**Detecting Suspicious Activity on Solana using On-Chain Analytics**

**Objective:**

To identify and expose fraudulent or manipulative wallet behaviours on the Solana blockchain using real-time on-chain data from Flipside Crypto. This analysis was submitted as part of a Solana ecosystem bounty challenge.

**Step-by-Step Breakdown of Findings: Detecting Suspicious Wallet Activity on Solana**

**Step 1: Suspicious Self-Transfers (Sender = Receiver)**

**What we did:**

* Queried all transfers on Solana in the last 30 days where the TX\_FROM = TX\_TO.
* Focused on SOL transfers (MINT = So111...12), which are native to the Solana network.
* Counted how many self-transfers each wallet made per day.

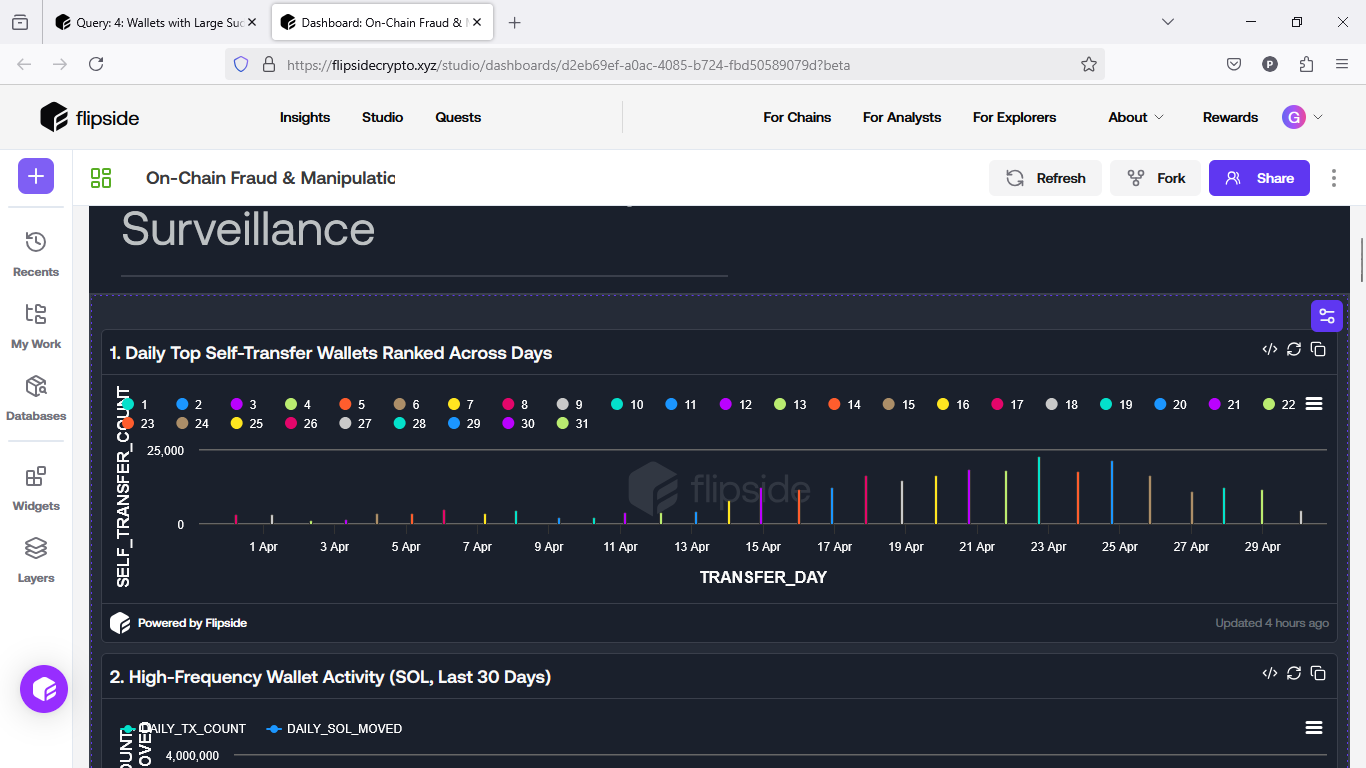
**Why it matters:**

* Self-transfers are rarely used in regular user behaviour.
* They can indicate:
  + Wash trading
  + Attempted Sybil attacks
  + Gaming of airdrop metrics

**What we found:**

* Certain wallets made dozens to hundreds of transfers to themselves in a day.
* Some wallets consistently appeared as top self-transfer actors across multiple days.

**Query Used and Visualization**



1. WITH self\_transfer\_activity AS (

2. SELECT

3. DATE\_TRUNC('day', BLOCK\_TIMESTAMP) AS transfer\_day,

4. TX\_FROM AS wallet,

5. COUNT(\*) AS self\_transfer\_count,

6. SUM(AMOUNT / 1e9) AS total\_sol\_transferred

7. FROM solana.core.fact\_transfers

8. WHERE

9. BLOCK\_TIMESTAMP >= CURRENT\_DATE - INTERVAL '30 days'

10. AND TX\_FROM = TX\_TO

11. AND MINT = 'So11111111111111111111111111111111111111112' -- SOL

12. GROUP BY 1, 2

13. ),

14.

15. daily\_top\_wallets AS (

16. SELECT \*

17. FROM (

18. SELECT \*,

19. ROW\_NUMBER() OVER (PARTITION BY transfer\_day ORDER BY self\_transfer\_count DESC) AS daily\_rank

20. FROM self\_transfer\_activity

21. ) sub

22. WHERE daily\_rank = 1

23. ),

24.

25. final\_ranked AS (

26. SELECT \*,

27. RANK() OVER (ORDER BY self\_transfer\_count DESC) AS overall\_rank

28. FROM daily\_top\_wallets

29. )

30.

31. SELECT \*

32. FROM final\_ranked

33. ORDER BY overall\_rank;

34.

**Step 2: High-Frequency Transfers in Short Windows**

**What we did:**

* Aggregated transaction counts per wallet per day.
* Looked for wallets making unusually high volumes of transactions — often hundreds in 24 hours.
* Calculated how much SOL was moved in total, regardless of receiver.

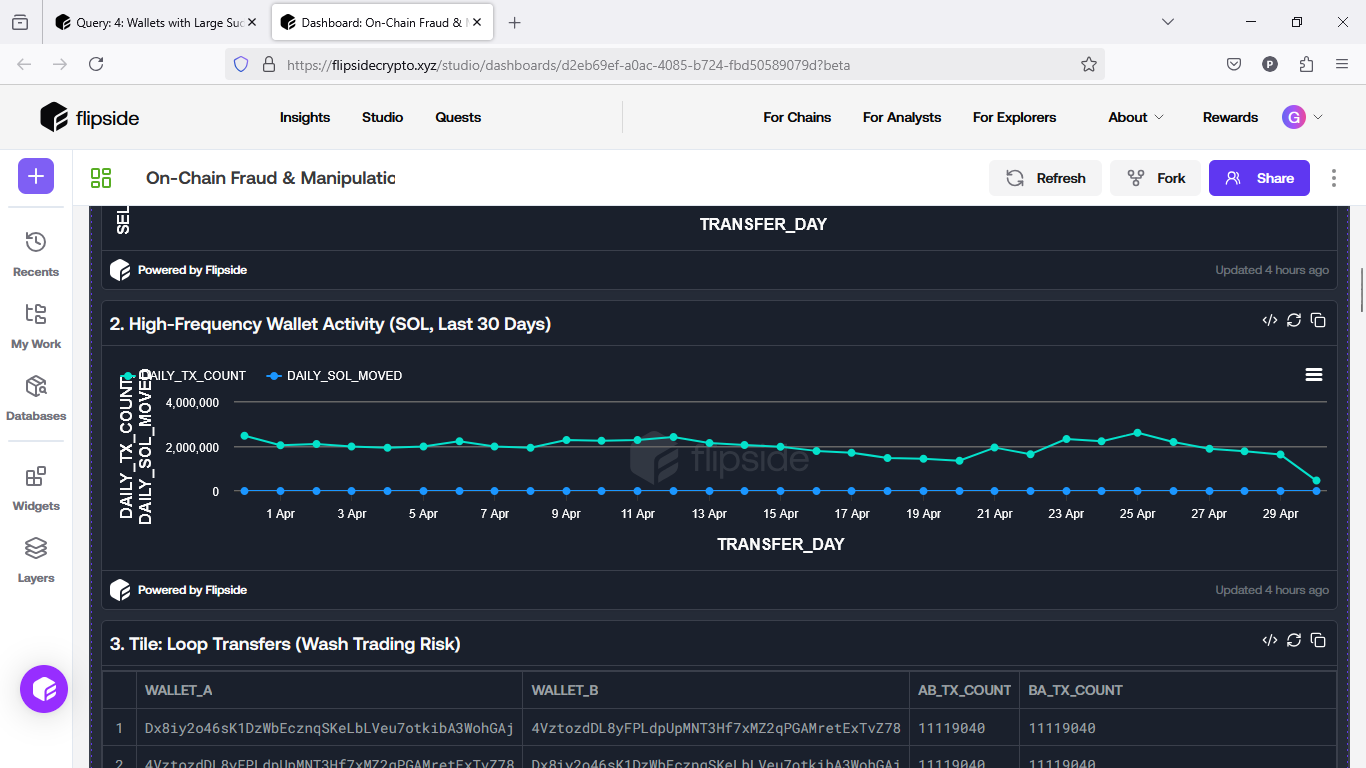
**Why it matters:**

* Bots or scripts often use high-frequency transactions to:
  + Mimic user activity
  + Farm network-based incentives
  + Disguise coordinated manipulation

**What we found:**

* Some wallets had extremely high transfer counts, often sending tiny amounts of SOL.
* Many showed burst activity for 1–2 days and then vanished — another red flag.

**Query Used and Visualization**

****

1. WITH wallet\_daily\_activity AS (

2. SELECT

3. DATE\_TRUNC('day', BLOCK\_TIMESTAMP) AS transfer\_day,

4. TX\_FROM AS wallet,

5. COUNT(\*) AS daily\_tx\_count,

6. SUM(AMOUNT / 1e9) AS daily\_sol\_moved

7. FROM solana.core.fact\_transfers

8. WHERE

9. BLOCK\_TIMESTAMP >= CURRENT\_DATE - INTERVAL '30 days'

10. AND MINT = 'So11111111111111111111111111111111111111112' -- SOL

11. GROUP BY 1, 2

12. ),

13.

14. daily\_top\_wallets AS (

15. SELECT \*

16. FROM (

17. SELECT \*,

18. ROW\_NUMBER() OVER (PARTITION BY transfer\_day ORDER BY daily\_tx\_count DESC) AS daily\_rank

19. FROM wallet\_daily\_activity

20. ) ranked

21. WHERE daily\_rank = 1

22. ),

23.

24. final\_ranked\_wallets AS (

25. SELECT \*,

26. RANK() OVER (ORDER BY daily\_tx\_count DESC) AS overall\_rank

27. FROM daily\_top\_wallets

28. )

29.

30. SELECT \*

31. FROM final\_ranked\_wallets

32. ORDER BY overall\_rank;

33.

**Step 3: Loop Transfers Between Wallet Pairs (A ↔ B)**

**What we did:**

* Tracked transfer flows between wallet pairs.
* Flagged wallet pairs that exchanged tokens back and forth repeatedly over a short time period.
* Checked for repeated usage of the same token and similar transfer amounts.

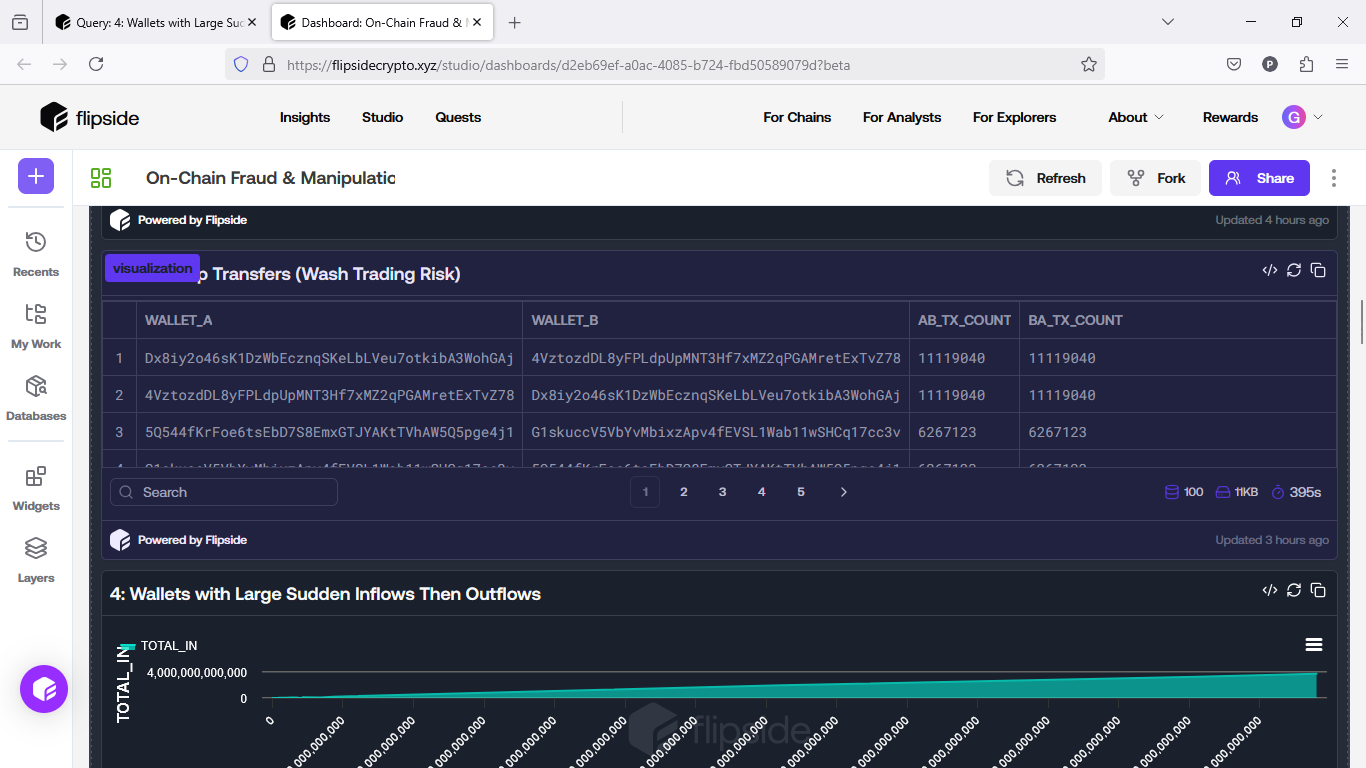
**Why it matters:**

* Loop transfers often simulate organic market activity.
* Used in wash trading to fake volume on DEXs or NFT platforms.
* Makes protocols or tokens look more active than they are.

**What we found:**

* Identified wallet pairs with consistent back-and-forth movement of the same assets.
* Some executed dozens of trades per day without significant value change — indicative of spoofed behaviour.

**Query Used and Visualization**



1. SELECT

2. f1.TX\_FROM AS wallet\_a,

3. f1.TX\_TO AS wallet\_b,

4. COUNT(\*) AS ab\_tx\_count,

5. (

6. SELECT COUNT(\*)

7. FROM solana.core.fact\_transfers f2

8. WHERE f2.TX\_FROM = f1.TX\_TO AND f2.TX\_TO = f1.TX\_FROM

9. AND f2.BLOCK\_TIMESTAMP >= CURRENT\_DATE - INTERVAL '30 days'

10. ) AS ba\_tx\_count

11. FROM solana.core.fact\_transfers f1

12. WHERE f1.BLOCK\_TIMESTAMP >= CURRENT\_DATE - INTERVAL '30 days'

13. GROUP BY wallet\_a, wallet\_b

14. HAVING ab\_tx\_count >= 5 AND ba\_tx\_count >= 5

15. ORDER BY ab\_tx\_count + ba\_tx\_count DESC;

16. limit 100

**Step 4: Wallets with Large Sudden Inflows Then Outflows**

**What we did:**

* Searched for wallets receiving a large amount of SOL in one or two transactions.
* Tracked how fast these wallets sent the SOL back out, and to how many recipients.
* Measured net balance changes over time.

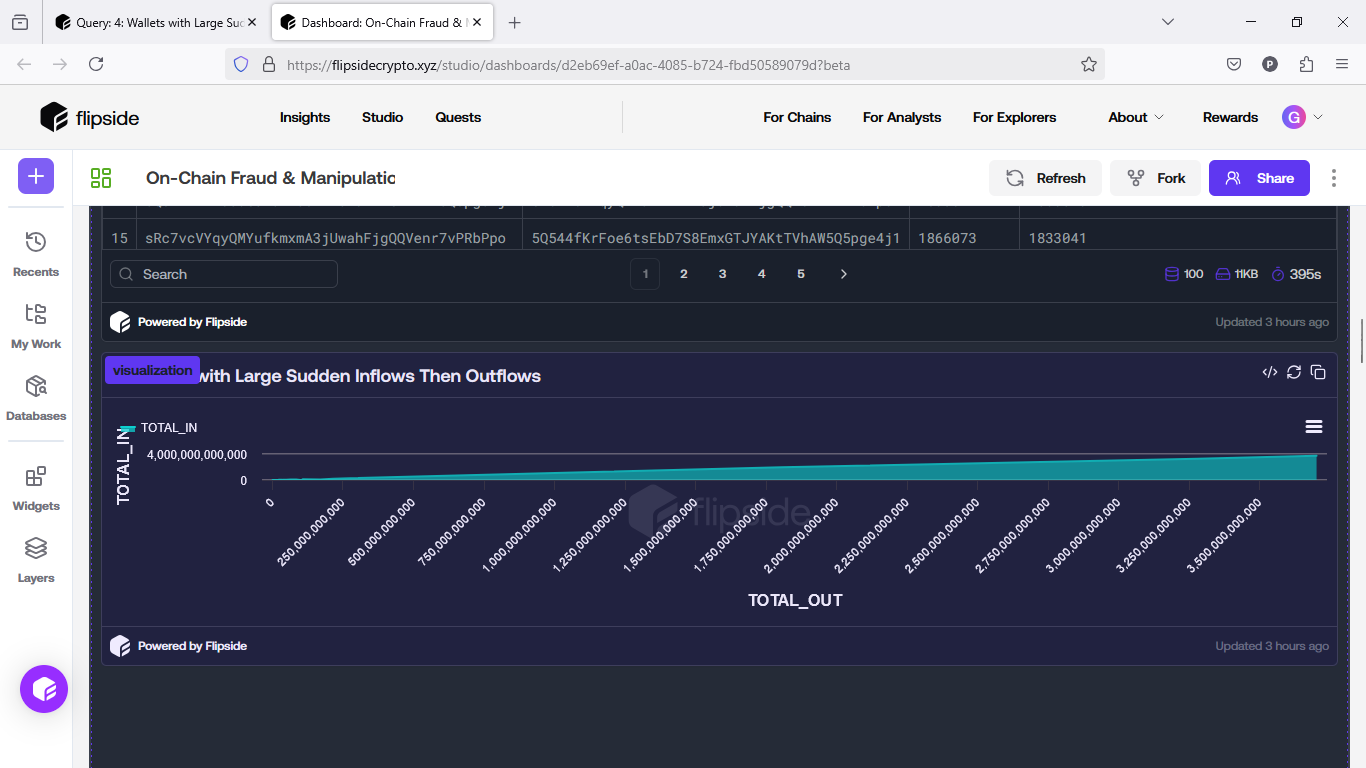
**Why it matters:**

* These patterns may indicate:
  + Flash loan usage or abuse
  + Front-running or arbitrage
  + Exit scams or laundering

**What we found:**

* Several wallets received large inflows, paused briefly, then emptied out quickly.
* Some of these also matched behavior in Steps 1–3 — adding to their risk profile.

**Query Used and Visualization**



1. WITH flow\_summary AS (

2. SELECT

3. TX\_TO AS wallet,

4. SUM(AMOUNT / 1e6) AS total\_in

5. FROM solana.core.fact\_transfers

6. WHERE BLOCK\_TIMESTAMP >= CURRENT\_DATE - INTERVAL '7 days'

7. GROUP BY TX\_TO

8. ), outflow\_summary AS (

9. SELECT

10. TX\_FROM AS wallet,

11. SUM(AMOUNT / 1e6) AS total\_out

12. FROM solana.core.fact\_transfers

13. WHERE BLOCK\_TIMESTAMP >= CURRENT\_DATE - INTERVAL '7 days'

14. GROUP BY TX\_FROM

15. )

16.

17. SELECT

18. f.wallet,

19. f.total\_in,

20. o.total\_out,

21. (o.total\_out / NULLIF(f.total\_in, 0)) AS outflow\_ratio

22. FROM flow\_summary f

23. JOIN outflow\_summary o ON f.wallet = o.wallet

24. WHERE f.total\_in >= 100000 AND o.total\_out >= 100000

25. AND (o.total\_out / NULLIF(f.total\_in, 0)) >= 0.9

26. ORDER BY outflow\_ratio DESC;

27.

**📈 Deliverables:**

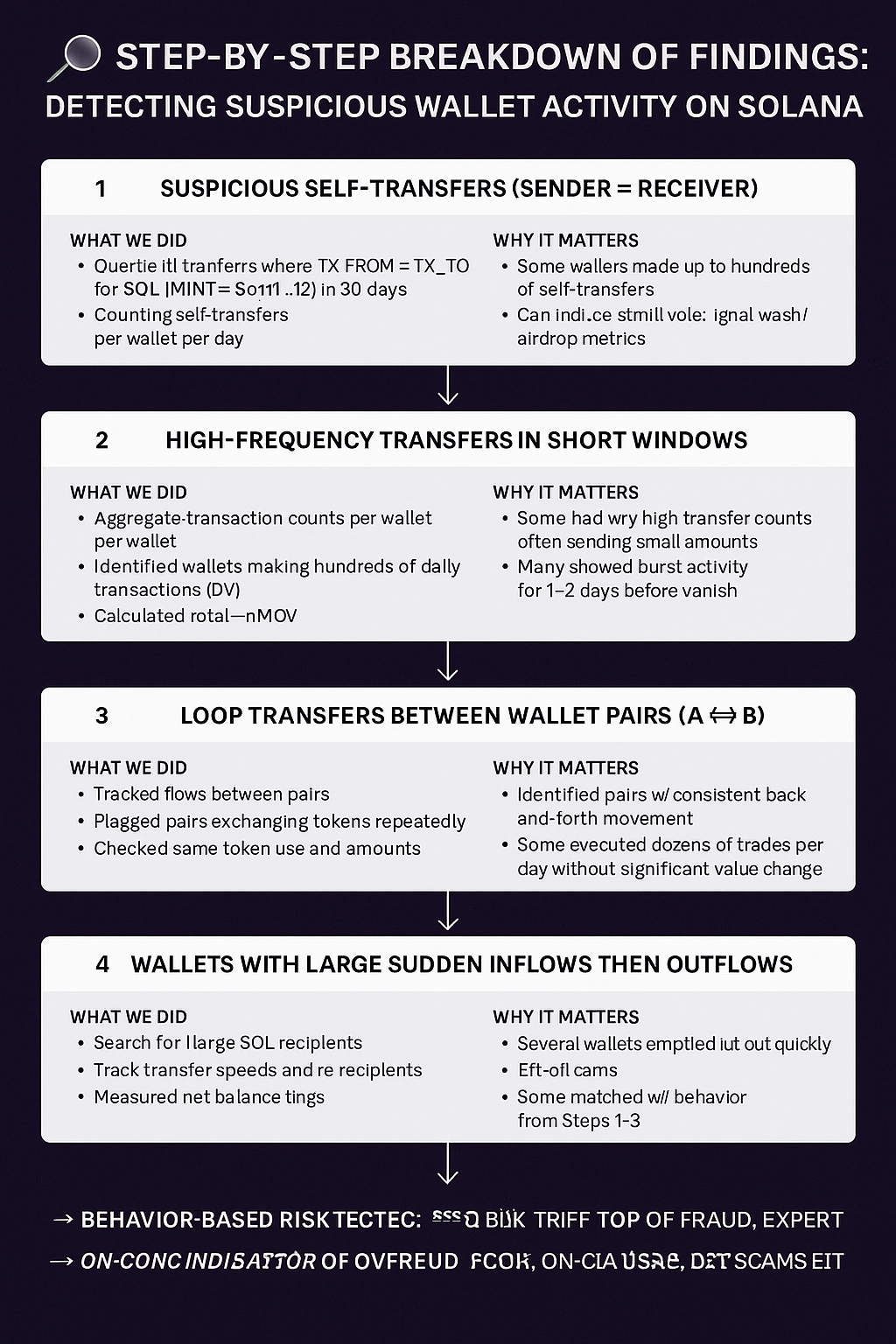
* A Flipside-powered dashboard visualizing all four behaviors with daily breakdowns.
* An X thread summarizing findings and implications.
* A dark-themed infographic summarizing the detection pipeline and risk signals.

**🧠 Impact & Insights:**

This project not only highlighted suspicious wallet behaviors but also proposed a practical risk-scoring approach for Solana-based projects and exchanges to integrate into fraud detection systems.

**🔗 Links:**

* 👉 [**Full Dashboard**](https://flipsidecrypto.xyz/ghostiemoh/on-chain-fraud-manipulation-detector-solana-surveillance-_VVM1H)
* 🧵 [**Twitter Thread Summary**](https://x.com/Ghostiemoh/status/1917582832089850072)
* 📎 **Infographic** (see below)



**✅ Conclusion: Multi-Signal Risk Detection**

By combining all four methods, we built a profile of wallets that:

* Engage in **self-transfers**
* Trigger **high-frequency activity**
* Participate in **ping-pong loops**
* Display **sudden large flows**