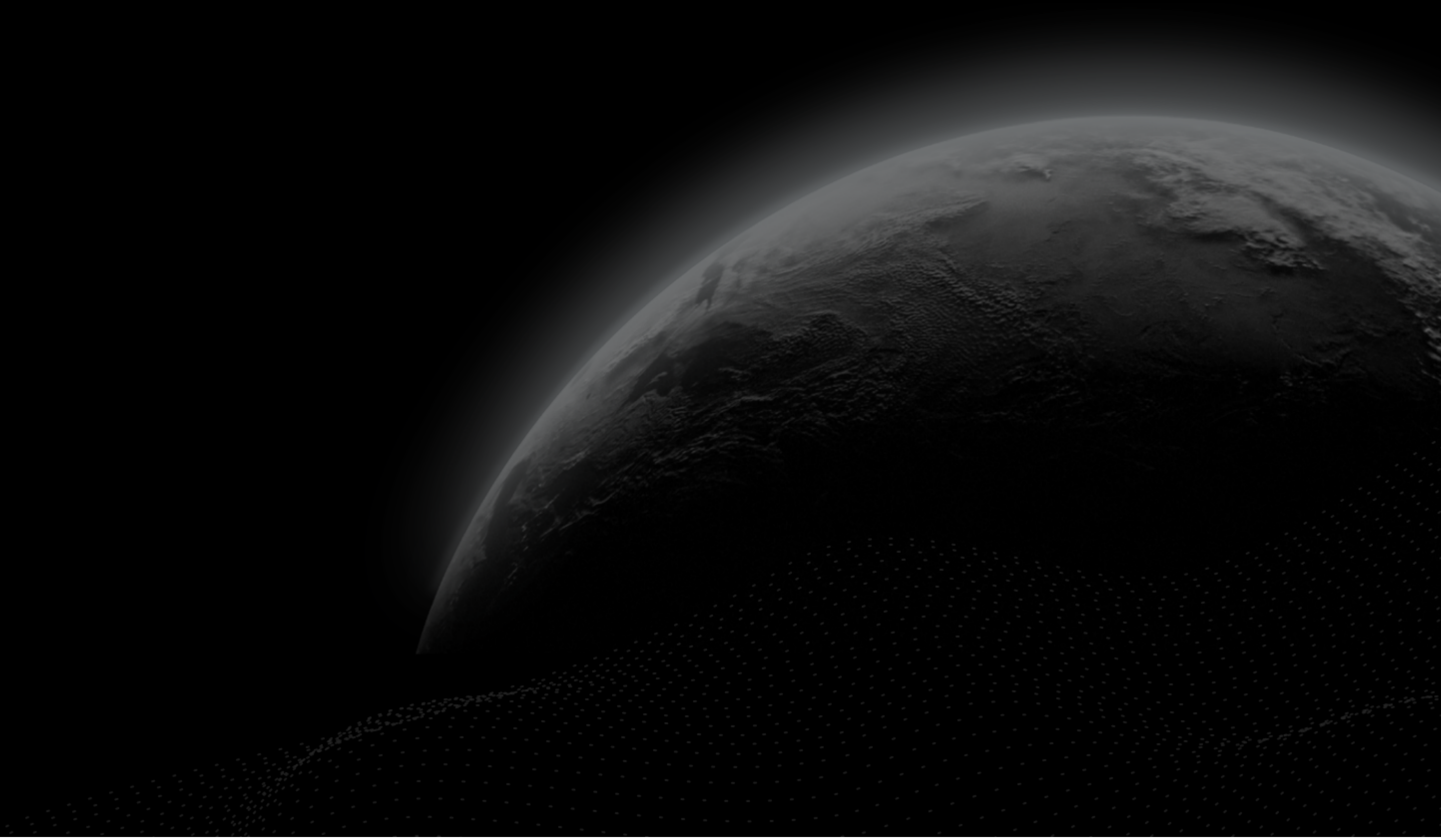
CERTIK

Security Assessment

# Trust Wallet Extension

CertiK Verified on Feb 24th, 2023



CertiK Verified on Feb 24th, 2023

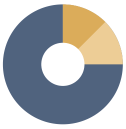
# Trust Wallet Extension

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

## Executive Summary

| TYPES | ECOSYSTEM | METHODS |
|---|---|---|
| Wallet | Browser Extension | Dynamic Testing, Manual Review |
| LANGUAGE | TIMELINE | KEY COMPONENTS |
| Typescript | Delivered on 02/24/2023 | Wallet |

## Vulnerability Summary



| 8 | 8 | 0 | 0 | 0 | 0 | 0 |
|---|---|---|---|---|---|---|
| Total Findings | Resolved | Mitigated | Partially Resolved | Acknowledged | Declined | Unresolved |

| | | | | |
|---|---|---|---|---|
| 🟥 | 0 | Critical | | Critical risks are those that impact the safe functioning of a platform and must be addressed immediately. Users should be cautious when interacting with any application with outstanding critical risks. |
| 🟧 | 0 | High | | High risks can include centralization issues and logical errors. Under specific circumstances, these major risks can lead to loss of funds, thief of user data, and/or loss control of the application. |
| 🟨 | 1 | Medium | 1 Resolved | Medium risks may not pose a security risk at a large scale, but they can affect the overall functioning of a platform or be used to target a certain group of users. |
| 🟨 | 1 | Low | 1 Resolved | Low risks can be any of the above, but on a smaller impact. They generally do not compromise the overall integrity of the project. |
| 🟦 | 6 | Informational | 6 Resolved | Informational errors are often recommendations to improve the configuration or certain operations to fall within industry best practices. They usually do not affect the overall functioning of the application. |

# TABLE OF CONTENTS | TRUST WALLET EXTENSION

# SCOPE | TRUST WALLET EXTENSION

| | |
|---|---|
| Extension(Version 0.0.200) | https://chrome.google.com/webstore/detail/trust-wallet/egjidjbpglichdcondbcbdnbeeppgdph |
| MD5 hash of the source code Zip file | 770adc680e29026605a18f3205af0a8d |

# APPROACH & METHODS | TRUST WALLET EXTENSION

This report has been prepared for Trustwallet to discover issues and vulnerabilities in the Trust wallet browser extension. The Trust wallet browser extension is a multi-chain crypto wallet that allows users to browse the web and interact with Dapps in the EVM chains, sign messages and transactions, and securely manage and store their private keys and assets.

The pentest was a manual assessment of the security of the application's functionality, business logic, and vulnerabilities, such as those cataloged in the OWASP Top 10. The assessment also included a review of security controls and requirements listed in the OWASP Application Security Verification Standard (ASVS). The pentesters leveraged tools to facilitate their work. However, the majority of the assessment involved manual analysis.

The main objective of the engagement is to test the overall resiliency of the application to various real-world attacks against the application's controls and functions and thereby be able to identify its weaknesses and provide recommendations to fix and improve its overall security posture.

Two members of the CertiK team were involved in completing the engagement, which took place over the course of 10 days in December 2022 and yielded 8 security-relevant findings. The one notable finding is the lack of a Dapp disconnect option. Other weaknesses were also found and are detailed in the Findings section of the report. We recommend addressing these findings to ensure a high level of security standards and industry practices and to raise the security posture of the application.

### Re-test

CertiK performed the re-test on February 22, 2023. Trustwallet has worked diligently to remediate security vulnerabilities discovered by CertiK, greatly increasing the overall security posture of their application. We suggest that Trustwallet maintain this level of security in future development and leverage our team for a follow-up Penetration Test within 6 months, or immediately after and major development changes.

# REVIEW NOTES | TRUST WALLET EXTENSION

The assessment focus on evaluating the security of the wallet and the implementation of the extension. The auditors prepare a list of questions to guide through the source code review and dynamic testing process.

### General wallet security related

- How does the application generate the seed phrase and private key?
- How and where do the application store the seed phrase and private key?
- Does the wallet connect to a trustworthy blockchain node?
- Does the application allow users to configure a custom blockchain node? If so, what can a malicious blockchain node do to the application?
- Does the application utilize a cartelized server, and what information is sent from the client to the server?
- If the server stores sensitive data, how are they stored?
- Does the application enforce a strong password policy?
- Does the application require a 2FA or pin code when users attempt to access sensitive information or transfer tokens?
- Does the application use vulnerable third-party libraries?
- Any secret(ex. API keys, AWS credentials) leaks in the source code repository?
- Any notable bad coding practices (ex. misuse of cryptography) in the codebase?

### Browser extension specific

- What permissions does the extension require?
- How does the extension interact with the web page?
- How does the extension decide which website is allowed to communicate with the extension?
- Does the extension(often the background script) correctly check the origin of the message before processing it?
- Does the transaction prompt display all the information correctly?
- Can a malicious website exploit vulnerabilities such as XSS(cross-site scripting) in the extension page or other active tabs in the browser by exploiting a vulnerability in the extension?
- Can a malicious website read or modify data that belongs to the extension without the user's consent?
- Is the extension vulnerable to clickjacking?
- Does the application implement an effective content security policy?

## Out of scope dependency

The following mission-critical wallet function implementations are imported from external libraries and will not be included in the scope of the security assessment.

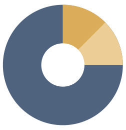
Functions

- Wallet creation
- Vault encryption and decryption
- Password hashing
- Key derivation

External libraries

- HDWallet from '@trustwallet/wallet-core/dist/src/wallet-core'
- BrowserPassworder from '@metamask/browser-passworder';
- WalletCore from '@trustwallet/wallet-core';

# FINDINGS | TRUST WALLET EXTENSION



| 8 | 0 | 0 | 1 | 1 | 6 |
|---|---|---|---|---|---|
| Total Findings | Critical | High | Medium | Low | Informational |

This report has been prepared to discover issues and vulnerabilities for Trust Wallet Extension. Through this security assessment, we have uncovered 8 issues ranging from different severity levels. Utilizing the techniques of Dynamic Testing & Manual Review to complement rigorous testing process, we discovered the following findings:

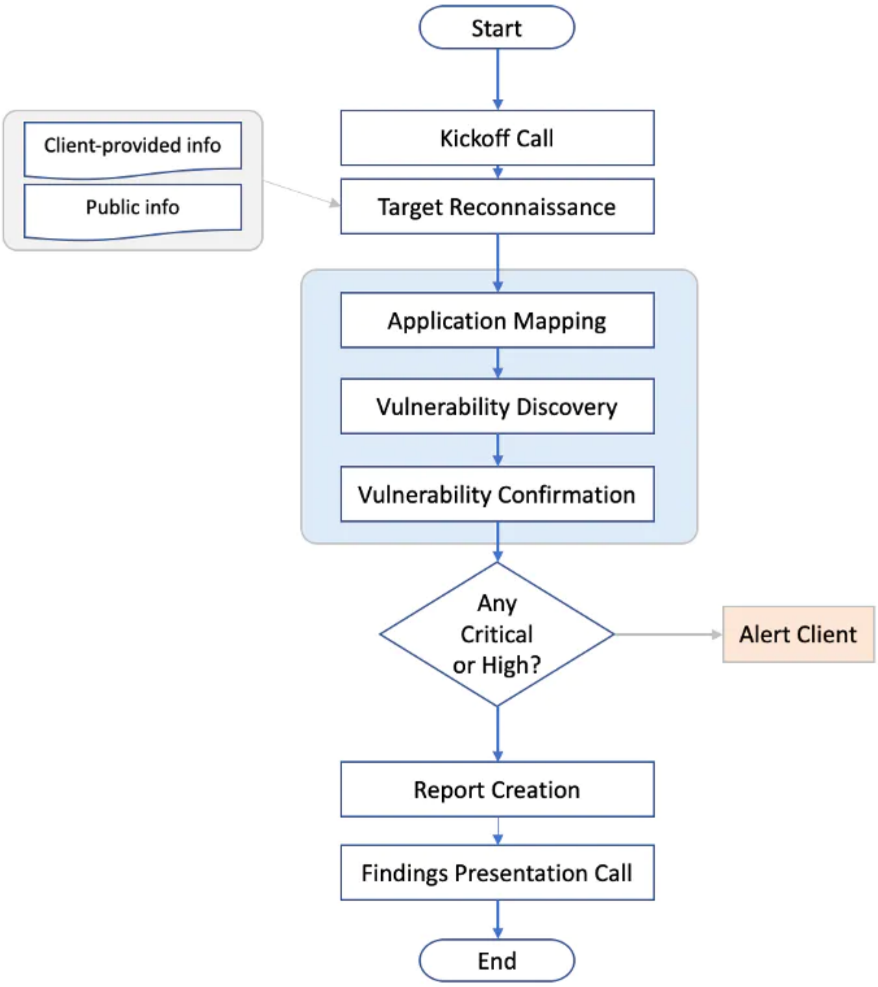
| ID | Title | Category | Severity | Status |
|---|---|---|---|---|
| TW-01 | Lack Of "Disconnect" Option | Logic Flaws | Medium | ● Resolved |
| TW-02 | Lack Of Token Name, Symbol And Decimal Validation | Application Resource Handling | Low | ● Resolved |
| TW-03 | Bug: Change Language Will Crash The Wallet | Security Misconfiguration | Informational | ● Resolved |
| TW-04 | Bug: Incorrect Display For Contract Deployment | Logic Flaws | Informational | ● Resolved |
| TW-05 | Wallet Crashes When Transaction Contains An Incorrect Value For Certain Fields | Logic Flaws | Informational | ● Resolved |
| TW-06 | Bug: Wallet Crashes When Viewing A Contract Deployment Transaction History | Logic Flaws | Informational | ● Resolved |
| TW-07 | Wallet Has Insufficient Control Against Continues Connect Requests | Logic Flaws | Informational | ● Resolved |
| TW-08 | Plaintext Secret Phrase Exist In The Memory For A Short Period Of Time | Insufficient Cryptography | Informational | ● Resolved |

# APPENDIX | TRUST WALLET EXTENSION

## Methodology

CertiK uses a comprehensive penetration testing methodology which adheres to industry best practices and standards in security assessments including from OWASP (Open Web Application Security Project), NIST, PTES (Penetration Testing Execution Standard).

Below is a flowchart of our assessment process:



## Coverage and Prioritization

As many components as possible will be tested manually. Priority is generally based on three factors: critical security controls, sensitive data, and the likelihood of vulnerability.

Critical security controls will always receive the top priority in the test. If a vulnerability is discovered in the critical security control, the entire application is likely to be compromised, resulting in a critical-risk to the business. For most applications, critical controls will include the login page, but it could also include major workflows such as the checkout function in an online store.

The Second priority is given to application components that handle sensitive data. This is dependent on business priorities, but common examples include payment card data, financial data, or authentication credentials.

Final priority includes areas of the application that are most likely to be vulnerable. This is based on CertiK’ experience with similar applications developed using the same technology or with other applications that fit the same business role. For example, large applications will often have older sections that are less likely to utilize modern security techniques.

## Reconnaissance

CertiK gathers information about the target application from various sources depending on the type of test being performed. CertiK obtains whatever information that is possible and appropriate from the client during scoping and supplements it with relevant information that can be gathered from public sources. This helps provide a better overall picture and understanding of the target.

## Application Mapping

CertiK examines the application, reviewing its contents, and mapping out all its functionalities and components. CertiK makes use of different tools and techniques to traverse the entire application and document all input areas and processes. Automated tools are used to scan the application and it is then manually examined for all its parameters and functionalities. With this, CertiK creates and widens the overall attack surface of the target application.

## Vulnerability Discovery

Using the information that is gathered, CertiK comes up with various attack vectors to test against the application. CertiK uses a combination of automated tools and manual techniques to identify vulnerabilities and weaknesses. Industry-recognized testing tools will be used, including Burp Suite, Nikto, Metasploit, and Kali. Furthermore, any controls in place that would inhibit the successful exploitation of a particular system will be noted.

## Vulnerability Confirmation

After discovering vulnerabilities in the application, CertiK validates the vulnerabilities and assesses its overall impact. To validate, CertiK performs a Proof-of-Concept of an attack on the vulnerability, simulating real world scenarios to prove the risk and overall impact of the vulnerability.

Through CertiK's knowledge and experience on attacks and exploitation techniques, CertiK is able to process all weaknesses and examine how they can be combined to compromise the application. CertiK may use different attack chains, leveraging different weaknesses to escalate and gain a more significant compromise.

To minimize any potential negative impact, vulnerability exploitation was only attempted when it would not adversely affect production applications and systems, and then only to confirm the presence of a specific vulnerability. Any attack with the potential to cause system downtime or seriously impact business continuity was not performed. Vulnerabilities were never exploited to delete or modify data; only read-level access was attempted. If it appeared possible to modify data, this was noted in the list of vulnerabilities below.

## Immediate Escalation of High or Critical Findings

If critical or high findings are found whereby application elements are compromised, client's key security contacts will be notified immediately.

## Risk Assessment

| Risk Level | CVSS Score | Impact | Exploitability |
|---|---|---|---|
| Critical | 9.0-10.0 | Root-level or full-system compromise, large-scale data breach | Trivial and straightforward |
| High | 7.0-8.9 | Elevated privilege access, significant data loss or downtime | Easy, vulnerability details or exploit code are publicly available, but may need additional attack vectors (e.g., social engineering) |
| Medium | 4.0-6.9 | Limited access but can still cause loss of tangible assets, which may violate, harm, or impede the org's mission, reputation, or interests. | Difficult, requires a skilled attacker, needs additional attack vectors, attacker must reside on the same network, requires user privileges |
| Low | 0.1-3.9 | Very little impact on an org's business | Extremely difficult, requires local or physical system access |
| Informational | 0.0 | Discloses information that may be of interest to an attacker. | Not exploitable but rather is a weakness that may be useful to an attacker should a higher risk issue be found that allows for a system exploit |

# 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.

CertiK | **Securing** the **Web3** World

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.