
Gabbiadini et al. [117]	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗
Ours	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

including mixers, privacy coins, exchanges, chain-hopping, NFTs, crypto ATMs, and regulatory arbitrage. However, discussions included in the paper are example-driven and fail to formalize laundering mechanisms or attacker strategies. The absence of a structured taxonomy limits its utility for analytics or forensics.

Almeida et al. [6] are among the few sources that attempt a structured classification of laundering methods by mapping them to PLI stages. They discuss several practical techniques which include in-person and P2P transactions, cryptocurrency ATMs, prepaid and gift cards, gambling, decentralized exchanges, and mixers. However, their categorization lacks granularity, omits many modern Web3 laundering mechanisms, and provides only brief descriptions of each tactic. Our work complements and extends their stage-based view by introducing a two-dimensional taxonomy encompassing both laundering intent and intermediary implementation.

Comolli and Korver [63] provide a narrative overview of various laundering techniques and enforcement challenges in Web3. They refer to several elements also contained in our taxonomy such as commingling, mixers, jurisdictional arbitrage, and exchanges, while also touching on chain-hopping via atomic swaps and DEXs. However, their analysis does not differentiate strategies from mechanisms, nor does it cover emerging techniques such as cross-chain bridges, consensus participation, or NFT-based laundering. Our taxonomy refines and extends an unstructured list of laundering tools into a coherent framework.

Möser et al. [204] explore transaction flow obfuscation patterns and the role of mixing services. Their study contributes early insights into disconnecting fund flow using swapping but does not aim to catalog laundering strategies or infrastructure comprehensively.

Mooij [199] focuses specifically on money laundering risks in the metaverse, particularly involving NFTs. While the analysis is valuable for platform-specific vulnerabilities, it does not examine broader laundering schemes or mechanisms and is best understood as a complementary resource.

Gabbiadini et al. [117], in a Bank of Italy occasional paper, trace illicit cryptocurrency across the placement, layering, and integration stages. They cover a broad set of channels, including exchanges, crypto ATMs, mixers and privacy coins, cross-chain bridges and atomic swaps, DeFi, and NFT trading, and they treat chain-hopping and the exploitation of regulatory gaps at length; their discussion of NFTs turns on the subjective valuation of unique assets, mirroring our own. Their account is organised around AML regulation and laundering typologies rather than a structured taxonomy that separates strategies from mechanisms, and it leaves out schemes such as gambling, ICOs, consensus participation, and payment channel networks.

In contrast to all prior work, our study introduces a unified two-dimensional taxonomy that separates laundering strategies from their enabling mechanisms and maps them to the stages of the laundering lifecycle. We further identify the nature of forensic traces they leave, whether on-chain, off-chain, or cross-chain, enabling a more operationally useful classification. Our approach is grounded in qualitative thematic analysis and conceptual clustering, drawing from academic literature, regulatory reports, and forensic case studies. This allows us to capture under-explored techniques such as laundering via participation in mining and validating transactions, which are absent from mentioned sources. Finally, where prior surveys list privacy tools separately with labels such as *mixers* and privacy coins, we retire these labels and group them under one deployment-based taxonomy (§5.2.1).