SECURITY AUDIT

META - AUDITS

×

WnD - Token

Contents

Commission

Audited Project	**WnD Smart Contract**
Contract Address	**0x70D1300F5a28C57f9EbdfC8095086143DA6e2a01**
Blockchain	**Ethereum Mainnet**

Block Solutions was commissioned by WnD Smart Contract owners to perform an audit of their main smart contract. The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Disclaimer

This is a limited report on our finding based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below please make sure to read it in full.

DISCLAIMER: By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and Block Solution and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (Block Solution) owe no duty of care towards you or any other person, nor does Block Solution make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and Block Solution hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, Block Solution hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against Block Solution, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security.

Wizards & Dragons Game TOKEN Properties

Token name	Wizards & Dragons Game Token
Symbol	WnD
Token Holders	0
Total Supply	0
Transfers	0
Mintable	Yes
Burnable	Yes
Owner Wallet Address	0xc7defa20ec54917669f29e15d1acb7c121b4780c
Creator Wallet Address	0xC7dEFA20Ec54917669f29e15D1ACB7c121b4780c
Contract Address	0x70D1300F5a28C57f9EbdfC8095086143DA6e2a01

Contract Functions

View

i. function balanceOf(address owner) public view virtual override(ERC721, IERC721) disallowIfStateIsChanging returns (uint256)

ii. function getApproved(uint256 tokenId) external view returns (address operator)

iii. function getMaxTokens() external view override returns (uint256)

iv. function getNumDragons() external view disallowIfStateIsChanging returns (uint16)

v. function getNumDragonsStolen() external view disallowIfStateIsChanging returns (uint16)

vi. function getNumDragonsBurned() external view disallowIfStateIsChanging returns (uint16)

vii. function getNumWizardsBurned() external view disallowIfStateIsChanging returns (uint16)

viii. function getNumWizards() external view disallowIfStateIsChanging returns (uint16)

ix. function getPaidTokens() external view override returns (uint256)

x. function getTokenTraits(uint256 tokenId) external view override disallowIfStateIsChanging returns (WizardDragon memory)

xi. function name() external view returns (string memory)

xii. function owner() public view virtual returns (address)

xiii. function ownerOf(uint256 tokenId) public view virtual override(ERC721, IERC721) disallowIfStateIsChanging returns (address)

xiv. function paused() public view virtual returns (bool)

xv. function supportsInterface(bytes4 interfaceId) public view virtual override(IERC165, ERC721) returns (bool)

xvi. function symbol() external view returns (string memory)

xvii. function tokenByIndex(uint256 index) public view virtual override returns (uint256)

xviii. function tokenOfOwnerByIndex(address owner, uint256 index) public view virtual override(ERC721Enumerable, IERC721Enumerable) disallowIfStateIsChanging returns (uint256)

xix. function tokenTraits(uint256 tokenId) external view returns (bool a, uint8 b, uint8 c, uint8 d, uint8 e, uint8 f, uint8 g, uint8 h, uint8 i, uint8 j)

xx. function tokenURI(uint256 tokenId) public view override disallowIfStateIsChanging returns (string memory)

xxi. function totalSupply() public view virtual override returns (uint256)

Executables

i. function approve(address to, uint256 tokenId) external function transferFrom(address from,address to,uint256 tokenId) public virtual override(ERC721, IERC721)
ii. function burn(uint256 tokenId) external override whenNotPaused
iii. function mint(address recipient, uint256 seed) external override whenNotPaused
iv. function safeTransferFrom(address from,address to, uint256 tokenId) public virtual
v. function setApprovalForAll(address operator, bool approved) public virtual override override
vi. function transferFrom(address from,address to,uint256 tokenId) public virtual override(ERC721, IERC721)
vii. function updateOriginAccess() external override

Owner Executables

i. function addAdmin(address addr) external onlyOwner
ii. function removeAdmin(address addr) external onlyOwner
iii. function renounceOwnership() public virtual onlyOwner
iv. function setContracts(address _traits, address _tower) external onlyOwner
v. function setPaidTokens(uint256 _paidTokens) external onlyOwner
vi. function setPaused(bool _paused) external requireContractsSet onlyOwner
vii. function transferOwnership(address newOwner) public virtual onlyOwner
viii. function withdraw() external onlyOwner

Checklist

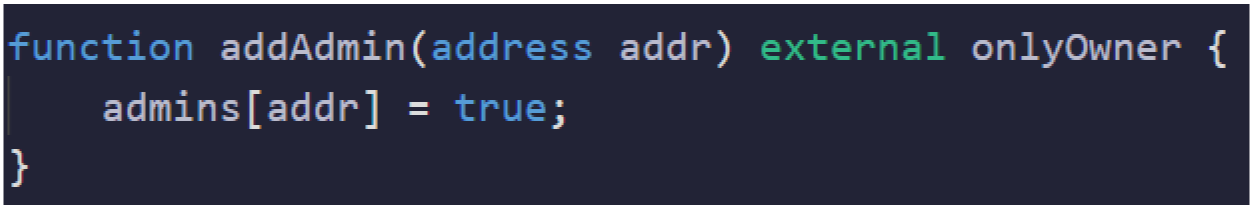
Compiler errors.	Passed
Possible delays in data delivery.	Passed
Timestamp dependence.	Passed
Integer Overflow and Underflow.	Passed
Race Conditions and Reentrancy.	Passed
DoS with Revert.	Passed
DoS with block gas limit.	Passed
Methods execution permissions.	Passed
Economy model of the contract.	Passed
Private user data leaks.	Passed
Malicious Events Log.	Passed
Scoping and Declarations.	Passed
Uninitialized storage pointers.	Passed
Arithmetic accuracy.	Passed
Design Logic.	Passed
Impact of the exchange rate.	Passed
Oracle Calls.	Passed
Cross-function race conditions.	Passed
Fallback function security.	Passed
Front Running.	Not-Checked

Safe Open Zeppelin contracts and implementation usage.	Passed
Whitepaper-Website-Contract correlation.	Not-Checked

Owner privileges

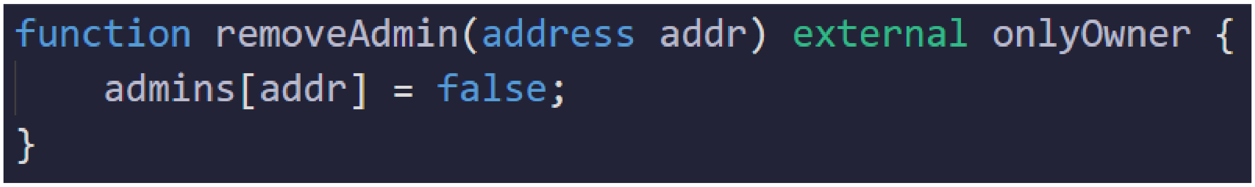
WND Contract

Enables an address to mint / burn. “addr” is the address to enable. Only current owner can call this function.



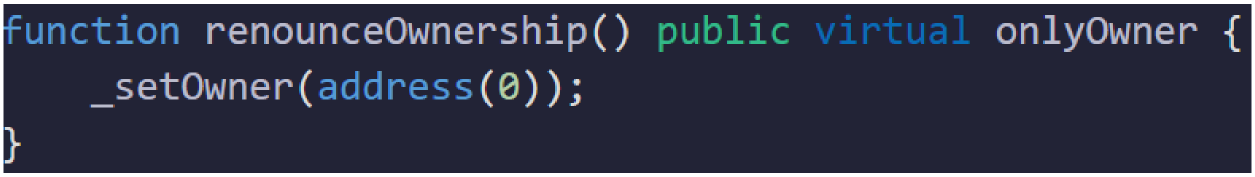
```
function addAdmin(address addr) external onlyOwner {
    admins[addr] = true;
}
```

Disables an address from minting / burning. “addr” the address to disable. Only current owner can call this function.



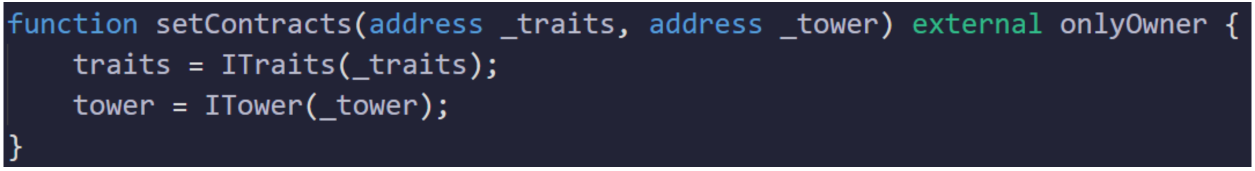
```
function removeAdmin(address addr) external onlyOwner {
    admins[addr] = false;
}
```

Leaves the contract without owner. It will not be possible to call `onlyOwner` functions anymore. Can only be called by the current owner. Renouncing ownership will leave the contract without an owner, thereby removing any functionality that is only available to the owner.



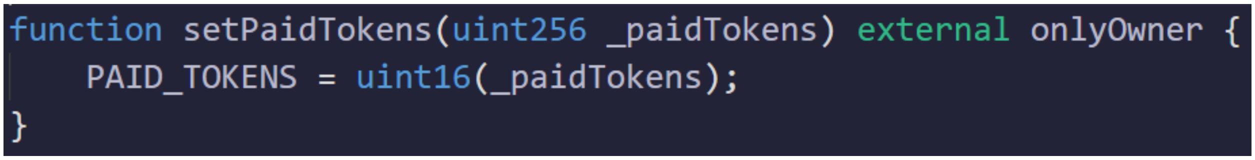
```
function renounceOwnership() public virtual onlyOwner {
    _setOwner(address(0));
}
```

OnlyOwner can set the new traits and tower contract address.



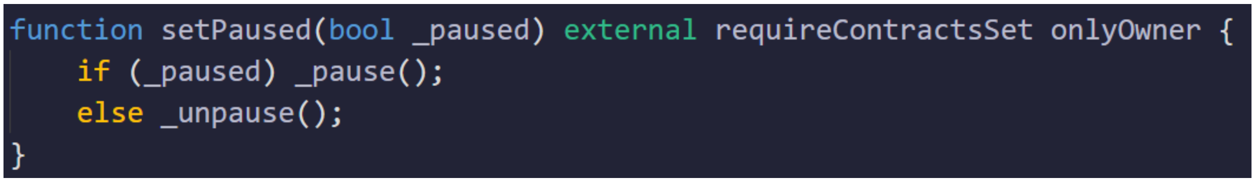
```
function setContracts(address _traits, address _tower) external onlyOwner {
    traits = ITraits(_traits);
    tower = ITower(_tower);
}
```

Updates the number of tokens for sale and owner can execute this function.



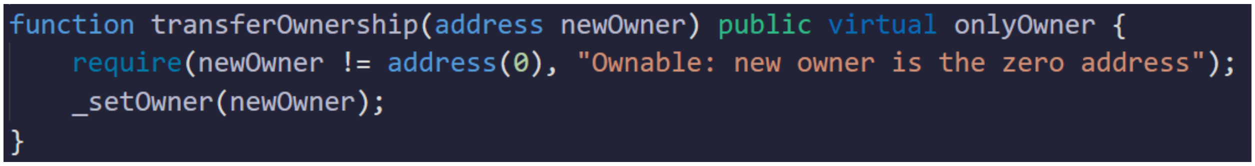
```
function setPaidTokens(uint256 _paidTokens) external onlyOwner {
    PAID_TOKENS = uint16(_paidTokens);
}
```

Enables owner to pause / unpause minting.



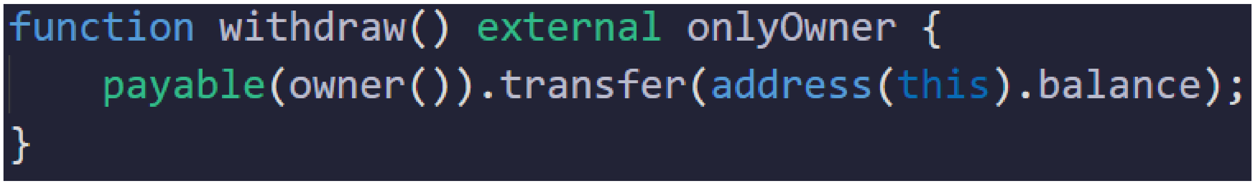
```
function setPaused(bool _paused) external requireContractsSet onlyOwner {
    if (_paused) _pause();
    else _unpause();
}
```

Transfers ownership of the contract to a new account (`newOwner`). Can only be called by the current owner.



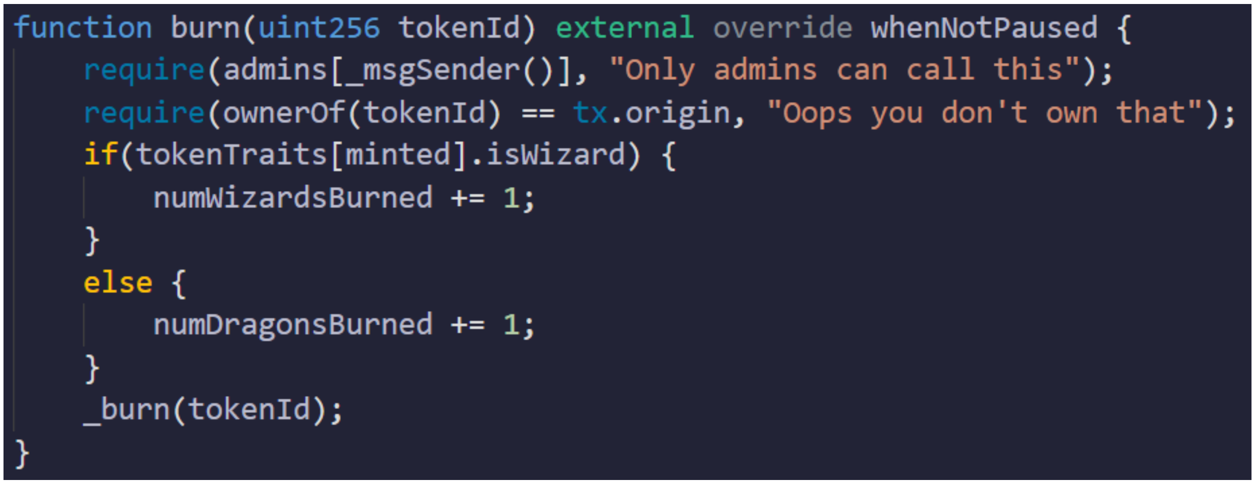
```
function transferOwnership(address newOwner) public virtual onlyOwner {
    require(newOwner != address(0), "Ownable: new owner is the zero address");
    _setOwner(newOwner);
}
```

Allows owner to withdraw funds from minting.



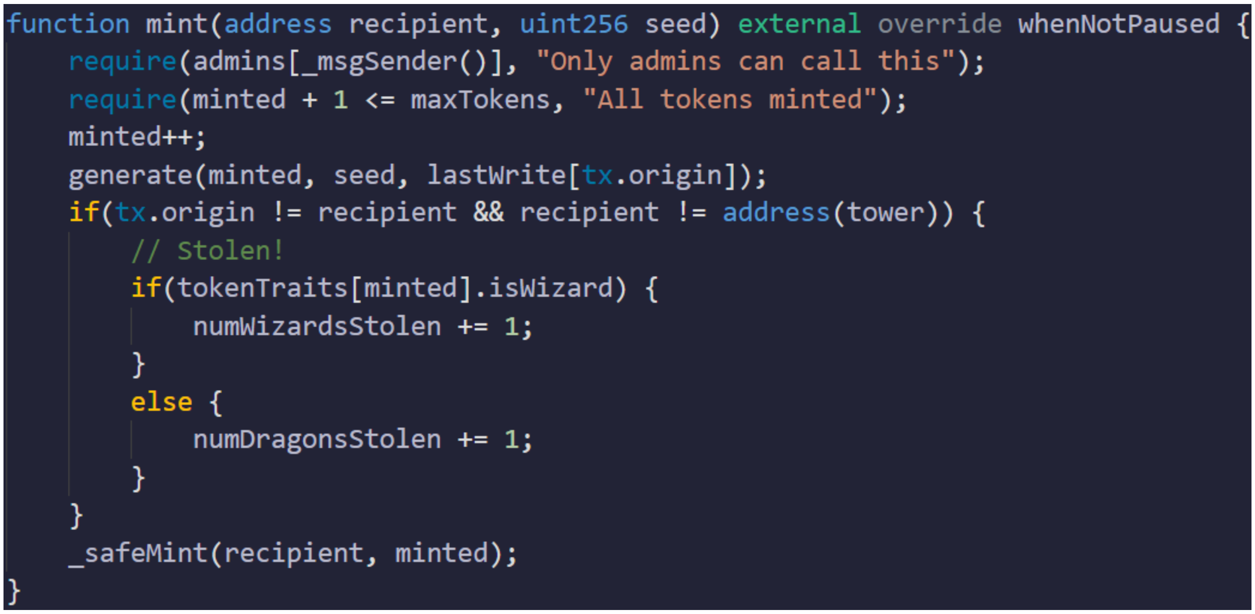
```
function withdraw() external onlyOwner {
    payable(owner()).transfer(address(this).balance);
}
```

Burn a token - any game logic should be handled before this function. Only admins can call this function.



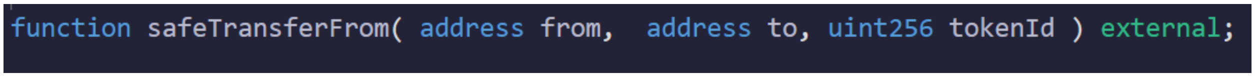
```
function burn(uint256 tokenId) external override whenNotPaused {
    require(admins[_msgSender()], "Only admins can call this");
    require(ownerOf(tokenId) == tx.origin, "Oops you don't own that");
    if(tokenTraits[minted].isWizard) {
        numWizardsBurned += 1;
    }
    else {
        numDragonsBurned += 1;
    }
    _burn(tokenId);
}
```

Mint a token - any payment / game logic should be handled in the game contract. This will just generate random traits and mint a token to a designated address. Only admins can call this .



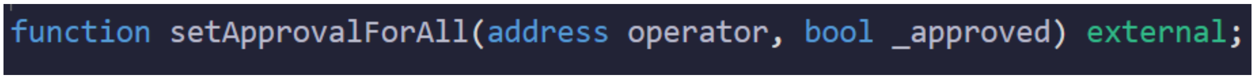
```
function mint(address recipient, uint256 seed) external override whenNotPaused {
    require(admins[_msgSender()], "Only admins can call this");
    require(minted + 1 <= maxTokens, "All tokens minted");
    minted++;
    generate(minted, seed, lastWrite[tx.origin]);
    if(tx.origin != recipient && recipient != address(tower)) {
        // Stolen!
        if(tokenTraits[minted].isWizard) {
            numWizardsStolen += 1;
        }
        else {
            numDragonsStolen += 1;
        }
    }
    _safeMint(recipient, minted);
}
```

Safely transfers `tokenId` token from `from` to `to`, checking first that contract recipients are aware of the ERC721 protocol to prevent tokens from being forever locked.
Requirements: `from` cannot be the zero address. `to` cannot be the zero address. `tokenId` token must exist and be owned by `from`. If the caller is not `from`, it must be have been allowed to move this token by either {approve} or {setApprovalForAll}. If `to` refers to a smart contract, it must implement {IERC721Receiver-onERC721Received}, which is called upon a safe transfer.



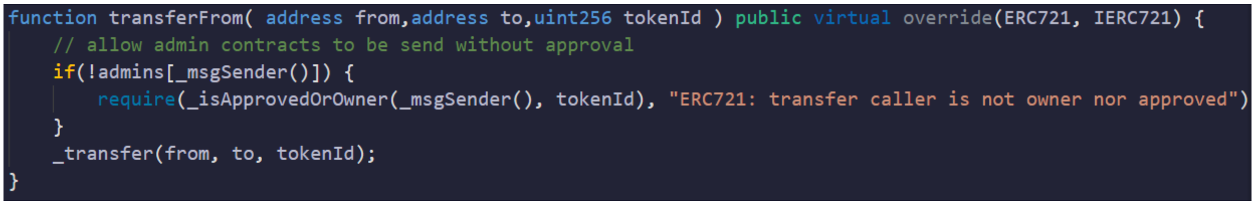
```
function safeTransferFrom( address from,  address to, uint256 tokenId ) external;
```

Approve or remove `operator` as an operator for the caller. Operators can call {transferFrom} or {safeTransferFrom} for any token owned by the caller. Requirements: The `operator` cannot be the caller.



```
function setApprovalForAll(address operator, bool _approved) external;
```

Allow admin contracts to be send without approval. transfer caller must be owner or approved.



```
function transferFrom( address from,address to,uint256 tokenId ) public virtual override(ERC721, IERC721) {
    // allow admin contracts to be send without approval
    if(!admins[_msgSender()]) {
        require(_isApprovedOrOwner(_msgSender(), tokenId), "ERC721: transfer caller is not owner nor approved")
    }
    _transfer(from, to, tokenId);
}
```

Stats:

Main Category	Subcategory	Result
Contract Programming	Solidity version not specified	Passed
	Solidity version too old	Passed
	Integer overflow/underflow	Passed
	Function input parameters lack of check	Passed
	Function input parameters check bypass	Passed
	Function access control lacks management	Passed
	Critical operation lacks event log	Passed
	Human/contract checks bypass	Passed
	Random number generation/use vulnerability	N/A
	Fallback function misuse	N/A
	Race condition	Passed
	Logical vulnerability	Passed
	Other programming issues	Passed
Code Specification	Visibility not explicitly declared	Passed
	Var. storage location not explicitly declared	Passed
	Use keywords/functions to be deprecated	Passed
	Other code specification issues	Passed
Gas Optimization	Assert () misuse	Passed
	High consumption ‘for/while’ loop	Passed
	High consumption ‘storage’ storage	Passed
	“Out of Gas” Attack	Passed
Business Risk	The maximum limit for mintage not set	Passed
	“Short Address” Attack	Passed
	“Double Spend” Attack	Passed

Overall Audit Result: PASSED

Executive Summary

According to the standard audit assessment, Customer`s solidity smart contract is Well-secured. Again, it is recommended to perform an Extensive audit assessment to bring a more assured conclusion.

Insecure
Poor secured
Secure
Well-secured
you are here

We used various tools like Mythril, Slither and Remix IDE. At the same time this finding is based on critical analysis of the manual audit.

All issues found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the Quick Stat section.

We found 0 critical, 0 high, 0 medium and 1 low level issues.

Code Quality

The WND ERC721 Token protocol consists of one smart contract. It has other inherited contracts like IWnD, ERC721Enumerable, Ownable, Pausable. These are compact and well written contracts. Libraries used in WND ERC721 Token are part of its logical algorithm. They are smart contracts which contain reusable code. Once deployed on the blockchain (only once), it is assigned a specific address and its properties / methods can be reused many times by other contracts in protocol. The BLOCKSOLUTIONS team has **not** provided scenario and unit test scripts, which would help to determine the integrity of the code in an automated way.

Overall, the code is not commented. Commenting can provide rich documentation for functions, return variables and more.

Documentation

As mentioned above, it’s recommended to write comments in the smart contract code, so anyone can quickly understand the programming flow as well as complex code logic. We were given a WND ERC721 Token smart contract code in the form of File.

Use of Dependencies

As per our observation, the libraries are used in this smart contract infrastructure that are based on well-known industry standard open-source projects. And even core code blocks are written well and systematically. This smart contract does not interact with other external smart contracts.

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to token loss etc.
High	High-level vulnerabilities are difficult to exploit; however, they also have significant impact on smart contract execution, e.g. public access to crucial functions
Medium	Medium-level vulnerabilities are important to fix; however, they can’t lead to tokens lose
Low	Low-level vulnerabilities are mostly related to outdated, unused etc. code snippets, that can’t have significant impact on execution
Lowest / Code Style / Best Practice	Lowest-level vulnerabilities, code style violations and info statements can’t affect smart contract execution and can be ignored.

Audit Findings

Critical

No critical severity vulnerabilities were found.

High

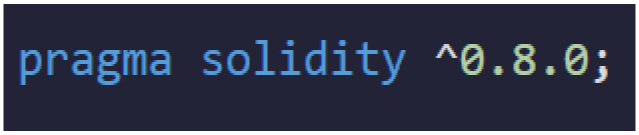
No high severity vulnerabilities were found.

Medium

No Medium severity vulnerabilities were found.

Low

(1) Compiler version can be upgraded.



```
pragma solidity ^0.8.0;
```

Although this does not raise any security vulnerability, using the latest compiler version can help to prevent any compiler level bugs.

Solution: This issue is acknowledged.

Conclusion

The Smart Contract code passed the audit successfully on the Ethereum Mainnet with some considerations to take. There were one low severity warnings raised meaning that they should be taken into consideration but if the confidence in the owner is good, they can be dismissed. The last change is advisable in order to provide more security to new holders. Nonetheless this is not necessary if the holders and/or investors feel confident with the contract owners. We were given a contract code. And we have used all possible tests based on given objects as files. So, it is good to go for production.

Since possible test cases can be unlimited for such extensive smart contract protocol, hence we provide no such guarantee of future outcomes. We have used all the latest static tools and manual observations to cover maximum possible test cases to scan everything. Smart contracts within the scope were manually reviewed and analyzed with static analysis tools. Smart Contract's high-level description of functionality was presented in Quick Stat section of the report.

Audit report contains all found security vulnerabilities and other issues in the reviewed code.

Security state of the reviewed contract is "Well Secured".

Our Methodology

We like to work with a transparent process and make our reviews a collaborative effort. The goals of our security audits are to improve the quality of systems we review and aim for sufficient remediation to help protect users. The following is the methodology we use in our security audit process.

Manual Code Review:

In manually reviewing all of the code, we look for any potential issues with code logic, error handling, protocol and header parsing, cryptographic errors, and random number generators. We also watch for areas where more defensive programming could reduce the risk of future mistakes and speed up future audits. Although our primary focus is on the in-scope code, we examine dependency code and behavior when it is relevant to a particular line of investigation.

Vulnerability Analysis:

Our audit techniques included manual code analysis, user interface interaction, and whitebox penetration testing. We look at the project's web site to get a high-level understanding of what functionality the software under review provides. We then meet with the developers to gain an appreciation of their vision of the software. We install and use the relevant software, exploring the user interactions and roles. While we do this, we brainstorm threat models and attack surfaces. We read design documentation, review other audit results, search for similar projects, examine source code dependencies, skim open issue tickets, and generally investigate details other than the implementation.

Documenting Results:

We follow a conservative, transparent process for analyzing potential security vulnerabilities and seeing them through successful remediation. Whenever a potential issue is discovered, we immediately create an Issue entry for it in this document, even though we have not yet verified the feasibility and impact of the issue. This process is conservative because we document our suspicions early even if they are later shown to not represent exploitable vulnerabilities. We generally follow a process of first documenting the suspicion with unresolved questions, then confirming the issue through code analysis, live experimentation, or automated tests. Code analysis is the most tentative, and we strive to provide test code, log captures, or screenshots demonstrating our confirmation. After this we analyze the feasibility of an attack in a live system.

Suggested Solutions:

We search for immediate mitigations that live deployments can take, and finally we suggest the requirements for remediation engineering for future releases. The mitigation and remediation recommendations should be scrutinized by the developers and deployment engineers, and successful mitigation and remediation is an ongoing collaborative process after we deliver our report, and before the details are made public.

Disclaimers

Privacy Block Solutions Disclaimer

Block Solutions team has analyzed this smart contract in accordance with the best industry practices at the date of this report, in relation to: 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).

Due to the fact that the total number of test cases are unlimited, the audit makes no statements or warranties on security of the code. It also cannot be considered as a sufficient assessment regarding the utility and safety of the code, bug free status or any other statements of the contract. 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 also suggest conducting a bug bounty program to confirm the high level of security of this smart contract.

Technical Disclaimer

Smart contracts are deployed and executed on the blockchain platform. The platform, its programming language, and other software related to the smart contract can have their own vulnerabilities that can lead to hacks.

Thus, the audit can’t guarantee explicit security of the audited smart contracts.

META - AUDITS

THANK YOU

Request Your Audit -

t.me/MetaAudit

www.Meta-Audit.io