FREQUENCY & CORRELATION ANALYSIS OF SMART CONTRACT RISKS

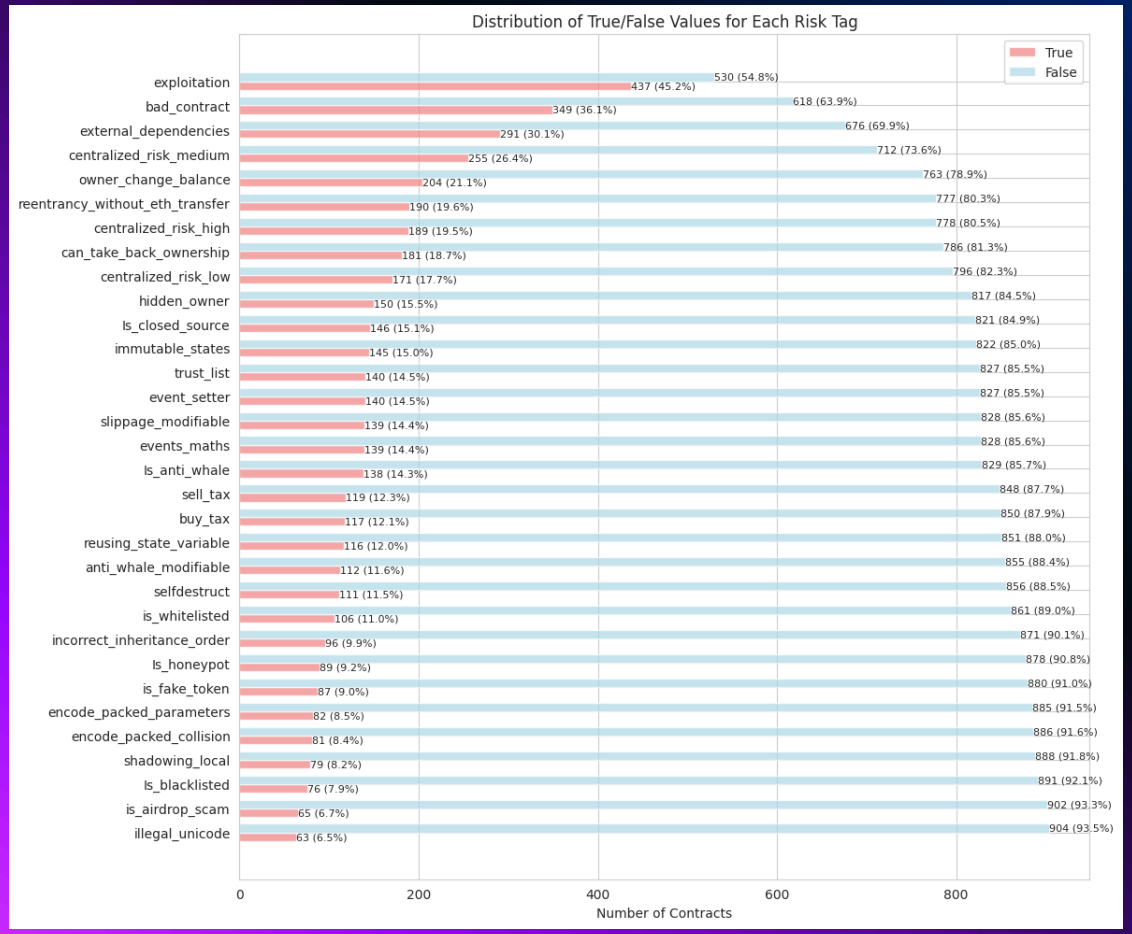
TASK-3

BY

VYSHNAVI DAKA

SMART CONTRACT RISK ANALYSIS: KEY FINDINGS

- Total number of contracts analyzed: 967
- Most frequent risk is 'Exploitation' - 437 contracts affected (45.2%), highlighting the primary security concern in smart contract development
- Strongest risk correlation of 0.71 demonstrates predictable patterns in smart contract risks.
- Key Insight: Smart contract risks follow predictable patterns, allowing for proactive security measures and improved risk assessment.

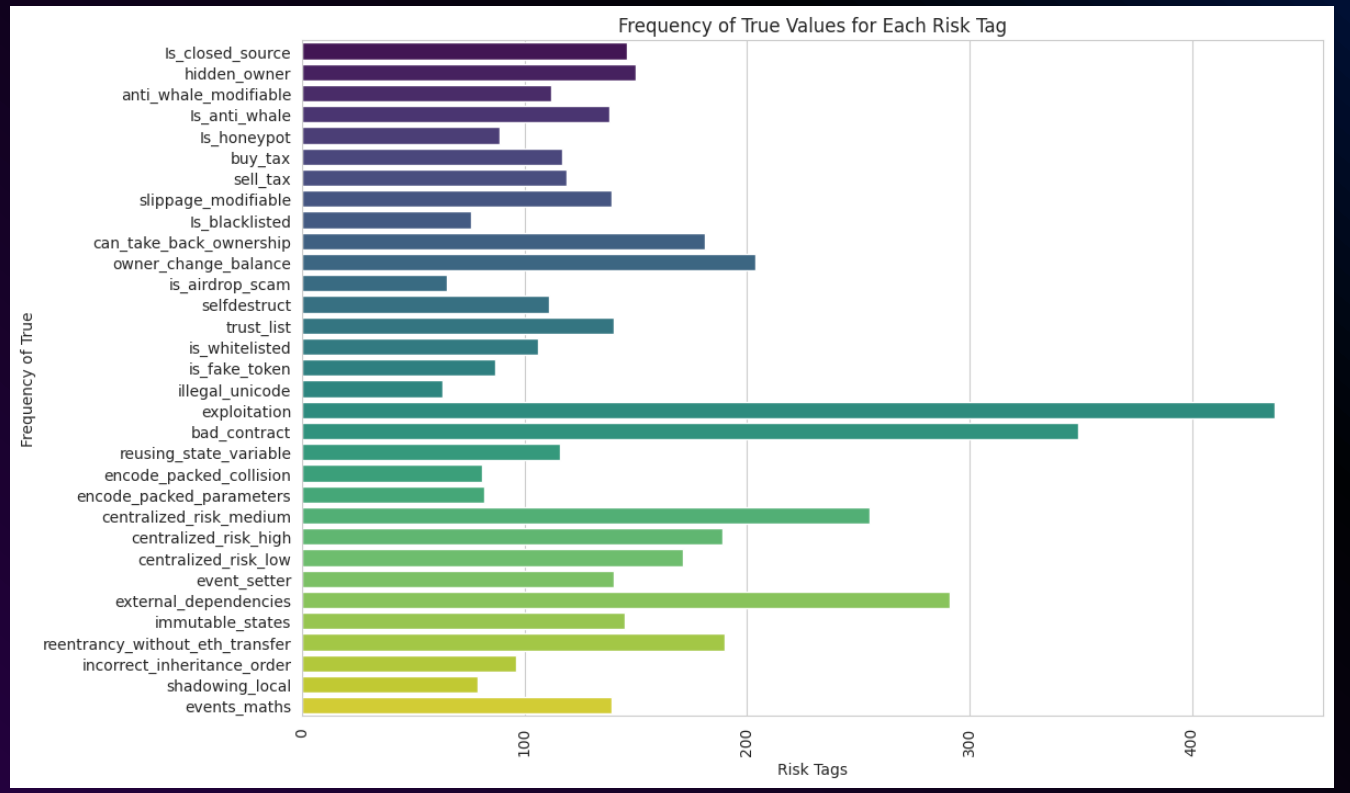


FREQUENCY ANALYSIS

- Top 5 risks include are - Exploitation (45.2%), Bad contracts (36.1%), External dependencies (30.1%), Centralized risk medium (26.4%), Owner change balance (21.1%).

FREQUENCY ANALYSIS – KEY OBSERVATIONS

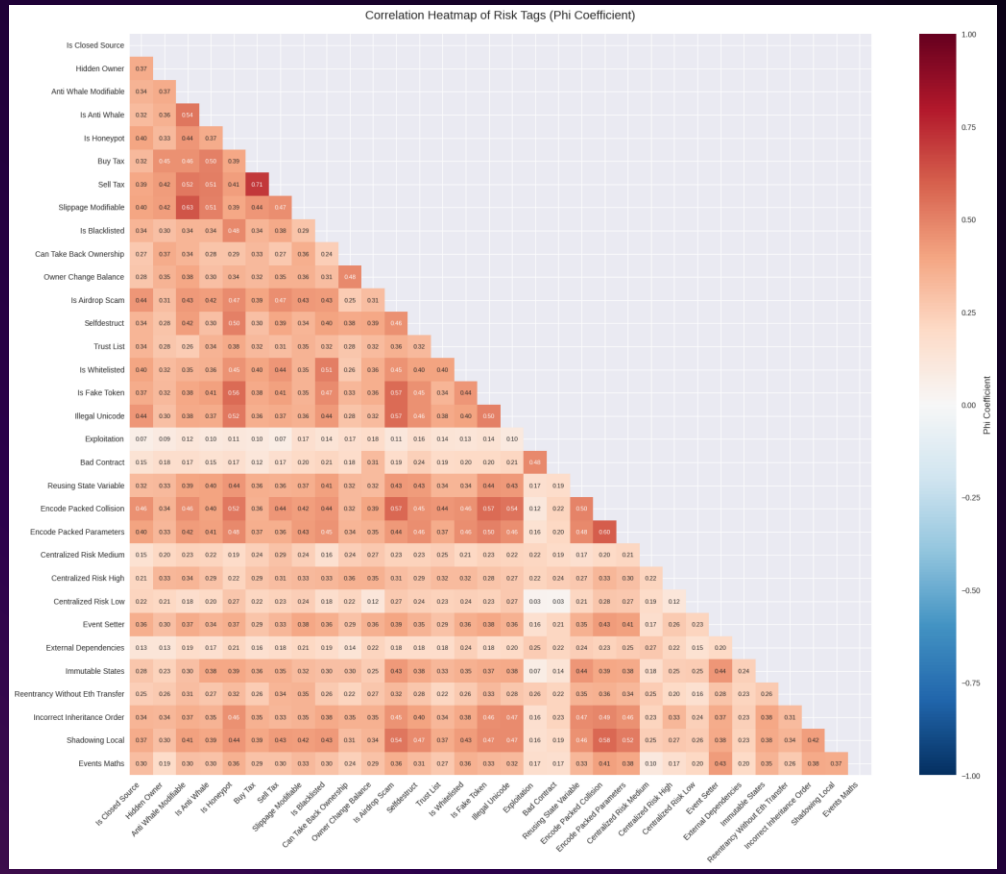
1. Nearly half of the contracts are vulnerable to exploitation.
2. One-third of the contracts have fundamental structure issues
3. Significant centralization concerns in terms of control concentration.
4. Prominent governance risks



IMPACT ON SECURITY PRACTICES

- Prioritized Vulnerability Detection with a focus on exploitation risks through automated security checks.
- Enhanced code quality controls through standardized development patterns and strict review protocols.
- Focus on external dependency checks using integration security testing and third-party contract verification.
- Assessment of governance risk structure and administrative access controls for centralized risk monitoring.

CORRELATION ANALYSIS – KEY RISK PATTERNS



Strongest Risk Tag Correlations (Phi Coefficient):

Risk Tag 1	Risk Tag 2	Phi Coefficient
buy_tax	sell_tax	0.710
anti_whale_modifiable	slippage_modifiable	0.625
encode_packed_collision	encode_packed_parameters	0.605
encode_packed_collision	shadowing_local	0.578
is_airdrop_scam	encode_packed_collision	0.575
is_fake_token	encode_packed_collision	0.570
is_airdrop_scam	is_fake_token	0.565
is_airdrop_scam	illegal_unicode	0.565
Is_honeypot	is_fake_token	0.563
illegal_unicode	encode_packed_collision	0.540
is_airdrop_scam	shadowing_local	0.538
anti_whale_modifiable	Is_anti_whale	0.536
Is_honeypot	illegal_unicode	0.525
Is_honeypot	encode_packed_collision	0.524
anti_whale_modifiable	sell_tax	0.523

CORRELATION ANALYSIS – KEY RISK PATTERNS

1. 'Buy_tax' and 'sell_tax' show strong correlation (0.71) and 'Anti_whale' features linked to 'slippage_modifiable' (0.625) indicates paired trading restrictions. This is critical for detecting manipulative trading setups.
2. Strong correlation of 0.605 between 'encode_packed_parameters' and 'encode_packed_collision' connected to shadowing_local issues (0.578) forms identifiable technical vulnerability sequence and enables systematic vulnerability detection.
3. Predictable scam signatures are identified through 'Airdrop scams' being strongly linked to 'encode_packed_collison' (0.575), 'fake_token' (0.565) and 'illegal_unicode' (0.565).

STRATEGIC BUSINESS IMPACT

- Optimized Threat Detection
  - Fccus on most frequent risks and target correlated patterns
- Enhanced Security Solutions
  - Pattern-based detection, predictive risk assessment, comprehensive vulnerability scanning
- Strategic Product Development
  - Build security tools based on risk patterns
  - Create early warning systems using pattern recognition

THANK YOU