CERTIK

Security Assessment

Buff Doge Coin

Dec 9th, 2021

Table of Contents

Summary

This report has been prepared for Buff Doge Coin to discover issues and vulnerabilities in the source code of the Buff Doge Coin project as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Static Analysis and Manual Review techniques.

The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

The security assessment resulted in findings that ranged from critical to informational. We recommend addressing these findings to ensure a high level of security standards and industry practices. We suggest recommendations that could better serve the project from the security perspective:

- Enhance general coding practices for better structures of source codes;
- Add enough unit tests to cover the possible use cases;
- Provide more comments per each function for readability, especially contracts that are verified in public;
- Provide more transparency on privileged activities once the protocol is live.

Overview

Project Summary

Project Name	Buff Doge Coin
Platform	BSC
Language	Solidity
Codebase	https://bscscan.com/address/0x23125108bc4c63E4677b2E253Fa498cCb4B3298b#code
Commit	

Audit Summary

Delivery Date	Dec 09, 2021
Audit Methodology	Static Analysis, Manual Review
Key Components	

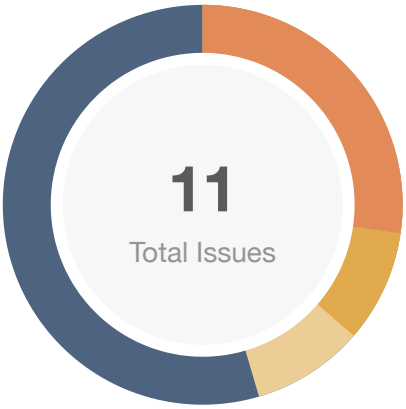
Vulnerability Summary

Vulnerability Level	Total	Pending	Declined	Acknowledged	Partially Resolved	Resolved
Critical	0	0	0	0	0	0
Major	3	0	0	2	1	0
Medium	1	0	0	0	1	0
Minor	1	0	0	1	0	0
Informational	6	0	0	6	0	0
Discussion	0	0	0	0	0	0

Audit Scope

ID	File	SHA256 Checksum

Findings



Critical	**0** (0.00%)
Major	**3** (27.27%)
Medium	**1** (9.09%)
Minor	**1** (9.09%)
Informational	**6** (54.55%)
Discussion	**0** (0.00%)

ID	Title	Category	Severity	Status
BDC-01	Typos in the contract	Coding Style	Informational	Acknowledged
BDC-02	Incorrect error message	Logical Issue	Informational	Acknowledged
BDC-03	Contract gains non-withdrawable BNB via the `swapAndLiquify` function	Logical Issue	Medium	Partially Resolved
BDC-04	Centralized risk in `addLiquidity`	**Centralization / Privilege**	**Major**	Partially Resolved
BDC-05	Return value not handled	Volatile Code	Informational	Acknowledged
BDC-06	Variable could be declared as `constant`	Gas Optimization	Informational	Acknowledged
BDC-07	3rd party dependencies	Control Flow	Minor	Acknowledged
BDC-08	Missing event emitting	Coding Style	Informational	Acknowledged
BDC-09	Redundant code	Logical Issue	Informational	Acknowledged
BDC-10	Privileged ownership	**Centralization / Privilege**	**Major**	Acknowledged
BDC-11	Possible to gain ownership after renouncing the contract ownership	**Logical Issue, Centralization / Privilege**	**Major**	Acknowledged

BDC-01 | Typos in the contract

Category	Severity	Location	Status
Coding Style	Informational	BuffDogeCoin.sol (0x23125): 895, 723	Acknowledged

Description

There are several typos in the code and comments.

1. In the following code snippet, `tokensIntoLiqudity` should be `tokensIntoLiquidity`.

```
event SwapAndLiquify(
        uint256 tokensSwapped,
        uint256 ethReceived,
        uint256 tokensIntoLiqudity
    );
```

2. `recieve` should be `receive` and `swaping` should be `swapping` in the line of comment `//to recieve ETH from uniswapV2Router when swaping`.

Recommendation

We recommend correcting all typos in the contract.

Alleviation

[Buff Doge Team]: We acknowledge the findings, and given that deployed contracts cannot be renewed, decided to keep the codebase unchanged.

BDC-02 | Incorrect error message

Category	Severity	Location	Status
Logical Issue	Informational	BuffDogeCoin.sol (0x23125): 846	Acknowledged

Description

The error message in `require(_isExcluded[account], "Account is already excluded")` does not describe the error correctly.

Recommendation

The message "Account is already excluded" can be changed to "Account is not excluded".

Alleviation

[Buff Doge Team]: We acknowledge the findings, and given that deployed contracts cannot be renewed, decided to keep the codebase unchanged.

BDC-03 | Contract gains non-withdrawable BNB via the `swapAndLiquify` function

Category	Severity	Location	Status
Logical Issue	Medium	BuffDogeCoin.sol (0x23125): 1034	Partially Resolved

Description

The `swapAndLiquify` function converts half of the `contractTokenBalance` BuffDogeCoin tokens to BNB. The other half of BuffDogeCoin tokens and part of the converted BNB are deposited into the BuffDogeCoin-BNB pool on pancakeswap as liquidity. For every `swapAndLiquify` function call, a small amount of BNB leftover in the contract. This is because the price of BuffDogeCoin drops after swapping the first half of BuffDogeCoin tokens into BNBs, and the other half of BuffDogeCoin tokens require less than the converted BNB to be paired with it when adding liquidity. The contract doesn't appear to provide a way to withdraw those BNB, and they will be locked in the contract forever.

Recommendation

It's not ideal that more and more BNB are locked into the contract over time. The simplest solution is to add a `withdraw` function in the contract to withdraw BNB. Other approaches that benefit the BuffDogeCoin token holders can be:

- Distribute BNB to BuffDogeCoin token holders proportional to the amount of token they hold.
- Use leftover BNB to buy back BuffDogeCoin tokens from the market to increase the price of BuffDogeCoin.

Alleviation

[Buff Doge Team]: In order to maintain the token price, we often use the BNB to buy back. You can check our buy back transactions here: https://bscscan.com/token/0x23125108bc4c63E4677b2E253Fa498cCb4B3298b?a=0x357c8ef37AF2E6C751759d22D71A218598A6fB1C

In the future we will continue to buy back at the right time to increase the price of Buff Doge Coin.- We also use the $DOGECOINtokenforproductstakingrewardonHOTBITwith50$DOGECOIN.

https://www.hotbit.io/invest/detail/1200?__cf_chl_jschl_tk__=1d8FvrmlHCS7Gp7N1Zvi5dg5BUm08hgNTf51HiTw38w-1638434338-0-gaNycGzNCZE-

We have Double Burn Protocol where each burn will double in its quantity to the previous burn. It is written on our website https://www.buffdogecoin.io.

Proof:https://bscscan.com/token/0x23125108bc4c63E4677b2E253Fa498cCb4B3298b?a=0x000000000000000000000000000000000000dead

Later we will burn all the remaining tokens. Therefore Buff Doge Coin is hyper deflationary tokens.

BDC-04 | Centralized risk in `addLiquidity`

Category	Severity	Location	Status
Centralization / Privilege	Major	BuffDogeCoin.sol (0x23125): 1085	Partially Resolved

Description

```
// add the liquidity
uniswapV2Router.addLiquidityETH{value: ethAmount}(
    address(this),
    tokenAmount,
    0, // slippage is unavoidable
    0, // slippage is unavoidable
    owner(),
    block.timestamp
);
```

The `addLiquidity` function calls the `uniswapV2Router.addLiquidityETH` function with the `to` address specified as `owner()` for acquiring the generated LP tokens from the `BuffDogeCoin-BNB` pool. As a result, over time the `_owner` address will accumulate a significant portion of LP tokens.If the `_owner` is an EOA (Externally Owned Account), mishandling of its private key can have devastating consequences to the project as a whole.

Recommendation

We advise the `to` address of the `uniswapV2Router.addLiquidityETH` function call to be replaced by the contract itself, i.e. `address(this)`, and to restrict the management of the LP tokens within the scope of the contract's business logic. This will also protect the LP tokens from being stolen if the `_owner` account is compromised. In general, we strongly recommend centralized privileges or roles in the protocol to be improved via a decentralized mechanism or via smart-contract based accounts with enhanced security practices, f.e. Multisignature wallets.

Indicatively, here are some feasible solutions that would also mitigate the potential risk:

- Time-lock with reasonable latency, i.e. 48 hours, for awareness on privileged operations;
- Assignment of privileged roles to multi-signature wallets to prevent single point of failure due to the private key;
- Introduction of a DAO / governance / voting module to increase transparency and user involvement.

Alleviation

[Buff Doge Team]: We decide to take a serious step using Multisignature wallets and we will complete it as soon as possible. We have our LP locked immediately after launching and by increasing LP we will continue to lock 2, 3, 4, etc, and will continue to do so when LP is not needed. Now, we have locked in $1 million. And openly, we have a project that we are working on according to the whitepaper. We will not transfer ownership with the aim that we will not be hindered from completing the projects we are working on, facilitating marketing strategies, control so that Buff Doge Coin continues to grow in the long term. These are our LP Locked link:

https://dxsale.app/app/v2_9/dxlockview?id=0&add=0x357c8ef37AF2E6C751759d22D71A218598A6fB1C&type=lplock&chain=BSC

https://dxsale.app/app/v3/dxlockview?id=0&add=0x357c8ef37AF2E6C751759d22D71A218598A6fB1C&type=lplock&chain=BSC

https://dxsale.app/app/v3/dxlockview?id=1&add=0x357c8ef37AF2E6C751759d22D71A218598A6fB1C&type=lplock&chain=BSC

https://dxsale.app/app/v3/dxlockview?id=2&add=0x357c8ef37AF2E6C751759d22D71A218598A6fB1C&type=lplock&chain=BSC

BDC-05 | Return value not handled

Category	Severity	Location	Status
Volatile Code	Informational	BuffDogeCoin.sol (0x23125): 1080~1087	Acknowledged

Description

The return values of function `addLiquidityETH` are not properly handled.

```
        uniswapV2Router.addLiquidityETH{value: ethAmount}(
            address(this),
            tokenAmount,
            0, // slippage is unavoidable
            0, // slippage is unavoidable
            owner(),
            block.timestamp
        );
```

Recommendation

We recommend using variables to receive the return value of the functions mentioned above and handle both success and failure cases if needed by the business logic.

Alleviation

[Buff Doge Team]: We acknowledge the findings, and given that deployed contracts cannot be renewed, decided to keep the codebase unchanged.

BDC-06 | Variable could be declared as `constant`

Category	Severity	Location	Status
Gas Optimization	Informational	BuffDogeCoin.sol (0x23125)	Acknowledged

Description

Variables `_tTotal`, `numTokensSellToAddToLiquidity`, `_name`, `_symbol` and `_decimals` could be declared as `constant` since these state variables are never to be changed.

Recommendation

We recommend declaring those variables as `constant`.

Alleviation

[Buff Doge Team]: We acknowledge the findings, and given that deployed contracts cannot be renewed, decided to keep the codebase unchanged.

BDC-07 | 3rd party dependencies

Category	Severity	Location	Status
Control Flow	Minor	BuffDogeCoin.sol (0x23125)	Acknowledged

Description

The contract is serving as the underlying entity to interact with third party PancakeSwap protocols. The scope of the audit would treat those 3rd party entities as black boxes and assume its functional correctness. However in the real world, 3rd parties may be compromised that led to assets lost or stolen.

Recommendation

We understand that the business logic of the BuffDogeCoin protocol requires the interaction PancakeSwap protocol for adding liquidity to BuffDogeCoin-BNB pool and swap tokens. We encourage the team to constantly monitor the statuses of those 3rd parties to mitigate the side effects when unexpected activities are observed.

Alleviation

[Buff Doge Team]: Yes, we will constantly monitor the 3rd parties. Renouncing ownership of the contract will result in an inability to adapt to 3rd party changes to include exchanges. The team had the foresight to understand this, as our understanding of the Buff Doge Coin smart contract is the best. We already have contingency plans for likely upcoming 3rd party changes and growth.

BDC-08 | Missing event emitting

Category	Severity	Location	Status
Coding Style	Informational	BuffDogeCoin.sol (0x23125)	Acknowledged

Description

In contract `BuffDogeCoin`, there are a bunch of functions can change state variables. However, these function do not emit event to pass the changes out of chain.

Recommendation

Recommend emitting events, for all the essential state variables that are possible to be changed during runtime.

Alleviation

[Buff Doge Team]: We acknowledge the findings, and given that deployed contracts cannot be renewed, decided to keep the codebase unchanged.

BDC-09 | Redundant code

Category	Severity	Location	Status
Logical Issue	Informational	BuffDogeCoin.sol (0x23125): 1100	Acknowledged

Description

The condition `!_isExcluded[sender] && !_isExcluded[recipient]` can be included in `else` .

Recommendation

The following code can be removed:

```
... else if (!_isExcluded[sender] && !_isExcluded[recipient]) {
    _transferStandard(sender, recipient, amount);
} ...
```

Alleviation

[Buff Doge Team]: We acknowledge the findings, and given that deployed contracts cannot be renewed, decided to keep the codebase unchanged.

BDC-10 | Privileged ownership

Category	Severity	Location	Status
Centralization / Privilege	Major	BuffDogeCoin.sol (0x23125)	Acknowledged

Description

The owner of contract `BuffDogeCoin` has the permission to:

1. change the address that can receive LP tokens,
2. lock the contract,
3. exclude/include addresses from rewards/fees,
4. set `taxFee`, `liquidityFee` and `_maxTxAmount`,
5. enable `swapAndLiquifyEnabled` without obtaining the consensus of the community.

Recommendation

We advise the client to carefully manage the `[fixme]` account's private key to avoid any potential risks of being hacked. In general, we strongly recommend centralized privileges or roles in the protocol to be improved via a decentralized mechanism or smart-contract-based accounts with enhanced security practices, e.g., Multisignature wallets.

Indicatively, here is some feasible suggestions that would also mitigate the potential risk at the different level in term of short-term and long-term:

- Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations;
- Assignment of privileged roles to multi-signature wallets to prevent a single point of failure due to the private key;
- Introduction of a DAO/governance/voting module to increase transparency and user involvement.

Alleviation

[Buff Doge Team]: Consider the security issue about ownership of privileges. Our plan is to make the Multisignature contract for the contract owner function and set the contract owner for it. Until now, there will be no transfer of ownership, more than extra examination for security with key distribution between current council members. This will require 2/3 keys to take action on the contract.For now, Buff Doge Coin has been listed on Hotbit in November. We have also deal with 2 other CEX which will be listed on December 2021 and January 2022. Each CEX requires KYC, token audit and legal opinion to be listed. The Multisignature is underway and will be completed as soon as possible.

BDC-11 | Possible to gain ownership after renouncing the contract ownership

Category	Severity	Location	Status
Logical Issue, Centralization / Privilege	**Major**	BuffDogeCoin.sol (0x23125)	Acknowledged

Description

An owner is possible to gain ownership of the contract even if he calls function `renounceOwnership` to renounce the ownership. This can be achieved by performing the following operations:

1. Call `lock` to lock the contract. The variable `_previousOwner` is set to the current owner.
2. Call `unlock` to unlock the contract.
3. Call `renounceOwnership` to leave the contract without an owner.
4. Call `unlock` to regain ownership.

Recommendation

We advise updating/removing `lock` and `unlock` functions in the contract; or removing the `renounceOwnership` if such a privilege retains at the protocol level. If timelock functionality could be introduced, we recommend using the implementation of Compound finance as reference.

Reference: https://github.com/compound-finance/compound-protocol/blob/master/contracts/Timelock.sol

Alleviation

[Buff Doge Team]: We acknowledge the findings, and given that deployed contracts cannot be renewed, decided to keep the codebase unchanged.

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.

Checksum Calculation Method

The "Checksum" field in the "Audit Scope" section is calculated as the SHA-256 (Secure Hash Algorithm 2 with digest size of 256 bits) digest of the content of each file hosted in the listed source repository under the specified commit.

The result is hexadecimal encoded and is the same as the output of the Linux "sha256sum" command against the target file.

Disclaimer

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to you ("Customer" or the "Company") in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes, nor may copies be delivered to any other person other than the Company, without CertiK's prior written consent in each instance.

This report is not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any "product" or "asset" created by any team or project that contracts CertiK to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. CertiK's position is that each company and individual are responsible for their own due diligence and continuous security. CertiK's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze.

The assessment services provided by CertiK is subject to dependencies and under continuing development. You agree that your access and/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 and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.

ALL SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF ARE PROVIDED "AS IS" AND "AS

AVAILABLE" AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, CERTIK HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, CERTIK SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR TRADE PRACTICE. WITHOUT LIMITING THE FOREGOING, CERTIK MAKES NO WARRANTY OF ANY KIND THAT THE SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET CUSTOMER'S OR ANY OTHER PERSON'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM, OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR-FREE. WITHOUT LIMITATION TO THE FOREGOING, CERTIK PROVIDES NO WARRANTY OR UNDERTAKING, AND MAKES NO REPRESENTATION OF ANY KIND THAT THE SERVICE WILL MEET CUSTOMER'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULTS, BE COMPATIBLE OR WORK WITH ANY OTHER SOFTWARE, APPLICATIONS, SYSTEMS OR SERVICES, OPERATE WITHOUT INTERRUPTION, MEET ANY PERFORMANCE OR RELIABILITY STANDARDS OR BE ERROR FREE OR THAT ANY ERRORS OR DEFECTS CAN OR WILL BE CORRECTED.

WITHOUT LIMITING THE FOREGOING, NEITHER CERTIK NOR ANY OF CERTIK'S AGENTS MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS OR IMPLIED AS TO THE ACCURACY, RELIABILITY, OR CURRENCY OF ANY INFORMATION OR CONTENT PROVIDED THROUGH THE SERVICE. CERTIK WILL ASSUME NO LIABILITY OR RESPONSIBILITY FOR (I) ANY ERRORS, MISTAKES, OR INACCURACIES OF CONTENT AND MATERIALS OR FOR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF ANY CONTENT, OR (II) ANY PERSONAL INJURY OR PROPERTY DAMAGE, OF ANY NATURE WHATSOEVER, RESULTING FROM CUSTOMER'S ACCESS TO OR USE OF THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS.

ALL THIRD-PARTY MATERIALS ARE PROVIDED "AS IS" AND ANY REPRESENTATION OR WARRANTY OF OR CONCERNING ANY THIRD-PARTY MATERIALS IS STRICTLY BETWEEN CUSTOMER AND THE THIRD-PARTY OWNER OR DISTRIBUTOR OF THE THIRD-PARTY MATERIALS.

THE SERVICES, ASSESSMENT REPORT, AND ANY OTHER MATERIALS HEREUNDER ARE SOLELY PROVIDED TO CUSTOMER AND MAY NOT BE RELIED ON BY ANY OTHER PERSON OR FOR ANY PURPOSE NOT SPECIFICALLY IDENTIFIED IN THIS AGREEMENT, NOR MAY COPIES BE DELIVERED TO, ANY OTHER PERSON WITHOUT CERTIK'S PRIOR WRITTEN CONSENT IN EACH INSTANCE.

NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING

MATERIALS AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS.

THE REPRESENTATIONS AND WARRANTIES OF CERTIK CONTAINED IN THIS AGREEMENT ARE SOLELY FOR THE BENEFIT OF CUSTOMER. ACCORDINGLY, NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH REPRESENTATIONS AND WARRANTIES AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH REPRESENTATIONS OR WARRANTIES OR ANY MATTER SUBJECT TO OR RESULTING IN INDEMNIFICATION UNDER THIS AGREEMENT OR OTHERWISE.

FOR AVOIDANCE OF DOUBT, THE SERVICES, INCLUDING ANY ASSOCIATED ASSESSMENT REPORTS OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

About

Founded in 2017 by leading academics in the field of Computer Science from both Yale and Columbia University, CertiK is a leading blockchain security company that serves to verify the security and correctness of smart contracts and blockchain-based protocols. Through the utilization of our world-class technical expertise, alongside our proprietary, innovative tech, we're able to support the success of our clients with best-in-class security, all whilst realizing our overarching vision; provable trust for all throughout all facets of blockchain.