Blaize.Security

April 3rd, 2023 / V. 1.0

ANGELO MVP

SMART CONTRACT AUDIT CERTIFICATE

More information on the audit can be found in the full report presented to Angelo team

AUDIT SUMMARY

Audit conducted between **March 9th**, **2022**, and **April 3rd**, **2023**.

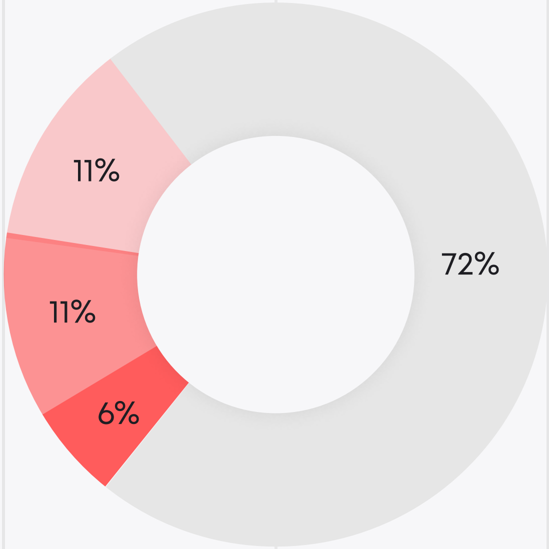
The code was delivered in the form of an archive.

Initial SHA256: ■ 97fba58261455f65bffb36a845dbe0076c289440b27b9d56bddda4c8c0bab343
Final SHA256: ■ 431d890f59c06dd98a33876e9fa6f59d860492995b359ed0f29ebce49a955daa

SCORE

9.4/10

THE GRAPH OF VULNERABILITIES DISTRIBUTION:



- 🟥 CRITICAL
- 🟥 HIGH
- 🟥 MEDIUM
- ⬜ LOW
- ⬜ LOWEST

A total of 21 problems were found. 19 issues were fixed or verified by the Angelo team.

	FOUND	FIXED/VERIFIED
Critical	1	1
High	2	0
Medium	2	2
Low	0	0
Lowest	16	16

SCOPE

The **scope** of the project includes Angelo MVP set of contracts:

contracts\ERC2981\ERC2981.sol
contracts\AngeloERC721.sol
contracts\FractionalNFT.sol
contracts\TokenVault.sol
contracts\WingToken.sol

SHORT SUMMARY

Blaize Security team performed a security audit for the Angelo MVP protocol. The audit included a manual review by the team of 2 security auditors and a security lead and several testing sessions for business logic against different attack vectors. Auditors assigned a security rating of 9.4 out of 10. The report contains 21 issues and raised questions, all successfully resolved, verified, or acknowledged by the team. Most serious issues were connected to funds transfer and fractions purchase - though they were successfully resolved/acknowledged by the Angelo team. Since the project is in the MVP stage and the team still seeks for the best implementation approach, auditors find the overall security to be at the acceptable level.

Contracts are well-written and gas-optimized, though there are several undocumented approaches. Angelo's team closed or verified all significant security gaps, and the Blaize Security team tested the protocol against the row of possible attack vectors. The Blaize Security team should notice the high level of centralization of the protocol, with the ability to withdraw locked NFT and un-purchased fraction at any moment or change the URI within the token vault. Angelo's team verified this functionality necessary for emergency cases, though auditors left the warning in the report.

Nevertheless, including good native test coverage, the Angelo MVP passed the security audit by Blaize Security.

	RATING
Security	8.8
Gas usage and logic optimization	9.8
Code quality	9.5
Test coverage **	9.7
Total	9.4

COMPLETE ANALYSIS

CRITICAL-1	✓ Resolved

Payment token might get stuck on contract’s balance.

HIGH-1	Acknowledged

Centralization risk: Curator can withdraw NFT with sold fractions

HIGH-2	Acknowledged

Owner is able to withdraw TokenVault tokens.

MEDIUM-1	✓ Resolved

ERC20 Tokens transfer is not validated.

MEDIUM-2	✓ Resolved

Ether is not refunded.

LOWEST-1	✓ Resolved

Lack of events for main admin actions

LOWEST-2	✓ Resolved

Custom errors should be used.

LOWEST-3	✓ Resolved

Duplicate `require` instead of a modifier.

LOWEST-4	✓ Resolved

Typos in parameters names

LOWEST-5 ✓ Verified

Unused fee variable

LOWEST-6 ✓ Resolved

Modifiers can be used for repeated functionality

LOWEST-7 ✓ Verified

The owner is able to change the URI of the token.

LOWEST-8 ✓ Resolved

Storage constant should be used.

LOWEST-9 ✓ Resolved

Royalty can be changed for non-existing token.

LOWEST-10 ✓ Verified

Validation of tokenomic for the token without supply cap.

LOWEST-11 ✓ Resolved

Non-configurable number of airdrop participants.

LOWEST-12 ✓ Resolved

Lack of validation for price and fee paramenters.

LOWEST-13 ✓ Resolved

The payment token and the ether should have the same purchase power

LOWEST-14	✓ Verified

Duplicate of ERC20 functionality.

LOWEST-15	✓ Resolved

Inaccurate solc version pragma.

LOWEST-16	✓ Verified

Only a curator can get fractions.

TEST COVERAGE RESULTS (AFTER AUDITORS TESTING STAGE)

FILE	% STMTS	% BRANCH	% FUNCS
ERC2981.sol	100	100	100
AngeloERC721.sol	100	100	100
FractionalNFT.sol	92.96	92.31	100
TokenVault.sol	98.33	97.5	94.74
WingToken.sol	100	100	100