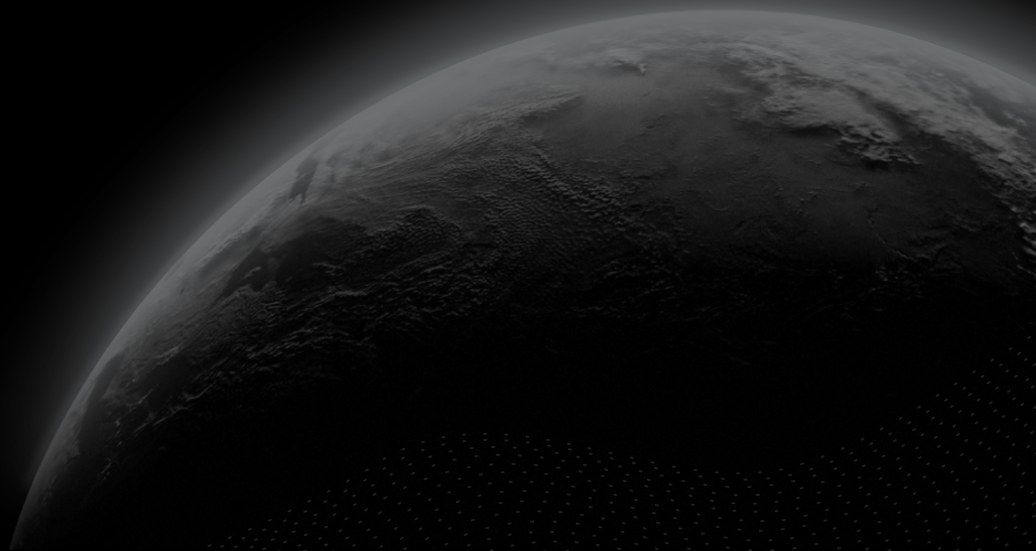




Security Assessment

Trustwallet barz Audit

CertiK Assessed on Jun 23rd, 2023





Certik Assessed on Jun 23rd, 2023

Trustwallet barz Audit

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

Executive Summary

TYPES

DeFi

ECOSYSTEM

Other

METHODS

Manual Review, Static Analysis

LANGUAGE

Solidity

TIMELINE

Delivered on 06/23/2023

KEY COMPONENTS

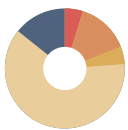
N/A

CODEBASE

The source is provided by the client in a Zip file. The MD5 hash of the Zip file is '2ee0b8266b24882ffd12bcc47857a7b1'

[View All in Codebase Page](#)

Vulnerability Summary



21

Total Findings

19

Resolved

0

Mitigated

0

Partially Resolved

2

Acknowledged

0

Declined

1 Critical

1 Resolved



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.

3 Major

3 Resolved



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.

1 Medium

1 Resolved



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

13 Minor

11 Resolved, 2 Acknowledged



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.

3 Informational

3 Resolved



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 | TRUSTWALLET BARZ AUDIT

■ Summary

[Executive Summary](#)

[Vulnerability Summary](#)

[Codebase](#)

[Audit Scope](#)

[Approach & Methods](#)

■ Review Notes

■ Findings

[LSB-01 : Insufficient Input Validation Allows Acceptance of Zero Signature](#)

[ART-04 : Missing Check Repeated Guardians](#)

[FAC-03 : Missing Check Repeated Approvers](#)

[GFB-01 : Dead Loop](#)

[RFB-01 : Lack Of Access Control](#)

[ART-02 : Missing Check `_recoveryPublicKey` is valid](#)

[ART-03 : No check recovery has been approved](#)

[Barz-01 : Third-Party Dependencies](#)

[FAC-04 : If the owner has approved, `_approvers` do not exclude the owner](#)

[FAC-05 : No check recovery exists](#)

[GFB-02 : Unused `isRemovalPending\(\)` function](#)

[LAS-01 : The condition `uint64\(block.timestamp\) == s.locks\[0\].release` is not included](#)

[LRT-01 : The `_recover\(\)` function does not support `safeBatchTransferFrom\(\)`](#)

[SMB-01 : Inconsistent owner approval checks](#)

[SVB-01 : Incorrect publicKey Length](#)

[TBK-01 : Lock check conditions are inconsistent](#)

[TBK-02 : Not Compliant with ERC-165 As `supportedInterfaces` Cannot be Updated in DiamondCut](#)

[TBK-03 : DiamondCut Can Potentially Introduce Storage Slot Collision If Used Incorrectly](#)

[LDB-01 : Inaccurate Error Message](#)

[LSB-02 : Incorrect Comment](#)

[TBP-02 : Supported Interface Not Updated](#)

■ Optimizations

[FAC-02 : `uint256` Compared to Zero](#)

LSB-03 : Optimization During Jacobian Doubling

■ **Appendix**

■ **Disclaimer**















CODEBASE | TRUSTWALLET BARZ AUDIT












Repository


















The source is provided by the client in a Zip file. The MD5 hash of the Zip file is '2ee0b8266b24882ffd12bcc47857a7b1'

AUDIT SCOPE | TRUSTWALLET BARZ AUDIT

47 files audited ● 2 files with Acknowledged findings ● 11 files with Resolved findings ● 34 files without findings

ID	File	SHA256 Checksum
● DCT	 contracts/facets/base/DiamondCutFacet.sol	08c47599b215bdb8049845549c4bc73680138885bb4c0120e18897dfae252aab
● LDB	 contracts/libraries/LibDiamond.sol	ad1360c25f7d60021e33f92ef806a54995f5ca90207802fb3567ff1e5b97eba
● DLT	 contracts/facets/base/DiamondLoupeFacet.sol	cd734ba18e904278d6530aa8115fe59a37d04c85c9994d34f4a174555e1270df
● SVB	 contracts/facets/verification/secp256k1/Secp256k1VerificationFacet.sol	fe84e047a51b23eadfdb0cf94e1b2a23ba94c93a1f83c2f46aab6c83b8d179e1
● LSB	 contracts/facets/verification/secp256r1/UtilsLibSecp256r1.sol	a8b9b32c726b27813c2c41561635a6f346a847011c62ce8a9664db8721ea04cf
● AFB	 contracts/facets/AccountFacet.sol	49bcd5db7133feb14819b6233a127e9b28a4b203e26a035d7f81274de9d23d13
● ART	 contracts/facets/AccountRecoveryFacet.sol	4b583d7f0b5a8b3080fa161eb9d5261d663262079b140f24ff8f4817c4199c34
● GFB	 contracts/facets/GuardianFacet.sol	4002c0895682a6a1de29cea02b3f8f740bafc44c06d614eab9bba630b8394676
● LFB	 contracts/facets/LockFacet.sol	ec2eaf9ca476e3dcd520a61f550831d25e1570a2cdc96764d3be988719cd0d94
● RFB	 contracts/facets/RestrictionsFacet.sol	b6751d10d24218a95cd36c9b05df111c9965e39c9562ee136c410b2fc8299d
● SMB	 contracts/facets/SignatureMigrationFacet.sol	cccf0256e1872397d4720a8338f33481bae13f15f0e01566a7951f4b48822cf
● LAT	 contracts/libraries/LibAppStorage.sol	e2173d379b3f4517d385952b190aa01757cba07b889555dc15ceabcfb0645e8
● LRT	 contracts/libraries/LibRecoverSpender.sol	d22c20332c2c4624f27b9d469093452704b4b5b1e0500359298a90a7129b35de
● IDT	 contracts/facets/base/interfaces/IDiamondCut.sol	0a85005b2aab093559244c4097c5be440ffb0834dc13a3a96ebbb16d8101ef68

ID	File	SHA256 Checksum
● IDB	 contracts/facets/base/interfaces/IDiamondLoupe.sol	e7b17a9c66b2d88ffbd79fdde2804fce051ac2e c0c48afb8d3dcc82339f173b2
● IAT	 contracts/facets/interfaces/IAccountFacet.sol	9ebd79a7dc348ba79695ade46f7569dc2dce0 6dcc498c50f7c7be9f0e00dd910
● IAB	 contracts/facets/interfaces/IAccountRecoveryFacet. sol	c5cfba8d28d9d7b13f276f2859069e6a4a9373 089e8d3088fa0dd6b21df103c5
● IGT	 contracts/facets/interfaces/IGuardianFacet.sol	f9fc38ff466f9253e78eef88c91501f6c546980fd 399c5e26ecd1e9687b62e5f
● ILT	 contracts/facets/interfaces/ILockFacet.sol	8ab99b47bcd53e986e6ee9da5c224078e627 2c5922b4e64a23108475bb39e0c3
● IRB	 contracts/facets/interfaces/IRestrictionsFacet.sol	896db005845ecaef7ea8880cd1e0d4dc13ce3 6b7d31d50f8c139c9a1fb19481
● ISF	 contracts/facets/interfaces/ISignatureMigrationFace t.sol	e18fceafeedc4df0c5b4f4a89e60b60e7adf8d7 45c678d6b75a2803f74c25f2c
● IVT	 contracts/facets/interfaces/IVerificationFacet.sol	db266ea3452b9dd3c86dfb56b1f7045177e08 98b1c857c63cacdd0ba1288b114
● BTK	 contracts/facets/verification/secp256r1/utls/Base64. sol	210329992e462a6b21fc2320fcb4f1a5cdaf2f5 3d70723ea9184c2efd96939cc
● SVC	 contracts/facets/verification/secp256r1/Secp256r1V erificationFacet.sol	b19b1000d7a75eef0ac0a507fe8b6157a2647 40c502880d3cab949e325bc2173
● MTC	 contracts/facets/Modifiers.sol	ad8f4c41097455fd1949a91342c0f1b81b09ae 4695ed6f0e73fe5dcd9b209ba9
● IFT	 contracts/infrastructure/interfaces/IFacetRegistry.sol	4de1a0c87ed5a8656d0fd4241cd9bd630104e 04047b68f224e608f32e68e79d3
● IGB	 contracts/infrastructure/interfaces/IGuardianStorag e.sol	ac5ebb4554ab9923274b2faa73d9b90f0e9d0 a2daaeb7d2b59bb4f67dd584a31
● ISB	 contracts/infrastructure/interfaces/ISecurityManager. sol	528764b77012277f054e7d18efc3894e3cc88 2e2442a9cfe017fd4bd79699040
● FRB	 contracts/infrastructure/FacetRegistry.sol	d328f6f5a34f6cf8762ab0b520f5a259922c516 7c1c5fa9496726351f7a6f6d5
● RSB	 contracts/infrastructure/RemoteStorage.sol	dd9e0e8652fc7d90a6502c4a9e5a7bc5253e2 e2d8a54bee1fd19622d282490b0

ID	File	SHA256 Checksum
● SMC	 contracts/infrastructure/SecurityManager.sol	54d8e942a811c7c158c99c6ed036081b92684 bbaa035cb01f8da5b8f3a9c0385
● WSB	 contracts/infrastructure/WhitelistStorage.sol	99ee1a398ba93b9161193b662c90d8ec66ae 568c23a7f227f1824ee4caa2da39
● IRR	 contracts/interfaces/ERC/Tokens/IERC1155.sol	ff804334352dcf4adef504b44f057171b1a9be4 bc31ca5e3d3d5d9bfc9cbe5c
● IRK	 contracts/interfaces/ERC/Tokens/IERC20.sol	e9c6a9d39185ed618734a00875ccf44ec899b 72ce28fbfcd91405822faf923c1
● IRP	 contracts/interfaces/ERC/Tokens/IERC721.sol	2774d4eba83103d994ef5efa657b0920b0914 94a6f386f061e4d521b70267904
● IEP	 contracts/interfaces/ERC/IERC1271.sol	a4a38d13326d3b8d495988a3ffc45bd4f8228e 69e0878fdded97000b2497ebcc5
● IRC	 contracts/interfaces/ERC/IERC165.sol	4e7999ac287d9987ad983302d557630e11a7 0a63d4a3ce73203bd89f33444d5
● IRE	 contracts/interfaces/ERC/IERC173.sol	9bbc819d9fc3070934f27b6bbb88ae2a94ffcfc 08cfc8f89ccc5a2dabf6a510a
● IBT	 contracts/interfaces/IBarzFactory.sol	7d817a915c39af82b08687aee34ff5eed195ea 13a7bd4d8208474a5fab8f13a0
● LFC	 contracts/libraries/LibFacetStorage.sol	a09d756a49da22ae180cd5d67961967c24a7 b43b7e413cdcf6e3a0a9dba8de0f
● LGB	 contracts/libraries/LibGuardian.sol	7fa3a6db48dbc07d2c4023e99b9fdfd2a76fe7 bcf69e49246c8d5037aa6a7b4d
● ITC	 contracts/restrictions/IRestriction.sol	049103a5661ede62926cc2829625b8ffe1bbff 38607878909acfa4ab79082a7a
● WRB	 contracts/restrictions/WhitelistRestriction.sol	f7c449ccee4abe323cf1783f062083c94e1c0b 0c77131726197f4b5b9e8da000
● DIT	 contracts/upgradeInitializers/DiamondInit.sol	6302d4c366b0a25294a0cc1d25aeca1e5036c d855447a6569a44bca4a5b0daf6
● BTP	 contracts/Barz.sol	64582e2877518ae1863ce8ad1fbd214e8e86 af303d1a45025c937658715560b
● BFB	 contracts/BarzFactory.sol	bb94b8e0b71e3b0bdac3c6f55d736923c60b4 0c15dcaea4477c179d6db23af61
● TRF	 projects/TrustwalletBarz/contracts/facets/TokenReceiverFacet.sol	20ccafde48d77ce3d963e81788d8e450165b6 fe85bba4c28efeb962ba699fb67

APPROACH & METHODS | TRUSTWALLET BARZ AUDIT

This report has been prepared for Trustwallet to discover issues and vulnerabilities in the source code of the Trustwallet barz Audit project as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing 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.

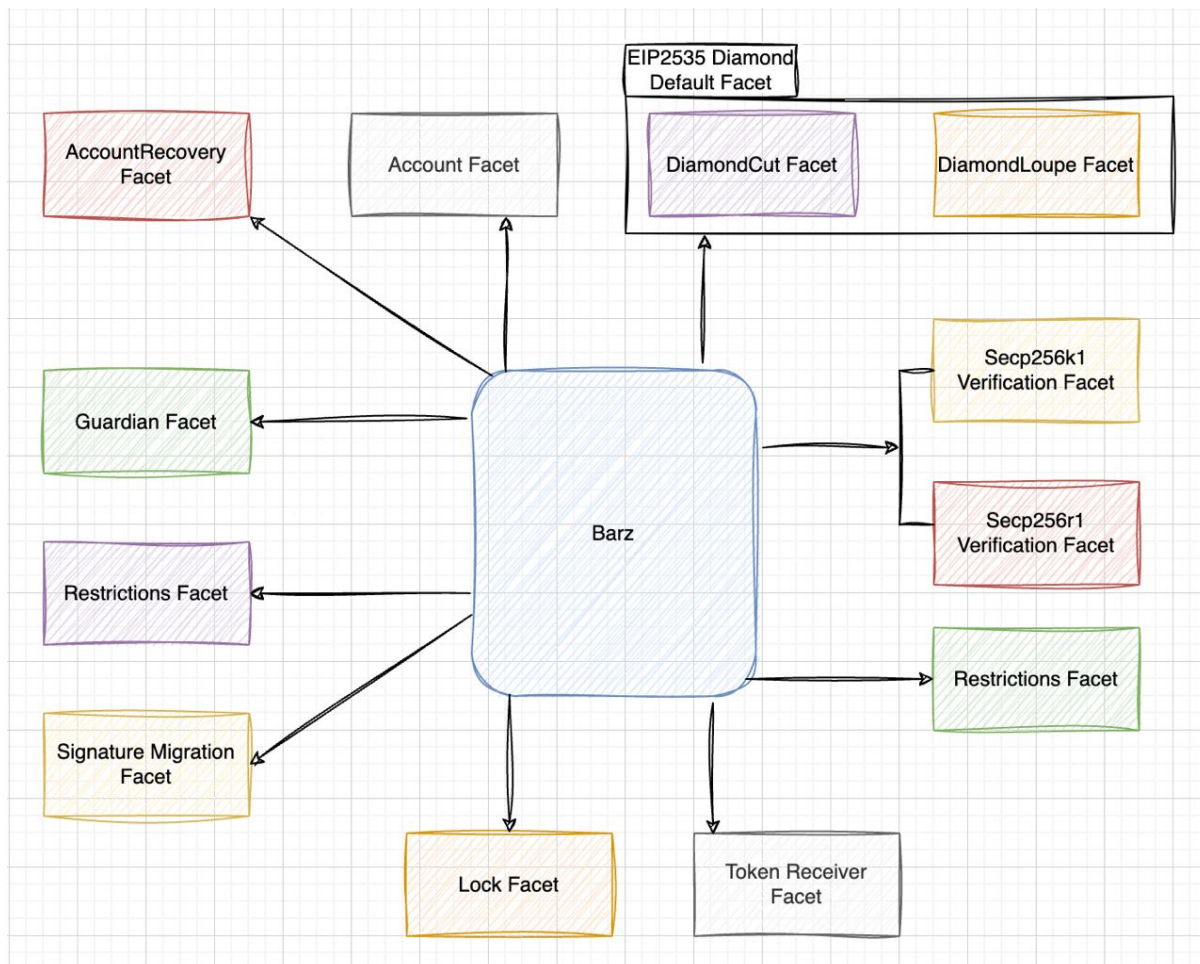
The security assessment resulted in findings that ranged from critical to informational. We recommend addressing these findings to ensure a high level of security standards and industry practices. We suggest recommendations that could better serve the project from the security perspective:

- 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.

REVIEW NOTES | TRUSTWALLET BARZ AUDIT

Barz is a smart contract wallet based on account abstraction (EIP4337). It has a highly modular architecture that allows customization by wallet users. Barz utilizes the Diamond Proxy pattern (introduced in <https://eips.ethereum.org/EIPS/eip-2535>) and provide each feature-set in a single facet attached to Diamond(Barz).

The overall architecture of the Barz wallet is summarized in the diagram below.



Most privileged functions are managed by the Barz wallet owner and its designated guardians, and they reflect the intended design. However, if a sufficient number of guardians are compromised, AND the owner doesn't hardstop, guardians can initiate recovery on their own and designated a new public key for the account without consent of the original Barz wallet owner. The responsibility falls on the Barz wallet owners that their designated guardians are reliable and behave in the wallet owner's best interest.

Additionally, the "Infrastructure" folder contains files that are used by Barz wallet users, and some important parameters are managed by the deployer/owner of these contracts. Specifically:

In the contract `FacetRegistry`, the role `_owner` has authority over the functions:

- `registerFacetFunctionSelectors()`
- `removeFacetFunctionSelectors()`

If the `_owner` role is compromised, Barz wallet users would be unable to add or replace specific function selectors from their wallet.

In the contract `SecurityManager`, the role `_owner` has authority over the functions:

- `initializeSecurityPeriod()`
- `initializeSecurityWindow()`
- `initializeRecoveryPeriod()`
- `initializeLockPeriod()`
- `initializeApprovalValidationPeriod()`
- `initializeMigrationPeriod()`

If the `_owner` role is compromised, these parameters could be initialized incorrectly, resulting in these security parameters being too low or too high.

We recommend carefully managing 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., multi-signature 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 (2/3, 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 of privileged operations;
AND
- Assignment of privileged roles to multi-signature wallets to prevent a single point of failure due to the private key being 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.

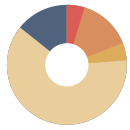
- Time-lock with reasonable latency, e.g., 48 hours, for awareness of privileged operations;
AND
- Introduction of a DAO/governance/voting module to increase transparency and user involvement;
AND
- A medium/blog link for sharing the timelock contract, multi-signers addresses, and DAO information with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

FINDINGS | TRUSTWALLET BARZ AUDIT



21

Total Findings

1

Critical

3

Major

1

Medium

13

Minor

3

Informational

This report has been prepared to discover issues and vulnerabilities for Trustwallet barz Audit. Through this audit, we have uncovered 21 issues ranging from different severity levels. Utilizing the techniques of Manual Review & Static Analysis to complement rigorous manual code reviews, we discovered the following findings:

ID	Title	Category	Severity	Status
LSB-01	Insufficient Input Validation Allows Acceptance Of Zero Signature	Volatile Code	Critical	● Resolved
ART-04	Missing Check Repeated Guardians	Logical Issue	Major	● Resolved
FAC-03	Missing Check Repeated Approvers	Logical Issue	Major	● Resolved
GFB-01	Dead Loop	Logical Issue	Major	● Resolved
RFB-01	Lack Of Access Control	Logical Issue	Medium	● Resolved
ART-02	Missing Check <code>_recoveryPublicKey</code> Is Valid	Logical Issue	Minor	● Resolved
ART-03	No Check Recovery Has Been Approved	Logical Issue	Minor	● Resolved
Barz-01	Third-Party Dependencies	Volatile Code	Minor	● Acknowledged
FAC-04	If The Owner Has Approved, <code>_approvers</code> Do Not Exclude The Owner	Logical Issue	Minor	● Resolved
FAC-05	No Check Recovery Exists	Logical Issue	Minor	● Resolved
GFB-02	Unused <code>isRemovalPending()</code> Function	Logical Issue	Minor	● Resolved

ID	Title	Category	Severity	Status
LAS-01	The Condition <code>uint64(block.timestamp) ==</code> <code>s.locks[0].release</code> Is Not Included	Volatile Code	Minor	● Resolved
LRT-01	The <code>_recover()</code> Function Does Not Support <code>safeBatchTransferFrom()</code>	Logical Issue	Minor	● Resolved
SMB-01	Inconsistent Owner Approval Checks	Logical Issue	Minor	● Resolved
SVB-01	Incorrect PublicKey Length	Incorrect Calculation, Coding Issue	Minor	● Resolved
TBK-01	Lock Check Conditions Are Inconsistent	Inconsistency	Minor	● Resolved
TBK-02	Not Compliant With ERC-165 As <code>supportedInterfaces</code> Cannot Be Updated In DiamondCut	Logical Issue	Minor	● Resolved
TBK-03	DiamondCut Can Potentially Introduce Storage Slot Collision If Used Incorrectly	Volatile Code	Minor	● Acknowledged
LDB-01	Inaccurate Error Message	Coding Style	Informational	● Resolved
LSB-02	Incorrect Comment	Inconsistency	Informational	● Resolved
TBP-02	Supported Interface Not Updated	Logical Issue	Informational	● Resolved

OPTIMIZATIONS | TRUSTWALLET BARZ AUDIT

ID	Title		Category	Severity	Status
FAC-02	<code>uint256</code>	Compared To Zero	Gas Optimization	Optimization	● Resolved
LSB-03	Optimization During Jacobian Doubling		Gas Optimization	Optimization	● Resolved

APPENDIX | TRUSTWALLET BARZ AUDIT

Finding Categories

Categories	Description
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.
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.
Inconsistency	Inconsistency findings refer to functions that should seemingly behave similarly yet contain different code, such as a constructor assignment imposing different require statements on the input variables than a setter function.
Coding Issue	Coding issue findings specify general coding issues.
Incorrect Calculation	Incorrect Calculation findings indicate incorrect caculation such as computation not according to the design, precision errors, rounding errors, etc.

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.

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.

