TENSET

Smart Contract Audit

EuroFusion2024

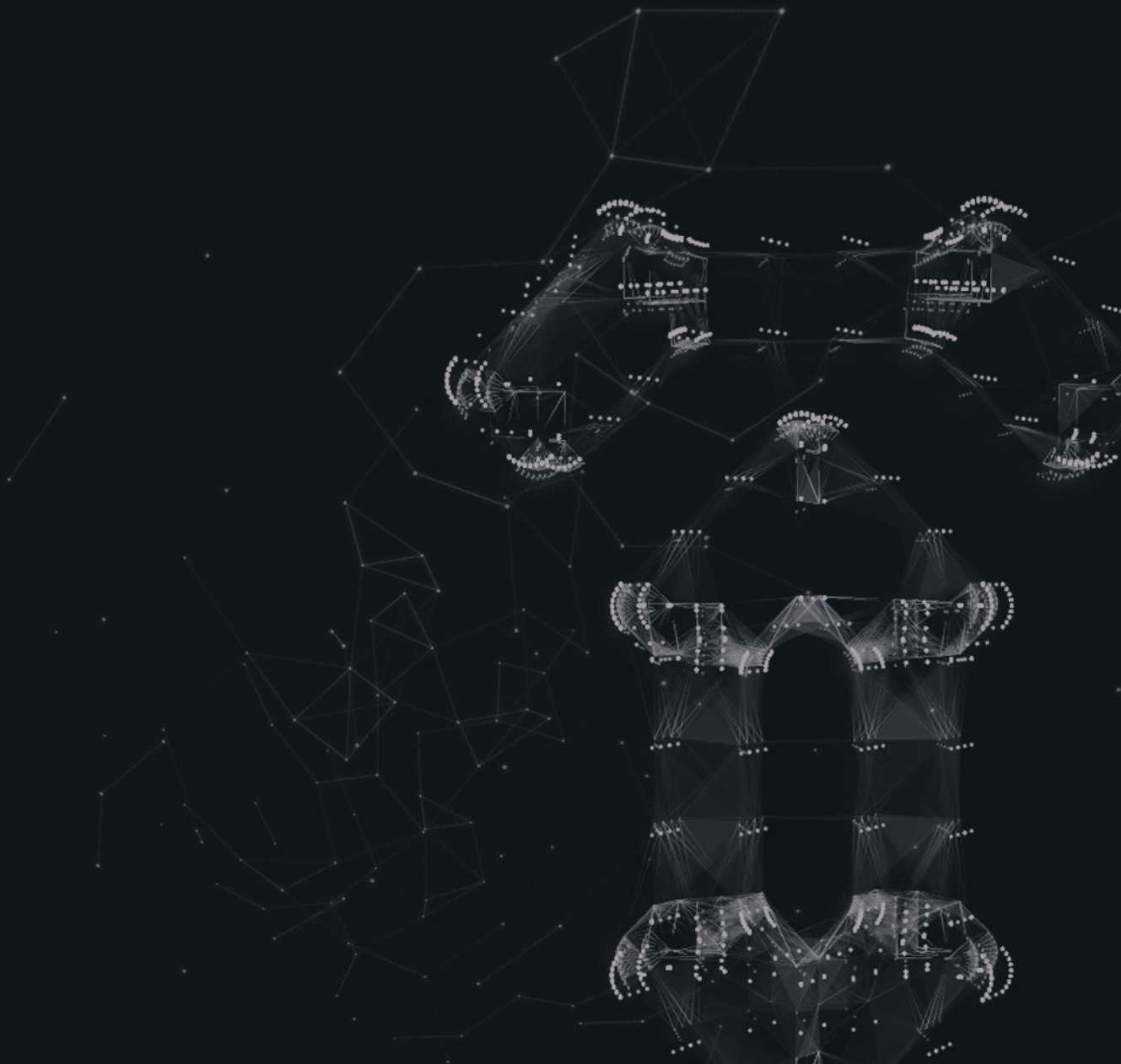

Table of Content

Executive Summary

Project Summary

Language	Codebase	Commits
Solidity	Private	5d2715585060bd382ee541ebba6e77cf6472b692

Audit Scope

ID	File	SHA256
ALB	Albania.sol	d98055dc96c6c8ffbc6d5568546c4 f8cb406eae0561263b036fd3d9a3c3321f4
AUS	Austria.sol	318944d11f7d1e5adb500abf9577b 93e727341cf1939483071bc35e021473b53
BLG	Belgium.sol	53bc2e71dc500a927a93037b2f763 e93e869539d31454ecd785e1ced75c8c994
CRT	Croatia.sol	f91a51fa8b5c3088f386fefb52e97 6321102cc0e9613442a7d7aa2e600f8cf16
CZH	Czechia.sol	285c80929551ee7d1a310e318efe2 17668fadb8992d8bc92b55b07fd669a526d
DNM	Denmark.sol	a53f80d2c57ef270a72236b5c3df1 25a15c1358b83d0dcd7edb1bba2e433f75d
ENG	England.sol	81b13bdacd68bd0e6959c6084248c 0eaa3b5d3c9c75c69fc0c738cf863c9419e
FRC	France.sol	ca170f6a635644e8d499926271916 4c73912e061564952fcab6c974e32b8ca1a

GRG	Georgia.sol	58ada84cae3c82f8a739c242d3abc 4ecc61fe172122509def761cca9dcee3e28
GRM	Germany.sol	d7cf1665199ef04d3a4df6a0e0494 b33282ab4f5048603c5fd15d3a91b72cb3a
HNG	Hungary.sol	befa02519ac2b9f7947a08b2ab645 e38cc39e654cc04acaff50e685b312fb09d
ITL	Italy.sol	0f61ae4d7688efa2a521c927ce7ed e031c16b82e130e186b726d25a36cab1ce6
NRL	Netherlands.sol	847ff1282c710b2503d346a9e3f77 2911fb792184d122e3fe8031124b4e0fdff
PLD	Poland.sol	1cdf146be730d43e96cde19c214e0 a18cb8596bdc09638873ea059dffb8a8360
PRT	Portugal.sol	b0ec5009e4f0b3aa11c6e22e29133 2116acf7110b0049ab79c50f97cdbe6bf89
RMN	Romania.sol	5ec535c26ea46200a94dfd1485f4b c3b2f36479218b8c2c607988023fd6f743e
SCT	Scotland.sol	081ad07781a3cd6640631cc65c478 52bddb4d374dd11bcaafea11ff0a6e76f0e
SRB	Serbia.sol	830b0f33710d0825bb451d34efdb9 31584e8103041bd7d3e80b09f9106bb6928
SLV	Slovakia.sol	20bd0fe57a19b083b7c7d7628911d b116b0d7f1e5ce9f46fe950996fd6cac1ee
SLN	Slovenia.sol	ff98fae381cf2fb52c4765432ebe1 ce49b3e6bf3270f5be73ae2c003d4a4c79a
SPN	Spain.sol	9e3ee5abb1ed2fcc11b8e9910c9c3 dec33ac62ea6e813060c6ced533e179a759
SWT	Switzerland.sol	57aa3522fc25303cf1ff86100f10c 746a8d212d946f817d83f9a689593911172
TRK	Turkey.sol	6aa5009b5969870b78e265bc1b554 b9b0e3c66b57a5b5c9e2957e5643fb32535
UKR	Ukraine.sol	74138cac65d698e440240aa4e7a3f 65cab3242acf68bdcb9acbffec3a64b93d6
LNC	Launchable.sol	da3ff2b314f210cbd7b26776e594a 7d9844e6e5e6fe57732dc43fd1819cdab89

General security assumptions

In conducting our security audit of the EuroFusion2024 Tokens, we have made a number of important security assumptions. These assumptions are fundamental to our analysis and should be considered when evaluating the overall security and potential vulnerabilities of the system:

Security of the Underlying Blockchain
Our security analysis is predicated on the assumption that the underlying blockchain (for example, Ethereum) is secure and functions as intended. Potential vulnerabilities or flaws in the blockchain protocol are outside the scope of this audit.

Trusted Environment
We assume that users of the smart contract will interact with it in a secure and trusted environment. This encompasses the use of secure, up-to- date software and hardware, which is free from malware or any potential interference from malicious third parties.

Private Key Security
Users of the smart contract are assumed to safeguard their private keys effectively. This involves not sharing private keys, securely storing key backups, and using hardware wallets or other secure means for key management.

These security assumptions form the basis of our audit. Deviations from these assumptions could potentially lead to risks or vulnerabilities not covered in this analysis. Therefore, the effective management of these factors is critical to ensure the ongoing security of the EuroFusion2024 Tokens.

Findings

Audit Overview

Issues

Severity	Found	Resolved	Partially Fixed	Acknowledged
Critical	0	0	0	0
High	0	0	0	0
Medium	0	0	0	0
Low	0	0	0	0
Informational	0	0	0	2
Total	**0**	**0**	**0**	**2**

LNC-1
Inefficient Storage Type for tradingStart Variable

Informational Acknowledged

Description

The variable tradingStart is currently declared as uint256 in the contract. Given that a uint64 is sufficient to store timestamp values (which will remain valid until the year 584,542,046), using uint256 is inefficient and results in unnecessary gas consumption.

Recommendation

Change the type of the tradingStart variable from uint256 to uint64. This optimization reduces gas costs and improves storage efficiency without impacting the functionality of the contract.

LNC-2
Lack of NatSpec Comments for Main Functions

Informational Acknowledged

Description

The contract lacks NatSpec comments for its main functions and variables. NatSpec (Ethereum Natural Language Specification Format) is crucial for documenting the purpose, behavior, and usage of functions and variables in smart contracts. The absence of these comments can lead to misunderstandings and misuse of the contract's functionalities.

Recommendation

Add comprehensive NatSpec comments to all main functions and variables in the contract. This documentation should include:

@notice for a brief description of the function or variable.

@param for each function parameter, describing its purpose.

@return for functions that return a value, explaining what is returned.

Any relevant @dev notes for developers.

Disclaimer

The smart contracts given for audit have been analyzed by the best industry practices at the date of this report, with cybersecurity vulnerabilities and issues in smart contract source code, the details of which are disclosed in this report (Source Code); the Source Code compilation, deployment, and functionality (performing the intended functions).

The report contains no statements or warranties on the identification of all vulnerabilities and security of the code. The report covers the code submitted to and reviewed, so it may not be relevant after any modifications. Do not consider this report as a final and sufficient assessment regarding the utility and safety of the code, bug-free status, or any other contract statements.

While we have done our best in conducting the analysis and producing this report, it is important to note that you should not rely on this report only — we recommend proceeding with several independent audits and a public bug bounty program to ensure the security of smart contracts. English is the original language of the report. The Consultant is not responsible for the correctness of the translated versions.

Smart contracts are deployed and executed on a blockchain platform. The platform, its programming language, and other software related to the smart contract can have vulnerabilities that can lead to hacks. Thus, Consultant cannot guarantee the explicit security of the audited smart contracts.