



Mbit Wallet - audit

Security Assessment

CertiK Assessed on Mar 7th, 2025





Certik Assessed on Mar 7th, 2025

Mbit Wallet - audit

The security assessment was prepared by Certik, the leader in Web3.0 security.

Executive Summary

TYPES

ERC-20, Marketplace

ECOSYSTEM

EVM Compatible

METHODS

Formal Verification, Manual Review, Static Analysis

LANGUAGE

Solidity

TIMELINE

Delivered on 03/07/2025

KEY COMPONENTS

N/A

CODEBASE

[commit:b6fcefa](#)[View All in Codebase Page](#)

COMMITTS

- [b6fcefaa978f6e878ae3a8aeffa82245fb79144](#)
- [ffa47177f60ecbb95fd19ad921ca69ce0b04ceb9](#)

[View All in Codebase Page](#)

Highlighted Centralization Risks

⚠️ Privileged role can mint tokens

Vulnerability Summary



3

Total Findings

2

Resolved

0

Mitigated

0

Partially Resolved

1

Acknowledged

0

Declined

■ 0 Critical

Critical risks are those that impact the safe functioning of a platform and must be addressed before launch. Users should not invest in any project with outstanding critical risks.

■ 1 Major

1 Acknowledged



Major risks can include centralization issues and logical errors. Under specific circumstances, these major risks can lead to loss of funds and/or control of the project.

■ 0 Medium

Medium risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform.

■ 2 Minor

2 Resolved



Minor risks can be any of the above, but on a smaller scale. They generally do not compromise the overall integrity of the project, but they may be less efficient than other solutions.

■ 0 Informational

Informational errors are often recommendations to improve the style of the code or certain operations to fall within industry best practices. They usually do not affect the overall functioning of the code.

TABLE OF CONTENTS | MBIT WALLET - AUDIT

I **Summary**

Executive Summary

Vulnerability Summary

Codebase

Audit Scope

Approach & Methods

I **Findings**

GLOBAL-01 : Centralization Related Risks

MTS-01 : Ensure `msg.value` is Zero when Token is Not Native Token

MTS-02 : Missing Zero Address Validation

I **Appendix**

I **Disclaimer**

CODEBASE | MBIT WALLET - AUDIT

Repository

[commit:b6fcefa](#)





Commit

- [b6fcef978f6e878ae3a8aeffa82245fb79144](#)
- [ffa47177f60ecbb95fd19ad921ca69ce0b04ceb9](#)

AUDIT SCOPE | MBIT WALLET - AUDIT

4 files audited ● 1 file with Resolved findings ● 3 files without findings



ID	Repo	File	SHA256 Checksum
● MTS	mbitwallet/mbit-contracts	 MbitTokenSale.sol	3a137fe3f0dd50976ce7a11a46375fb13e7279 b9e8214b227203d3fb072813b1
● IMT	mbitwallet/mbit-contracts	 interfaces/IMbitToken.sol	fbcb70906e89b621e7f43c059984e27e6bd65 802ab8659b995a17eb1f7394278
● IMS	mbitwallet/mbit-contracts	 interfaces/IMbitTokenSale.sol	9a4221a95af88a8922f3facf20ca46347aaa41 311f128702d71dd4075ac11a60
● MTB	mbitwallet/mbit-contracts	 MbitToken.sol	79b22c68c5fc745268f3d98819817afa3ec08c 4cbba68a8146e68d9a3b8686d6

APPROACH & METHODS | MBIT WALLET - AUDIT

This report has been prepared for Mbit Wallet to discover issues and vulnerabilities in the source code of the Mbit Wallet - audit project as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Formal Verification, Manual Review, and Static Analysis 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:

- Testing the smart contracts against both common and uncommon attack vectors;
- 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.

FINDINGS | MBIT WALLET - AUDIT



3

Total Findings

0

Critical

1

Major

0

Medium

2

Minor

0

Informational

This report has been prepared to discover issues and vulnerabilities for Mbit Wallet - audit. Through this audit, we have uncovered 3 issues ranging from different severity levels. Utilizing the techniques of Formal Verification, Manual Review & Static Analysis to complement rigorous manual code reviews, we discovered the following findings:

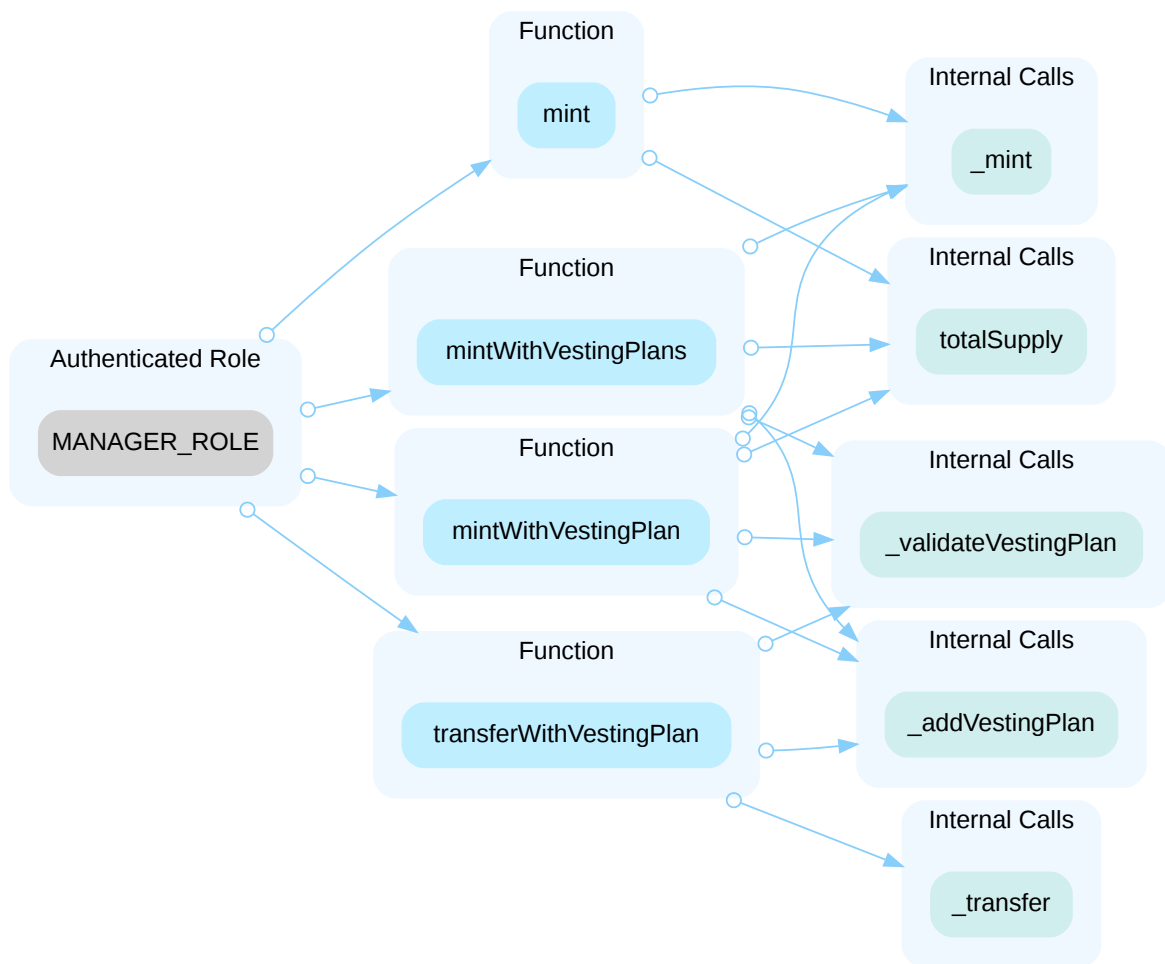
ID	Title	Category	Severity	Status
GLOBAL-01	Centralization Related Risks	Centralization	Major	● Acknowledged
MTS-01	Ensure <code>msg.value</code> Is Zero When Token Is Not Native Token	Volatile Code	Minor	● Resolved
MTS-02	Missing Zero Address Validation	Volatile Code	Minor	● Resolved

GLOBAL-01 | CENTRALIZATION RELATED RISKS

Category	Severity	Location	Status
Centralization	● Major		● Acknowledged

Description

In the contract `MbitToken`, the role `MANAGER_ROLE` has authority over the functions shown in the diagram below. Any compromise to the `MANAGER_ROLE` account may allow the hacker to take advantage of this authority and mint tokens with vesting plans, mint tokens with a vesting plan, transfer with a vesting plan, and mint tokens to an address. **The max supply of MbitToken is $316_988_658 * 10^{18}$.**

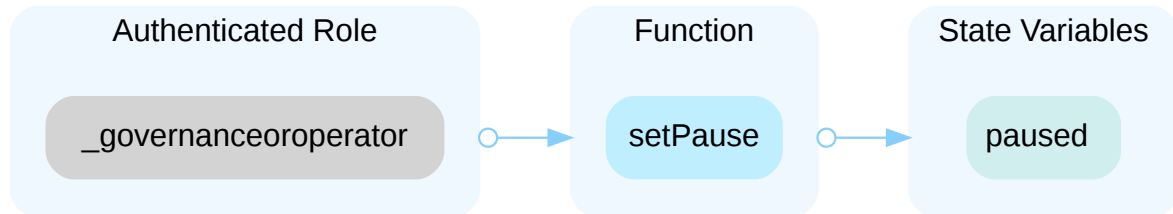


In the contract `MbitToken`, the role `DEFAULT_ADMIN_ROLE` has authority over the functions shown in the diagram below. Any compromise to the `MANAGER_ROLE` account may allow the hacker to take advantage of this authority and do the following:

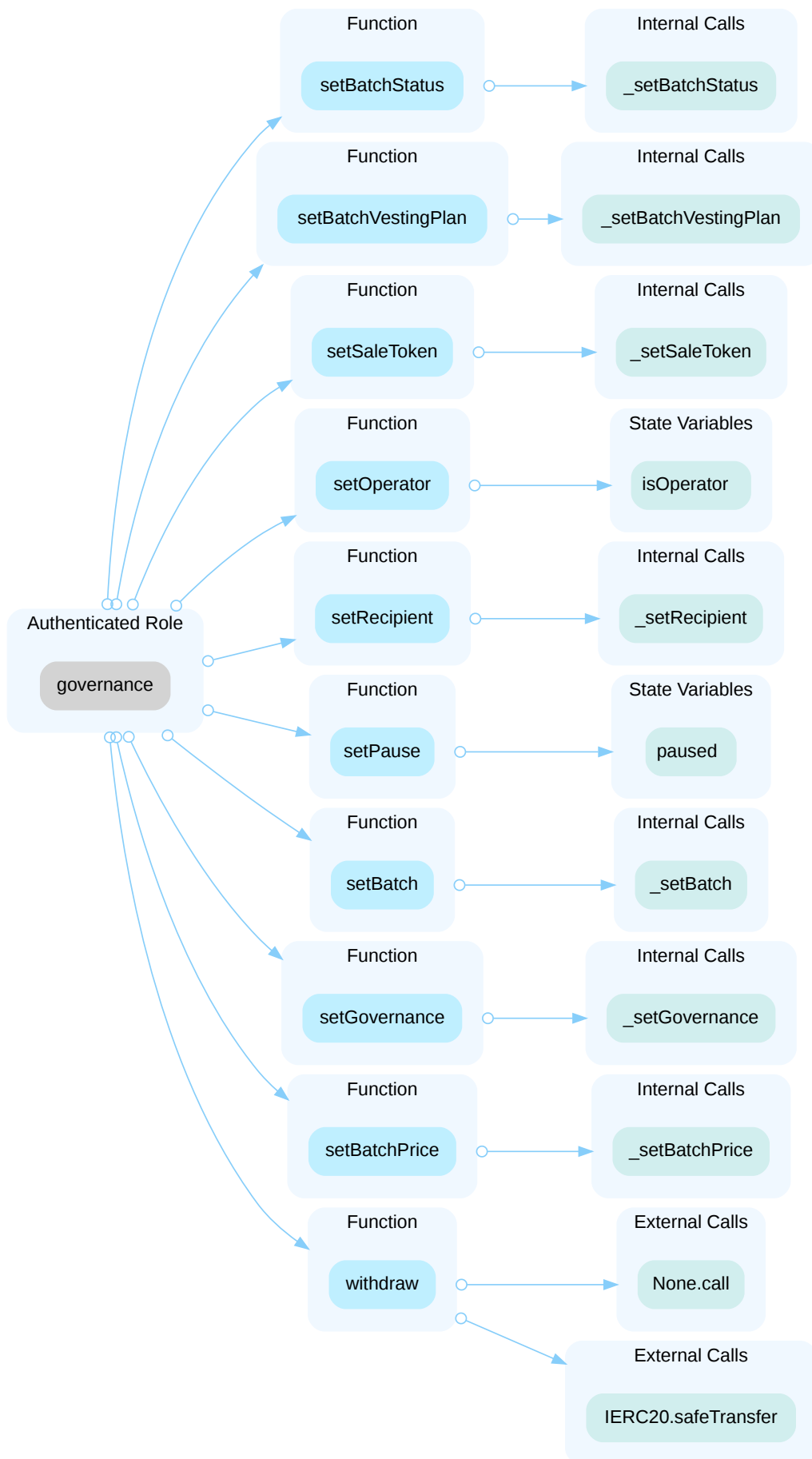
- `grantRole()`, grant role to malicious address.

- `revokeRole()` , revoke role from valid address.

In the contract `MbitTokenSale` , the role `_governanceoperator` has authority over the functions shown in the diagram below. Any compromise to the `_governanceoperator` account may allow the hacker to take advantage of this authority and set the pause state.



In the contract `MbitTokenSale` , the role `governance` has authority over the functions shown in the diagram below. Any compromise to the `governance` account may allow the hacker to take advantage of this authority and set batch status, set batch vesting plan, set the sale token address, set operator state, set recipient address, set the paused state, set the governance address, set batch price, and withdraw tokens to a recipient based on conditions.



Recommendation

The risk describes the current project design and potentially makes iterations to improve in the security operation and level of decentralization, which in most cases cannot be resolved entirely at the present stage. We advise the client to carefully manage the privileged account's private key to avoid any potential risks of being hacked. In general, we strongly recommend centralized privileges or roles in the protocol be improved via a decentralized mechanism or smart-contract-based accounts with enhanced security practices, e.g., multisignature wallets.

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

Short Term:

Timelock and Multi sign ($\frac{2}{3}$, $\frac{3}{5}$) combination *mitigate* by delaying the sensitive operation and avoiding a single point of key management failure.

- Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations;
AND
- Assignment of privileged roles to multi-signature wallets to prevent a single point of failure due to the private key compromised;
AND
- A medium/blog link for sharing the timelock contract and multi-signers addresses information with the public audience.

Long Term:

Timelock and DAO, the combination, *mitigate* by applying decentralization and transparency.

- Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations;
AND
- Introduction of a DAO/governance/voting module to increase transparency and user involvement.
AND
- A medium/blog link for sharing the timelock contract, multi-signers addresses, and DAO information with the public audience.

Permanent:

Renouncing the ownership or removing the function can be considered *fully resolved*.

- Renounce the ownership and never claim back the privileged roles.
OR
- Remove the risky functionality.

I Alleviation

[Mbit Wallet Team, 03/05/2025]: The team acknowledged this issue. We will follow the audit team's suggestion on address management, we need to keep contracts a bit centralized in the early stages.

[Certik, 03/05/2025]: It is suggested to implement the aforementioned methods to avoid centralized failure. Also, Certik strongly encourages the project team to periodically revisit the private key security management of all addresses related to centralized roles.

MTS-01 | ENSURE `msg.value` IS ZERO WHEN TOKEN IS NOT NATIVE TOKEN

Category	Severity	Location	Status
Volatile Code	Minor	MbitTokenSale.sol: 77	Resolved

Description

In the current contract context, two distinct pathways for asset transfers are provided: one for Ethereum (ETH) and another for ERC-20 tokens or similar. When ETH is chosen by the user, the transaction value is denoted by `msg.value`. For token transfers, however, the contract is expected to execute a transfer of the specified token amount from the user's address (`msg.sender`) to the desired destination.

However, the current function implementation does not confirm that `msg.value` is zero in cases where the asset being transferred is a non-ETH token. This omission creates a scenario where a user might inadvertently send ETH to the contract while intending to only transact with an ERC-20 token. Since the contract does not reject or refund the superfluous ETH, the user's funds could be lost.

Recommendation

To mitigate this risk and safeguard user assets, it is essential to introduce a conditional check within the contract function that enforces `msg.value` to be zero whenever a non-ETH token transfer is initiated. Implementing this check will ensure that only the intended operations are executed and prevent accidental financial loss due to user error when interacting with the contract.

Alleviation

[Mbit Wallet Team, 03/05/2025]: The team heeded the advice and resolved the issue in commit [ffa47177f60ecbb95fd19ad921ca69ce0b04ceb9](https://github.com/mbit-wallet/mbit-wallet/commit/ffa47177f60ecbb95fd19ad921ca69ce0b04ceb9)

MTS-02 | MISSING ZERO ADDRESS VALIDATION

Category	Severity	Location	Status
Volatile Code	Minor	MbitTokenSale.sol: 121	Resolved

Description

Addresses are not validated before assignment or external calls, potentially allowing the use of zero addresses and leading to unexpected behavior or vulnerabilities. For example, transferring tokens to a zero address can result in a permanent loss of those tokens.

```
123          (bool success, ) = address(_recipient).call{value: amount}(new  
bytes(0));
```

- `_recipient` is not zero-checked before being used.

Recommendation

It is recommended to add a zero-check for the passed-in address value to prevent unexpected errors.

Alleviation

[Mbit Wallet Team, 03/05/2025]: The team heeded the advice and resolved the issue in commit [ffa47177f60ecbb95fd19ad921ca69ce0b04ceb9](#)

APPENDIX | MBIT WALLET - AUDIT

Finding Categories

Categories	Description
Volatile Code	Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases and may result in vulnerabilities.
Centralization	Centralization findings detail the design choices of designating privileged roles or other centralized controls over the code.

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 | CERTIK

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.

Elevating Your Entire **Web3** Journey

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.

