Reflection on the Money Laundry Project: A Hackathon Adventure and the Open Source Future

Participating in this hackathon was, without a doubt, an intense and rewarding adventure. The challenge of creating a tool to map fund exfiltration methods on Solana in just 10 days was ambitious but incredibly stimulating. The result is **HackerDex**, a project born from the competition, but whose vision now extends beyond it.

From the beginning, the goal was to build more than just a submission; it was to lay the foundation for a robust and useful risk analysis tool for the Solana community. I dove into developing heuristics, integrating databases, interacting with the Solana RPC, and incorporating OSINT intelligence. I managed to implement a significant set of pattern detections, from interactions with mixers and bridges to more sophisticated techniques like Peel Chains and Fund Churning, culminating in a weighted risk scoring system. The detailed documentation accompanying the project reflects the depth of analysis I aimed to achieve.

Facing the Challenges:
The limited 10-day timeframe was, naturally, a significant constraint. It demanded focus, prioritization, and, inevitably, some simplifications. One of the biggest challenges, however, was external: the **power outage affecting Portugal, Spain, and France** that occurred during the hackathon period. This event not only consumed valuable development and testing time but also severely hampered the real-time collection of on-chain data, which would have been essential for one of the most complex parts of the challenge: **calculating the available liquidity in the exfiltration routes**.
Although I managed to identify routes and categorize the involved addresses using my database and heuristics, quantifying the liquidity (e.g., <$100k, <$1M) for each route became impractical due to the power instability and the remaining time. This remains a critical area for future development, as detailed in the README.md and the project roadmap. Similarly, creating exhaustive lists of non-freezable assets and their specific liquidity in different venues would require deeper data integrations than time allowed.
Deliverables vs. Reality:
I was able to produce:

1. **Methodology Documentation:** The detailed chapter-by-chapter documentation (generated during our interaction) describes the approach and results for each detected pattern.
2. **Route and Label Identification:** The system identifies potential routes via the FundTracer (albeit experimentally), and the analyze_known_wallets tool applies heuristic-based tags (labels) to the analyzed addresses, updating the database.

I couldn't fully deliver, due to the mentioned constraints:

- The CSV/Sheet list of non-freezable assets with **current liquidity** and venues.
- The CSV/Sheet list of exfiltration routes with the **quantification of launderable liquidity** and all associated details for *each* address in the route in a single consolidated file.

Notable Findings During Development:

Despite the time constraints and external challenges, practical analysis yielded promising results and valuable datasets:

- **Kelsier Ventures Blacklist:** I successfully compiled a list of over 200 wallet addresses directly linked to pump-and-dump schemes and scams associated with Kelsier Ventures. This dataset, located in `/samples/blacklist_kelsier_ventures_parse.csv`, provides a concrete set of addresses that should absolutely be flagged as "Known Hacker" or similar high-risk categories within the HackerDex database and Range Platform.
- **Binance Interaction Analysis:** An initial analysis run on over 1000 wallets known to have interacted with Binance indicated that approximately **1.3%** exhibited patterns potentially related to fund exfiltration, according to the heuristics developed. This preliminary finding highlights the potential of the heuristic engine to flag suspicious activity even within large datasets interacting with major exchanges, warranting further investigation and refinement of the rules.
- **Peel Chain Heuristic Adjustment:** The initial implementation of the Peel Chain detection heuristic was deactivated during the final stages. Testing revealed that the criteria based primarily on transaction timing, while conceptually sound, yielded a relatively high false positive rate (approximately 45%) in the analyzed datasets. Given the time constraints, I opted to disable this specific analysis via its feature flag (`peel_chain_exfiltration_enabled = false`) to ensure the overall results focused on heuristics with higher observed assertiveness. Refining the Peel Chain detection logic (potentially incorporating amount analysis) remains an important area for future work.

These findings underscore the practical applicability of the developed heuristics and the importance of curated address lists and iterative refinement in identifying illicit networks.

Exfiltration Analysis Summary: Run 1 (Completed April

29, 2025)

Summary Statistics:

- **Run Completed:** 2025-04-29T15:11:31Z
- **Duration:** 334 minutes 57 seconds
- **Total Wallets Analyzed:** 199
- **Wallets Tagged (Exfiltration Patterns Detected):** 13
- **Wallets with Analysis Errors:** 39
- **Detection Rate:** 6.5%

Most Common Exfiltration Patterns:

- **Automated Exfiltration Pattern:** 8 wallets (61.5% of tagged)
- **Advanced Obfuscation Techniques:** 5 wallets (38.5% of tagged)
- **Fund Churning:** 3 wallets (23.1% of tagged)

Tagged Wallet Identification:

- **Wallet:** `2tPm12mHPqhWShTwQss71veTD2T3ZSuBHzcDdyU6CsTk`
  - Tags: ["Fund Churning", "Advanced Obfuscation Techniques", "Automated Exfiltration Pattern"]
- **Wallet:** `6H1q8o9uUorBjyC8C6VEPQhSaPCipK4MRd31pC81qBvM`
  - Tags: ["Automated Exfiltration Pattern"]
- **Wallet:** `7P8N8mhzc8SMHomiHXuyJ7tX2kmNeZdFjuPS62jrB2U6`
  - Tags: ["Automated Exfiltration Pattern"]
- **Wallet:** `7kW6YyuMhCeG5vidhCfyYaEmxHwVfxG8ub68cgm4Ju8n`
  - Tags: ["Automated Exfiltration Pattern"]
- **Wallet:** `817vVbqDzU2U5qgEagCJEU2meTCe6PrLT5cx4J6fL1yZ`
  - Tags: ["Automated Exfiltration Pattern"]
- **Wallet:** `8aJiU9tu3QcKfZhem9kUZKaCfRGyEEKkhi35jAJgGxcX`
  - Tags: ["Fund Churning", "Advanced Obfuscation Techniques"]
- **Wallet:** `91PZ9AtSTwMiF6iCu125uTr2hAPPasr2dVweSHxzHGAJ`
  - Tags: ["Advanced Obfuscation Techniques"]
- **Wallet:** `AL5Crg5SqcvxUr3kq1BGrWPYsbRyqTcDN5fQRJ7SnTkz`
  - Tags: ["Fund Churning"]
- **Wallet:** `CCPWz1WreB5xRsAH7YQgzZPwWTEYuSqKRNBzoZMALWKL`
  - Tags: ["Automated Exfiltration Pattern"]
- **Wallet:** `EP3FmnQ3mBcGNihsCjgu2g9gof2w3aX7m1HQpoBbJBLT`
  - Tags: ["Automated Exfiltration Pattern"]
- **Wallet:** `H6a5ZsM6Lg6tAteBhXo3HETUXPnbGx7RHmhQppkMbaca`
  - Tags: ["Advanced Obfuscation Techniques"]

- **Wallet:** `ZG98FUCjb8mJ824Gbs6RsgVmr1FhXb2oNiJHa2dwmPd`
    - Tags: ["Automated Exfiltration Pattern"]
- **Wallet:** `fireH8ZNe3W1fN662qRx4AvzVoZZPWNhiANwfx2fAMU`
    - Tags: ["Advanced Obfuscation Techniques"]

Exfiltration Analysis Summary: Run 2 (Completed April 30, 2025)

Summary Statistics:

- **Run Completed:** 2025-04-30T17:57:14Z
- **Duration:** 1181 minutes 54 seconds
- **Total Wallets Analyzed:** 629
- **Wallets Tagged (Exfiltration Patterns Detected):** 10
- **Wallets with Analysis Errors:** 2
- **Detection Rate:** 1.6%

Most Common Exfiltration Patterns:

- **Fund Churning:** 5 wallets (50.0% of tagged)
- **Automated Exfiltration Pattern:** 5 wallets (50.0% of tagged)
- **Advanced Obfuscation Techniques:** 4 wallets (40.0% of tagged)

Tagged Wallet Identification:

- **Wallet:** `2C5xmwQCpHuDLc7eWo7ATs4kVBswUfmUEPyjVVJwHh6U`
    - Tags: ["Fund Churning", "Advanced Obfuscation Techniques"]
- **Wallet:** `3FryhGZRjMXej2fKuHadeM1BmE9zujoMPKv6aZ3zCHTU`
    - Tags: ["Fund Churning", "Advanced Obfuscation Techniques"]
- **Wallet:** `4c35jjbrgguCaujRrU7kwushk8J9axXR2UJfGNEwb5sS`
    - Tags: ["Automated Exfiltration Pattern"]
- **Wallet:** `5MxCbN9AXr3Y2BJ5aKJFp9ehFwg5gH3LTfh551JVijpc`
    - Tags: ["Automated Exfiltration Pattern"]
- **Wallet:** `6dUaYX9Z6aQPY66BgD4yzu1saifGAZLrhQqF9BugJxJ1`
    - Tags: ["Automated Exfiltration Pattern"]
- **Wallet:** `ACSzfEnXbGaxBN1iD2pR1C6tQYSiBvqGPx8Wx1ZTbV2o`
    - Tags: ["Fund Churning", "Advanced Obfuscation Techniques"]
- **Wallet:** `BPzzj8pmwaREUCjTQs5bk5BSdowx61R1cWtQ4Try5838`
    - Tags: ["Automated Exfiltration Pattern"]
- **Wallet:** `CdkLi5GK8kGTNmHCTe1dem2dXxgU2V2Yxh5s4xPuk9UY`

    - Tags: ["Automated Exfiltration Pattern"]
- **Wallet:** `DanYJfkWBkkbZnvngPZUyGVF8GDT2B9MkaUDtYUMFwHK`
    - Tags: ["Fund Churning", "Advanced Obfuscation Techniques"]
- **Wallet:** `E8s4wqQrGnr4BPVBxG5mNGvojux5BwDBSaiqdkEY2fBm`
    - Tags: ["Fund Churning"]

The Future is Open Source:
Despite the hackathon's limitations, I am immensely proud of what was built. HackerDex demonstrated the viability of combining heuristic analysis, database intelligence, and OSINT to detect complex patterns on Solana.
My hope and intention are that this project does not end here. By releasing it as **open source**, I invite the security community, Rust developers, and blockchain analysts to join this adventure. There is enormous potential to refine existing heuristics, add new detections, implement the missing features (like liquidity calculation and real RPC tracing), and build a truly powerful tool to protect the Solana ecosystem.
May HackerDex grow, evolve, and become a valuable resource for everyone concerned with security and transparency on the solana blockchain. It was a fantastic challenge, and I look forward to seeing where community collaboration can take this project.