Smart Contract Risk Analysis

This presentation examines risk factors in smart contracts based on data analysis. We'll explore correlations between different risk tags and their frequencies to identify key vulnerabilities.

by Shuvam Chatterjee

Overview of Risk Factors

1 **Data Source**

Analysis based on compiled risk data from 967 smart contract entries.

2 **Risk Tags**

32 different risk factors examined, including closed source, hidden owner, and anti-whale measures.

3 **Analysis Method**

Phi coefficients calculated to measure correlations between risk factors.

Correlation Heatmap

Key Findings

The heatmap reveals relationship between different risk factors. Stronger correlations appear in darker colors.

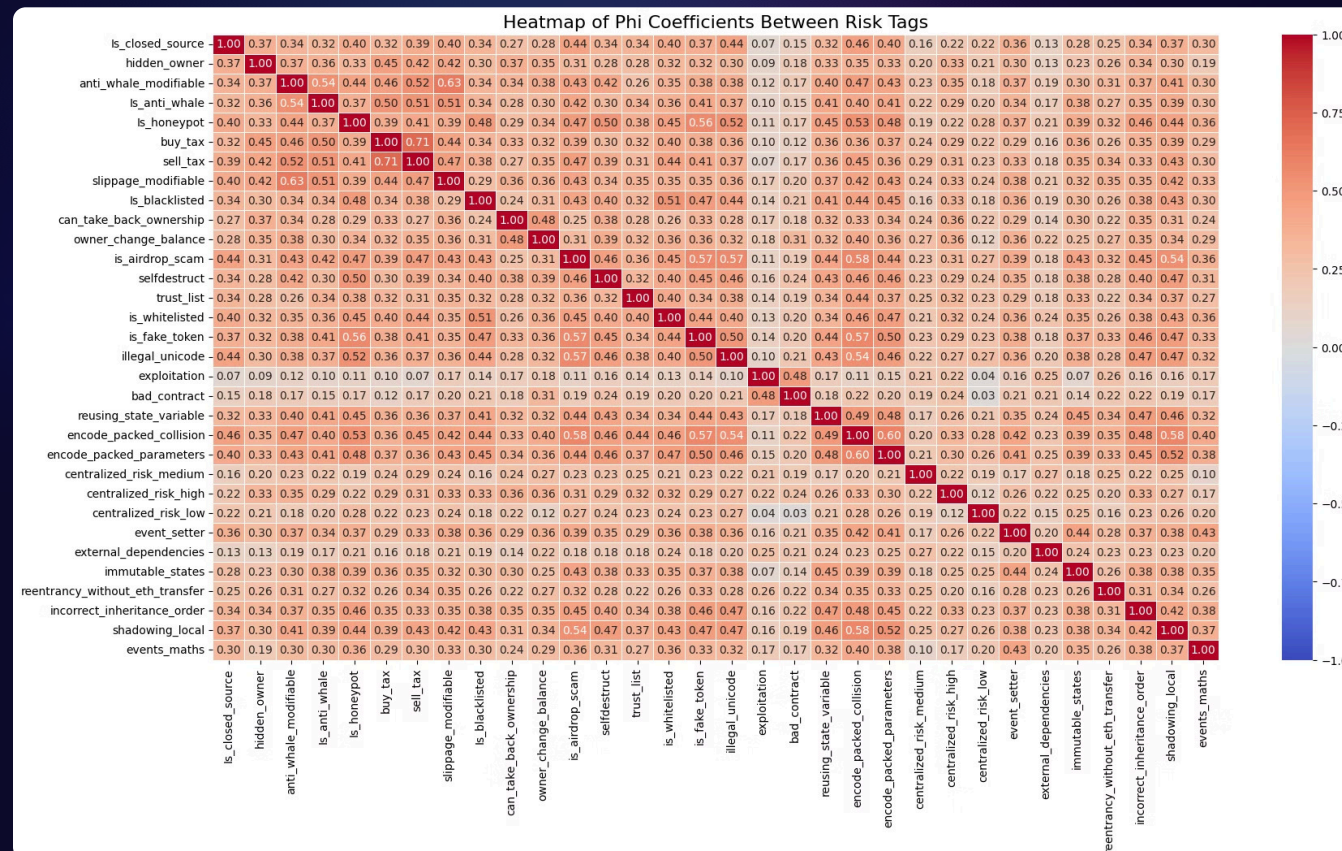Heatmap of Phi Coefficients Between Risk Tags

Interpretation

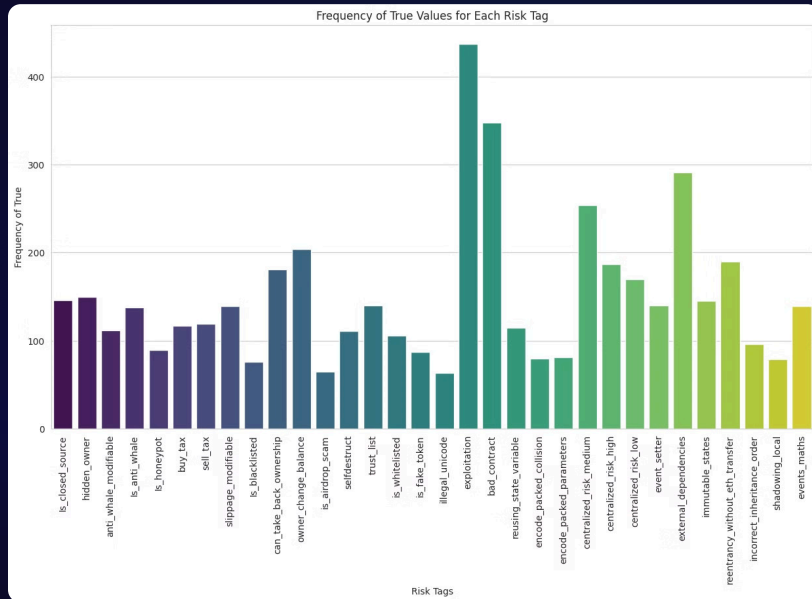Clustered dark areas indicate groups of related risk factors. Light areas show less correlation. Anti_whale_modifiable and slippage_modifiable pair has the most positive relation.

Implications

Understanding correlations helps identify potential compound risks in smart contracts.

Most Frequent Risk Factors

Frequency of True Values for Each Risk Tag

1 Exploitation (437)

Highest occurrence, indicating vulnerability to malicious attacks.

2 Bad Contract (348)

Second most common, suggesting overall poor contract quality.

3 External Dependencies (291)

Third highest, highlighting reliance on external systems as a risk.

Distribution of True Values for Risk Tags

Centralized Risks

Risk Level	Frequency
Medium	254
High	187
Low	170

Centralized risks are significant across all levels. Medium risk is most common, followed by high and low.

Ownership and Control Risks

Hidden Owner

150 occurrences, posing transparency issues.

Closed Source

146 cases, limiting code visibility.

Owner Change Balance

204 instances, indicating potential for manipulation.

Transaction-Related Risks

Slippage Modifiable

139 occurrences, potentially affecting trade execution.

Anti-Whale Measures

138 cases of anti-whale implementation, 112 with modifiable settings.

Buy/Sell Taxes

117 buy tax and 119 sell tax instances, impacting transaction costs.

Conclusion and Recommendations

1 **Identify**

Recognize the most frequent and correlated risk factors like anti_whale_modifiable and slippage_modifiable in smart contracts.

2 **Mitigate**

Implement measures to address top risks like exploitation, bad contracts, external dependencies and centralization.

3 **Monitor**

Continuously assess contracts for emerging risks and correlations.