CRACKEN

Smart Contract Security Audit

Project: Ocean World Token

Mar 19, 2023

OWT

Contract Address

0x197e1264c2d68c3fe0834ab6d520a2833de2929a

Table of Contents

Disclaimer

The contents of this report reflect only the CRACKEN TECH audit team's understanding of the current progress and status of the security of the code audited, to verify the integrity of the code provided for the scope of this audit. You agree that your access and/or use, including but not limited to any associated services, products, protocols, platforms, content, and materials, will be at your sole risk. Given the size of the project, the findings detailed here are not to be considered exhaustive, and further testing and audit are recommended after the issues covered are fixed. We do not warrant, endorse, guarantee, or assume responsibility for any product or service advertised or offered by a third party through the product, any open source or third-party software, code, libraries, materials, or information linked to, called by, referenced by or accessible through the report, its content, and the related services and products, any hyperlinked websites, any websites or mobile applications appearing on any advertising, and we will not be a party to or in any way be responsible for monitoring any transaction between you and any third-party providers of products or services.

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 in this report.

The review does not address the compiler layer, any other areas beyond the programming language, or other programming aspects that could present security risks. If the audited source files are smart contract files, risks or issues introduced by using data feeds from off-chain sources are not extended by this review either.

Audit Review

The source code of the Ocean World Token was audited in order to acquire a clear impression of how the project was implemented. The Cracken Tech audit team conducted in-depth research, analysis, and scrutiny, resulting in a series of observations. A detailed list of each issue found, and vulnerabilities in the source code will be included in the audit report. The problems and potential solutions are given in this report, we will identify common sources for such problems and comments for improvement.

The auditing process will follow a routine as special considerations by Cracken:

- Review of the specifications, sources, and instructions provided to Cracken to make sure the contract logic meets the intentions of the client without exposing the user's funds to risk.
- Manual review of the entire codebase by our experts, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
- Specification comparison is the process of checking whether the code does what the specifications, sources, and instructions provided to Cracken describe.
- Test coverage analysis determines whether the test cases are covering the code and how much code is exercised when we run the test cases.
- Symbolic execution is analyzing a program to determine what inputs cause each part of a program to execute.
- Reviewing the codebase to improve maintainability, security, and control based on the established industry and academic practices.

Project Review

Token Summary

Parameter	Result
Token Name	**Ocean World Token**
Token Symbol	OWT
Token Decimal	18
Total Supply	1,225,000,000
Platform	BSC
Buy Tax Fee	10%
Sell Tax Fee	10%
Contract Creation Date	Mar 17, 2022
Liquidity Status	Unlocked
Compiler Version	v0.8.6+commit.11564f7e
Optimization	Yes with 200 runs
Contract Address	0x6f8768ae9273473fc067943c55974cbfd2a8b6be
Deployer Address	0xd29f8f207020ea4e44848f81390f5f075cdbbc7f
Owner Address	0x0000000000000000000000000000000000000000

Source Code

CRACKEN was commissioned by Ocean World Token to perform an audit based on the following smart contract:

https://bscscan.com/address/0x197e1264c2d68c3fe0834ab6d520a2833de2929a

Smart Contract Vulnerability Checks

Vulnerability	Auto-Scan	Manual-Scan	Result
Unencrypted Private Data On-Chain	Complete	Complete	Low / No Risk
Code With No Effects	Complete	Complete	Low / No Risk
Message call with hardcoded gas amount	Complete	Complete	Low / No Risk
Hash Collisions with Multiple Variable Length Arguments	Complete	Complete	Low / No Risk
Unexpected Ether balance	Complete	Complete	Low / No Risk
Presence of unused variables	Complete	Complete	Low / No Risk
Right-To-Left-Override control character (U+202E)	Complete	Complete	Low / No Risk
Typographical Error	Complete	Complete	Low / No Risk
DoS With Block Gas Limit	Complete	Complete	Low / No Risk
Arbitrary Jump with Function Type Variable	Complete	Complete	Low / No Risk
Insufficient Gas Grieving	Complete	Complete	Low / No Risk
Incorrect Inheritance Order	Complete	Complete	Low / No Risk
Write to Arbitrary Storage Location	Complete	Complete	Low / No Risk
Requirement Violation	Complete	Complete	Low / No Risk
Missing Protection against Signature Replay Attacks	Complete	Complete	Low / No Risk
Weak Sources of Randomness from Chain Attributes	Complete	Complete	Low / No Risk
Authorization through tx. origin	Complete	Complete	Low / No Risk
Delegate call to Untrusted Callee	Complete	Complete	Low / No Risk

Vulnerability	Auto-Scan	Manual-Scan	Result
Use of Deprecated Solidity Functions	Complete	Complete	Low / No Risk
Assert Violation	Complete	Complete	Low / No Risk
Reentrancy	Complete	Complete	Low / No Risk
Unprotected SELF-DESTRUCT Instruction	Complete	Complete	Low / No Risk
Unprotected Ether Withdrawal	Complete	Complete	Low / No Risk
Outdated Compiler Version	Complete	Complete	Low / No Risk
Integer Overflow and Underflow	Complete	Complete	Low / No Risk
Function Default Visibility	Complete	Complete	Low / No Risk

Manual Code Review

Classification of Issues

Severity	Description
🔴 High-Risk	A vulnerability that affects the desired outcome when using a contract, or provides the opportunity to use a contract in an unintended way.
🟠 Medium-Risk	A vulnerability that could affect the desired outcome of executing the contract in a specific scenario.
🟡 Low-Risk	A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective.
🔵 Informational	A vulnerability that has an informational character but is not affecting any of the code.

Findings

Severity	Found
🔴 High-Risk	0
🟠 Medium-Risk	1
🟡 Low-Risk	0
🔵 Informational	1
Total	2

🟠 **Medium-Risk: functions make cause a few bugs of the project. Should be fixed.**

Set blacklist users

Description:

The owner can set blacklist users

[Medium-RISK]

```
function setBlackList(address account, bool isBlack) public onlyOwner {

        isBlackList[account] = isBlack;

 }
```

Recommendation:

We recommend that the owner should disable the blacklist function.

🔵 **Informational: Implementation of certain corrective actions or accepting the risk.**

Set whitelist wallets

Description:

The owner can set whitelist wallets.

```
function setExcludeFromFees(address account, bool excluded) public onlyOwner {

        isExcludedFromFees[account] = excluded;

}
```

Privileged Functions

onlyOwner

Function Name	Parameters	Visibility
approve	address spender, uint256 amount	External
burn	address account, uint256 amount	Internal
decreaseAllowance	address spender, uint256 subtractedValue	Public
increaseAllowance	address spender, uint256 addedValue	Public
renounceOwnership	None	Public
rescueETH	None	External
rescueToken	address tokenAddress, uint256 tokens	Public
setAddrParam	address _ecologBuildAddr, address _ecologDevelopAddr	External
setBlackList	address account, bool isBlack	Public
setClubAddr	address _clubAddr	Public
setExcludeFromFees	address account, bool excluded	Public
setIsOpenSwap	bool _isOpenSwap	Public
transfer	address to, uint256 amount	External
transferFrom	address from,address to,uint256 amount	External
transferOwnership	address newOwner	Public

Contract Ownership

The contract ownership of Ocean World Token is currently being renounced. The ownership of the contract grants special powers to the protocol creators, making them the sole addresses that can call sensible ownable functions that may alter the state of the protocol.

The current owner is the address 0x0000000000000000000000000000000000000000
which can be viewed: HERE

The owner wallet has the power to call the functions displayed on the privileged functions list above, if the owner wallet is compromised these privileges could be exploited.

We recommend the team renounce ownership at the right time if possible, or gradually migrate to a time lock with governing functionalities in respect of transparency and safety considerations.

Liquidity Overview

Liquidity Information

Parameter	Result
Pair Address	0x02f2d41f1c0ae084b0e4b88cf1b3d2d6d1a2b03e
OWT Reserves	804983784442576.50 OWT
USDT Reserves	86.68K USDT
Liquidity Value	$173.37K USDT
Liquidity Ownership	The token does not have liquidity at the moment of the audit

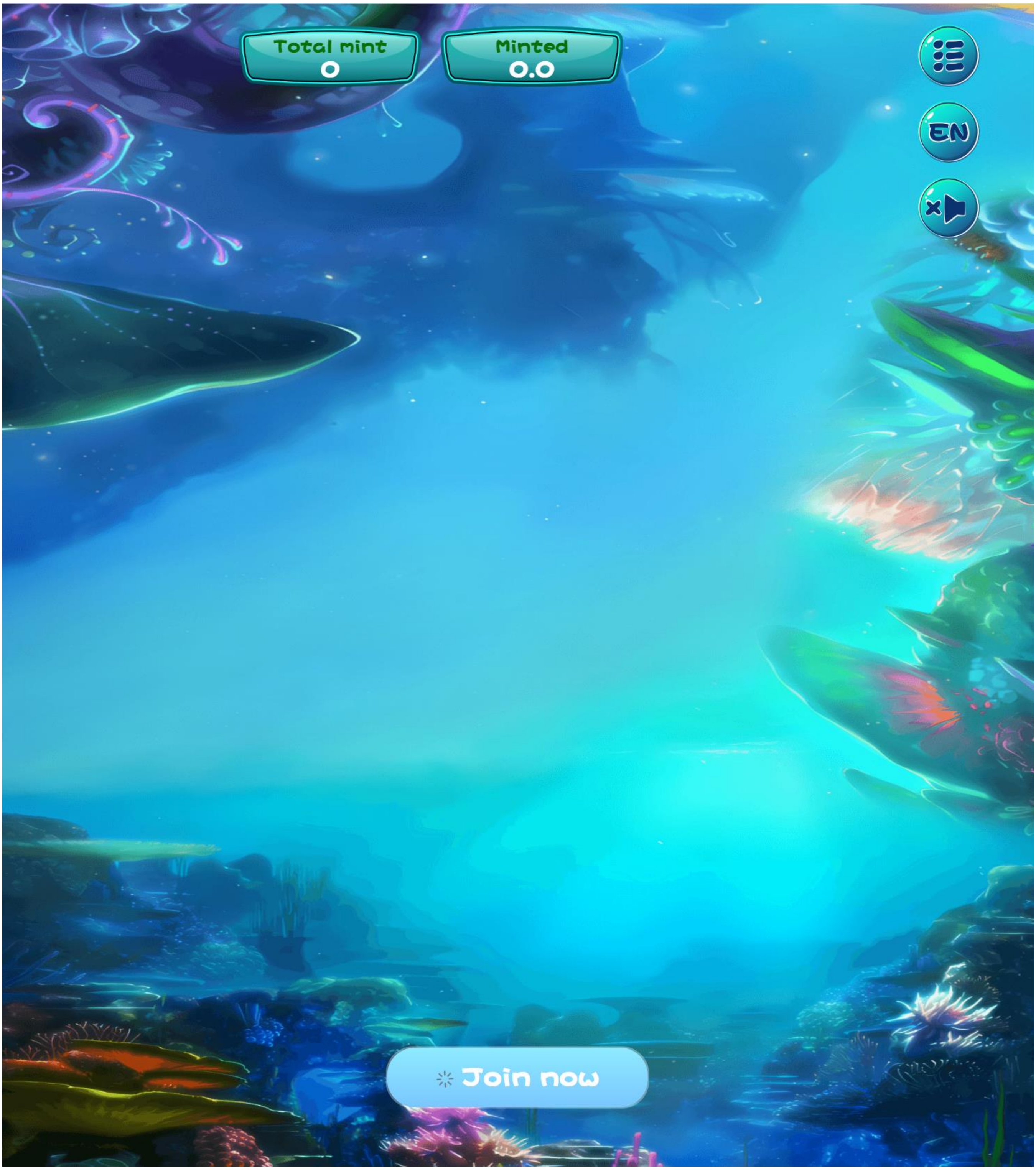
Tokenomics

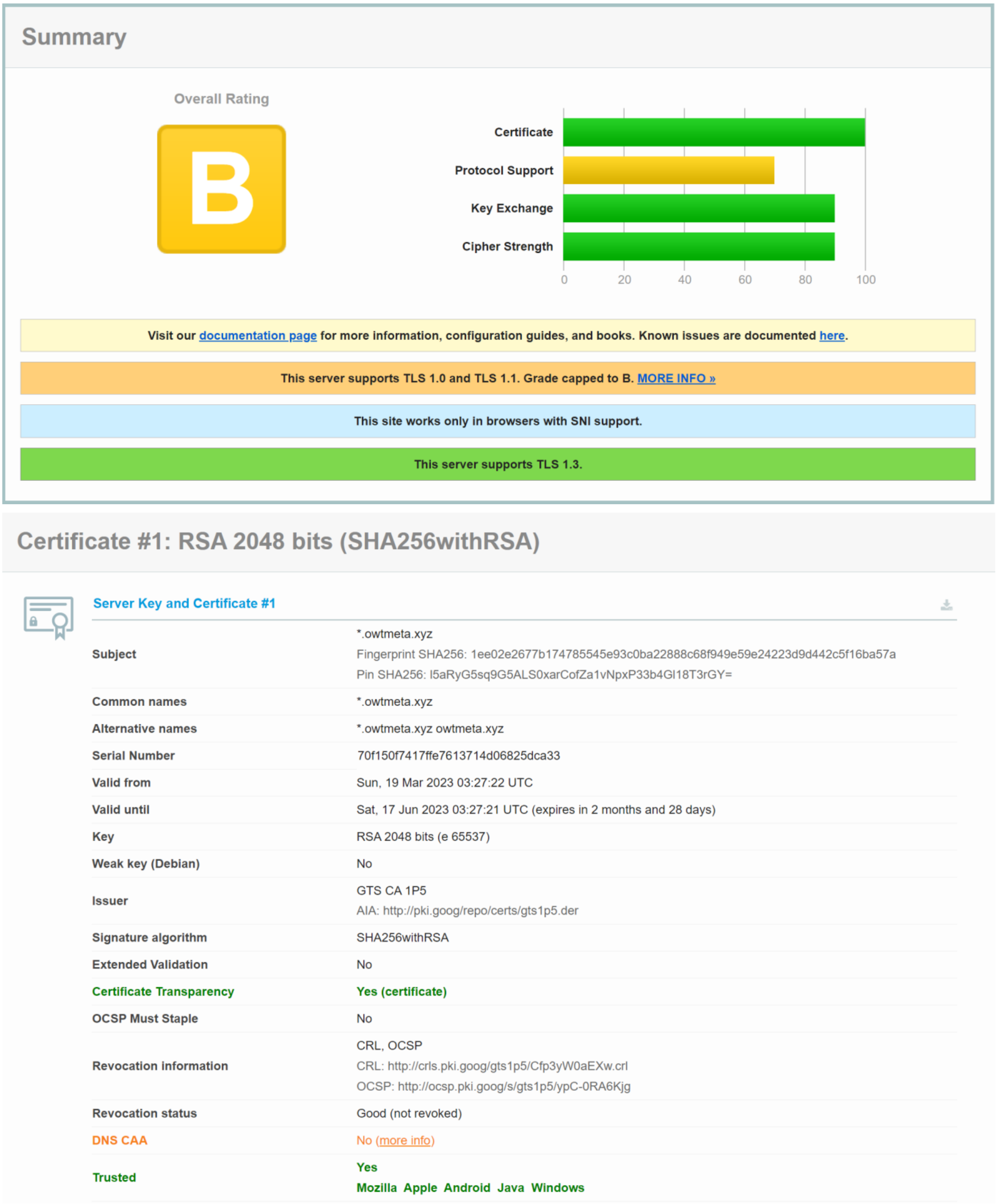
Rank	Address	Quantity (Token)	Percentage
1	0x711db5a4a2dfad2319ff106926c16bd189fc28d9	1,224,123,610	99.9301%
2	PancakeSwap V2: OWT-BSC-USD	347,651.93	0.0284%
3	0x56eb2c706714fd823e499b48cce79856162672a9	199,371.87	0.0163%
4	0x79d0f09d46a4192fe015bf2b93fc7b6b721bf780	22,443.07	0.0018%
5	0xd29f8f207020ea4e44848f81390f5f075cdbbc7f	19,724.40	0.0016%

Social Media Check

Social Media Type	Link	Result
Website	https://www.owtmeta.xyz/	Checked
Twitter	https://twitter.com/OWT_web3	Checked

Website Review





Summary

Overall Rating

B

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports TLS 1.0 and TLS 1.1. Grade capped to B. MORE INFO »

This site works only in browsers with SNI support.

This server supports TLS 1.3.

Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	*.owtmeta.xyz Fingerprint SHA256: 1ee02e2677b174785545e93c0ba22888c68f949e59e24223d9d442c5f16ba57a Pin SHA256: I5aRyG5sq9G5ALS0xarCofZa1vNpxP33b4Gl18T3rGY=
Common names	*.owtmeta.xyz
Alternative names	*.owtmeta.xyz owtmeta.xyz
Serial Number	70f150f7417ffe7613714d06825dca33
Valid from	Sun, 19 Mar 2023 03:27:22 UTC
Valid until	Sat, 17 Jun 2023 03:27:21 UTC (expires in 2 months and 28 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	GTS CA 1P5 AIA: http://pki.goog/repo/certs/gts1p5.der
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crls.pki.goog/gts1p5/Cfp3yW0aEXw.crl OCSP: http://ocsp.pki.goog/s/gts1p5/ypC-0RA6Kjg
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows

- Mobile Friendly
- Contains no code errors
- SSL is secured
- No spelling errors

Audit Conclusion

- The owner cannot pause trading
- The owner cannot mint new tokens
- **The owner can blacklist users [Medium-Risk]**
- The owner cannot change the max tx amount
- The owner cannot change buy/sell fees up.
- The owner can set whitelist wallets.

(No functions can be used due to the ownership is renounced)

AUDIT IS PASSED