



CFG NINJA AUDITS

Security Assessment

Ordinal CZ Token

June 14, 2023

Audit Status: Fail





Audit Edition: Advance














POWERED BY
BLADE POOL

Risk Analysis

Classifications of Manual Risk Results

Classification	Description
 Critical	Danger or Potential Problems.
 High	Be Careful or Fail test.
 Low	Pass, Not-Detected or Safe Item.
 Informational	Function Detected

Manual Code Review Risk Results

Contract Priviledge	Description
 Buy Tax	1
 Sale Tax	1
 Cannot Sale	Pass
 Cannot Sale	Pass
 Max Tax	20
 Modify Tax	Detected
 Fee Check	Pass
 Is Honeypot?	Detected, owner need to enable Trade.
 Trading Cooldown	Not Detected
 Can Pause Trade?	Fail,Owner need to enable Trade.
 Pause Transfer?	Detected, Owner need to enableTrade



Contract Priviledge	Description
● Max Tx?	Pass
● Is Anti Whale?	Not Detected
● Is Anti Bot?	Not Detected
● Is Blacklist?	Not Detected
● Blacklist Check	Pass
● is Whitelist?	Not Detected
● Can Mint?	Pass
● Is Proxy?	Not Detected
● Can Take Ownership?	Not Detected
● Hidden Owner?	Not Detected
👤 Owner	0x68182478231e0abfa2a9a952837f1a4b408c1243
● Self Destruct?	Not Detected
● External Call?	Not Detected
● Other?	Not Detected
● Holders	1
● Auditor Confidence	Low

The following quick summary it's added to the project overview; however, there are more details about the audit and its results. Please read every detail.



Project Overview

Token Summary

Parameter	Result
Address	0x3159ea6CE84CFa8FcF67135Bc7650789BD324Df3
Name	Ordinal CZ
Token Tracker	Ordinal CZ (oCZ)
Decimals	18
Supply	100,000,000,000,000,000
Platform	Binance Smart Chain
compiler	v0.8.18+commit.87f61d96
Contract Name	OrdinalCZ
Optimization	Yes with 200 runs
LicenseType	MIT
Language	Solidity
Codebase	https://bscscan.com/token/0x3159ea6CE84CFa8FcF67135Bc7650789BD324Df3#code
Payment Tx	0xab0f5b83f27cff6ffcf9c025f8aa1575edac749e7b2613c679e7f14541ec912b



Project Overview

Simulation Summary

Parameter	Result
Transfer From Owner	Pass
Transfer From Holder	Pass
Add Liquidity	Pass
RemoveLiquidity	Pass
Buy from Owner	Pass
Buy from Holder	Pass,after enableTrade
Sale from Owner	Pass
Sale from Holder	Pass,after enableTrade
Remove Liquidity	Pass
SwapAndLiquify	Pass
SwapAndSale w/Fee	Pass
SwapAndSale TX	https://testnet.bscscan.com/tx/0xafd419016a2af9bdcd0e4bc7ec9e0b11fa9ba561bc3d7313b24395dc2cf68ed3
SwapAndSaleNoFee	Pass
SwapAndSale No/Fee TX	https://testnet.bscscan.com/tx/0x2f2db6affe94ecff770af8320f8583e864b481d3cbb33bb936e1d3ac415629b8



Parameter	Result
ExcludeFromFees	Pass
LaunchPad	PinkSale
Pool Creation	Pass
Pool Creation TX	https://testnet.bscscan.com/tx/0x659914a2bb0e54232e5a658596efca9067bc6d717235b5af5aa77626f5899843
Pool Finalize	Pass
Pool Finalize TX	https://testnet.bscscan.com/tx/0x659914a2bb0e54232e5a658596efca9067bc6d717235b5af5aa77626f5899843
Enable	Pass

The following quick summary it's added to the project overview; however, there are more details about the audit and its results. Please read every detail.



Main Contract Assessed Contract Name

Name	Contract	Live
Ordinal CZ	0x3159ea6CE84CFa8FcF67135Bc7650789BD324Df3	Yes

TestNet Contract Assessed Contract Name

Name	Contract	Live
Ordinal CZ	0x4fA0ab77cdd1B6CBd12FcdE7e51f824Cb08D007C	Yes

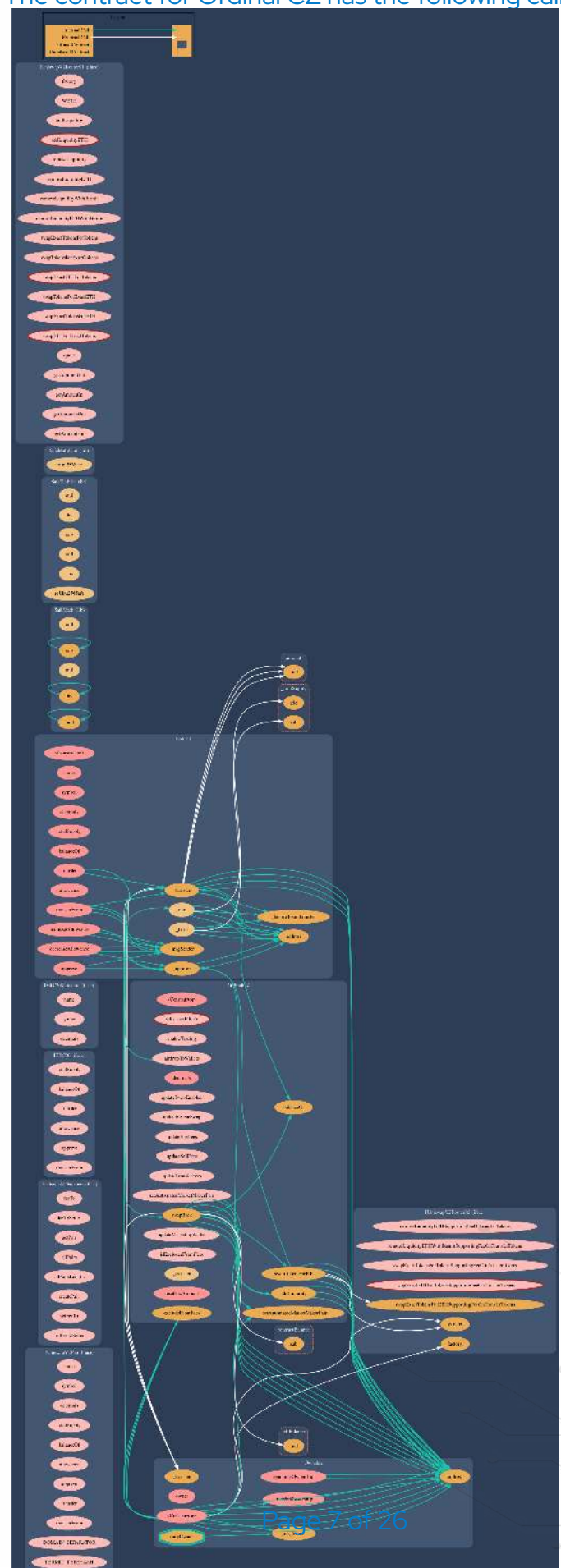
Solidity Code Provided

SolID	File Sha-1	FileName
OrdinalCZ	425ae2d6150bfdd3d794f5d461071cfd02f5145d	ordinalcz.sol
OrdinalCZ		
OrdinalCZ		
OrdinalCZ		



Call Graph

The contract for Ordinal CZ has the following call graph structure.



Smart Contract Vulnerability Checks

The Smart Contract Weakness Classification Registry (SWC Registry) is an implementation of the weakness classification scheme proposed in EIP-1470. It is loosely aligned to the terminologies and structure used in the Common Weakness Enumeration (CWE) while overlaying a wide range of weakness variants that are specific to smart contracts.

ID	Severity	Name	File	location
SWC-100	Pass	Function Default Visibility	ordinalcz.sol	L: 0 C: 0
SWC-101	Pass	Integer Overflow and Underflow.	ordinalcz.sol	L: 0 C: 0
SWC-102	Pass	Outdated Compiler Version file.	ordinalcz.sol	L: 0 C: 0
SWC-103	Low	A floating pragma is set.	ordinalcz.sol	L: 3 C: 0
SWC-104	Pass	Unchecked Call Return Value.	ordinalcz.sol	L: 0 C: 0
SWC-105	Pass	Unprotected Ether Withdrawal.	ordinalcz.sol	L: 0 C: 0
SWC-106	Pass	Unprotected SELFDESTRUCT Instruction	ordinalcz.sol	L: 0 C: 0
SWC-107	Pass	Read of persistent state following external call.	ordinalcz.sol	L: 0 C: 0
SWC-108	Pass	State variable visibility is not set..	ordinalcz.sol	L: 0 C: 0
SWC-109	Pass	Uninitialized Storage Pointer.	ordinalcz.sol	L: 0 C: 0
SWC-110	Pass	Assert Violation.	ordinalcz.sol	L: 0 C: 0



ID	Severity	Name	File	location
SWC-111	Pass	Use of Deprecated Solidity Functions.	ordinalcz.sol	L: 0 C: 0
SWC-112	Pass	Delegate Call to Untrusted Callee.	ordinalcz.sol	L: 0 C: 0
SWC-113	Pass	Multiple calls are executed in the same transaction.	ordinalcz.sol	L: 0 C: 0
SWC-114	Pass	Transaction Order Dependence.	ordinalcz.sol	L: 0 C: 0
SWC-115	Pass	Authorization through tx.origin.	ordinalcz.sol	L: 0 C: 0
SWC-116	Pass	A control flow decision is made based on The block.timestamp environment variable.	ordinalcz.sol	L: 0 C: 0
SWC-117	Pass	Signature Malleability.	ordinalcz.sol	L: 0 C: 0
SWC-118	Pass	Incorrect Constructor Name.	ordinalcz.sol	L: 0 C: 0
SWC-119	Pass	Shadowing State Variables.	ordinalcz.sol	L: 0 C: 0
SWC-120	Pass	Potential use of block.number as source of randommness.	ordinalcz.sol	L: 0 C: 0
SWC-121	Pass	Missing Protection against Signature Replay Attacks.	ordinalcz.sol	L: 0 C: 0
SWC-122	Pass	Lack of Proper Signature Verification.	ordinalcz.sol	L: 0 C: 0
SWC-123	Pass	Requirement Violation.	ordinalcz.sol	L: 0 C: 0
SWC-124	Pass	Write to Arbitrary Storage Location.	ordinalcz.sol	L: 0 C: 0
SWC-125	Pass	Incorrect Inheritance Order.	ordinalcz.sol	L: 0 C: 0



ID	Severity	Name	File	location
SWC-126	Pass	Insufficient Gas Griefing.	ordinalcz.sol	L: 0 C: 0
SWC-127	Pass	Arbitrary Jump with Function Type Variable.	ordinalcz.sol	L: 0 C: 0
SWC-128	Pass	DoS With Block Gas Limit.	ordinalcz.sol	L: 0 C: 0
SWC-129	Pass	Typographical Error.	ordinalcz.sol	L: 0 C: 0
SWC-130	Pass	Right-To-Left-Override control character (U+202E).	ordinalcz.sol	L: 0 C: 0
SWC-131	Pass	Presence of unused variables.	ordinalcz.sol	L: 0 C: 0
SWC-132	Pass	Unexpected Ether balance.	ordinalcz.sol	L: 0 C: 0
SWC-133	Pass	Hash Collisions with Multiple Variable Length Arguments.	ordinalcz.sol	L: 0 C: 0
SWC-134	Pass	Message call with hardcoded gas amount.	ordinalcz.sol	L: 0 C: 0
SWC-135	Pass	Code With No Effects (Irrelevant/Dead Code).	ordinalcz.sol	L: 0 C: 0
SWC-136	Pass	Unencrypted Private Data On-Chain.	ordinalcz.sol	L: 0 C: 0

We scan the contract for additional security issues using MYTHX and industry-standard security scanning tools.



Smart Contract Vulnerability Details

SWC-103 - Floating Pragma.

CWE-664: Improper Control of a Resource Through its Lifetime.

References:

Description:

Contracts should be deployed with the same compiler version and flags that they have been tested with thoroughly. Locking the pragma helps to ensure that contracts do not accidentally get deployed using, for example, an outdated compiler version that might introduce bugs that affect the contract system negatively.

Remediation:

Lock the pragma version and also consider known bugs (<https://github.com/ethereum/solidity/releases>) for the compiler version that is chosen.

Pragma statements can be allowed to float when a contract is intended for consumption by other developers, as in the case with contracts in a library or EthPM package. Otherwise, the developer would need to manually update the pragma in order to compile locally.

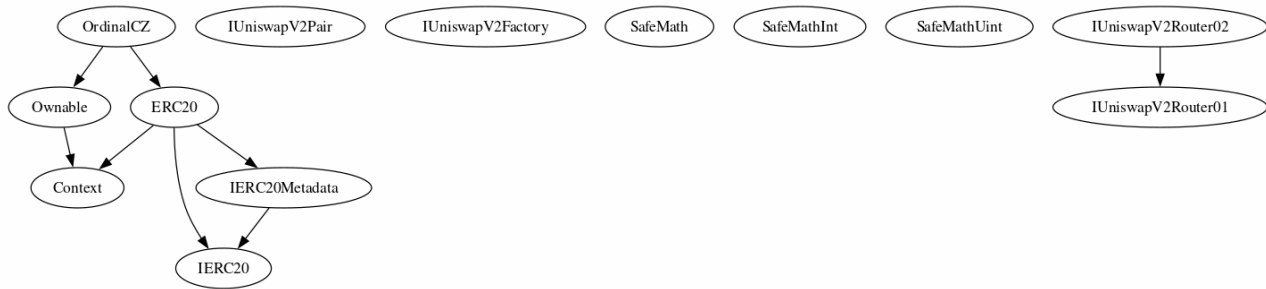
References:

Ethereum Smart Contract Best Practices - Lock pragmas to specific compiler version.



Inheritance

The contract for Ordinal CZ has the following inheritance structure.



Privileged Functions (onlyOwner)

Please Note if the contract is Renounced none of this functions can be executed.

Function Name	Parameters	Visibility
renounceOwnership		Public
transferOwnership	address newOwner	Public
resetTaxAmount		External
updateMarketingWallet		Public
excludeFromFees		External
updateTransferFees		External
updateSellFees		External
updateBuyFees		External
updateRescueSwap		External
updateSwapEnabled		Public
airdropToWallets		Public
enableTrading		Public



Smart Contract Advance Checks



ID	Severity	Name	Result	Status
oCZ-01	Low	Potential Sandwich Attacks.	Pass	Not-Found
oCZ-02	Low	Function Visibility Optimization	Fail	Detected
oCZ-03	Low	Lack of Input Validation.	Fail	Detected
oCZ-04	High	Centralized Risk In addLiquidity.	Pass	Not Detected
oCZ-05	Low	Missing Event Emission.	Fail	Detected
oCZ-06	Low	Conformance with Solidity Naming Conventions.	Pass	Not Detected
oCZ-07	Low	State Variables could be Declared Constant.	Pass	Not-Found
oCZ-08	Low	Dead Code Elimination.	Pass	Not-Found
oCZ-09	High	Third Party Dependencies.	Pass	Not Detected
oCZ-10	High	Initial Token Distribution.	Pass	Not-Found
oCZ-11	Low	AntiBot is present on the transfer.	Pass	Not Detected
oCZ-12	High	Centralization Risks In The X Role	Pass	Not-Found
oCZ-13	Informational	Extra Gas Cost For User..	Pass	Not Detected
oCZ-14	Medium	Unnecessary Use Of SafeMath	Fail	Detected
oCZ-15	Medium	Symbol Length Limitation due to Solidity Naming Standards.	Pass	Not-Found



ID	Severity	Name	Result	Status
oCZ-16	Medium	Taxes can be up to 100%	Pass	Not-Found
oCZ-17	Informational	Conformance to numeric notation best practice.	Pass	Not-Found
oCZ-18	Medium	Stop Transactions by using Enable Trade.	Fail	Detected



oCZ-02 | Function Visibility Optimization.

Category	Severity	Location	Status
Gas Optimization	 Low	ordinalcz.sol: L: 1177 C: 33	 Detected

Description

The following functions are declared as public and are not invoked in any of the contracts contained within the projects scope:

Function Name	Parameters	Visibility
resetTaxAmount		Public

The functions that are never called internally within the contract should have external visibility

Remediation



We advise that the function's visibility specifiers are set to external, and the array-based arguments change their data location from memory to calldata, optimizing the gas cost of the function.

References:

external vs public best practices.



oCZ-03 | Lack of Input Validation.

Category	Severity	Location	Status
Volatile Code	 Low	ordinalcz.sol: 1038,14	 Detected

Description

The given input is missing the check for the non-zero address.

The given input is missing the check for the excludeFromFees, onlyOwner are missing required function.

Remediation



We advise the client to add the check for the passed-in values to prevent unexpected errors as below:

```
...  
    require(receiver != address(0), "Receiver is the zero address");  
...  
...  
    require(value X limitation, "Your not able to do this function");  
...
```

We also recommend customer to review the following function that is missing a required validation. excludeFromFees, onlyOwner are missing required function.



oCZ-05 | Missing Event Emission.

Category	Severity	Location	Status
Volatile Code	 Low	ordinalcz.sol: 1024,14	 Detected

Description



Detected missing events for critical arithmetic parameters. There are functions that have no event emitted, so it is difficult to track off-chain changes. The linked code does not create an event for the transfer.

Remediation

Emit an event for critical parameter changes. It is recommended emitting events for the sensitive functions that are controlled by centralization roles.



oCZ-14 | Unnecessary Use Of SafeMath

Category	Severity	Location	Status
Logical Issue	 Medium	ordinalcz.sol: 454,9	 Detected

Description

The SafeMath library is used unnecessarily. With Solidity compiler versions 0.8.0 or newer, arithmetic operations

will automatically revert in case of integer overflow or underflow.

library SafeMath {

An implementation of SafeMath library is found.

using SafeMath for uint256;

SafeMath library is used for uint256 type in contract.

Remediation



We advise removing the usage of SafeMath library and using the built-in arithmetic operations provided by the

Solidity programming language

Project Action



oCZ-18 | Stop Transactions by using Enable Trade.

Category	Severity	Location	Status
Logical Issue	 Medium	ordinalcz.sol: 986, 13	 Detected

Description

Enable Trade is present on the following contract and when combined with Exclude from fees it can be considered a whitelist process, this will allow anyone to trade before others and can represent an issue for the holders.

Remediation






We recommend the project owner to carefully review this function and avoid problems when performing both actions.

Project Action








Technical Findings Summary

Classification of Risk

Severity	Description
 Critical	Risks are those that impact the safe functioning of a platform and must be addressed before launch. Users should not invest in any project with outstanding critical risks.
 High	Risks can include centralization issues and logical errors. Under specific circumstances, these major risks can lead to loss of funds and/or control of the project.
 Medium	Risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform
 Low	Risks can be any of the above but on a smaller scale. They generally do not compromise the overall integrity of the Project, but they may be less efficient than other solutions.
 Informational	Errors are often recommended to improve the code's style or certain operations to fall within industry best practices. They usually do not affect the overall functioning of the code.

Findings

Severity	Found	Pending	Resolved
 Critical	1	0	0
 High	0	0	0
 Medium	1	0	0
 Low	2	0	0
 Informational	1	0	0
Total	5	0	0



Social Media Checks

Social Media	URL	Result
Twitter	https://twitter.com/Ordinal_cz	Pass
Other		Fail
Website	http://ordinalcz.xyz/	Pass
Telegram	https://t.me/ordinalcz	Pass

We recommend to have 3 or more social media sources including a completed working websites.

Social Media Information Notes:

Auditor Notes: undefined

Project Owner Notes:



Assessment Results

Score Results

Review	Score
Overall Score	77/100
Auditor Score	78/100
Review by Section	Score
Manual Scan Score	35/53
SWC Scan Score	35 /37
Advance Check Score	7 /19

The Following Score System Has been Added to this page to help understand the value of the audit, the maximum score is 100, however to attain that value the project must pass and provide all the data needed for the assessment. Our Passing Score has been changed to 80 Points, if a project does not attain 80% is an automatic failure. Read our notes and final assessment below.

Audit Fail



Assessment Results

Important Notes:

- No issues or vulnerabilities were found.
- The following contract has the function to enableTrade, the owner will be able to buy and sell before anyone else can act.
- Please DYOR on the project.

Auditor Score =78
Audit Fail



Appendix

Finding Categories

Centralization / Privilege

Centralization / Privilege findings refer to either feature logic or implementation of components that act against the nature of decentralization, such as explicit ownership or specialized access roles in combination with a mechanism to relocate funds.

Gas Optimization

Gas Optimization findings do not affect the functionality of the code but generate different, more optimal EVM opcodes resulting in a reduction on the total gas cost of a transaction.

Logical Issue

Logical Issue findings detail a fault in the logic of the linked code, such as an incorrect notion on how block.timestamp works.

Control Flow

Control Flow findings concern the access control imposed on functions, such as owner-only functions being invoke-able by anyone under certain circumstances.

Volatile Code

Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases that may result in a vulnerability.

Coding Style

Coding Style findings usually do not affect the generated byte-code but rather comment on how to make the codebase more legible and, as a result, easily maintainable.

Inconsistency

Inconsistency findings refer to functions that should seemingly behave similarly yet contain different code, such as a constructor assignment imposing different requirements on the input variables than a setter function.

Coding Best Practices

ERC 20 Coding Standards are a set of rules that each developer should follow to ensure the code meets a set of criteria and is readable by all the developers.



Disclaimer

CFGNINJA has conducted an independent security assessment to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the reviewed code for the scope of this assessment. This report does not constitute agreement, acceptance, or advocacy for the Project, and users relying on this report should not consider this as having any merit for financial advice in any shape, form, or nature. The contracts audited do not account for any economic developments that the Project in question may pursue, and the veracity of the findings thus presented in this report relate solely to the proficiency, competence, aptitude, and discretion of our independent auditors, who make no guarantees nor assurance that the contracts are entirely free of exploits, bugs, vulnerabilities or deprecation of technologies.

All information provided in this report does not constitute financial or investment advice, nor should it be used to signal that any persons reading this report should invest their funds without sufficient individual due diligence, regardless of the findings presented. Information is provided 'as is, and CFGNINJA is under no covenant to audited completeness, accuracy, or solidity of the contracts. In no event will CFGNINJA or its partners, employees, agents, or parties related to the provision of this audit report be liable to any parties for, or lack thereof, decisions or actions with regards to the information provided in this audit report.

The assessment services provided by CFGNINJA are subject to dependencies and are under continuing development. You agree that your access or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies with high levels of technical risk and uncertainty. The assessment reports could include false positives, negatives, and unpredictable results. The services may access, and depend upon, multiple layers of third parties.

