AudiTBlock

KRYPTOTHUNGS

v0.8.18+commit.c7e474f2

✦ Low-Risk

low-risk code

✦ Medium-Risk

medium-risk code

✦ High-Risk

high-risk code

KRYPTOTHUNGS

Disclaimer AUDITBLOCK is not responsible for any financial losses. Nothing in this contract audit is financial advice, please do your own research.

Disclaimer

AudiTBlock is not responsible if a project turns out to be a scam, rug-pull or honeypot. We only provide a detailed analysis for your own research.

AudiTBlock is not responsible for any financial losses. Nothing in this contract audit is financial advice, please do your ownresearch.

The information provided in this audit is for informational purposes only and should not be considered investment advice. We does not endorse, recommend, support or suggest to invest in any project.

AudiTBlock can not be held responsible for when a project turns out to be a rug-pull, honeypot or scam.

Tokenomics

- EVM

Source Code

- AudiTBlock was complete audit phases to perform an audit based on the following smart contract:

Snapshot 0.1

```
OPERATOR_FILTER_REGISTRY: <constant> address
_BITMASK_ADDRESS_DATA_ENTRY: <constant> uint256
_BITPOS_NUMBER_MINTED: <constant> uint256
_BITPOS_NUMBER_BURNED: <constant> uint256
_BITPOS_AUX: <constant> uint256
_BITMASK_AUX_COMPLEMENT: <constant> uint256
_BITPOS_START_TIMESTAMP: <constant> uint256
_BITMASK_BURNED: <constant> uint256
_BITPOS_NEXT_INITIALIZED: <constant> uint256
_BITMASK_NEXT_INITIALIZED: <constant> uint256
_BITPOS_EXTRA_DATA: <constant> uint256
_BITMASK_EXTRA_DATA_COMPLEMENT: <constant> uint256
_BITMASK_ADDRESS: <constant> uint256
_MAX_MINT_ERC2309_QUANTITY_LIMIT: <constant> uint256
_TRANSFER_EVENT_SIGNATURE: <constant> bytes32
_currentIndex: 0 uint256
_burnCounter: 0 uint256
_name: KryptoThugs string
_symbol: KT string
_packedOwnerships: mapping(uint256 => uint256)
_packedAddressData: mapping(address => uint256)
_tokenApprovals: mapping(uint256 => struct
ERC721A.TokenApprovalRef)
_operatorApprovals: mapping(address => mapping(address => bool))
```

Snapshot 0.1

```
0:_setDefaultRoyalty(receiver,
feeNumerator) - 22702 gas
1:constructor() - 22702 gas

01147 JUMP - LINE 2165
01148 JUMPDEST - LINE 2165
01149 PUSH12 ffffffffffffffffffffffff -
LINE 2165
01162 AND - LINE 2165
01163 DUP2 - LINE 2165
01164 PUSH12 ffffffffffffffffffffffff -
LINE 2165
01177 AND - LINE 2165
01178 GT - LINE 2165
01179 ISZERO - LINE 2165
01180 PUSH3 0004dd -
LINE 2165
01184 JUMPI - LINE 2165
01185 PUSH1 40 -
01187 MLOAD -
01188 PUSH32
08c379a00000000000000000000
000000000000000000000000000
0000000000 -
01221 DUP2 -
01222 MSTORE -
01223 PUSH1 04 -
01225 ADD -
01226 PUSH3 0004d4 -
01230 SWAP1 -
01231 PUSH3 000abf -
01235 JUMP -
01236 JUMPDEST -
01237 PUSH1 40 -
01239 MLOAD -
01240 DUP1 -
01241 SWAP2 -
01242 SUB -
01243 SWAP1 -
01244 REVERT -
01245 JUMPDEST - LINE 2165
01246 PUSH1 00 -
01248 PUSH20
ffffffffffffffffffffffffffffffffffffffff -
01269 AND -
01270 DUP3 -
01271 PUSH20
ffffffffffffffffffffffffffffffffffffffff -
01292 AND -
01293 SUB -
01294 PUSH3 00054f -
01298 JUMPI -
01299 PUSH1 40 -
01301 MLOAD -
01302 PUSH32
08c379a00000000000000000000
000000000000000000000000000
0000000000 -
01335 DUP2 -
01336 MSTORE -
01337 PUSH1 04 -
01339 ADD -
01340 PUSH3 000546 -
01344 SWAP1 -
01345 PUSH3 000b31 -
01349 JUMP -
01350 JUMPDEST -
01351 PUSH1 40 -
01353 MLOAD -
01354 DUP1 -
01355 SWAP2 -
01356 SUB -
01357 SWAP1 -
01358 REVERT -
01359 JUMPDEST -
01360 PUSH1 40 -
01362 MLOAD -
01363 DUP1 -
01364 PUSH1 40 -
01366 ADD -
01367 PUSH1 40 -
01369 MSTORE -
01370 DUP1 -
01371 DUP4 -
01372 PUSH20
ffffffffffffffffffffffffffffffffffffffff -
01393 AND -
01394 DUP2 -
01395 MSTORE -
01396 PUSH1 20 -
01398 ADD -
01399 DUP3 -
01400 PUSH12 ffffffffffffffffffffffff -
01413 AND -
01414 DUP2 -
01415 MSTORE -
01416 POP -
01417 PUSH1 09 -
01419 PUSH1 00 -
01421 DUP3 -
01422 ADD -
01423 MLOAD -
01424 DUP2 -
01425 PUSH1 00 -
01427 ADD -
01428 PUSH1 00 -
01430 PUSH2 0100 -
01433 EXP -
01434 DUP2 -
01435 SLOAD -
01436 DUP2 -
01437 PUSH20
ffffffffffffffffffffffffffffffffffffffff -
01458 MUL -
01459 NOT -
01460 AND -
01461 SWAP1 -
```

Tested Contract Files

The following are the MD5 hashes of the reviewed files. A file with a different MD5 hash has been modified, intentionally or otherwise,
after the security review. You are cautioned that a different MD5 hash could be (but is not necessarily) an indication of a changed
condition or potential vulnerability that was not within the scope of the review

File	Fingerprint (MD5
Contracts/KRYPTOTHUNGS.sol	640484c015957ec80809294fdcb465eb

Used Code from other Frameworks/Smart Contracts (direct imports)

Dependency / Import Path	Source Sha1 Hash
Contracts/openzeppelin,	0ca1f7e32def098d55dc0b0050349671e45dadcc

Auto

```
block.chainid:0xd05
block.coinbase:0x000000000
0000000000000000000000000
00000
block.difficulty:0
block.gaslimit:4270090
block.number:1
block.timestamp:1687370600
msg.sender:0x5B38Da6a701c5
68545dCfcB03FcB875f56beddC
4
msg.sig:0x60806040
msg.value:0 Wei
tx.origin:0x5B38Da6a701c56
8545dCfcB03FcB875f56beddC4
block.basefee:1 Wei (1)
```

```
"0x60566050600b82828239805160001a6073146043577f4e487b71000000000000000000000000000000
00000000000000000000000000600052600060045260246000fd5b30600052607381538281f3fe7300000
0000000000000000000000000000000000030146080604052600080fdfea2646970667358221220cb6cd1
843f247598bd0fd0ad1b8ca79feebe0e1b1f162470d87e8b8be631890d64736f6c634300080f0033" ]
```

0.2 SOLIDITY UNIT TESTING

```
Progress:  Starting
PASS ✓  Tested


✓ Check winning proposal
✓ Check winning proposal with return value
✓ Before all
✓ Check success
✓ Check success2
✓ Check sender and value




Result for tests Passed:
                                          0Time Taken: 0.54s
```

Manual and Automated Vulnerability Test

CRITICAL ISSUES

During the audit, AudiTBlock experts found **0 medium Critical issues** in the code of the smart contract.

HIGH ISSUES

During the audit, AudiTBlock experts found **0 High issues** in the code of the smart contract.

MEDIUM ISSUES

During the audit, AudiTBlock experts found **Medium issues** in the code of the smart contract.

LOW ISSUES

During the audit, AudiTBlock experts found **1 Low issues** in the code of the smart contract.

INFORMATIONAL ISSUES

During the audit, AuditBlock experts
found **0 Informational issues** in the code of the smart contract.

SWC Attacks

ID	Title		Test Result
SWC-131	Presence of unused variables	CWE-1164: Irrelevant Code	✓
SWC-130	Right-To-Left-Override control character (U+202E)	CWE-451: User Interface (UI) Misrepresentation of Critical Information	✓
SWC-129	Typographical Error	CWE-480: Use of Incorrect Operator	✓
SWC-128	DoS With Block Gas Limit	CWE-400: Uncontrolled Resource Consumption	✓
SWC-127	Arbitrary Jump with Function TypeVariable	CWE-695: Use of Low-Level Functionality	✓
SWC-125	Incorrect Inheritance Order	CWE-696: Incorrect Behavior Order	✓
SWC-124	Write to Arbitrary Storage Location	CWE-123: Write-what-where Condition	✓
SWC-123	**Requirement Violation**	**CWE-573: Improper Following of Specification by Caller**	✓

ID	Title		Test Result
SWC-113	DoS with Failed Call	CWE-703: Improper Check or Handling of Exceptional Conditions	✓
SWC-112	Delegatecall to Untrusted Callee	CWE-829: Inclusion of Functionality from Untrusted Control Sphere	✓
SWC-111	Use of Deprecated Solidity Functions	CWE-477: Use of Obsolete Function	✓
SWC-110	Assert Violation	CWE-670: Always-Incorrect Control Flow Implementation	✓
SWC-109	Uninitialized Storage Pointer	CWE-824: Access of Uninitialized Pointer	✓
SWC-108	State Variable Default Visibility	CWE-710: Improper Adherence to Coding Standards	✓
SWC-107	Reentrancy	CWE-841: Improper Enforcement of Behavioral Workflow	✓
SWC-106	Unprotected SELFDESTRUCT Instruction	CWE-284: Improper Access Control	✓
SWC-105	Unprotected Ether Withdrawal	CWE-284: Improper Access Control	✓
SWC-104	**Unchecked Call Return Value**	**CWE-252: Unchecked Return Value**	✓

Owner privileges

- Status: tested 1 and verified✓
- Status: tested 2 and verified✓
- Status: tested 3 and verified✓
- Status: tested 4 and verified✓

Executive Summary

Two (2) independent AuditBlock experts performed an unbiased and isolated audit of the smart contract. The final debriefs

The overall code quality is good and not overloaded with unnecessary functions, these is greatly

benefiting the security of the contract. It correctly implemented widely used and reviewed contracts he main goal of the audit was to verify the claims regarding the security of the smart contract and the claims inside the scope of work.

During the audit, no Critical issues were found after the manual and automated security testing.

Tester On EVM

VERIFIED ✔

File: CONTRACT/KRYPTOTHUNGS.sol