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

Executive Summary

This report is submitted to the Swiss Federal Supervisory Authority for Foundations (FSAF) to highlight significant concerns regarding the activities of the Interchain Foundation (ICF) within the Cosmos ecosystem. The report outlines various incidents involving security vulnerabilities, potential misuse of the foundation's mandate, and instances of retaliation against individuals raising legitimate concerns. The aim is to bring these issues to the attention of the regulatory body responsible for overseeing foundations in Switzerland, ensuring that the ICF operates within legal and ethical boundaries.

A PDF version of this report is available here, which is automatically generated upon each update to this markdown document.

Table of Contents

1. Introduction
2. Background on the Interchain Foundation
3. About the Author
4. Summary of Key Concerns
    - Alterations to Security Policies
    - Actions by Strangelove Ventures
    - Unaddressed Security Vulnerabilities
        - P2P Storms Exploits
        - Banana King Vulnerability
    - Use of Deprecated Protocols
5. Financial Transparency Issues
    - Proposal 787: Request for Full Financial Transparency
6. Regulatory Compliance Concerns
    - Proposal 952: Concerns Regarding ICF's Mandate
7. Retaliation and Safety Concerns
8. Impact on the Cosmos Ecosystem
9. Recommendations
10. Conclusion
11. Glossary
12. Appendices

Introduction

The Cosmos ecosystem is a decentralized network of independent, scalable, and interoperable blockchains, with the Interchain Foundation (ICF) playing a pivotal role in its governance and development. As the regulatory body overseeing foundations in Switzerland, the FSAF's attention is drawn to several issues that may indicate a misuse or abandonment of the ICF's mandated responsibilities.

This report consolidates incidents and concerns that question the ethical and legal compliance of the ICF, potentially impacting the integrity and trustworthiness of the Cosmos network.

Background on the Interchain Foundation

The Interchain Foundation is a Swiss-based non-profit entity established to support the development of open and decentralized systems, specifically the Cosmos Network. According to public records:

- **CHE Registration Number:** CHE-229.562.129
- **Date of Establishment:** February 2, 2017

The ICF's mandate includes fostering innovation, ensuring network security, and promoting transparency within the Cosmos ecosystem. The foundation's stated purpose is:

> "Promoting and developing new technologies and applications, especially in the fields of new open and decentralized software architectures. A dominating but not exclusive focus is set on the promotion and development of the Cosmos Network, the Polkadot Protocol, and the related technologies as well as to conduct the necessary fundraising."

About the Author

I am Jacob Anthony Gadikian, CEO and Founder of Notional Ventures. My involvement with the Cosmos ecosystem began in 2016, transitioning to full-time work in 2020. Notional Ventures previously operated 45 validators within the Cosmos network, contributing to its security and functionality.

While my company has benefited from delegations by the ICF, which generated approximately $60,000 annually through over 800,000 ATOMs delegated, it is crucial to address the conflicts of interest and transparency issues that have arisen. To mitigate any potential conflicts, I have since departed from the Cosmos ecosystem, as announced publicly here.

Summary of Key Concerns

Alterations to Security Policies

Incident Overview:

Amulet, a security contractor for the ICF, modified its security reporting policies following the submission of a bug report by a community member, Joe Bowman. This alteration aimed to exclude the reported incident from qualifying for remediation or reward.

Details:

- **Original Report:** A bug affecting the Cosmos Hub's fee market was reported by Joe Bowman. The timestamped report is available in the repository.
- **Evidence of Policy Changes:**
  - Timestamps and archived versions of the security policies before and after the changes are available, demonstrating retroactive alterations.
  - Emails and official communications from Amulet acknowledging the report and explaining the policy changes are stored in the emails folder with timestamps.

Concerns:

- **Ethical Implications:** Changing policies retroactively undermines trust and disincentivizes the reporting of security vulnerabilities.
- **Mandate Misuse:** Such actions may indicate a deviation from the foundation's responsibilities to maintain network security.

Actions by Strangelove Ventures

Incident Overview:

Strangelove Ventures, funded by the ICF, engaged in activities that may have hindered the growth of the Inter-Blockchain Communication (IBC) network, specifically impacting the efforts of the Composable team.

Details:

- **Key Figures:** Jack Zampolin and team members of Strangelove Ventures.
- **Actions Taken:**
  - Proposed deploying Composable's Polkadot client code on other platforms to preempt their market release, a strategy referred to as "business stabby."
  - Preserved Telegram chat logs with Jack Zampolin and the core-1 team from Juno, where both Jack and Ethereal One from Strangelove Ventures promoted this strategy. Excerpts from these logs include:
    ```
    Jack Zampolin, [Apr 29, 2023 at 12:13:24 PM]:
    I just get business stabby
    ```
- **Impact on Composable:**

  - The actions resulted in delays, financial losses, and reputational damage for Composable and affected the broader Cosmos ecosystem.
- **ICF's Response:**
  - Concerns were reported to the ICF. The IBC-go team expressed shared concern, but the Foundation Council did not respond.
  - The matter was made public via social media to bring attention to these practices.

Concerns:

- **Conflict of Interest:** The ICF's continued funding of Strangelove Ventures despite actions that may harm the ecosystem raises questions about oversight.
- **Mandate Abandonment:** These behaviors may suggest a deviation from the foundation's mission to promote collaboration and growth within the ecosystem.

Unaddressed Security Vulnerabilities

P2P Storms Exploits Incident Overview:

Multiple network exploits, termed "P2P Storms," have financially impacted projects like Luna Classic and Osmosis due to unaddressed vulnerabilities in peer-to-peer communication protocols.

Simplified Explanation:

P2P Storms occur when the network becomes overwhelmed with transaction volume, causing it to become unresponsive. This renders the blockchain unusable during critical times, potentially leading to significant financial losses.

Details:

- **First Reported:** The issue was first reported to the ICF on November 9th, 2021. The initial report is available here.
- **Chronology of Reports and Incidents:**
  - **2020:** Issues identified during the Game of Zones but not investigated.
  - **2021:** Sentinel network experiences related problems.
  - **2022:** Potential oracle manipulation on Luna Classic during its collapse, resulting in approximately $70 billion in economic losses. Detailed analysis can be found here.
  - **2023:** Stride and Osmosis networks suffered from transaction spam and block delays. Full documentation, including videos replicating the issue, was provided to the ICF before the Osmosis incident.
- **ICF's Inaction:**
  - ICF-funded teams, specifically Strangelove Ventures and Informal Systems, dismissed the issue, claiming it was overstated.
  - In the Tendermint Slack channel, Jack Zampolin publicly criticized efforts to highlight the vulnerability, attempting to discredit the findings. Excerpts from the discussion include:
    `Jack Zampolin, [7 months ago]:`
    `Jacob, you aren't a security researcher. This is a longstanding issue in the codebase with many e`
- **Community Support:**
  - Teams such as Archway, Osmosis, and Sentinel recognized the validity of the findings.
  - Range Security collaborated on the original report and published an analysis confirming the exploit on Osmosis. The report is available here.

Concerns:

- **Neglect:** The ICF did not adequately investigate or address these vulnerabilities despite multiple reports.
- **Financial Impact:** Failure to act may have exacerbated economic losses in the ecosystem.
- **Mandate Failure:** Suggests an abandonment of the foundation's duty to ensure network security.

Banana King Vulnerability Incident Overview:

A lack of field length limitations in the IBC protocol, known as the "Banana King" issue, creates potential for network attacks.

Details:

- **Reports Submitted:**
  - Multiple reports were submitted by community members, including [@ctrl_felix](https://x.com/@ctrl_felix) and [@getcoldy](https://x.com/@getcoldy). These reports were initially ignored.
- **Technical Explanation:**
  - The vulnerability allows excessively large messages to be sent through IBC, which can overwhelm the network and cause timing-based attacks.
- **Attempts at Resolution:**
  - After continued inaction, the issue was made public to raise awareness.
- **Community Response:**
  - The broader community expressed concern once the issue was disclosed publicly.
- **ICF's Inaction:**
  - Despite the severity, the ICF did not prioritize addressing the vulnerability.

Concerns:

- **Inaction:** The ICF's failure to address known vulnerabilities compromises network integrity.
- **Ethical Responsibility:** Neglecting such issues indicates a misuse of their mandate to protect the ecosystem.

Use of Deprecated Protocols

Incident Overview:

The Cosmos Hub continued using an obsolete version of the IBC protocol (v3.0.0) despite known vulnerabilities, leading to an exploit where user funds became inaccessible.

Details:

- **Vulnerabilities:**
  - **Dragonberry Vulnerability:** A critical security flaw in the outdated protocol.
  - **ICA Channel Issues:** Allowed attackers to block channel creation.
- **Reporting:**
  - The issue was reported to the ICF and Informal Systems two weeks prior to the exploit. Exact dates and evidence of the reports are available.
- **Outcome:**
  - An exploit resulted in 30,000 ATOMs being locked, directly affecting users. User testimonials and data illustrating the impact are documented.
- **ICF's Response:**
  - The ICF delayed in taking action, and there was minimal communication to affected users.

Concerns:

- **Delayed Response:** Ignoring reports of deprecated protocols jeopardized user funds.
- **Mandate Violation:** Failing to maintain up-to-date security measures contradicts the foundation's responsibilities.

Financial Transparency Issues

Proposal 787: Request for Full Financial Transparency

Overview:

Proposal 787 was authored to formally request complete financial transparency from the Interchain Foundation. The proposal emphasizes the need for the ICF to disclose all financial activities to ensure accountability and compliance with their mandate.

Details:

- **Proposal Link:** Proposal 787
- **Key Points:**
  - Demand for detailed financial reports and audits.
  - Transparency in funding allocations and delegations.
  - Accountability for financial decisions affecting the ecosystem.

- **Community Reaction:**
  - The proposal received significant support from the community, highlighting widespread concern over the ICF's lack of transparency.
  - Discussions and comments reflected a desire for greater accountability.

Concerns:

- **Lack of Transparency:** The ICF has not provided sufficient financial disclosures.
- **Accountability:** Without transparency, stakeholders cannot assess whether the ICF is fulfilling its mandate ethically and effectively.

Regulatory Compliance Concerns

Proposal 952: Concerns Regarding ICF's Mandate

Overview:

Proposal 952 raises concerns about the Interchain Foundation's adherence to its foundational mandate and regulatory obligations under Swiss law.

Details:

- **Proposal Link:** Proposal 952
- **Key Issues Raised:**
  - Potential misuse or abandonment of the ICF's mandate.
  - Calls for regulatory scrutiny to ensure compliance.
  - Highlights the need for the ICF to align its actions with its stated mission.
- **Legal Obligations:**
  - Swiss foundation laws require organizations to operate transparently and in accordance with their stated purposes.
  - The ICF's actions may be in violation of specific statutes related to financial disclosure, fiduciary duty, and adherence to the foundation's purpose as defined under the Swiss Civil Code (Zivilgesetzbuch - ZGB), particularly Articles 80-89bis.

Concerns:

- **Legal Compliance:** Questions arise whether the ICF is operating within the legal framework governing Swiss foundations.
- **Mandate Integrity:** The actions and inactions of the ICF may represent a deviation from their mandated purpose.

Retaliation and Safety Concerns

Personal Experience:

Reporting security issues and advocating for transparency has led to:

- **Harassment:**
  - Receiving hostile responses from ICF representatives.
  - In an IBC-Go call, which was recorded and made public, Jack Zampolin stated that Notional Ventures shipped code with numerous bugs, aiming to discredit our work.
  - Informal Systems ceased collaboration with Notional Ventures following our opposition to certain business practices.
- **Professional Risks:**
  - Facing potential damage to career and business due to raising concerns.
  - Other community members have faced similar retaliation, leading to a culture of fear.
- **Impact on Reporting Culture:**
  - The hostile environment discourages individuals from reporting critical security issues, jeopardizing the ecosystem's integrity.

Concerns:

- **Unhealthy Environment:** Such retaliation creates a hostile atmosphere that discourages the reporting of critical security issues.
- **Risk to Ecosystem:** Suppressing valid concerns undermines the security and integrity of the entire network.

Impact on the Cosmos Ecosystem

The issues outlined have broader consequences on the health and growth of the Cosmos ecosystem:

- **Erosion of Trust:**
  - Trust between the ICF and community members has deteriorated due to lack of transparency and accountability.
- **Financial Impact:**
  - The value of ATOM, the native cryptocurrency, has declined significantly, potentially reflecting diminished confidence in the ecosystem.
- **Community Fragmentation:**
  - The lack of collaborative engagement and perceived retaliation has led to fragmentation within the community.
- **Stagnation of Development:**
  - Critical vulnerabilities remain unaddressed, hindering technological progress and innovation.

Recommendations

To address these issues and ensure the ICF fulfills its mandate ethically and effectively, the following actions are recommended:

1. **Regulatory Review:**
   - **Action:** The FSAF should conduct a thorough investigation of the ICF's activities and compliance with Swiss foundation laws.
   - **Benefit:** Ensures that the ICF operates within legal and ethical boundaries.
2. **Mandate Reassessment:**
   - **Action:** Reevaluate the ICF's adherence to its foundational mandate, potentially redefining responsibilities and oversight mechanisms.
   - **Benefit:** Aligns the foundation's actions with its mission to support and secure the Cosmos ecosystem.
3. **Financial Audits:**
   - **Action:** Implement regular, independent financial audits with publicly available results.
   - **Benefit:** Enhances transparency and accountability, rebuilding trust with stakeholders.
4. **Security Policy Standardization:**
   - **Action:** Establish clear, immutable security policies that cannot be altered retroactively.
   - **Benefit:** Encourages the reporting of vulnerabilities and ensures consistent handling of security issues.
5. **Safe Reporting Channels:**
   - **Action:** Create protected channels for individuals to report concerns without fear of retaliation.
   - **Benefit:** Promotes a culture of openness and proactive security management.
6. **Independent Oversight:**
   - **Action:** Appoint independent oversight bodies to monitor the ICF's activities, particularly where conflicts of interest may exist.
   - **Benefit:** Mitigates risks associated with dual roles and ensures objective decision-making.
7. **Community Engagement:**
   - **Action:** Involve the broader Cosmos community in governance decisions and policy formations.
   - **Benefit:** Fosters collaboration and ensures diverse perspectives are considered.

Conclusion

The concerns outlined in this report suggest that the Interchain Foundation may be misusing or neglecting its mandated responsibilities, potentially violating Swiss foundation laws and undermining the integrity of the Cosmos ecosystem. It is imperative that the FSAF takes action to investigate these issues, ensuring that the ICF operates transparently, ethically, and in alignment with its foundational mandate.

By addressing these issues, we aim to restore trust, promote innovation, and secure the future of the Cosmos ecosystem for all stakeholders.

Glossary

- **FSAF:** Swiss Federal Supervisory Authority for Foundations.
- **ICF:** Interchain Foundation.
- **Cosmos Ecosystem:** A decentralized network of independent blockchains.
- **IBC:** Inter-Blockchain Communication protocol.
- **ATOM:** The native cryptocurrency of the Cosmos Hub.
- **Amulet:** A security contractor for the ICF.
- **P2P Storms:** Network exploits affecting peer-to-peer communication.
- **Dragonberry Vulnerability:** A security flaw in an outdated IBC protocol.
- **CHE Registration Number:** Official registration number for Swiss entities.
- **Mandate:** The foundational mission and responsibilities assigned to the ICF.
- **Swiss Civil Code (ZGB):** The body of laws governing civil matters in Switzerland.

Appendices

Appendix A: Detailed Incident Reports and Proposals

- **Fee Market Bug Report**
- **Sentinel Network Report**
- **Luna Classic Exploit Analysis**
- **Osmosis Exploit Analysis**
- **Proposal 787: Full Financial Transparency**
- **Proposal 952: Concerns Regarding ICF's Mandate**

Appendix B: Supporting Documentation

- **ICF Delegation Information**
- **Versioned Security Policy Changes**
- **Juno Network Feature Announcement**
- **Banana King Issue Details**
- **Emails and Communications from Amulet**
- **Initial P2P Storms Report**
- **Departure Announcement**