Ether Authority

www.EtherAuthority.io
audit@etherauthority.io

SMART CONTRACT

Security Audit Report

Project: Dusktopia Token
Platform: Ethereum Network
Language: Solidity
Date: June 10th, 2022

Table of contents

Email: audit@EtherAuthority.io

`

THIS IS SECURITY AUDIT REPORT DOCUMENT AND WHICH MAY CONTAIN INFORMATION WHICH IS CONFIDENTIAL. WHICH INCLUDES ANY POTENTIAL VULNERABILITIES AND MALICIOUS CODES WHICH CAN BE USED TO EXPLOIT THE SOFTWARE. THIS MUST BE REFERRED INTERNALLY AND ONLY SHOULD BE MADE AVAILABLE TO THE PUBLIC AFTER ISSUES ARE RESOLVED.

Email: audit@EtherAuthority.io

Introduction

EtherAuthority was contracted by the Desktopia team to perform the Security audit of the Dusktopia smart contract code. The audit has been performed using manual analysis as well as using automated software tools. This report presents all the findings regarding the audit performed on June 10th, 2022.

The purpose of this audit was to address the following:

- Ensure that all claimed functions exist and function correctly.
- Identify any security vulnerabilities that may be present in the smart contract.

Project Background

Dusktopia Contracts have functions like dusklistMint, reserveMint, publicMint, release, etc. The Dusktopia contract inherits the Ownable, ECDSA, PaymentSplitter standard smart contracts from the OpenZeppelin library. These OpenZeppelin contracts are considered community-audited and time-tested, and hence are not part of the audit scope.

Audit scope

Name	**Code Review and Security Analysis Report for Dusktopia Smart Contract**
Platform	**Ethereum / Solidity**
File	Dusktopia.sol
File MD5 Hash	AB249E010CAB46644E270CC02BA7C267
Audit Date	June 10th, 2022

Email: audit@EtherAuthority.io

Claimed Smart Contract Features

Claimed Feature Detail	Our Observation
Tokenomics: • Name: Dusktopia • Symbol: DUSK • Dusk List Limit: 2 • Reserve Limit: 1 • Public Limit: 1 • Maximum Supply: 5555 • Reserved Tokens: 55 • DL Supply: 4055	**YES, This is valid.**
Ownership Control: • Dusktopia owners can set a new signer address. • Dusktopia owners can set a new Dusklist token limit. • Dusktopia owners can set a new reserve token limit.	**YES, This is valid.**

Audit Summary

According to the standard audit assessment, Customer`s solidity based smart contracts are **“Secured”**. This token contract does contain owner control, which does not make it fully decentralized.

We used various tools like Slither, Solhint 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 Audit overview section. General overview is presented in AS-IS section and all identified issues can be found in the Audit overview section.

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

Investors Advice: Technical audit of the smart contract does not guarantee the ethical nature of the project. Any owner controlled functions should be executed by the owner with responsibility. All investors/users are advised to do their due diligence before investing in the project.

Technical Quick 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	Passed
	Race condition	Passed
	Logical vulnerability	Passed
	Features claimed	Passed
	Other programming issues	Moderated
Code Specification	Function visibility not explicitly declared	Passed
	Var. storage location not explicitly declared	Passed
	Use keywords/functions to be deprecated	Passed
	Unused code	Passed
Gas Optimization	“Out of Gas” Issue	Passed
	High consumption ‘for/while’ loop	Passed
	High consumption ‘storage’ storage	Passed
	Assert() misuse	Passed
Business Risk	The maximum limit for mintage not set	Passed
	“Short Address” Attack	Passed
	“Double Spend” Attack	Passed

Overall Audit Result: **PASSED**

Email: audit@EtherAuthority.io

Code Quality

This audit scope has 1 smart contract. Smart contract contains Libraries, Smart contracts, inherits and Interfaces. This is a compact and well written smart contract.

The libraries in Dusktopia Token are part of its logical algorithm. A library is a different type of smart contract that contains 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 the Dusktopia Token.

The Dusktopia Token team has **not** provided scenario and unit test scripts, which would have helped to determine the integrity of the code in an automated way.

Code parts are **well** commented on in the smart contracts. Ethereum's NatSpec commenting style is recommended.

Documentation

We were given a Dusktopia Token smart contract code in the form of a file. The hash of that code is mentioned above in the table.

As mentioned above, code parts are **well** commented. So it is easy to quickly understand the programming flow as well as complex code logic. Comments are very helpful in understanding the overall architecture of the protocol.

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.

Apart from libraries, its functions are used in external smart contract calls.

AS-IS overview

Functions

Sl.	Functions	Type	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	_startTokenId	internal	Passed	No Issue
3	totalSupply	read	Passed	No Issue
4	_totalMinted	internal	Passed	No Issue
5	supportsInterface	read	Passed	No Issue
6	balanceOf	read	Passed	No Issue
7	_numberMinted	internal	Passed	No Issue
8	_numberBurned	internal	Passed	No Issue
9	_getAux	internal	Passed	No Issue
10	_setAux	internal	Passed	No Issue
11	_ownershipOf	internal	Passed	No Issue
12	ownerOf	read	Passed	No Issue
13	name	read	Passed	No Issue
14	symbol	read	Passed	No Issue
15	tokenURI	read	Passed	No Issue
16	_baseURI	internal	Passed	No Issue
17	approve	write	Passed	No Issue
18	getApproved	read	Passed	No Issue
19	setApprovalForAll	write	Passed	No Issue
20	isApprovedForAll	read	Passed	No Issue
21	transferFrom	write	Passed	No Issue
22	safeTransferFrom	write	Passed	No Issue
23	safeTransferFrom	write	Passed	No Issue
24	_exists	internal	Passed	No Issue
25	_safeMint	internal	Passed	No Issue
26	_mint	internal	Passed	No Issue
27	_transfer	internal	Passed	No Issue
28	_burn	internal	Passed	No Issue
29	_burn	internal	Passed	No Issue
30	_approve	write	Passed	No Issue
31	_checkContractOnERC721Received	write	Passed	No Issue
32	_beforeTokenTransfers	internal	Passed	No Issue
33	_afterTokenTransfers	internal	Passed	No Issue
34	owner	read	Passed	No Issue
35	onlyOwner	modifier	Passed	No Issue
36	renounceOwnership	write	access only Owner	No Issue
37	transferOwnership	write	access only Owner	No Issue
38	_transferOwnership	internal	Passed	No Issue
39	receive	external	Passed	No Issue
40	totalShares	read	Passed	No Issue
41	totalReleased	read	Passed	No Issue

42	totalReleased	read	Passed	No Issue
43	shares	read	Passed	No Issue
44	released	read	Passed	No Issue
45	payee	read	Passed	No Issue
46	releasable	read	Passed	No Issue
47	release	write	Passed	No Issue
48	_pendingPayment	read	Passed	No Issue
49	_addPayee	write	Passed	No Issue
50	dusklistMint	external	Passed	No Issue
51	reserveMint	external	Passed	No Issue
52	publicMint	external	Passed	No Issue
53	_teamMint	internal	Passed	No Issue
54	setSaleState	external	access only Owner	No Issue
55	setBaseTokenURI	external	access only Owner	No Issue
56	setSignerAddress	external	access only Owner	No Issue
57	setTokenCost	external	access only Owner	No Issue
58	setDusklistLimit	external	access only Owner	No Issue
59	setReserveLimit	external	access only Owner	No Issue
60	setPublicLimit	external	access only Owner	No Issue
61	signerAddress	external	Passed	No Issue
62	release	write	Passed	No Issue
63	_startTokenId	internal	Passed	No Issue
64	_baseURI	internal	Passed	No Issue
65	_verifySignature	internal	Passed	No Issue

Severity Definitions

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
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.

Email: audit@EtherAuthority.io

Audit Findings

Critical Severity

No Critical severity vulnerabilities were found.

High Severity

No High severity vulnerabilities were found.

Medium

No Medium severity vulnerabilities were found.

Low

No Low severity vulnerabilities were found.

Very Low / Informational / Best practices:

No Very Low / Informational severity vulnerabilities were found.

Email: audit@EtherAuthority.io

Centralization

This smart contract has some functions which can be executed by the Admin (Owner) only. If the admin wallet private key would be compromised, then it would create trouble. Following are Admin functions:

- setSaleState: Owner can set a new sale state.
- setBaseTokenURI: Owner can set a new token URI.
- setSignerAddress: Owner can set a new signer address.
- setTokenCost: Owner can set a new token cost.
- setDusklistLimit: Owner can set a new Dusklist token limit.
- setReserveLimit: Owner can set a new reserve token limit.
- setPublicLimit: Owner can set a new public token limit.

To make the smart contract 100% decentralized, we suggest renouncing ownership in the smart contract once its function is completed.

Conclusion

We were given a contract code form of a file. And we have used all possible tests based on given objects as files. We have not observed any major issues. So, **Smart Contract is good for production**.

Since possible test cases can be unlimited for such smart contracts protocol, 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 the As-is overview section of the report.

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

Security state of the reviewed smart contract, based on standard audit procedure scope, is **"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

EtherAuthority.io Disclaimer

EtherAuthority 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).

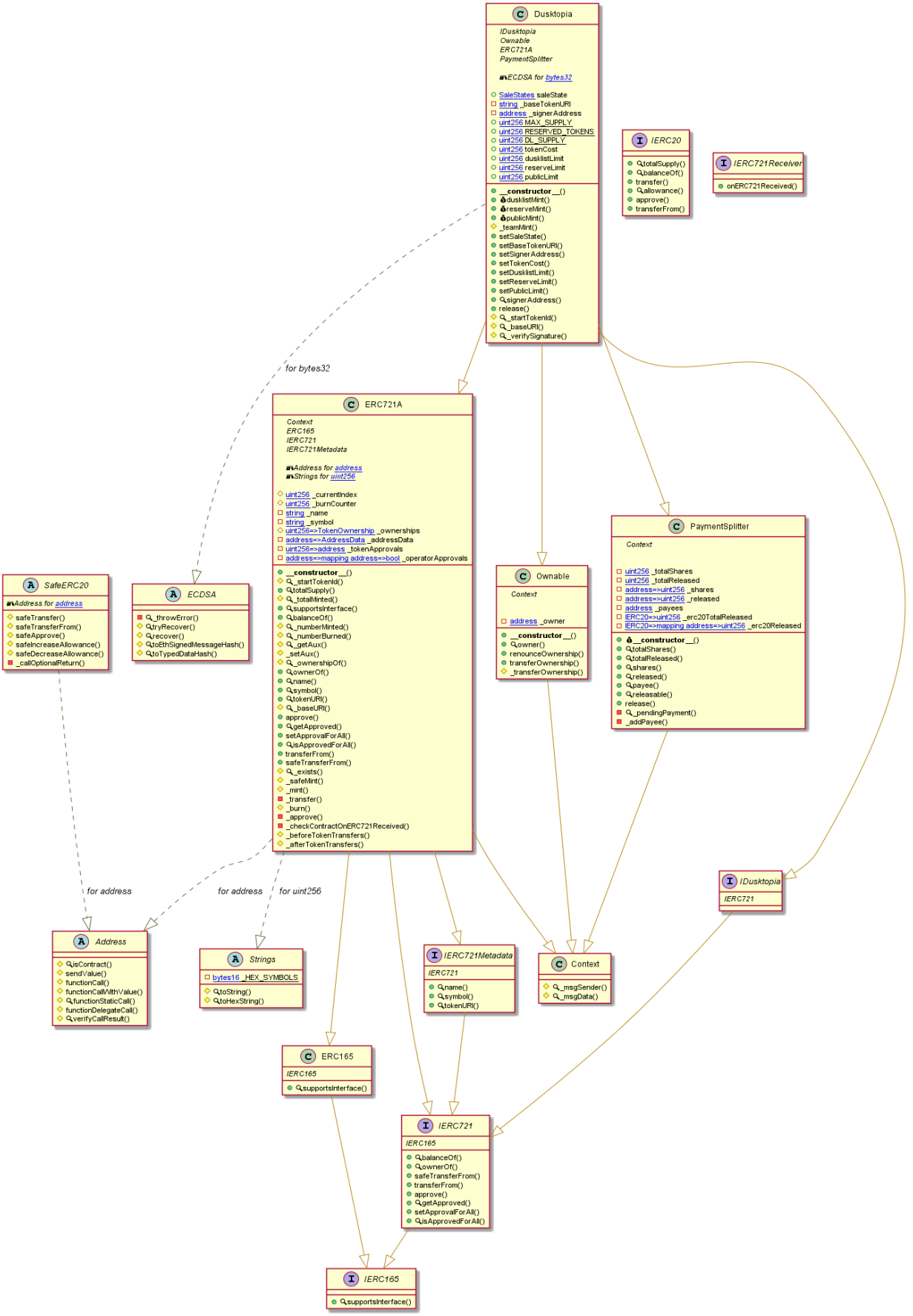
Due to the fact that the total number of test cases are unlimited, the audit makes no statements or warranties on security of the code. It also cannot be considered as a sufficient assessment regarding the utility and safety of the code, bugfree status or any other statements of the contract. While we 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.

Appendix

Code Flow Diagram - Dusktopia Token



Slither Results Log

Slither Log >> Dusktopia.sol

```
INFO:Detectors:
Dusktopia.setSignerAddress(address).newSignerAddress (Dusktopia.sol#873) lacks a zero-check on :
                - _signerAddress = newSignerAddress (Dusktopia.sol#874)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#missing-zero-address-validation
INFO:Detectors:
Variable 'ECDSA.tryRecover(bytes32,bytes).r (Dusktopia.sol#262)' in ECDSA.tryRecover(bytes32,bytes) (Dusktopia.sol#260-282) po
tially used before declaration: r = mload(uint256)(signature + 0x20) (Dusktopia.sol#275)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#pre-declaration-usage-of-local-variables
INFO:Detectors:
Reentrancy in PaymentSplitter.release(address) (Dusktopia.sol#772-784):
        External calls:
        - Address.sendValue(account,payment) (Dusktopia.sol#782)
        Event emitted after the call(s):
        - PaymentReleased(account,payment) (Dusktopia.sol#783)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-3
INFO:Detectors:
Address.verifyCallResult(bool,bytes,string) (Dusktopia.sol#123-141) uses assembly
        - INLINE ASM (Dusktopia.sol#133-136)
ECDSA.tryRecover(bytes32,bytes) (Dusktopia.sol#260-282) uses assembly
        - INLINE ASM (Dusktopia.sol#265-269)
        - INLINE ASM (Dusktopia.sol#274-277)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#assembly-usage
INFO:Detectors:
Address.functionCall(address,bytes) (Dusktopia.sol#66-70) is never used and should be removed
Address.functionCallWithValue(address,bytes,uint256) (Dusktopia.sol#72-78) is never used and should be removed
Address.functionCallWithValue(address,bytes,uint256,string) (Dusktopia.sol#80-91) is never used and should be removed
Address.functionDelegateCall(address,bytes) (Dusktopia.sol#108-110) is never used and should be removed
Address.functionDelegateCall(address,bytes,string) (Dusktopia.sol#112-121) is never used and should be removed
Address.functionStaticCall(address,bytes) (Dusktopia.sol#93-95) is never used and should be removed
Address.functionStaticCall(address,bytes,string) (Dusktopia.sol#97-106) is never used and should be removed
Address.isContract(address) (Dusktopia.sol#53-56) is never used and should be removed
Address.verifyCallResult(bool,bytes,string) (Dusktopia.sol#123-141) is never used and should be removed
Context._msgData() (Dusktopia.sol#364-366) is never used and should be removed
Dusktopia._teamMint(address) (Dusktopia.sol#861-863) is never used and should be removed
Dusktopia._verifySignature(bytes,string) (Dusktopia.sol#909-914) is never used and should be removed
ECDSA._throwError(ECDSA.RecoverError) (Dusktopia.sol#246-258) is never used and should be removed
ECDSA.recover(bytes32,bytes) (Dusktopia.sol#284-288) is never used and should be removed
```

```
ECDSA.recover(bytes32,bytes) (Dusktopia.sol#284-288) is never used and should be removed
ECDSA.recover(bytes32,bytes32,bytes32) (Dusktopia.sol#300-308) is never used and should be removed
ECDSA.recover(bytes32,uint8,bytes32,bytes32) (Dusktopia.sol#331-340) is never used and should be removed
ECDSA.toEthSignedMessageHash(bytes) (Dusktopia.sol#346-348) is never used and should be removed
ECDSA.toEthSignedMessageHash(bytes32) (Dusktopia.sol#342-344) is never used and should be removed
ECDSA.toTypedDataHash(bytes32,bytes32) (Dusktopia.sol#350-352) is never used and should be removed
ECDSA.tryRecover(bytes32,bytes) (Dusktopia.sol#260-282) is never used and should be removed
ECDSA.tryRecover(bytes32,bytes32,bytes32) (Dusktopia.sol#290-298) is never used and should be removed
ECDSA.tryRecover(bytes32,uint8,bytes32,bytes32) (Dusktopia.sol#310-329) is never used and should be removed
ERC721A._baseURI() (Dusktopia.sol#516-518) is never used and should be removed
ERC721A._burn(uint256) (Dusktopia.sol#628-630) is never used and should be removed
ERC721A._burn(uint256,bool) (Dusktopia.sol#632-646) is never used and should be removed
ERC721A._exists(uint256) (Dusktopia.sol#561-564) is never used and should be removed
ERC721A._getAux(address) (Dusktopia.sol#488-490) is never used and should be removed
ERC721A._mint(address,uint256) (Dusktopia.sol#572-591) is never used and should be removed
ERC721A._numberBurned(address) (Dusktopia.sol#484-486) is never used and should be removed
ERC721A._numberMinted(address) (Dusktopia.sol#480-482) is never used and should be removed
ERC721A._safeMint(address,uint256) (Dusktopia.sol#566-568) is never used and should be removed
ERC721A._setAux(address,uint64) (Dusktopia.sol#492-494) is never used and should be removed
ERC721A._startTokenId() (Dusktopia.sol#454-456) is never used and should be removed
ERC721A._totalMinted() (Dusktopia.sol#464-468) is never used and should be removed
SafeERC20.safeApprove(IERC20,address,uint256) (Dusktopia.sol#185-195) is never used and should be removed
SafeERC20.safeDecreaseAllowance(IERC20,address,uint256) (Dusktopia.sol#206-217) is never used and should be removed
SafeERC20.safeIncreaseAllowance(IERC20,address,uint256) (Dusktopia.sol#197-204) is never used and should be removed
SafeERC20.safeTransferFrom(IERC20,address,address,uint256) (Dusktopia.sol#176-183) is never used and should be removed
Strings.toHexString(uint256) (Dusktopia.sol#27-38) is never used and should be removed
Strings.toHexString(uint256,uint256) (Dusktopia.sol#40-50) is never used and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code
INFO:Detectors:
Pragma version^0.8.4 (Dusktopia.sol#2) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6
solc-0.8.4 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
```

```
INFO:Detectors:
Low level call in Address.sendValue(address,uint256) (Dusktopia.sol#58-63):
        - (success) = recipient.call{value: amount}() (Dusktopia.sol#61)
Low level call in Address.functionCallWithValue(address,bytes,uint256,string) (Dusktopia.sol#80-91):
        - (success,returndata) = target.call{value: value}(data) (Dusktopia.sol#89)
Low level call in Address.functionStaticCall(address,bytes,string) (Dusktopia.sol#97-106):
        - (success,returndata) = target.staticcall(data) (Dusktopia.sol#104)
Low level call in Address.functionDelegateCall(address,bytes,string) (Dusktopia.sol#112-121):
        - (success,returndata) = target.delegatecall(data) (Dusktopia.sol#119)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls
INFO:Detectors:
Variable ERC721A._currentIndex (Dusktopia.sol#432) is not in mixedCase
Variable ERC721A._burnCounter (Dusktopia.sol#434) is not in mixedCase
Variable ERC721A._ownerships (Dusktopia.sol#440) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions
INFO:Detectors:
Dusktopia (Dusktopia.sol#824-916) does not implement functions:
        - IERC721.safeTransferFrom(address,address,uint256,bytes) (Dusktopia.sol#400-405)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#unimplemented-functions
INFO:Detectors:
ERC721A._burnCounter (Dusktopia.sol#434) should be constant
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-constant
```

```
INFO:Detectors:
totalSupply() should be declared external:
        - ERC721A.totalSupply() (Dusktopia.sol#458-462)
balanceOf(address) should be declared external:
        - ERC721A.balanceOf(address) (Dusktopia.sol#477-478)
name() should be declared external:
        - ERC721A.name() (Dusktopia.sol#502-504)
symbol() should be declared external:
        - ERC721A.symbol() (Dusktopia.sol#506-508)
tokenURI(uint256) should be declared external:
        - ERC721A.tokenURI(uint256) (Dusktopia.sol#510-514)
approve(address,uint256) should be declared external:
        - ERC721A.approve(address,uint256) (Dusktopia.sol#520-527)
getApproved(uint256) should be declared external:
        - ERC721A.getApproved(uint256) (Dusktopia.sol#529-532)
setApprovalForAll(address,bool) should be declared external:
        - ERC721A.setApprovalForAll(address,bool) (Dusktopia.sol#534-538)
transferFrom(address,address,uint256) should be declared external:
        - ERC721A.transferFrom(address,address,uint256) (Dusktopia.sol#544-550)
safeTransferFrom(address,address,uint256) should be declared external:
        - ERC721A.safeTransferFrom(address,address,uint256) (Dusktopia.sol#552-558)
renounceOwnership() should be declared external:
        - Ownable.renounceOwnership() (Dusktopia.sol#689-691)
transferOwnership(address) should be declared external:
        - Ownable.transferOwnership(address) (Dusktopia.sol#693-696)
totalShares() should be declared external:
        - PaymentSplitter.totalShares() (Dusktopia.sol#734-736)
shares(address) should be declared external:
        - PaymentSplitter.shares(address) (Dusktopia.sol#746-748)
payee(uint256) should be declared external:
        - PaymentSplitter.payee(uint256) (Dusktopia.sol#758-760)
release(IERC20,address) should be declared external:
        - PaymentSplitter.release(IERC20,address) (Dusktopia.sol#786-798)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#public-function-that-could-be-declared-external
INFO:Slither:Dusktopia.sol analyzed (16 contracts with 75 detectors), 73 result(s) found
INFO:Slither:Use https://crytic.io/ to get access to additional detectors and Github integration
```

Solidity Static Analysis

Dusktopia.sol

Security

Transaction origin:

Use of tx.origin: "tx.origin" is useful only in very exceptional cases. If you use it for authentication, you usually want to replace it by "msg.sender", because otherwise any contract you call can act on your behalf.
more
Pos: 1261:29:

Check-effects-interaction:

Potential violation of Checks-Effects-Interaction pattern in SafeERC20.safeDecreaseAllowance(contract IERC20,address,uint256): Could potentially lead to re-entrancy vulnerability. Note: Modifiers are currently not considered by this static analysis.
more
Pos: 274:4:

Inline assembly:

The Contract uses inline assembly, this is only advised in rare cases. Additionally static analysis modules do not parse inline Assembly, this can lead to wrong analysis results.
more
Pos: 923:19:

Block timestamp:

Use of "block.timestamp": "block.timestamp" can be influenced by miners to a certain degree. That means that a miner can "choose" the block.timestamp, to a certain degree, to change the outcome of a transaction in the mined block.
more
Pos: 881:48:

Gas & Economy

Gas costs:

Gas requirement of function PaymentSplitter.release is infinite: If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)
Pos: 1331:7:

For loop over dynamic array:

Loops that do not have a fixed number of iterations, for example, loops that depend on storage values, have to be used carefully. Due to the block gas limit, transactions can only consume a certain amount of gas. The number of iterations in a loop can grow beyond the block gas limit which can cause the complete contract to be stalled at a certain point. Additionally, using unbounded loops incurs in a lot of avoidable gas costs. Carefully test how many items at maximum you can pass to such functions to make it successful.
more
Pos: 1028:11:

Email: audit@EtherAuthority.io

Miscellaneous

Constant/View/Pure functions:

Dusktopia._verifySignature(bytes,string) : Is constant but potentially should not be. Note: Modifiers are currently not considered by this static analysis.
more
Pos: 1350:7:

Similar variable names:

PaymentSplitter._addPayee(address,uint256) : Variables have very similar names "_shares" and "shares_". Note: Modifiers are currently not considered by this static analysis.
Pos: 1176:36:

No return:

ERC721A.balanceOf(address): Defines a return type but never explicitly returns a value.
Pos: 660:7:

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.
more
Pos: 1171:11:

Data truncated:

Division of integer values yields an integer value again. That means e.g. 10 / 100 = 0 instead of 0.1 since the result is an integer again. This does not hold for division of (only) literal values since those yield rational constants.
Pos: 1160:18:

Solhint Linter

Dusktopia.sol

```
Dusktopia.sol:279:18: Error: Parse error: missing ';' at '{'
Dusktopia.sol:642:18: Error: Parse error: missing ';' at '{'
Dusktopia.sol:648:18: Error: Parse error: missing ';' at '{'
Dusktopia.sol:684:18: Error: Parse error: missing ';' at '{'
Dusktopia.sol:803:18: Error: Parse error: missing ';' at '{'
Dusktopia.sol:834:18: Error: Parse error: missing ';' at '{'
Dusktopia.sol:874:18: Error: Parse error: missing ';' at '{'
Dusktopia.sol:894:48: Error: Parse error: mismatched input ';'
expecting '('
Dusktopia.sol:897:18: Error: Parse error: missing ';' at '{'
Dusktopia.sol:1184:16: Error: Parse error: mismatched input '('
expecting {';', '='}
Dusktopia.sol:1185:26: Error: Parse error: mismatched input '('
expecting {';', '='}
Dusktopia.sol:1186:27: Error: Parse error: mismatched input '('
expecting {';', '='}
Dusktopia.sol:1187:28: Error: Parse error: mismatched input '('
expecting {';', '='}
Dusktopia.sol:1188:28: Error: Parse error: mismatched input '('
expecting {';', '='}
Dusktopia.sol:1189:28: Error: Parse error: mismatched input '('
expecting {';', '='}
Dusktopia.sol:1190:27: Error: Parse error: mismatched input '('
expecting {';', '='}
Dusktopia.sol:1191:26: Error: Parse error: mismatched input '('
expecting {';', '='}
Dusktopia.sol:1192:30: Error: Parse error: mismatched input '('
expecting {';', '='}
Dusktopia.sol:1193:26: Error: Parse error: mismatched input '('
expecting {';', '='}
Dusktopia.sol:1232:50: Error: Parse error: mismatched input '('
expecting {';', '='}
Dusktopia.sol:1233:69: Error: Parse error: mismatched input '('
expecting {';', '='}
Dusktopia.sol:1234:76: Error: Parse error: mismatched input '('
expecting {';', '='}
Dusktopia.sol:1235:72: Error: Parse error: mismatched input '('
expecting {';', '='}
Dusktopia.sol:1236:90: Error: Parse error: mismatched input '('
expecting {';', '='}
Dusktopia.sol:1237:77: Error: Parse error: mismatched input '('
expecting {';', '='}
Dusktopia.sol:1246:50: Error: Parse error: mismatched input '('
expecting {';', '='}
Dusktopia.sol:1247:68: Error: Parse error: mismatched input '('
expecting {';', '='}
Dusktopia.sol:1248:61: Error: Parse error: mismatched input '('
expecting {';', '='}
Dusktopia.sol:1249:76: Error: Parse error: mismatched input '('
expecting {';', '='}
```

```
Dusktopia.sol:1250:72: Error: Parse error: mismatched input '('
expecting {';', '='}
Dusktopia.sol:1251:71: Error: Parse error: mismatched input '('
expecting {';', '='}
Dusktopia.sol:1252:76: Error: Parse error: mismatched input '('
expecting {';', '='}
Dusktopia.sol:1261:50: Error: Parse error: mismatched input '('
expecting {';', '='}
Dusktopia.sol:1262:67: Error: Parse error: mismatched input '('
expecting {';', '='}
Dusktopia.sol:1263:60: Error: Parse error: mismatched input '('
expecting {';', '='}
Dusktopia.sol:1264:76: Error: Parse error: mismatched input '('
expecting {';', '='}
Dusktopia.sol:1265:72: Error: Parse error: mismatched input '('
expecting {';', '='}
Dusktopia.sol:1266:75: Error: Parse error: mismatched input '('
expecting {';', '='}
Dusktopia.sol:1282:78: Error: Parse error: mismatched input '('
expecting {';', '='}
Dusktopia.sol:1307:59: Error: Parse error: mismatched input '('
expecting {';', '='}
Dusktopia.sol:1313:58: Error: Parse error: mismatched input '('
expecting {';', '='}
Dusktopia.sol:1319:57: Error: Parse error: mismatched input '('
expecting {';', '='}
Dusktopia.sol:1332:58: Error: Parse error: mismatched input '('
expecting {';', '='}
```

Software analysis result:

These software reported many false positive results and some are informational issues. So, those issues can be safely ignored.

Privacy Ninja

Email: audit@EtherAuthority.io