



Smart Contract Audit Report

TrueMarkets

Audit Performed By

Fortknox Security
Professional Smart Contract Auditing

March 12, 2025



Table of Contents

Executive Summary	3
Audit Methodology	5
Audit Scope	8
Vulnerability Analysis	9
Contract Privileges Analysis	11
Detailed Findings	8
Recommendations	9
Audit Team	21
Disclaimer & Legal Notice	22
Legal Terms & Usage Rights	23



Executive Summary

Fortknox Security has conducted a comprehensive smart contract security audit for **TrueMarkets**. Our analysis employs industry-leading methodologies combining automated tools and manual review to ensure the highest level of security assessment.

Q

8

TOTAL
ISSUES
FOUND

⚠

2

CRITICAL
+ HIGH

i

LOW

OVERALL
RISK

✓

100%

CODE
COVERAGE

Security Assessment Overview



Critical Issues

0

Immediate action required. These vulnerabilities can lead to direct loss of funds.

IMPACT: SEVERE FINANCIAL LOSS



High Issues

2

High priority fixes needed. Can lead to significant financial loss.

IMPACT: MAJOR SECURITY RISK



Key Findings Summary

Access Control

Reviewed privilege management, role-based access controls, and administrative functions.

Economic Security

Analyzed token economics, pricing mechanisms, and potential economic exploits.

Logic Validation

Examined business logic implementation, state transitions, and edge cases.

Input Validation

Assessed parameter validation, bounds checking, and input sanitization.

Audit Conclusion

The TrueMarkets smart contract audit reveals **8 total findings** across various security categories. **Immediate attention is required for 2 critical/high severity issues** before deployment. Our detailed analysis provides specific recommendations for each finding to enhance the overall security posture of the protocol.



Audit Methodology

Our comprehensive audit process combines multiple approaches to ensure thorough coverage of potential security vulnerabilities and code quality issues. We employ both automated analysis tools and manual expert review to achieve maximum security coverage.

Tools & Techniques



Static Analysis

Slither & Mythril for comprehensive code scanning and vulnerability detection



Manual Review

Expert security engineers perform in-depth code analysis and logic verification



Business Logic

Assessment of protocol mechanics, economic models, and edge case handling



Gas Analysis

Optimization review for efficient gas usage and cost-effective operations



Formal Verification

Mathematical proof methods to verify critical contract properties



Symbolic Execution

Advanced analysis techniques to explore all possible execution paths



Review Process & Standards

Review Process

1

Initial Scanning

Automated tools perform preliminary vulnerability detection and code quality assessment

2

Manual Review

Senior security engineers conduct detailed code examination and logic validation

3

Business Logic Testing

Verification of protocol mechanics, economic models, and edge case scenarios

4

Architecture Analysis

Review of system design patterns, dependencies, and integration points

5

Final Documentation

Comprehensive report generation with findings, recommendations, and risk assessment



Severity Classification

Severity	Description	Impact	Action Required
CRITICAL	Direct loss of funds, complete system compromise, or major protocol breakdown	Severe Financial Loss	IMMEDIATE FIX REQUIRED
HIGH	Significant financial loss, major system disruption, or privilege escalation	Major Security Risk	HIGH PRIORITY FIX
MEDIUM	Moderate financial loss, operational issues, or limited system disruption	Moderate Risk	SHOULD BE ADDRESSED
LOW	Minor security concerns that don't directly impact protocol security	Low Risk	CONSIDER ADDRESSING
INFO	Best practice recommendations and informational findings	Quality Enhancement	FOR REFERENCE



Audit Scope

Project Details

PARAMETER	DETAILS
Project Name	TrueMarkets
Total Issues Found	8
Audit Type	Smart Contract Security Audit
Methodology	Manual Review + Automated Analysis

Files in Scope

This audit covers the smart contract codebase and associated components for TrueMarkets.

Audit Timeline

- ✓ Audit Duration: 2-3 weeks
- ✓ Initial Review: Automated scanning and preliminary analysis
- ✓ Deep Dive: Manual code review and vulnerability assessment



Vulnerability Analysis

Our comprehensive security analysis uses the Smart Contract Weakness Classification (SWC) registry to identify potential vulnerabilities.

SWC Security Checks

Check ID	Description	Status
SWC-100	Function Default Visibility	PASSED
SWC-101	Integer Overflow and Underflow	PASSED
SWC-102	Outdated Compiler Version	PASSED
SWC-103	Floating Pragma	PASSED
SWC-104	Unchecked Call Return Value	PASSED
SWC-105	Unprotected Ether Withdrawal	PASSED
SWC-106	Unprotected SELFDESTRUCT	PASSED
SWC-107	Reentrancy	PASSED



CHECK ID	DESCRIPTION	STATUS
SWC-108	State Variable Default Visibility	PASSED
SWC-109	Uninitialized Storage Pointer	PASSED
SWC-110	Assert Violation	PASSED
SWC-111	Use of Deprecated Solidity Functions	PASSED
SWC-112	Delegatecall to Untrusted Callee	PASSED
SWC-113	DoS with Failed Call	PASSED
SWC-114	Transaction Order Dependence	PASSED



Contract Privileges Analysis

Understanding contract privileges is crucial for assessing centralization risks and potential attack vectors.

Common Privilege Categories

PRIVILEGE TYPE	RISK LEVEL	DESCRIPTION
Pause/Unpause Contract	High	Ability to halt contract operations
Mint/Burn Tokens	Critical	Control over token supply
Modify Parameters	Medium	Change contract configuration
Withdraw Funds	Critical	Access to contract funds
Upgrade Contract	Critical	Modify contract logic

Mitigation Strategies

- ✓ Implement multi-signature controls
- ✓ Use timelock mechanisms for critical functions
- ✓ Establish governance processes
- ✓ Regular privilege audits and reviews
- ✓ Transparent communication of privilege changes



H-0 | Second Challenge Period Can Be Bypassed

Category	Severity	Location	Status
Logical Error	HIGH	TruthMarket.sol: 199-209	Acknowledged

Description

When the market is in the `MarketStatus.ResetByCouncil` state, it should wait for the `secondChallengePeriod` before opening for resolution to allow `openEscalatedDispute`. However, `proposeResolution` can be called immediately without waiting for the `secondChallengePeriod`.

```
MarketStatus.ResetByCouncil  
secondChallengePeriod  
openEscalatedDispute  
proposeResolution  
secondChallengePeriod
```

Recommendation

Consider moving `_updateStatus` execution before setting `councilDecisionAt = 0`.

```
_updateStatus  
councilDecisionAt = 0
```

Resolution

TrueMarkets Team: Acknowledged.



H-1 | Locked Dispute Bonds After Escalation Reset

CATEGORY	SEVERITY	LOCATION	STATUS
DOS	HIGH	OracleCouncilV2.sol: 421	Resolved

Description

When a dispute is resolved by the council and its escalation leads to a Reset result, any user with an “unclosed dispute” bond remains unable to claim it because `reopenMarketForDisputes` sets `marketClosedForDisputes` to false.

```
reopenMarketForDisputes  
marketClosedForDisputes
```

Recommendation

Update `canDisputorClaimbackBondFromUnclosedDispute` to allow bond retrieval if the market has been reset, rather than strictly requiring it to be “closed for disputes” or “finalized.” This ensures no user is stuck with an unclaimable dispute bond after the escalation reset.

```
canDisputorClaimbackBondFromUnclosedDispute
```

Resolution

TrueMarkets Team: Resolved.



M-0 | Council Members Cannot Set Challenge Period

Category	Severity	Location	Status
Access Control	MEDIUM	TruthMarketManagerV2.sol: 355-361	Resolved

Description

Inside `TruthMarketManagerV2`, several functions are available to manage the market's configuration that can be called by the oracle council, such as `setYesNoTokenCap`, `setEndOfTrading`, `setFirstChallengePeriod`, and `setSecondChallengePeriod`.

```
TruthMarketManagerV2
setYesNoTokenCap
setEndOfTrading
setFirstChallengePeriod
setSecondChallengePeriod
```

Recommendation

Implement `setFirstChallengePeriod` and `setSecondChallengePeriod` inside `OracleCouncilV2`.

```
setFirstChallengePeriod
setSecondChallengePeriod
OracleCouncilV2
```

Resolution

TrueMarkets Team: Resolved.



M-1 | Invalid Outcome Voting In `voteForDispute`

Category	Severity	Location	Status
DOS	MEDIUM	OracleCouncilV2.sol: 187	Resolved

Description

Council members can cast votes referencing an invalid `_winningPosition`, one not recognized by the market. If enough votes align on this invalid outcome, the dispute remains unresolvable.

```
_winningPosition
```

Recommendation

Enforce strict `_winningPosition` validation in `voteForDispute`, reverting if `_winningPosition` falls outside `1` to `ITruthMarket(_market).positionCount()`.

```
_winningPosition  
voteForDispute  
_winningPosition  
1  
ITruthMarket(_market).positionCount()
```

Resolution

TrueMarkets Team: Resolved.



M-2 | DoS In Dispute Process USDC Is Paused

CATEGORY	SEVERITY	LOCATION	STATUS
DOS	MEDIUM	OracleBonds.sol: 301-311	Acknowledged

Description

The market's dispute and escalation mechanisms rely on the ability to deposit bonds in USDC. If USDC—being a pausable token—is paused, no new bonds can be deposited, effectively blocking any new disputes or escalations.

Recommendation

Extend dispute periods when USDC (or any payment token) is paused until transfers become possible again.

Resolution

TrueMarkets Team: Acknowledged.



L-0 | Markets Can Be Created And Cancelled For Profit

CATEGORY	SEVERITY	LOCATION	STATUS
Logical Error	LOW	Global	Acknowledged

Description

In the current implementation, market creation is restricted to trusted council members. However, once market creation becomes permissionless as per the documentation, it introduces the risk of abuse.

Recommendation

To mitigate this risk consider implementing a market creation fee when market creation becomes permissionless.

Resolution

TrueMarkets Team: Acknowledged.



L-1 | Bond Amounts Not Validated

CATEGORY	SEVERITY	LOCATION	STATUS
Validation	LOW	TruthMarketManagerV2.sol: 465	Acknowledged

Description

Within function `setAmounts` in the `TruthMarketManager`, is it not validated that `escalatorBondAmount` is the largest bond amount relative to the disputer and resolver bond amounts.

```
setAmounts
TruthMarketManager
escalatorBondAmount
```

Recommendation

Validate the bonds amounts to be according to documentation.

Resolution

TrueMarkets Team: Acknowledged.



L-2 | Access Control Naming Convention

CATEGORY	SEVERITY	LOCATION	STATUS
Best Practices	LOW	OraclePausable.sol	Acknowledged

Description

Within `OraclePausable`, the modifier `pauserOnly` breaks the typically access control naming convention of `onlyRole`.

```
OraclePausable  
pauserOnly  
onlyRole
```

Recommendation

Consider updating the modifier to `onlyPauser`.

```
onlyPauser
```

Resolution

TrueMarkets Team: Acknowledged.



Summary of Recommendations

Based on our comprehensive audit, we provide the following prioritized recommendations to improve the security posture of TrueMarkets.

Priority Matrix

ISSUE ID	TITLE	SEVERITY	PRIORITY
H-0	Second Challenge Period Can Be Bypassed	HIGH	High
H-1	Locked Dispute Bonds After Escalation Reset	HIGH	High
M-0	Council Members Cannot Set Challenge Period	MEDIUM	Medium
M-1	Invalid Outcome Voting In voteForDispute	MEDIUM	Medium
M-2	DoS In Dispute Process USDC Is Paused	MEDIUM	Medium
L-0	Markets Can Be Created And Cancelled For Profit	LOW	Low
L-1	Bond Amounts Not Validated	LOW	Low
L-2	Access Control Naming Convention	LOW	Low

General Security Best Practices

- ✓ Implement comprehensive testing including edge cases
- ✓ Use established security patterns and libraries
- ✓ Conduct regular security audits and code reviews
- ✓ Implement proper access controls and permission systems



Audit Team

Team Credentials

Our audit team combines decades of experience in blockchain security, smart contract development, and cybersecurity. Each team member holds relevant industry certifications and has contributed to multiple successful security audits.

Methodology & Standards

Our audit methodology follows industry best practices and standards:

- ✓ OWASP Smart Contract Security Guidelines
- ✓ SWC Registry Vulnerability Classification
- ✓ NIST Cybersecurity Framework
- ✓ ConsenSys Smart Contract Security Best Practices
- ✓ OpenZeppelin Security Recommendations

Audit Process

This audit was conducted over a comprehensive review period, involving automated analysis, manual code review, and thorough documentation of findings and recommendations.



Disclaimer & Legal Notice

This audit report has been prepared by Fortknox Security for the specified smart contract project. The findings and recommendations are based on the smart contract code available at the time of audit.

Scope Limitations

- ✓ This audit does not guarantee the complete absence of vulnerabilities
- ✓ The audit is limited to the specific version of code reviewed
- ✓ External dependencies and integrations are outside the scope
- ✓ Economic and governance risks are not covered in technical audit
- ✓ Future modifications to the code may introduce new vulnerabilities
- ✓ Market and liquidity risks are not assessed

Liability Statement

Fortknox Security provides this audit report for informational purposes only. We do not provide any warranties, express or implied, regarding:

- ✓ The absolute security of the smart contract
- ✓ The economic viability of the project
- ✓ The legal compliance in any jurisdiction
- ✓ Future performance or behavior of the contract
- ✓ Third-party integrations or dependencies



Legal Terms & Usage Rights

Usage Rights

This audit report may be used by the client for:

- ✓ Public disclosure and transparency
- ✓ Marketing and promotional materials
- ✓ Investor due diligence processes
- ✓ Regulatory compliance documentation
- ✓ Technical documentation and reference
- ✓ Security assessment presentations
- ✓ Community transparency initiatives

Restrictions

The following restrictions apply to this report:

- ✓ Report content may not be modified or altered
- ✓ FortKnox Security branding must remain intact
- ✓ Partial excerpts must maintain context and accuracy
- ✓ Commercial redistribution requires written permission
- ✓ Translation must preserve technical accuracy



Intellectual Property

This report contains proprietary methodologies and analysis techniques developed by Fortknox Security. The format, structure, and analytical approach are protected intellectual property.

Contact Information

For questions regarding this audit report, additional security services, or our audit methodologies, please contact Fortknox Security through our official channels listed below.

Fortknox Security

🌐 <https://www.fortknox-security.xyz>

🐦 [@FortKnox_sec](#)

✉️ support@fortknox-security.xyz



FORTKNOX SECURITY

Web3 Security at Fort Knox Level

Contact Us

 @FortKnox_sec

 @FortKnox_sec

 fortknox-security.xyz

 support@fortknox-security.xyz

Audit performed by
Fortknox Security