Report to the Swiss Federal Supervisory Authority for Foundations (FSAF)

Executive Summary

This report highlights significant concerns regarding the activities of the Interchain Foundation (ICF) and its handling of security issues within the Cosmos ecosystem. It outlines multiple incidents where the ICF allegedly ignored critical security vulnerabilities, altered policies retroactively, and failed to act on reports of infiltration by hostile entities, including North Korean operatives. The report is submitted publicly to ensure transparency and to protect the author and colleagues from potential retaliation.

Table of Contents

About Me

My name is **Jacob Anthony Gadikian**. I have worked in the Cosmos ecosystem since around 2016 and began full-time work in 2020. I am the CEO and founder of **Notional Ventures**, which used to run 45 validators in the Cosmos ecosystem.

- I am a direct and general beneficiary of the Interchain Foundation, as my validator nodes received delegations from them. However, this is not noted in the ICF's public-facing delegation documents, which have commits only from Informal Systems team members:
    - ICF Delegation Information
        - Authored by Informal Systems members
    - Notional received a delegation of over 800,000 ATOMs, yielding revenue of around $60,000 a year.
- My company was elected as the security provider to the Cosmos Hub.

Over time, I have noticed that issues with reporting are worsening instead of improving.

I am also a security researcher whose work focuses on the interplay between systems in cryptocurrency. My work has been categorically denied by the Interchain Foundation, despite ample proof. I prefer to speak and act directly, so I am making this report public. My report to the FSAF is this repository. I will communicate with the FSAF only over Signal, other than the initial email that I send them with this repository and my Signal contact information.

I fear retaliation, both personal and professional, and I believe that being direct about my complaint and publishing it is the safest path forward for myself and my family.

I am aware that my colleagues also fear retaliation, both personal and professional.

I believe we have good reason to be afraid.

That is why I mentioned that fear in Cosmos Hub Proposal 787: Formally Request Full Financial Transparency from Interchain Foundation, which I authored.

In fact, the only reason I am making this report is that I think it is less risky to speak now and speak fully than to simply walk away.

Advice for Security Reporters in Cosmos

If you have security issues, I strongly recommend that you go directly to Dev Ojha, who is extremely accomplished, ethical, and professional. I cannot recommend contacting the Interchain Foundation due to the risks that:

- You may be harassed.
- Your issue may not be handled appropriately.
- You may incur economic losses due to your report.

For the P2P storms issue in particular, I needed to "disclose by demonstration," working in conjunction with SEAL911, a security reporting body of last resort. I also had to spend my company's funds to make a legal threat to the Interchain Foundation, as they refused to remove my company's name from a provably inaccurate report they published concerning an issue involving over $70,000,000,000 in economic losses.

Incidents

Due to exploits following several of my reports, it is hard for me to say if it is safe from a network security perspective to bring security issues to the Interchain Foundation.

Infiltration of TCV by North Korea

Overview In April 2023, I became aware of a serious security breach involving **TerraCVita (TCV)**, a group working on the Luna Classic blockchain. It appears that TCV unknowingly hired an individual from North Korea to build **Terraport**, a decentralized exchange (DEX) forked from Astroport. This individual allegedly embedded malicious code into Terraport, allowing them to drain funds from the platform.

On-Chain Evidence An analysis of blockchain data suggests that TCV was directly involved in the deployment of code that facilitated fund exfiltration from Terraport. A detailed Twitter thread documents this evidence:

- [Twitter Thread by @ShBar70](https://twitter.com/ShBar70/status/1645746621466959873)

Additionally, there are indications that **High Stakes Validator** is in possession of TCV's validator operator wallet:

- [Tweet by @CosmoSreXx](https://twitter.com/CosmoSreXx/status/1646883869088464898)

In January 2023, TCV stated that High Stakes did not have access to their validator wallet:

- [Tweet by @TerracVita](https://twitter.com/TerracVita/status/1617538306081685504)

Further on-chain evidence suggests potential exfiltration routes were created by TCV:

- [Tweet by @0x_Ears](https://twitter.com/0x_Ears/status/1646777713607229442)

TCV also proposed governance proposals on various platforms:

- Terra Proposal 11468
- Injective Proposal 218

According to on-chain evidence, High Stakes later claimed responsibility.

Conflicting Statements:

- High Stakes claims it sold their validator key to TCV.
- TCV claims that High Stakes is part of their team.

These conflicting statements raise concerns about the relationship between TCV and High Stakes Validator.

North Korea Narrative After I posted a governance proposal calling for action against TCV:

- Proposal: Punish TCV for Theft

TCV contacted me, claiming they had evidence exonerating them. They facilitated contact with an individual from **Binance**, who confirmed that North Korean actors were involved. The Binance representative stated:

> "We (Binance) were the ones to investigate this and confirm the attribution; the claim of North Korea's involvement is not coming from Terraport. I can guarantee it was not a coordinated team rug or theft."

He further elaborated:

> "That person was advertising on a freelance website and using a fake identity and persona to do so. I've attributed this same individual (or cell) from North Korea in previous similar attacks as well, unfortunately."

Binance has taken steps to freeze some of the stolen funds, although the recovery process is ongoing.

Concerns and Observations

- **Inconsistencies:** The situation raises several questions. The on-chain evidence points directly to TCV, yet Binance suggests North Korean involvement.
- **Validator Security:** There is a well-documented issue with compromised validator operator seed phrases on Luna Classic. I have previously documented this problem:
  - Document on Validator Seed Phrase Compromise
- **Community Vulnerability:** The Luna Classic community includes numerous accounts that may be manipulated by malicious actors, potentially including North Korean entities.

Recommendations for Cosmos Blockchains

- **Examine High Stakes Validator:** Chains such as Gaia, Secret, Injective, Terra2, and others should investigate the activities of High Stakes Validator.
- **Validator Accountability:** There is a lack of distinction between validators as service providers and original validators. Entities like High Stakes and TCV appear indistinct. Governance actions should be considered to censure validators that compromise network security.
- **Education and Best Practices:**
  - Educate the user community about the risks associated with Validators-as-a-Service (VaaS).
  - Emphasize the importance of key custody and validator originality.
  - Encourage strict definitions of validator responsibilities, specifically regarding the holder of the operator wallet and private validator key.
  - Provide resources on operating validators securely from personal or professional premises.
  - Develop methods for validators to assert their originality and integrity.

Supporting Documentation Additional supporting documents exist but are not being published in this report.

Recent Developments In October 2024, a CoinDesk article reported that North Korean agents infiltrated the crypto industry, including involvement in developing the Liquidity Staking Module (LSM) in the Cosmos ecosystem. This further substantiates concerns about North Korean infiltration into Cosmos-based projects.

Key Excerpts Involving Zaki Manian:

- **Zaki Manian**, a prominent blockchain developer, acknowledged that he inadvertently hired two DPRK IT workers to help develop the **Cosmos Hub blockchain** in 2021.
- Manian stated: "Everyone is struggling to filter out these people."
- The DPRK IT workers funneled their earnings to individuals on the **OFAC's sanctions list**, specifically **Kim Sang Man** and **Sim Hyon Sop**.
- The CoinDesk investigation identified more than a dozen crypto companies that unknowingly hired IT workers from North Korea, including well-established blockchain projects like **Injective**.

Implications:

- The infiltration by North Korean operatives poses significant security risks to the Cosmos ecosystem.

- The Interchain Foundation did not respond to my report on this matter, raising concerns about their responsiveness to critical security issues.

Amulet and the Fee Market

Please see:

- Issue on the Cosmos Hub Relating to the Discrepancy Between Amulet Standards and the Hub
  - Backed Up

Amulet, the security contractor to the Interchain Foundation, changed their Cosmos Hub reporting policies after the submission of a bug report by **Joe Bowman**, claiming that the incident was not covered by their reporting policy.

Here is the Original Report.

Key Points:

- **HackerOne**, the reporting service selected by the Interchain Foundation and Amulet, keeps versioned changes of security reports.
- Changes were made to the reporting policy **after** the report was submitted.
- The security reporting process described on the Cosmos Hub does not match the one described by Amulet:
  - Cosmos Hub Security Docs
  - Amulet/HackerOne Security Docs
    - Go to the section "A Note on Gaia."
    - Versioned Edition of the reporting standards.
- Amulet attempted to shift blame to **Skip**, a third party that made the fee market module.
  - Joe Bowman tested **Osmosis** to see if the vulnerability was present there; it was not due to differences in integration.
  - This was a **Cosmos Hub issue**.

Threats Made by Strangelove Ventures

I observed **Jack Zampolin** and others associated with **Strangelove Ventures**—the team currently leading the growth of **IBC**—describe various means to stop the growth of IBC via **Composable** specifically. To date, Composable is the only team that has meaningfully grown the IBC network. Composable has built IBC clients for both Cosmos and Polkadot and designed **08-Wasm**, a client interface.

Proposal 104

Proposal 104

Proposal 104 selected my company, **Notional**, as the security provider to the Cosmos Hub.

- Issue #852

Key Points:

- During the time that Notional was the security provider to the Cosmos Hub, members of **Informal Systems** refused to update the Hub's security contact information.
- As such, security issues were **not reported** to the team working on the Hub's security.

P2P Storms

I have extensively documented **P2P storms** in many ways and have included PDF files here that describe them. You can find those in the p2p-storms folder.

Chronology of Exploits:

- **Game of Zones - 2020**
  - All Cosmos Hub Game of Zones participants noted this issue, yet it was not investigated.
- **Sentinel - 2021**
  - The report linked here references the precise set of issues present in P2P storms.

- **Luna Classic - May 2022**
- **Stride - August 2023**
- **Osmosis - December 2023** (Corrected from December 2024)

Implications:

- Only the exploits on Luna and Osmosis were financially consequential.
- A P2P storm is essentially the ultimate form of a deniable blockchain attack.
- Addressing this issue when it was first reported may have prevented or lessened the catastrophic impact of **Luna's UST stablecoin failure**.

My reports predate any of the financial exploits and date back to 2021.

- Levana Security Incident Analysis

Banana King: Lack of Field Length Limitations in IBC

Reports

- First reported by [@ctrl_felix](https://x.com/@ctrl_felix) to the Interchain Foundation using their formal security reporting process.
  - **Ignored**
- Reported by [@getcoldy](https://x.com/@getcoldy) to me.
- Reported by me to the Interchain Foundation.
  - **Ignored for years** until I opened a public issue.

Public Issue Opened:

- Lack of Field Length Limitations in IBC

Key Points:

- Myself and other reporters avoided making any comments in public.
- An analyst later found the issue:
  - Web3 Analyst
- I discussed both Banana King and P2P storms with **Jessica**:
  - Interview with Jessica
- The content of IBC messages that exhibited Banana King surpasses any reasonable bounds:
  - Example Banana King Transaction

Implications:

- Banana King could be used to execute P2P storm-style attacks.
- The window to execute Banana King attacks was left open by the Interchain Foundation despite multiple reports.
- Banana King did not result in any financial losses, but many Cosmos chains remain vulnerable to it today.

IBC Version 3.0.0 and the Cosmos Hub

Use of Deprecated Module on Cosmos Hub, Leading to an Exploit That Caused 30,000 ATOM of User Funds to Get Stuck Contrary to repeated, false claims made by the Interchain Foundation, the Cosmos Hub has been successfully exploited, with financial consequences for users (inability to access funds). This happened two weeks after I reported to both the Interchain Foundation and Informal Systems that the Cosmos Hub was using an obsolete version of **IBC** that was tagged as `deprecated` because:

- It was subject to the **Dragonberry** vulnerability.
- It allowed **Interchain Accounts (ICA)** channels to be created only by using the counterparty's module name, enabling an attacker to block the creation of the ICA channel.

Conclusion

The incidents outlined above highlight systemic issues within the Interchain Foundation's handling of security reports and interactions with the Cosmos ecosystem's contributors and stakeholders. These include:

- **Ignoring Critical Security Vulnerabilities:** Multiple reports were ignored or inadequately addressed, including those related to P2P storms and Banana King.
- **Retroactive Policy Changes:** Altering security policies after the fact to avoid responsibility, as seen in the Amulet and fee market incident.
- **Failure to Update Contact Information:** The refusal to update the Cosmos Hub's security contact information hindered effective communication and response to security issues.
- **Threats and Conflicts of Interest:** Instances of threats made towards ecosystem participants by entities funded by the Interchain Foundation, such as Strangelove Ventures.
- **Lack of Transparency and Accountability:** Ongoing concerns about financial transparency and the Interchain Foundation's responsiveness to critical security threats, including infiltration by hostile entities like North Korean operatives.

I urge the Swiss Federal Supervisory Authority for Foundations to investigate these matters thoroughly to ensure the integrity of the Cosmos ecosystem and the proper conduct of the Interchain Foundation.

Note: I have made this report public to ensure transparency and to protect myself and my colleagues from potential retaliation. I will communicate with the FSAF via Signal for further discussions.