INCA DIGITAL

# Center of Excellence in AML

●●●

Cybercrime and Crypto

INCA DIGITAL

# Bybit Hack

●●●

$1.4B in ETH Stolen, Insolvency Concerns Rise

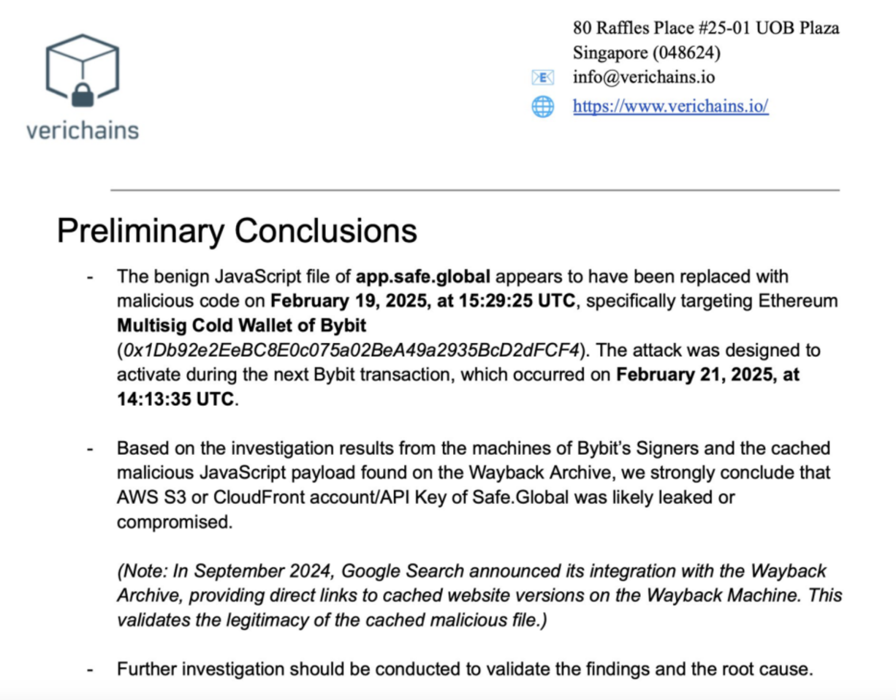
# $1.4+ Billion Stolen by Lazarus Group

- North Korean State Actors, specifically TraderTraitor, targeted & hacked Bybit's ETH cold wallet.
- 514,722 ETH + ETH derivative tokens withdrawn from Bybit.
    - 94.7% of Bybit's ETH holdings.

| Asset | Quantity | Approximate $ Value |
|---|---|---|
| ETH | 401,346.76 | $1.1 billion |
| Lido Staked ETH | 90,375.54 | $250.6 million |
| Mantle Restaked ETH | 15,000* | $44.0 million |
| Mantle Staked ETH | 8,000 | $23.5 million |

# Lazarus Group Targeted Bybit's ETH Wallet

- Bybit's four multisig signers made a routine transaction.
- Hacker(s) spoofed transaction details on Safe Wallet interface.
    - Signed transaction changed the smart contract logic of Bybit's ETH cold wallet.
- Malicious code originated from Safe Wallet's infrastructure, not Bybit's.
    - A Safe Wallet developer machine was compromised.
    - A Javascript file of app.safe.global was replaced with malicious code on February 19.
    - Code specifically targeted Bybit's ETH multisig wallet on the next transaction made.



verichains

80 Raffles Place #25-01 UOB Plaza
Singapore (048624)
info@verichains.io
https://www.verichains.io/

## Preliminary Conclusions

- The benign JavaScript file of **app.safe.global** appears to have been replaced with malicious code on **February 19, 2025, at 15:29:25 UTC**, specifically targeting Ethereum **Multisig Cold Wallet of Bybit** (*0x1Db92e2EeBC8E0c075a02BeA49a2935BcD2dFCF4*). The attack was designed to activate during the next Bybit transaction, which occurred on **February 21, 2025, at 14:13:35 UTC**.

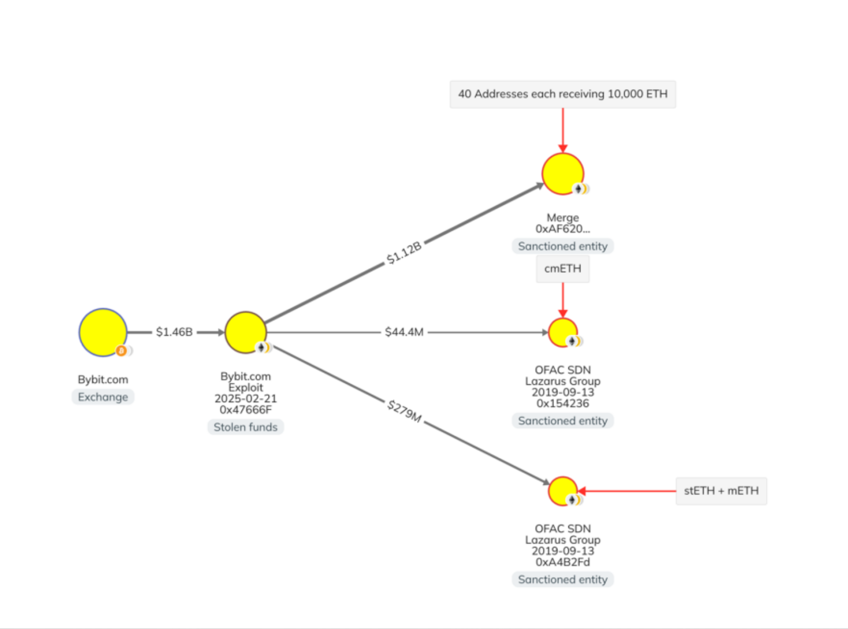
- Based on the investigation results from the machines of Bybit's Signers and the cached malicious JavaScript payload found on the Wayback Archive, we strongly conclude that AWS S3 or CloudFront account/API Key of Safe.Global was likely leaked or compromised.

  *(Note: In September 2024, Google Search announced its integration with the Wayback Archive, providing direct links to cached website versions on the Wayback Machine. This validates the legitimacy of the cached malicious file.)*

- Further investigation should be conducted to validate the findings and the root cause.

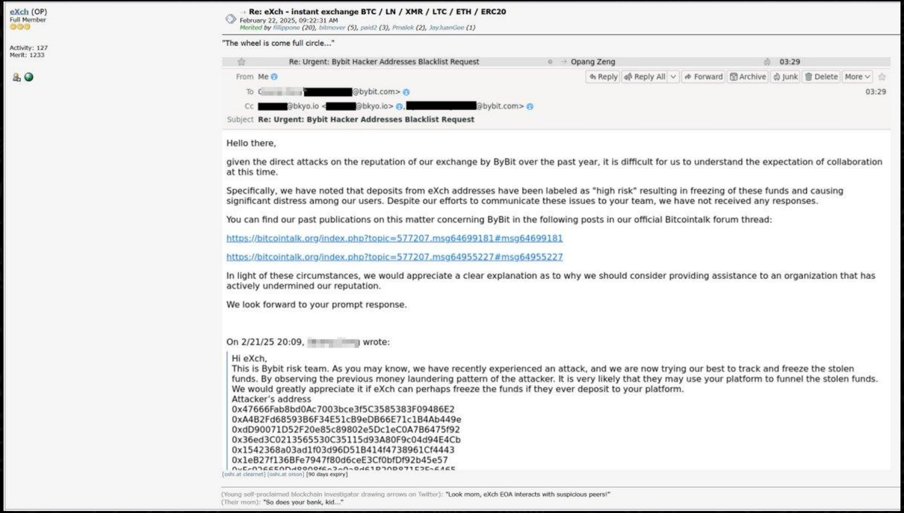
# Lazarus Quickly Laundering ETH

- Hacker(s) have sent funds to more than 13,000 addresses.
    - Difficult for exchanges to monitor and freeze.
- Exchanges, including Mantle and Bitget, have frozen $42.8 million (3.07% of total hack amount).
    - Majority ( 15,000 cmETH) recovered by the mETH Protocol Team immediately after hack.



# Lack of Cooperation by eXch

- Hacker(s) have sent $94.2 million to eXch, but they have refused to respond to Bybit's requests.
- eXch is a centralized, non KYC exchange registered in Belize.
- eXch uses Thorchain when lack of liquidity.
  - Thorchain primarily used to bridge ETH into BTC.
  - 3 validators voted to halt ETH trading on Thorchain.
  - Lead dev stepped down on February 27.



eXch (OP)
Full Member

Activity: 127
Merit: 1233

Re: eXch - instant exchange BTC / LN / XMR / LTC / ETH / ERC20
February 22, 2025, 09:22:31 AM
Merited by fillippone (20), bitmover (5), paid2 (3), Pmalek (2), JayJuanGee (1)

"The wheel is come full circle..."

Re: Urgent: Bybit Hacker Addresses Blacklist Request → Opang Zeng 03:29

From Me
To C[redacted]@bybit.com> 03:29
Cc [redacted]@bkyo.io <[redacted]@bkyo.io>, [redacted]@bybit.com>
Subject **Re: Urgent: Bybit Hacker Addresses Blacklist Request**

Hello there,

given the direct attacks on the reputation of our exchange by ByBit over the past year, it is difficult for us to understand the expectation of collaboration at this time.

Specifically, we have noted that deposits from eXch addresses have been labeled as "high risk" resulting in freezing of these funds and causing significant distress among our users. Despite our efforts to communicate these issues to your team, we have not received any responses.

You can find our past publications on this matter concerning ByBit in the following posts in our official Bitcointalk forum thread:

https://bitcointalk.org/index.php?topic=577207.msg64699181#msg64699181

https://bitcointalk.org/index.php?topic=577207.msg64955227#msg64955227

In light of these circumstances, we would appreciate a clear explanation as to why we should consider providing assistance to an organization that has actively undermined our reputation.

We look forward to your prompt response.

On 2/21/25 20:09, [redacted] wrote:

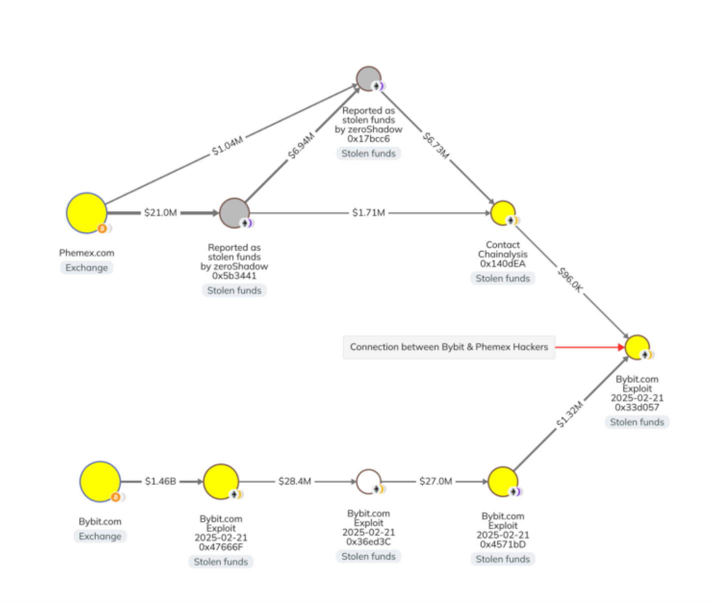
> Hi eXch,
> This is Bybit risk team. As you may know, we have recently experienced an attack, and we are now trying our best to track and freeze the stolen funds. By observing the previous money laundering pattern of the attacker. It is very likely that they may use your platform to funnel the stolen funds. We would greatly appreciate it if eXch can perhaps freeze the funds if they ever deposit to your platform.
> Attacker's address
> 0x47666Fab8bd0Ac7003bce3f5C3585383F09486E2
> 0xA4B2Fd68593B6F34E51cB9eDB66E71c1B4Ab449e
> 0xdD90071D52F20e85c89802e5Dc1eC0A7B6475f92
> 0x36ed3C0213565530C35115d93A80F9c04d94E4Cb
> 0x1542368a03ad1f03d96D51B414f4738961Cf4443
> 0x1eB27f136BFe7947f80d6ceE3Cf0bfDf92b45e57

[oshi.at clearnet] [oshi.at onion] [90 days expiry]

(Young self-proclaimed blockchain investigator drawing arrows on Twitter): "Look mom, eXch EOA interacts with suspicious peers!"
(Their mom): "So does your bank, kid..."

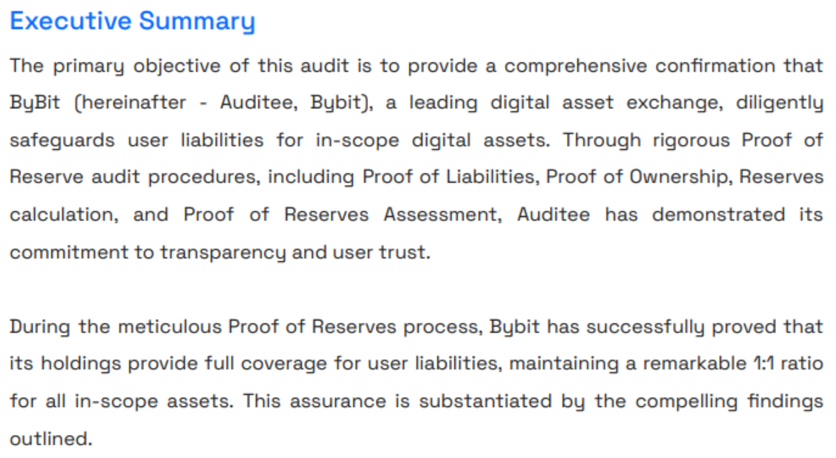
# Address Overlap Leads to Lazarus Connection

- In January 2025, Phemex, a Singapore based centralized exchange was hacked for more than $85 million by Lazarus Group.
  - The hackers behind Phemex sent approximately $96,000 to 0x33d05.
  - Bybit hackers sent $1.32 million into this address.
- Similarities to Previous Lazarus Hacks
  - WazirX
  - Radiant Capital


$1.04M
$6.94M
$6.73M
Reported as stolen funds by zeroShadow 0x17bcc6
Stolen funds
$21.0M
$1.71M
Phemex.com
Exchange
Reported as stolen funds by zeroShadow 0x5b3441
Stolen funds
Contact Chainalysis 0x140dEA
Stolen funds
$96.0K
Connection between Bybit & Phemex Hackers
Bybit.com Exploit 2025-02-21 0x33d057
Stolen funds
$1.32M
$1.46B
$28.4M
$27.0M
Bybit.com
Exchange
Bybit.com Exploit 2025-02-21 0x47666F
Stolen funds
Bybit.com Exploit 2025-02-21 0x36ed3C
Stolen funds
Bybit.com Exploit 2025-02-21 0x4571bD
Stolen funds

# Bybit at Insolvency Risk

- Majority of Bybit's ETH holdings were stolen.
    - 514,722 ETH stolen.
    - 543,453 ETH in reserves at time of hack.
- So far, Bybit has been able to process all of its withdrawals.
    - Inca continues to monitor for user reports.
- Bybit secured the total amount of hacked ETH through bridge loans, OTC purchases, and other purchases.
    - Updated Proof of Reserves report on February 23 indicates Bybit returned to full 1:1 backing on client assets.



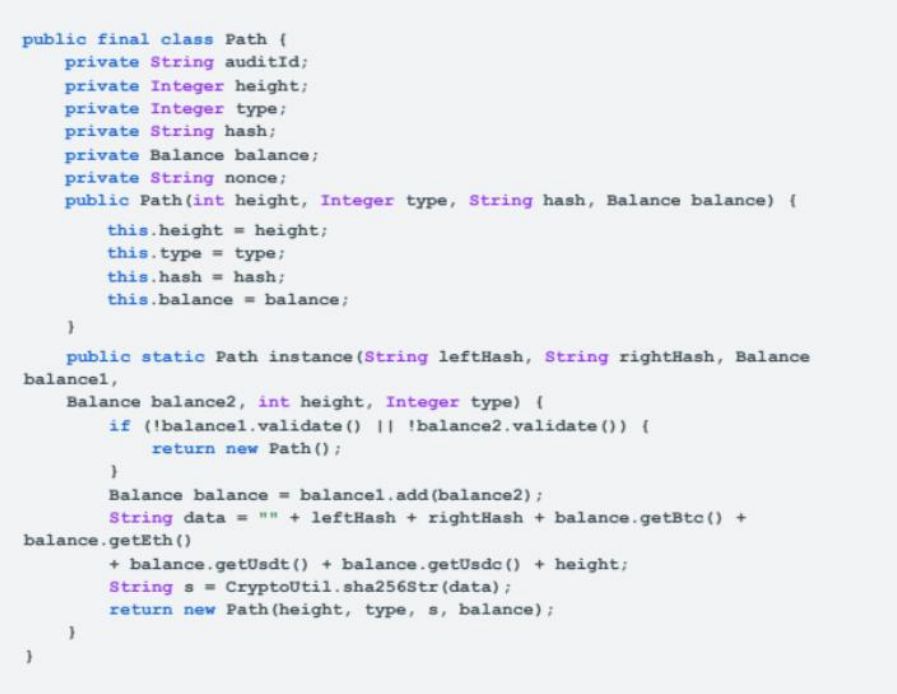
## Executive Summary

The primary objective of this audit is to provide a comprehensive confirmation that ByBit (hereinafter - Auditee, Bybit), a leading digital asset exchange, diligently safeguards user liabilities for in-scope digital assets. Through rigorous Proof of Reserve audit procedures, including Proof of Liabilities, Proof of Ownership, Reserves calculation, and Proof of Reserves Assessment, Auditee has demonstrated its commitment to transparency and user trust.

During the meticulous Proof of Reserves process, Bybit has successfully proved that its holdings provide full coverage for user liabilities, maintaining a remarkable 1:1 ratio for all in-scope assets. This assurance is substantiated by the compelling findings outlined.

# Bybit may be Underreporting Liabilities

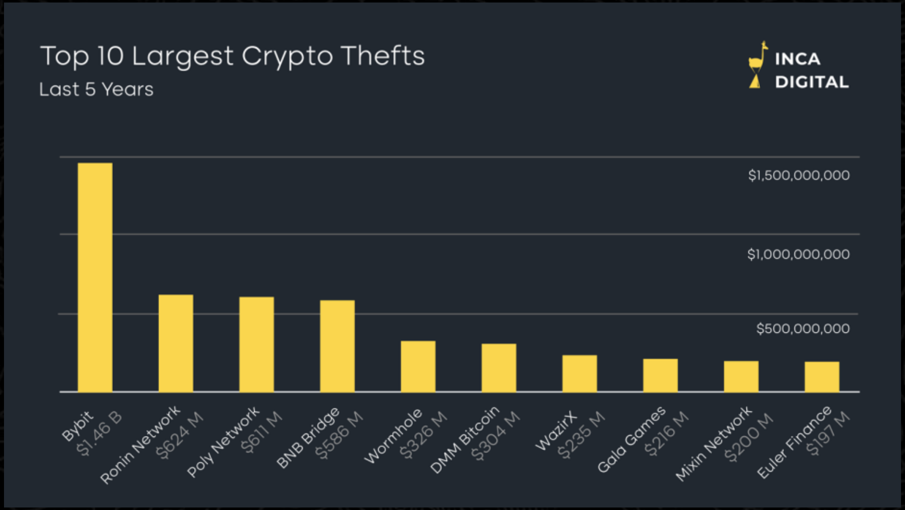
- Bybit uses a Merkle tree implementation that may enable them to underreport liabilities.
    - The 'Path' instance can be constructed to only reflect the highest balance while the remaining balances are omitted.
        - The total liability displayed would be significantly lower than the actual liability sum.
- A sudden large mass of withdrawals could lead to Bybit not being able to meet customer liabilities.



```
public final class Path {
    private String auditId;
    private Integer height;
    private Integer type;
    private String hash;
    private Balance balance;
    private String nonce;
    public Path(int height, Integer type, String hash, Balance balance) {
        this.height = height;
        this.type = type;
        this.hash = hash;
        this.balance = balance;
    }
    public static Path instance(String leftHash, String rightHash, Balance
balance1,
    Balance balance2, int height, Integer type) {
        if (!balance1.validate() || !balance2.validate()) {
            return new Path();
        }
        Balance balance = balance1.add(balance2);
        String data = "" + leftHash + rightHash + balance.getBtc() +
balance.getEth()
        + balance.getUsdt() + balance.getUsdc() + height;
        String s = CryptoUtil.sha256Str(data);
        return new Path(height, type, s, balance);
    }
}
```

# Hacks will Continue to get Worse

- Largest cryptocurrency theft to date, and nearly $800 million more than Ronin Network's $624 million hack in 2022.
- Lazarus Group continuously evolving.
  - Laundering outpacing tracing overwhelms exchanges.
  - Always searching for new attack vectors.
  - Traditional intelligence techniques similar to Inca.

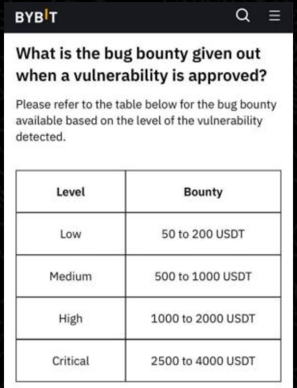


Top 10 Largest Crypto Thefts

Last 5 Years

# Preventing Future Attacks

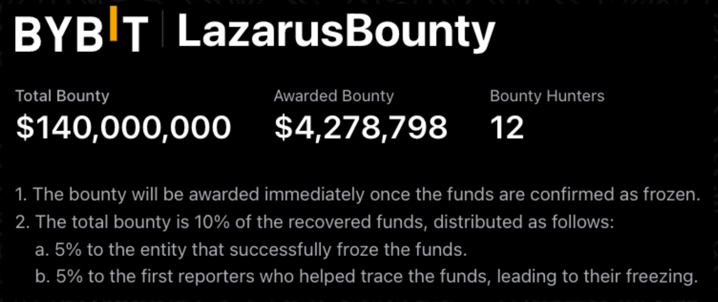
- Risk intelligence.
- Coordination between exchanges
- Custody risk mitigation
    - Separation of Cold Wallets
    - Bug Bounty Programs
        - Higher bounties encourage white hats to monitor for vulnerabilities.
        - Small price relative to 10% bounty instituted by Bybit on stolen funds.
    - Verification Tools
        - Ensure transaction shown is what is actually being signed.



**What is the bug bounty given out when a vulnerability is approved?**

Please refer to the table below for the bug bounty available based on the level of the vulnerability detected.

| Level | Bounty |
|---|---|
| Low | 50 to 200 USDT |
| Medium | 500 to 1000 USDT |
| High | 1000 to 2000 USDT |
| Critical | 2500 to 4000 USDT |

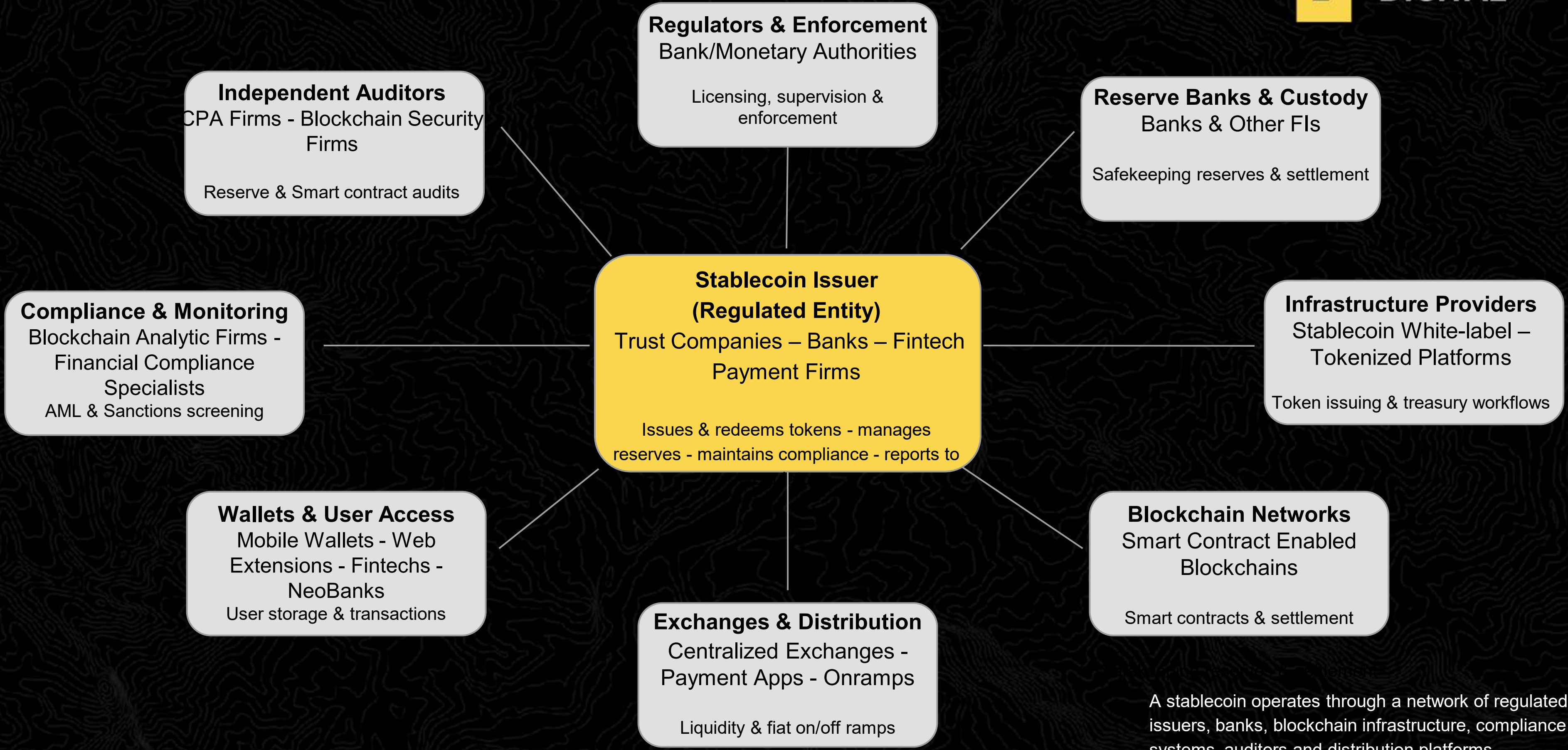


BYBIT | LazarusBounty

| Total Bounty | Awarded Bounty | Bounty Hunters |
|---|---|---|
| $140,000,000 | $4,278,798 | 12 |

1. The bounty will be awarded immediately once the funds are confirmed as frozen.
2. The total bounty is 10% of the recovered funds, distributed as follows:
    a. 5% to the entity that successfully froze the funds.
    b. 5% to the first reporters who helped trace the funds, leading to their freezing.

# Stablecoin Ecosystem Map



**Regulators & Enforcement**
Bank/Monetary Authorities
Licensing, supervision & enforcement

**Independent Auditors**
CPA Firms - Blockchain Security Firms
Reserve & Smart contract audits

**Reserve Banks & Custody**
Banks & Other FIs
Safekeeping reserves & settlement

**Compliance & Monitoring**
Blockchain Analytic Firms - Financial Compliance Specialists
AML & Sanctions screening

**Stablecoin Issuer (Regulated Entity)**
Trust Companies – Banks – Fintech Payment Firms
Issues & redeems tokens - manages reserves - maintains compliance - reports to

**Infrastructure Providers**
Stablecoin White-label – Tokenized Platforms
Token issuing & treasury workflows

**Wallets & User Access**
Mobile Wallets - Web Extensions - Fintechs - NeoBanks
User storage & transactions

**Blockchain Networks**
Smart Contract Enabled Blockchains
Smart contracts & settlement

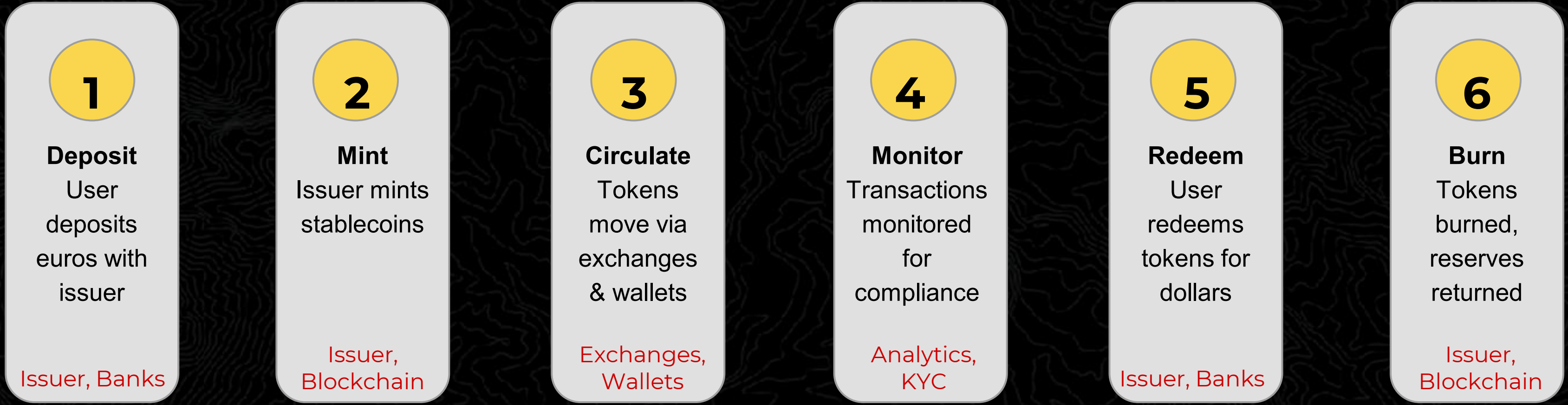
**Exchanges & Distribution**
Centralized Exchanges - Payment Apps - Onramps
Liquidity & fiat on/off ramps

A stablecoin operates through a network of regulated issuers, banks, blockchain infrastructure, compliance systems, auditors and distribution platforms.

INCA DIGITAL

# Lifecycle of a Stablecoin Transaction

At each stage, the stablecoin issuer remains the regulated entity responsible for maintaining reserves, regulatory reporting, and compliance programs.



1 **Deposit** User deposits euros with issuer — Issuer, Banks

2 **Mint** Issuer mints stablecoins — Issuer, Blockchain

3 **Circulate** Tokens move via exchanges & wallets — Exchanges, Wallets

4 **Monitor** Transactions monitored for compliance — Analytics, KYC

5 **Redeem** User redeems tokens for dollars — Issuer, Banks

6 **Burn** Tokens burned, reserves returned — Issuer, Blockchain

**Stakeholders by Stage:**

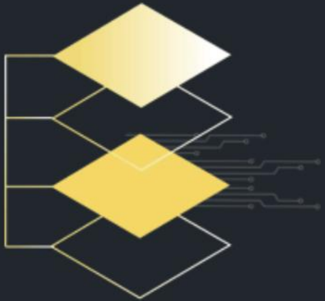
- Deposit/Redeem: Banks, Issuer compliance team
- Mint/Burn: Blockchain networks/infrastructure providers
- Circulate: Exchanges, Wallets, On-ramps
- Monitor: Analytics, KYC, Auditors

INCA DIGITAL

Inca Digital collects complex data and turns it into clear, risk-focused intelligence for crypto and banking.

## Collection

Aggregating multi-source data: real-time trading data, dark web data, blockchain transactions, social media (Twitter, Reddit, Telegram, Discord), and proprietary client data.



## Analysis

Applying AI-driven analytics to unstructured data, detecting trends, anomalies, and emerging threats. Custom models identify tactics, techniques, and procedures (TTPs) impacting your business.

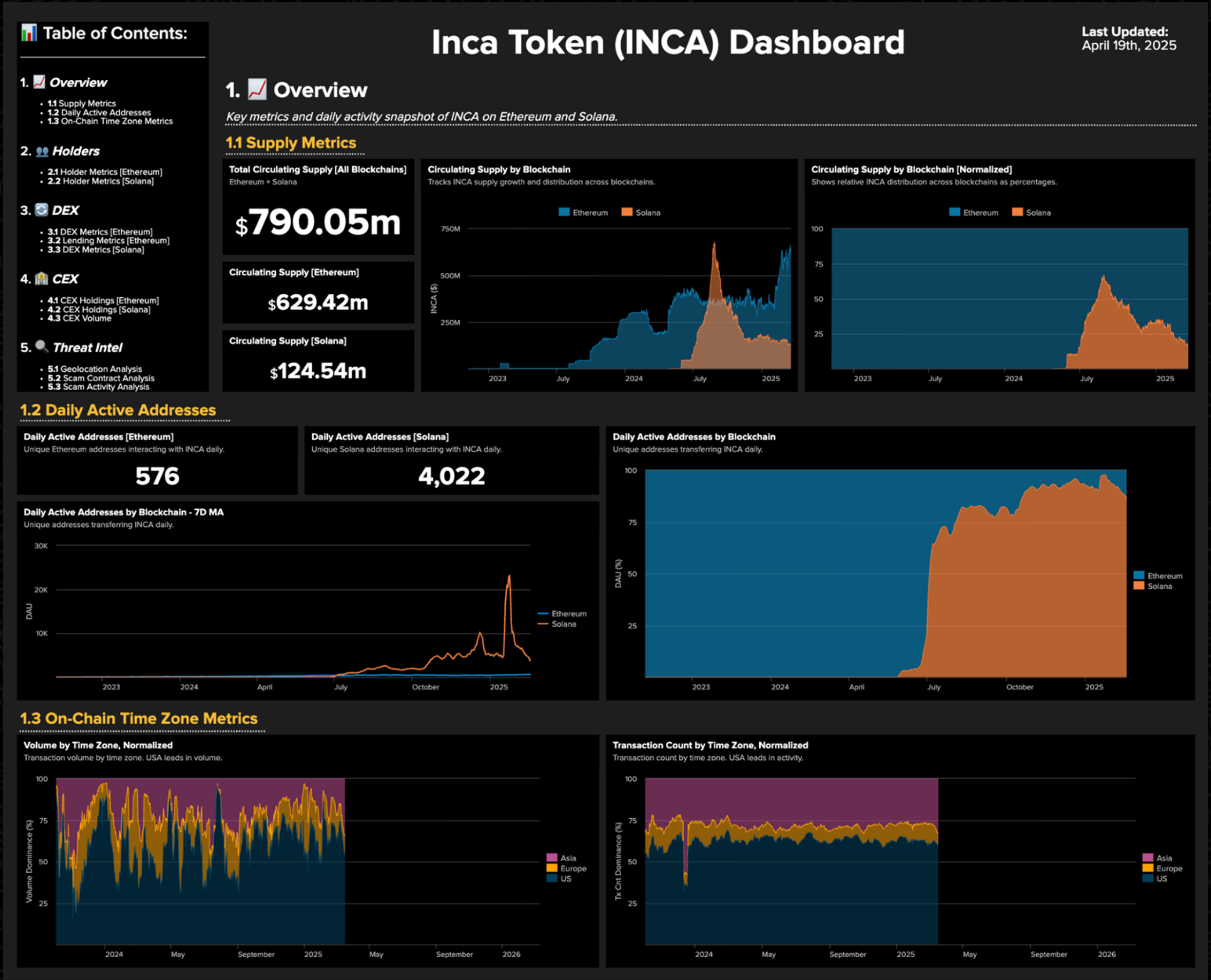
## Intelligence

Delivering actionable insights through tailorec intelligence reports, citation- backed raw data feeds, automated threat flags, and interactive dashboards—all with hands-on support from your assigned military intelligence expert.

## Action

Turning intelligence into outcomes: direct collaboration with law enforcement and regulators, support for BSA/SAR filings, takedown requests, and asset recovery through Inca's litigation division.

INCA DIGITAL



# Inca Token (INCA) Dashboard

**Last Updated:**
April 19th, 2025

## 1. 📈 Overview

*Key metrics and daily activity snapshot of INCA on Ethereum and Solana.*

### 1.1 Supply Metrics

**Total Circulating Supply [All Blockchains]**
Ethereum + Solana

$790.05m

**Circulating Supply [Ethereum]**

$629.42m

**Circulating Supply [Solana]**

$124.54m

**Circulating Supply by Blockchain**
Tracks INCA supply growth and distribution across blockchains.

**Circulating Supply by Blockchain [Normalized]**
Shows relative INCA distribution across blockchains as percentages.

### 1.2 Daily Active Addresses

**Daily Active Addresses [Ethereum]**
Unique Ethereum addresses interacting with INCA daily.

576

**Daily Active Addresses [Solana]**
Unique Solana addresses interacting with INCA daily.

4,022

**Daily Active Addresses by Blockchain - 7D MA**
Unique addresses transferring INCA daily.

**Daily Active Addresses by Blockchain**
Unique addresses transferring INCA daily.

### 1.3 On-Chain Time Zone Metrics

**Volume by Time Zone, Normalized**
Transaction volume by time zone. USA leads in volume.

**Transaction Count by Time Zone, Normalized**
Transaction count by time zone. USA leads in activity.

# 2. 👥 Holders

*Analysis of INCA holder distribution on Ethereum and Solana.*

## 2.1 Holder Metrics [Ethereum]

**Top 100 INCA Holders [Ethereum]**

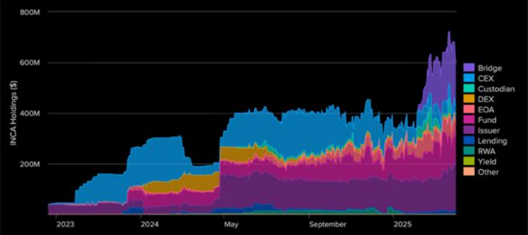
Largest INCA holders on Ethereum ranked by balance. Issuer leads all other holders by 2x.

| | | | | | | |
|---|---|---|---|---|---|---|
| 0x769f...699c | | | $ 23,185,255 | $ 14,126,151 | $ 20,520,531 | $ 22,671,209 |
| 0x6ae4...83e0 | DeFiance Capital | Fund | $ 19,510,204 | $ 0 | $ 0 | $ 0 |
| 0xf5ad...0c79 | Crypto.com: Hot Wallet | CEX | $ 19,798,008 | $ 18,945,652 | $ 847,705 | $ 10,401,042 |
| 0x6f64...dc2b | Crypto.com: Hot Wallet | CEX | $ 16,730,897 | $ -25,133,702 | $ 16,585,211 | $ 16,375,358 |
| 0xb73a...b453 | DeFiance Capital | Fund | $ 16,144,474 | $ 0 | $ 0 | $ 0 |
| 0xfec5...a22d | Issuer: Hot Wallet | Issuer | $ 12,676,018 | $ 171,639 | $ 852,523 | $ 2,903,394 |
| 0xee89...22df | Aave: Aave Ethereum INCA (aEthINCA) | Lending | $ 10,731,860 | $ 3,637,211 | $ 8,337,278 | $ 7,966,246 |
| 0xfc13...165a | Curve.fi: CurveStableSwapNG | DEX | $ 7,859,761 | $ 1,574,248 | $ 1,109,977 | $ 5,235,408 |
| 0xf6db...b4bb | LayerZero: INCALocker | Bridge | $ 7,041,136 | $ 2,548,819 | $ 7,083,374 | $ 6,836,021 |
| 0xbc5c...8cf7 | LayerZero: INCALocker | Bridge | $ 6,951,278 | $ 2,418,161 | $ 7,466,839 | $ 7,384,987 |
| 0x0eef...429c | Bybit: Hot Wallet | CEX | $ 6,055,766 | $ 1,165,897 | $ 1,932,748 | $ 5,499,477 |

‹ Prev 1 2 3 4 5 ... Next ›

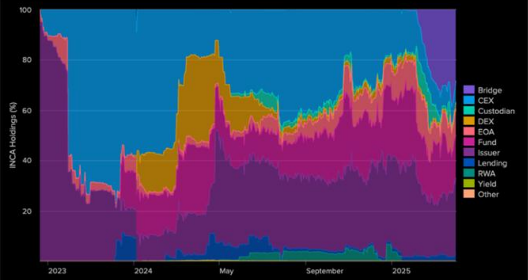
**Holdings by Entity Type Over Time [Ethereum]**

Normalized distribution of INCA holders on Ethereum over time.



**Holdings by Entity Type Over Time, Normalized [Ethereum]**

Normalized distribution of INCA holders on Ethereum over time.



**INCA Holdings by Entity [Ethereum]**

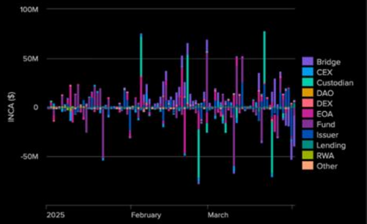
Shows the current INCA holdings by entity type on Ethereum.

| Entity | Balance | 1M Δ | 3M Δ |
|---|---|---|---|
| Issuer | $ 207,308,446 | $ 83,157,157 | $ 84,270,446 |
| Bridge | $ 166,537,335 | $ -8,845,558 | $ 166,160,586 |
| Fund | $ 85,784,664 | $ -66,893,178 | $ 7,346,974 |
| EOA | $ 61,790,465 | $ 15,873,169 | $ 25,059,616 |
| CEX | $ 49,097,996 | $ -8,013,027 | $ -20,983,090 |
| Lending | $ 14,145,841 | $ 3,307,925 | $ 9,390,486 |
| DEX | $ 11,488,708 | $ 4,303,450 | $ 1,066,241 |
| RWA | $ 6,770,188 | | $ -5,360,452 |
| Custodian | $ 3,730,234 | $ -29,704,851 | $ 573,327 |
| DAO | $ 13,874 | $ 0 | $ 0 |

‹ Prev 1 2 Next ›

**Daily INCA Holdings NetFlow by Entity Type [Ethereum]**

Past 3 Months



### 2.1.1 Bridge Holdings [Ethereum]

**Berachain - INCA Holdings**

Total amount of INCA held on Berachain.

**$202,766,283**

**Fraxtal Bridge - INCA Holdings**

Total amount of INCA held on Fraxtal.

**$189,168**

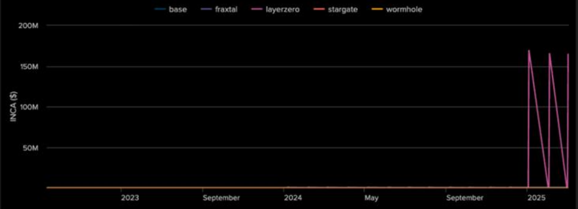
**Wormhole Bridge - INCA Holdings**

Total amount of INCA held on Wormhole.

**$288**

**INCA Holdings by Bridge**

Tracks total amount of INCA held in known bridges over time.

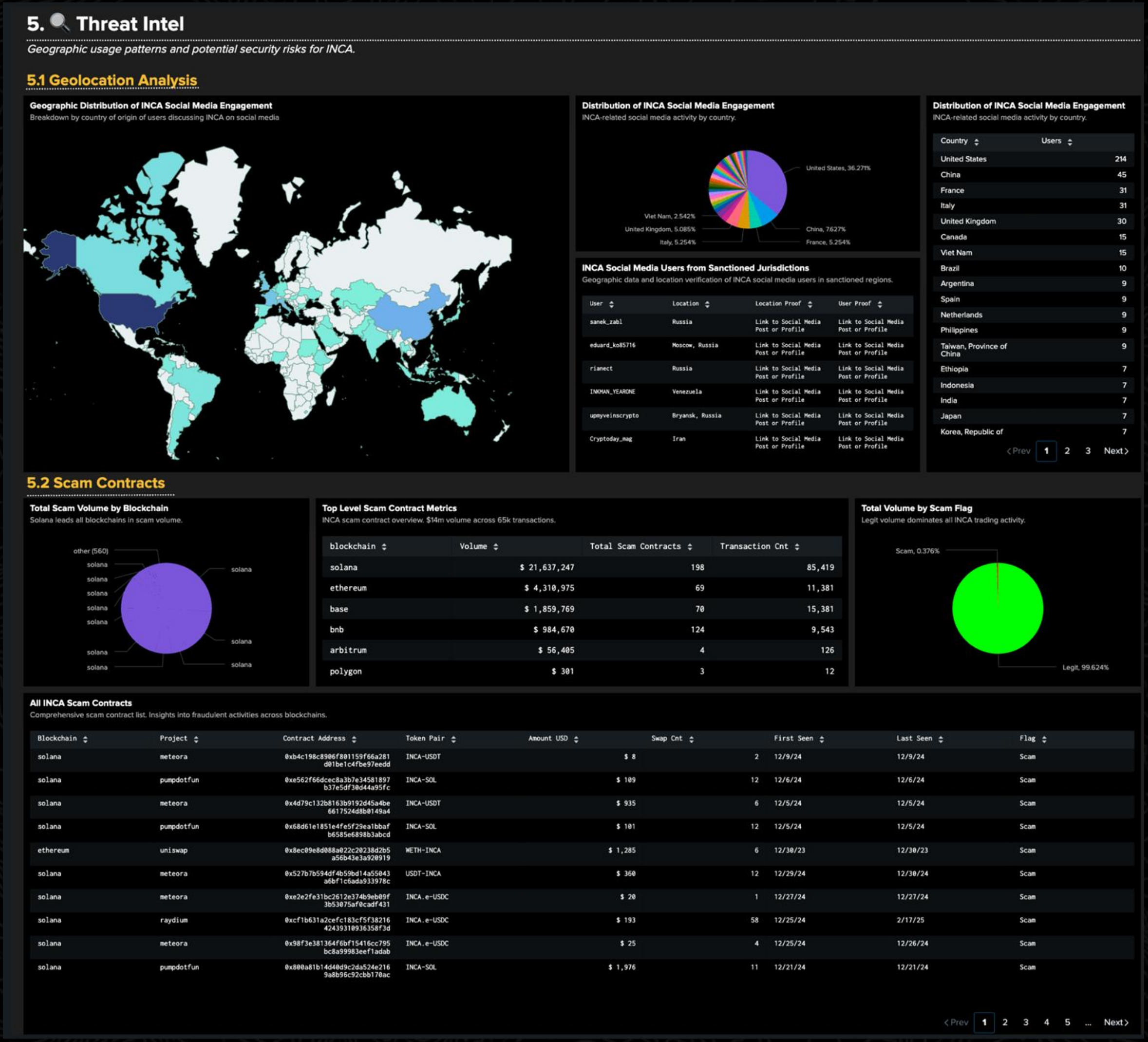


**Top Bridge Users by Holdings - BeraChain**

LayerZero INCAOFTADAPTER

| Address | Label | Balance | Total USD Deposited | Total USD Withdrawm |
|---|---|---|---|---|
| 0xb93a70fee1286a71b98e0b99d39013553d69df65 | yawnn.eth | $ 21,912,737 | $ 23,416,441 | $ -1,503,703 |
| 0xe883bb59d0c5a383cd414cea7c7fbc32902ef027 | | $ 19,009,990 | $ 19,009,990 | $ 0 |
| 0x2ab2c9e5606b933534a829829177383109dc8090 | takeita.eth | $ 17,650,326 | $ 17,961,210 | $ -310,884 |
| 0x9f0c59868ed8052692bc7c94559d9fdb370163f7 | | $ 14,601,000 | $ 14,601,000 | $ 0 |
| 0x829e290ad2c1efaa554b457d4abe881c9af1c9cc | Nexo | $ 12,816,371 | $ 12,816,371 | $ 0 |
| 0x37ee49463da954dcc10f2e4850e7dfe58c555671 | Gnosis Safe Proxy | $ 9,000,000 | $ 9,000,000 | $ 0 |
| 0xd46530bc823808dff2f57c48b5d2e31706bac2e9 | | $ 5,267,857 | $ 5,267,857 | $ 0 |
| 0xdffe69dfcee0e70a71aaf01538d1e50515041066 | | $ 5,000,000 | $ 5,000,000 | $ 0 |
| 0x5e61a5d0a66a49d403c2d999dd69031685dae7fb | | $ 4,565,407 | $ 4,565,407 | $ 0 |
| 0xd78cb3daf491f1143ce08d39dfd558a262038aa7 | | $ 4,507,260 | $ 4,872,802 | $ -365,542 |

‹ Prev 1 2 3 4 5 ... Next ›



## 5. Threat Intel

*Geographic usage patterns and potential security risks for INCA.*

### 5.1 Geolocation Analysis

**Geographic Distribution of INCA Social Media Engagement**

Breakdown by country of origin of users discussing INCA on social media

**Distribution of INCA Social Media Engagement**

INCA-related social media activity by country.

**INCA Social Media Users from Sanctioned Jurisdictions**

Geographic data and location verification of INCA social media users in sanctioned regions.

| User | Location | Location Proof | User Proof |
|---|---|---|---|
| sanek_zabl | Russia | Link to Social Media Post or Profile | Link to Social Media Post or Profile |
| eduard_ko85716 | Moscow, Russia | Link to Social Media Post or Profile | Link to Social Media Post or Profile |
| rianect | Russia | Link to Social Media Post or Profile | Link to Social Media Post or Profile |
| INKMAN_YEARONE | Venezuela | Link to Social Media Post or Profile | Link to Social Media Post or Profile |
| upmyveinscrypto | Bryansk, Russia | Link to Social Media Post or Profile | Link to Social Media Post or Profile |
| Cryptoday_mag | Iran | Link to Social Media Post or Profile | Link to Social Media Post or Profile |

**Distribution of INCA Social Media Engagement**

INCA-related social media activity by country.

| Country | Users |
|---|---|
| United States | 214 |
| China | 45 |
| France | 31 |
| Italy | 31 |
| United Kingdom | 30 |
| Canada | 15 |
| Viet Nam | 15 |
| Brazil | 10 |
| Argentina | 9 |
| Spain | 9 |
| Netherlands | 9 |
| Philippines | 9 |
| Taiwan, Province of China | 9 |
| Ethiopia | 7 |
| Indonesia | 7 |
| India | 7 |
| Japan | 7 |
| Korea, Republic of | 7 |

### 5.2 Scam Contracts

**Total Scam Volume by Blockchain**

Solana leads all blockchains in scam volume.

**Top Level Scam Contract Metrics**

INCA scam contract overview. $14m volume across 65k transactions.

| blockchain | Volume | Total Scam Contracts | Transaction Cnt |
|---|---|---|---|
| solana | $ 21,637,247 | 198 | 85,419 |
| ethereum | $ 4,310,975 | 69 | 11,381 |
| base | $ 1,859,769 | 70 | 15,381 |
| bnb | $ 984,670 | 124 | 9,543 |
| arbitrum | $ 56,405 | 4 | 126 |
| polygon | $ 301 | 3 | 12 |

**Total Volume by Scam Flag**

Legit volume dominates all INCA trading activity.

**All INCA Scam Contracts**

Comprehensive scam contract list. Insights into fraudulent activities across blockchains.

| Blockchain | Project | Contract Address | Token Pair | Amount USD | Swap Cnt | First Seen | Last Seen | Flag |
|---|---|---|---|---|---|---|---|---|
| solana | meteora | 0xb4c198c8906f801159f66a281d01be1c4fbe97eedd | INCA-USDT | $ 8 | 2 | 12/9/24 | 12/9/24 | Scam |
| solana | pumpdotfun | 0xe562f66dcec8a3b7e34581897b37e5df30d44a95fc | INCA-SOL | $ 109 | 12 | 12/6/24 | 12/6/24 | Scam |
| solana | meteora | 0x4d79c132b8163b9192d45a4be6617524d8b0149a4 | INCA-USDT | $ 935 | 6 | 12/5/24 | 12/5/24 | Scam |
| solana | pumpdotfun | 0x68d61e1851e4fe5f29ea1bbafb6585e6898b3abcd | INCA-SOL | $ 101 | 12 | 12/5/24 | 12/5/24 | Scam |
| ethereum | uniswap | 0x8ec09e8d088a022c20238d2b5a56b43e3a920919 | WETH-INCA | $ 1,285 | 6 | 12/30/23 | 12/30/23 | Scam |
| solana | meteora | 0x527b7b594df4b59bd14a55043a6bf1c6ada933978c | USDT-INCA | $ 360 | 12 | 12/29/24 | 12/30/24 | Scam |
| solana | meteora | 0xe2e2fe31bc2612e374b9eb09f3b53075af0cadf431 | INCA.e-USDC | $ 20 | 1 | 12/27/24 | 12/27/24 | Scam |
| solana | raydium | 0xcf1b631a2cefc183cf5f3821642439310936358f3d | INCA.e-USDC | $ 193 | 58 | 12/25/24 | 2/17/25 | Scam |
| solana | meteora | 0x98f3e381364f6bf15416cc795bc8a99983eef1adab | INCA.e-USDC | $ 25 | 4 | 12/25/24 | 12/26/24 | Scam |
| solana | pumpdotfun | 0x800a81b14d40d9c2da524e2169a8b96c92cbb170ac | INCA-SOL | $ 1,976 | 11 | 12/21/24 | 12/21/24 | Scam |

# How Inca can Help

This situation further underscores the necessity of advanced, data-driven ecosystem and risk intelligence to preempt and mitigate risk at scale. Blockchain forensics firms excel in post-incident analysis, however, a holistic solution is needed to detect systemic vulnerabilities and anticipate emerging threats before they happen.

Inca's intelligence infrastructure continuously monitors transactional flows, market anomalies, adversarial network behaviors, social media, corporate structure, and code repositories, providing real-time insights into risks before they escalate into full-scale incidents. This proactive approach is critical in an environment where nation-state actors like Lazarus operate with increasing sophistication and speed, and where the operational maturity of large crypto services like Bybit are largely unknown.

pamela.clegg@inca.digital