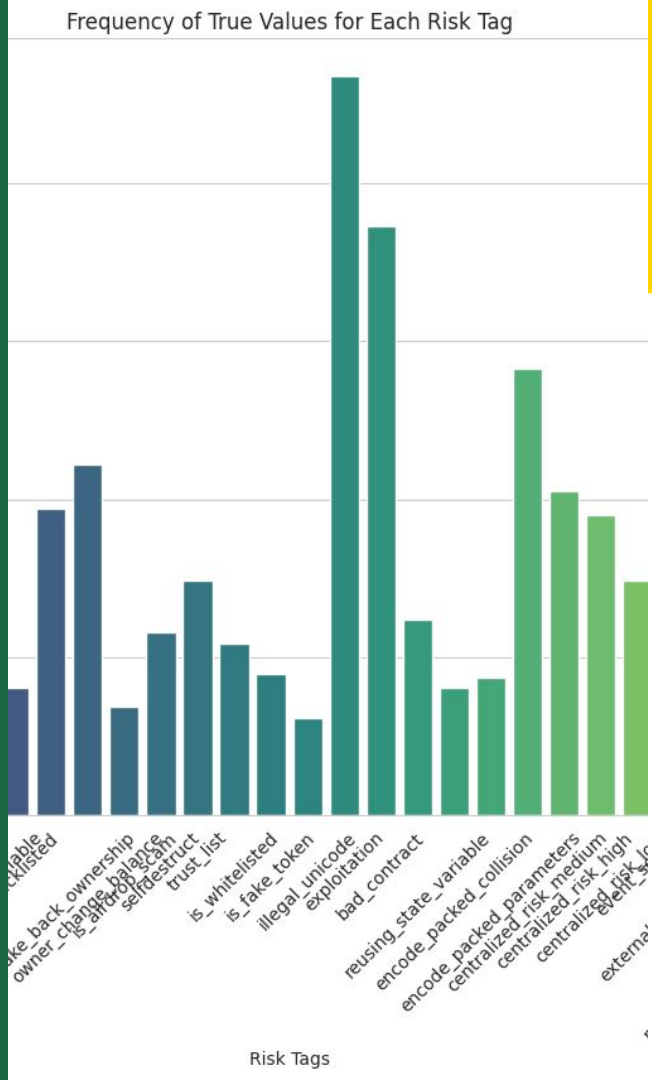
Web3 Risk Analysis: Understanding Vulnerabilities in Smart Contracts

Analyzing Risks and Correlations in Web3 Projects

Table of Contents



1

Smart Contract Risks Overview

Risk Frequency

1. Most Frequent Risk Tag:

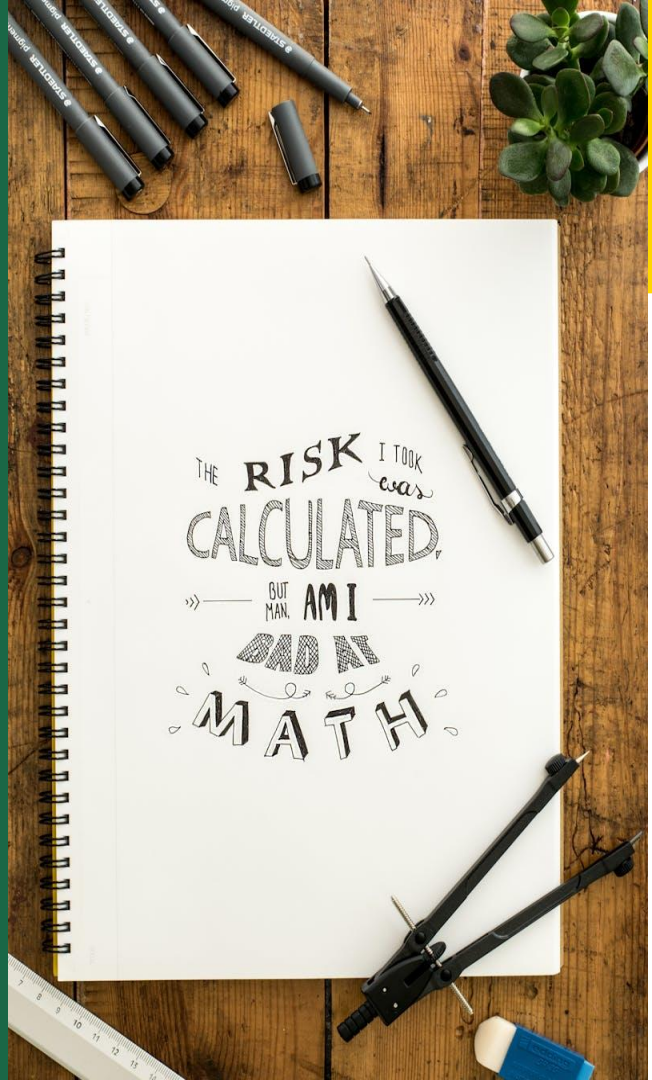
- "Exploitation" (468 occurrences)

2. Relevance:

- Expected due to common vulnerabilities in smart contracts.

3. Typical Mitigation:

- Security Audits, Code Reviews & Testing
- Bug Bounty Programs



2

Concerning Risk Tag Analysis

Unexpected Tag: "External Dependencies" was more frequent than expected.

Reason for Surprise: Reliance on external systems introduces risks if they fail or are compromised.

Literature vs. Dataset: Literature often emphasizes other risks; the high frequency here suggests emerging issues or poor implementation.

Possible Reasons:

- Poor management of dependencies
- Increased vulnerability exposure
- Complex integrations

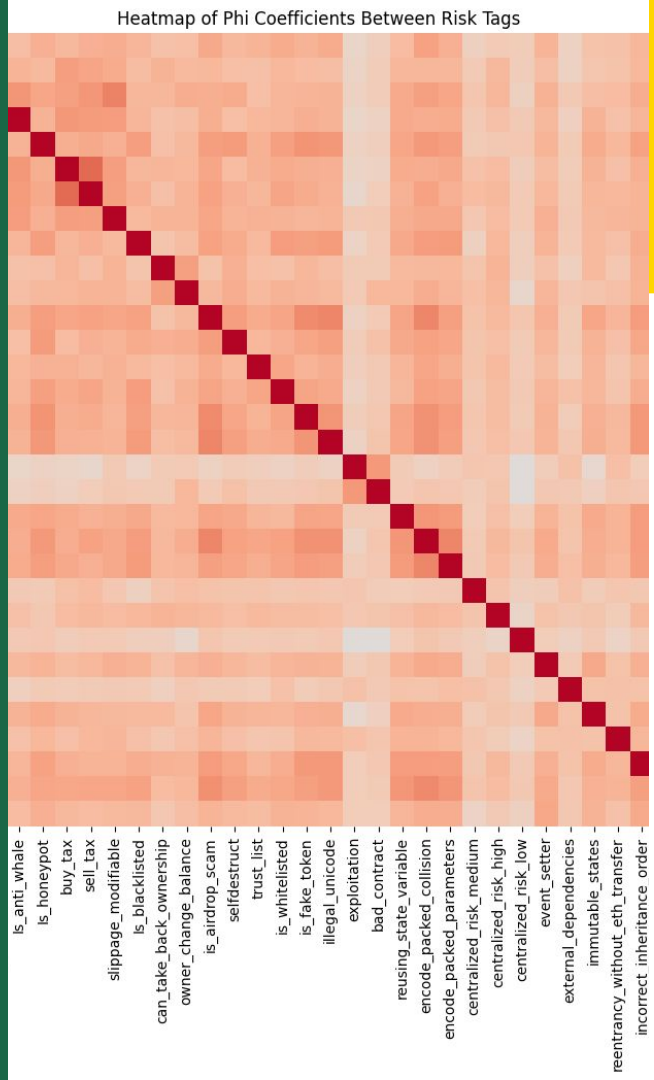
Further Investigation Needed: To understand if this reflects broader trends or specific issues.

3

Phi-Coefficient and Hidden Patterns

Smart Contract Correlation

- The Phi-Coefficient between "hidden_owner" and "is_airdrop_scam" was 0.33, suggesting a moderate positive correlation.
- Not all airdrops are scams, and hidden owners can have valid reasons for their privacy.
- The correlation level indicates a potential link between hidden owners and airdrop scams.
- Understanding the correlations can help in assessing the legitimacy of smart contract features.



4

Interconnected Risks in Smart Contracts

Buy tax & Sell tax

- "buy_tax" and "sell_tax" show a strong relationship.
- High transaction fees can be a headache for normal users.
- The Phi-Coefficient value of 0.7 suggests a significant correlation between the two risks.