Mapping Solana Exfiltration Routes and Wallet Labeling

Introduction -

Solana's rapid growth in decentralized finance has brought unprecedented innovation – and new security challenges. When an on-chain exploit occurs, attackers rush to exfiltrate the stolen funds before they can be frozen or traced. Mapping these exfiltration routes is crucial for defenders and investigators: it reveals how hackers convert ill-gotten crypto into hard-to-trace assets, and it helps the community block or recover those funds. High-profile Solana breaches illustrate this urgency. For example, the Wormhole bridge hack in February 2022 saw an attacker mint 120,000 wrapped ETH (WeETH) on Solana (roughly $320 million) by exploiting a smart-contract flaw.

In the aftermath, on-chain analysts tracked how that stolen ETH was converted and moved across chains. By closely monitoring the attacker's wallets, researchers noted that investigators' vigilance can make it "virtually impossible for the hacker to move the funds undetected".

This report surveys the methods and tools used to trace such laundering paths on Solana. We describe common attacker tactics, the investigative workflow, key assets involved, and insights gleaned from recent cases – all to help security teams, investigators, and developers better defend the Solana ecosystem.

How Exfiltration Works -

Once a hacker has drained assets from a Solana protocol, the priority becomes laundering – quickly transforming and fragmenting the stolen crypto to hide its origin. Attackers typically start by moving funds into the most liquid markets. They may use DEX swaps to convert exotic or protocol-specific tokens into widely traded assets like SOL or stablecoins. This often involves "peel chains," where funds are split into many smaller transfers through intermediate wallets and trading pairs to avoid triggering alarms.

Cross-chain bridges are another key tool: by passing stolen funds through protocols like Wormhole or THORChain, criminals can move value to chains such as Ethereum, where they can swap into other currencies. For example, Chainalysis reported that after the Wormhole hack, the attacker bridged back to Ethereum and converted the remaining WeETH into SOL, wrapped SOL (wSOL), and Solana-USDC

Once on a new chain, funds may be further fragmented via mixers (e.g. Tornado Cash) or converted into privacy coins like Monero to sever on-chain links. Finally, attackers often deposit the laundered coins into centralized exchanges or over-the-counter (OTC) markets to cash out. In short, exfiltration on Solana leverages a combination of DEX trading, cross-chain bridges, mixers, and exchange deposits – all layered to obscure the trail.

Investigation Approach -

Investigators trace these routes using blockchain analytics tools and heuristics, assuming attackers will favor fungible, high-liquidity assets and regulated endpoints. The typical workflow begins by identifying the exploited protocol's drain address and then following outbound transactions. Analysts use Solana block explorers (e.g. Solscan, Solana.fm) and advanced platforms (Chainalysis, Elliptic, TRM, Nansen, and custom tools like Range Trail) to map the flows. They look for patterns such as repeated trades, common signers, and known service addresses. For example, clustering algorithms group all associated token accounts under a single owner by tracking fund ownership changes.

When an address interacts with a known exchange deposit key, it can be labeled accordingly. The process often involves iterating: tracing funds through a DEX, then into a bridge, then onto another chain, and so on. Analysts also monitor for "peel chain" splitting (many small transfers) and use heuristics to reassemble distributed funds. Throughout, they rely on both automated alerts and manual insight. Chainalysis, for instance, highlights that their system detects every value transfer on-chain and clusters addresses controlled by the same entity.

In practice, investigators feed such cluster data and known wallet labels (e.g. exchange hot wallets, mixer addresses) into graph queries to follow the money. Transparency of the chain is a powerful ally: as one study notes, moving stolen assets through flagged addresses means "none of the accused's actions covered [his] tracks or fooled law enforcement".

By combining on-chain data with off-chain intelligence (e.g. exchange cooperation), investigators can build a near-real-time picture of an exploit's money trail.

Non-Freezable Assets on Solana -

Criminals favor assets that cannot be easily frozen or reversed. On Solana, the native currency SOL is non-freezable by design – there's no authority that can arbitrarily block SOL transfers. Similarly, popular SPL tokens with their freeze authorities revoked are viewed as safe to move, because no one can suddenly blacklist those coins. In general, attackers stick to *high-liquidity* tokens and stablecoins that exchange readily. These include Solana's liquid staking derivatives (like mSOL, stSOL), wrapped major assets (e.g. wETH, wBTC), and stablecoins on Solana (USDC, USDT). Chainalysis observed this in action: after a large hack, the stolen WeETH was largely converted into SOL, wSOL, and Solana-based USDC.

Notably, the Solana community warns that any token still carrying an active freeze or mint authority is effectively unusable for thieves – such tokens are usually considered scams. In short, the liquidity tier on Solana means stolen funds move through the most widely accepted coins, which are least likely to be stopped by a token administrator.

Common Exfiltration Routes -

Attackers employ a variety of platforms to launder funds, typically in the order of greatest liquidity and cross-chain connectivity:

- Decentralized Exchanges (DEXes): Solana's on-chain AMMs (Serum, Raydium, Orca, Jupiter aggregates) are often the first stop. Here thieves swap niche or stolen tokens for major assets. This exploits the deep liquidity pools and low slippage of these DEXes. By sweeping large orders through multiple pools, criminals can also obscure the origination of funds. In one enforcement case, the hacker "carried out token swaps" on Solana as part of the laundering process.
- DEXes allow nearly instantaneous trades without an account, making them a common anonymization layer.
- Cross-Chain Bridges: Bridges like Wormhole, Allbridge, and THORChain enable stolen assets to hop between blockchains. For example, the Wormhole exploit itself relied on bridging: the attacker minted WeETH on Solana without collateral, then later bridged much of it back to Ethereum (ultimately holding ~93,750 ETH in one address).
- In another case, the Bybit hack funds were moved through ThorChain from Ethereum to Bitcoin.
- Bridges leverage high liquidity across ecosystems: by converting to an asset on another chain, criminals can exploit fresh markets and additional mixing tools.
- ThorChain's usage graph illustrates this effect – after the Bybit exploit, its 24-hour swap volume surpassed $1 billion, signaling massive cross-chain flows of stolen funds.
- Centralized Exchanges (CEXes): Ultimately, many routes converge at major exchanges, where illicit crypto can be converted to fiat or stable assets. Even supposedly private transactions lead here: Chainalysis reported the Wormhole

hacker paid for gas via Tornado Cash and then sent 0.1 ETH to an international exchange deposit address.

- In the U.S. case against a Solana exploit, the accused moved funds through “overseas cryptocurrency exchanges” after swaps and bridges.
- Exchanges are attractive endpoints because of their liquidity and off-chain settlement, but they also provide enforcement chokepoints – on receipt, exchanges can freeze or report suspicious deposits.
- Mixers and Privacy Tools: On-chain coin mixers remain a go-to for some threat actors. Services like Tornado Cash on Ethereum (and its analogs on other chains) aggregate coins from many users. Hackers mix stolen funds here to break the on-chain lineage. For instance, analysts note that Lazarus Group often converts funds into Bitcoin or ETH and then passes them through mixers such as Tornado Cash, Sinbad, and others.
- However, increased sanctions on mixers have led many criminals to seek alternatives. Hybrid platforms like THORChain (which combines bridging with internal liquidity pools) are increasingly used in place of pure mixers.
- Still, any use of mixers adds complexity – unwinding them typically requires specialized chain analysis and, increasingly, law enforcement cooperation.
- Fintech and OTC Channels: Beyond pure crypto venues, attackers may exploit on/off-ramp applications and over-the-counter desks. For example, some criminals route funds into stablecoins or fiat via payment apps, peer-to-peer exchanges, or crypto debit-card services that operate on Solana. These channels often have lower on-chain volume (hence “fintech apps” are a lower liquidity tier), but they bypass on-chain tracing once funds exit into the traditional financial system. While detailed data is scarce, investigators know to watch for large transfers into such gateways as a sign that stolen funds are about to leave crypto rails entirely.

Risk Patterns and Observations -

- **Studying real-world cases uncovers strategic patterns.** Transaction layering is ubiquitous: criminals use thousands of intermediary addresses and rapidly chain transactions across multiple platforms to obfuscate the source.
- **In effect,** they “flood the zone” with on-chain activity – large, rapid trades and bridges designed to overwhelm both automated AML tools and human analysts
- **Forensic reports note that** the more hops and networks involved, the harder stolen funds are to trace: “complex laundering patterns involving multiple hops and network bridges…require manual intervention”. This is by design – each layer erodes the direct link between the hack and the cash-out. Mixers further

magnify the effort needed, since demixing stolen coins demands painstaking analysis.

- **Another observation is that** many laundering chains end at a handful of high-confidence targets (especially well-known exchanges). Investigators exploit this by tagging those final addresses. Importantly, the transparency of the blockchain can backfire on criminals: in the Wormhole case, vigilant monitoring of one key address – along with broad community scrutiny – effectively locked down the stolen funds, as analysts highlighted that tracking made movement “virtually impossible…without detection”.

In short, exfiltration routes are designed to stay one step ahead of sanctions, but their patterns often reveal themselves under close analysis.

Wallet Identification -

At the heart of tracing is address clustering and labeling. Blockchain analysts group Solana addresses into clusters representing real entities by exploiting Solana’s account structure. As Chainalysis describes, its Solana knowledge graph was built by clustering addresses that share control (for example, token accounts owned by the same main wallet) .

In practice, if two SPL token accounts consistently transfer together or belong to the same system address, they are assigned to one wallet cluster. Known entities – such as an exchange’s hot wallet or a mixer contract – are tagged by their on-chain behavior (large deposits or code signatures) and then applied retroactively to all addresses in that cluster. Investigators also use ground-truth data: for instance, deposit addresses that exchanges publish for Solana, or known phishing/malicious wallet lists. Combined, these labels convert abstract addresses into actionable intelligence. By following clusters instead of raw addresses, analysts can map the full scope of the laundering operation. The result is a labeled flowchart: theft begins at the exploited protocol, follows through a chain of clustered wallet labels (DEXes, bridges, mixers, exchanges), and ends in the points of cash-out. This systematic approach transforms raw transaction logs into a narrative of the exploit – and it underpins the forensic value of the entire investigation.

Methodology & Tools -

To trace laundering routes, we adopt a **forensic on-chain analysis** workflow. First, we assume a compromised wallet or contract (the “hacker’s address”) and **query all outgoing transactions**. Using Solana explorers (e.g. Solscan or Solana.fm) and public on-chain data (via BigQuery or Helius API), we identify where funds go and in what amounts. We pay special attention to patterns of splitting, repeated timing, or multiple small transfers – common tactics to obscure trails. At each step we annotate known protocols or addresses (e.g. if a transfer hits a mixer contract or an exchange deposit address). Iteratively, we follow the flow through swaps, transfers, and bridges.

Analytical tools are crucial. Range's own **Range Trail** platform provides powerful cross-chain forensics: it clusters related addresses and traces funds across protocols. External intelligence suites like Arkham Intelligence can similarly **cluster wallets** and flag high-risk entities. In practice we use any tool available – explorers, dashboards, data platforms – as Range suggests. For example, dashboards like Step Finance or Jupiter aggregate DEX liquidity, helping estimate how much volume a DEX pool can handle. Custom SQL on Solana's BigQuery dataset or APIs (Helius, QuickNode) help find transaction histories. We also cross-reference on-chain findings with OSINT or reporting (e.g. public analyses by Chainalysis or independent researchers on Lazarus Group activity). Throughout, any addresses we suspect are labeled or queried against known watchlists (Range, Arkham, etc.) to validate identities and prevent false positives.

High-Liquidity Non-Freezable Assets -

A key output of this analysis is an **inventory of tokens** an attacker would use – focusing on high-liquidity, non-freezable assets. In Solana terms, this means assets that can be swapped or withdrawn in large volume without a central issuer being able to "freeze" them. Obvious examples include:

- **SOL (native SOL/Wrapped SOL):** The chain's base currency is universally liquid (all DEXes, bridges, CEXes) and cannot be frozen. SOL is almost always used as a medium for swaps and bridge routing.

- **Bridged major cryptos:** Wrapped Bitcoin (Wormhole-wBTC) and Wrapped Ethereum (Wormhole-wETH) on Solana carry massive liquidity and have no Solana-native freeze authority. They can be quickly swapped on DEXes (Serum, Raydium) or bridged out for large value.

- **Stablecoins:** USDC and USDT on Solana are extremely liquid (holding ~38% of all inbound bridge volume, making them natural swap targets. *However*, these are issued by centralized entities (Circle/Tether) with freeze keys, so in theory can be blacklisted. Attackers may still use them up to the point of off-ramp, then exit via decentralized routes to avoid compliance checks.

- **Other highly-traded SPL tokens:** Certain large DeFi tokens (e.g. Raydium's RAY, Bonfida's FIDA) or algorithmic stables may have significant liquidity on Solana-native markets. Each must be checked for freeze authority (many SPL tokens do have an issuer key). In general, the safer picks are **stable, high-cap tokens bridged from other chains** with no freeze (SOL, wBTC, wETH, renBTC, etc).

We justify each asset by its **liquidity venues**: for example, SOL and stables have deep order books on Serum and many liquidity pools; bridged BTC/ETH have large pools on Raydium and can be redeemed via bridges. The framework is to list tokens that a thief could trade in or out of quickly without tripping a freeze. A formal answer should enumerate SOL plus any non-freezable tokens backed by cross-chain protocols – essentially what the bounty describes as "assets (SOL and non-SOL) with high liquidity and no freeze authority".

Recommendations -

To counter these threats, both security teams and developers must bolster prevention and response:

- **Improve Protocol Security:** Rigorous code audits and safety reviews are essential. Chainalysis emphasizes that "extremely rigorous code audits" should be the gold standard for DeFi protocols.
- **Protocol designers** should identify and fix vulnerabilities before any launch, and maintain active bug bounty programs. Redundancies such as multi-signature controls on key operations can also mitigate exploit risk.
- **Revoke Freeze Authorities:** Tokens should ship with zero authorities unless absolutely necessary. Any SPL token with an unrevoked freeze key is a red flag .
- Developers of tokens and bridges should disable administrative controls once deployed, preventing emergency freezes from being misused or rendering tokens ineffective for legitimate use.
- **Real-Time Monitoring and Analytics:** Security operations should integrate blockchain intelligence tools that alert on large or unusual transactions. As laundering schemes grow in sophistication, real-time analytics (pattern detection, flow clustering, and cross-chain correlation) become critical. Specialists note that advanced laundering "underscores the need for advanced tools and expertise".

Thus, organizations should partner with forensic analysts or subscribe to investigative platforms.

- **Collaboration with Exchanges:** Open communication channels with centralized exchanges and over-the-counter desks are vital. If a hack is detected, quickly notifying exchanges and providing wallets to blacklist can prevent cash-out. Moreover, exchanges can implement stricter Know-Your-Transaction (KYT) filters for suspect chains and addresses. For example, the U.S. DOJ's criminal case against a Solana attacker shows that authorities could follow the money precisely because exchanges cooperated in tracing deposit addresses.
- **Community Intelligence Sharing:** Maintain and contribute to shared databases of labeled malicious wallets, phishing contracts, and scam tokens. Public watchlists and dashboards (e.g. Nansen, Solana-based block explorers) help the entire ecosystem flag suspicious activity sooner. Encouraging transparent reporting of incidents also raises collective awareness of emerging laundering trends.

Taken together, these measures make Solana a harder target for money launderers. While no system can guarantee absolute security, each layer of oversight—from secure code to vigilant monitoring—raises the effort required to move stolen funds.

Conclusion -

On Solana, Laundering is a cat-and-mouse game - attackers exploit Solana's speed and liquidity to vanish with stolen crypto, while investigators leverage the chain's transparency to reconnect the dots. By systematically mapping exfiltration routes, the security community can turn the tables. As demonstrated by the Wormhole and other exploits, diligent on-chain analysis and cross-system collaboration can corner even the most determined launderer.

Defenders who understand the common tactics – swapping on DEXes, bridging across networks, and layering through intermediaries – can better anticipate and intercept those moves. Ultimately, reinforcing smart-contract security, token governance, and analytical capabilities will deter abuse and protect honest users. The Solana ecosystem's resilience depends on staying one step ahead: every traced transaction and labeled wallet narrows the shadows in which attackers can hide. By weaving these intelligence threads into protocol design and incident response, Solana's builders and security teams can safeguard the chain against sophisticated laundering schemes.
Sources: This analysis draws on blockchain research and incident reports from Chainalysis, SlowMist, CCN, and others, reflecting real-world cases of Solana exploits and laundering tactics.