



Maalchain

Security Assessment

CertiK Assessed on Oct 9th, 2024





Certik Assessed on Oct 9th, 2024

Maalchain

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

Executive Summary

TYPES

Chain

ECOSYSTEM

Evmos | Cosmos (ATOM)

METHODS

Manual Review, Static Analysis

LANGUAGE

Golang

TIMELINE

Delivered on 10/09/2024

KEY COMPONENTS

N/A

CODEBASE

[maalchain_l1](#)[View All in Codebase Page](#)

COMMITTS

[ac2e04accfc7510ec98c19d4ed547125d31f7b3c](#)[View All in Codebase Page](#)

Vulnerability Summary



2

Total Findings

2

Resolved

0

Mitigated

0

Partially Resolved

0

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.

0 Major

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.

1 Minor

1 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.

1 Informational

1 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 | MAALCHAIN

I Summary

Executive Summary

Vulnerability Summary

Codebase

Audit Scope

Approach & Methods

I System Overview

I Review Notes

Known Issues

System Configuration

I Findings

FEE-01 : Missing Validation of GasWanted Against Block Gas Limit

TXC-01 : Offline Transaction Creation from Raw Data

I Appendix

I Disclaimer

CODEBASE | MAALCHAIN

Repository

[maalchain_l1](#)















Commit


















[ac2e04accfc7510ec98c19d4ed547125d31f7b3c](#)


















AUDIT SCOPE | MAALCHAIN


















68 files audited ● 1 file with Resolved findings ● 67 files without findings






ID	Repo	File	SHA256 Checksum
● TXC	maalchain/maalchain_l1	 x/evm/client/cli/tx.go	914dd1702774fffd65d4c63d913f05d2ade65c0e756f66d4b2602b377ba58597
● GEN	maalchain/maalchain_l1	 x/evm/genesis.go	6dd883bc1aed0698abb4d1452a18703df86f862c51d1af791c06b79d138650d3
● HAN	maalchain/maalchain_l1	 x/evm/handler.go	784f169d8d4c1b767d2ce359c987264b8e928f688f15a90ddd8f9579ead64370
● MOD	maalchain/maalchain_l1	 x/evm/module.go	54fcd8abb5f6cd2f1daed4f9d2d1b707b992825e72df0dec079a473be9950534
● ABC	maalchain/maalchain_l1	 x/evm/keeper/abci.go	d3bcea978f8839be9b62be8a76f71bad287f71932ce4055072df2226e3461ea5
● CON	maalchain/maalchain_l1	 x/evm/keeper/config.go	f7d6c684cc89b5bbb4e776f6a9168a6a741ef6540ac048e60e3e37498a6a2938
● GAS	maalchain/maalchain_l1	 x/evm/keeper/gas.go	59b3a53abe7038f0e026a2c8fa60a770b282793001a52efca5de16d7a4748a92
● GRP	maalchain/maalchain_l1	 x/evm/keeper/grpc_query.go	dc3db87746d1c48b985695519bb1d2660a0eaa34f4d54b515bb6811178230dac
● HOO	maalchain/maalchain_l1	 x/evm/keeper/hooks.go	3c2794987754c4317c7e64569161274ac344d6de82890e31f1079cbd2e8feb
● KEE	maalchain/maalchain_l1	 x/evm/keeper/keeper.go	b2709c122a97d65674384f93df4e608e5aa37f0f46f06401702003b31ba7e660
● MIG	maalchain/maalchain_l1	 x/evm/keeper/migrations.go	2b394e5770feec8efa478abe8e53aade81828ac5c500d724beed067295c2185b
● MSG	maalchain/maalchain_l1	 x/evm/keeper/msg_server.go	c5e23667d9bc690b5bb84ca4455b49bc8239fc9aec969771ed475e6fcfc8baf
● PAR	maalchain/maalchain_l1	 x/evm/keeper/params.go	ab0fc9aa2748a4396eacc100a57ee078f041e22c8649aa3200d12da98f29c7be
● PAA	maalchain/maalchain_l1	 x/evm/keeper/params_test.go	05aa786c447608414e76cf17f3691fedfe6dcb35118c5f773349ab1756a6bb09

ID	Repo	File	SHA256 Checksum
● STA	maalchain/maalchain_l1	 x/evm/keeper/state_transition.go	149e1b1eb739c455f9eca00e55333c93456e0b2f725fa7e7fe2e9cddf1f4dacc
● STT	maalchain/maalchain_l1	 x/evm/keeper/statedb.go	805eadc0f0d18cb07d90486faac0312f35c506da8d8970d956c6f697051a5046
● UTI	maalchain/maalchain_l1	 x/evm/keeper/utis.go	a533349381a93d65bd91c4d724c4ede9605c6f47d107742c6577b37cc85b309a
● ACC	maalchain/maalchain_l1	 x/evm/statedb/access_list.go	2a7ec58885346d71f585209822c3a8cf089cbe875ea52e574c83d30f80e0bb5
● COF	maalchain/maalchain_l1	 x/evm/statedb/config.go	9b562a552c11cdca4894945e02c57f255829bc0ba4723fa92b36ba84816e85b2
● INT	maalchain/maalchain_l1	 x/evm/statedb/interfaces.go	6b84b2fb62fdb81b7581140df7b5ea46aab777e17cbfba717958bb87282fd97
● JOU	maalchain/maalchain_l1	 x/evm/statedb/journal.go	02b61fd7f973ee3be0c7bff661bae6e71c4b79eccb015423cdd959a8a6bea02b
● NAT	maalchain/maalchain_l1	 x/evm/statedb/native.go	e9cdfef136eca01c422468da2e35987db7b8fc0173c02fab366f6dcb764408b13
● STE	maalchain/maalchain_l1	 x/evm/statedb/state_object.go	8e5703e7c98d1729c5b574991a47f4e6ac05822db02b546f60950db53131f1ae
● STD	maalchain/maalchain_l1	 x/evm/statedb/statedb.go	81dc5d070988207e24118f1834a5ccb5b603a54abf5d591e3f195ca6760deb1f
● TRA	maalchain/maalchain_l1	 x/evm/statedb/transient_storage.go	fab0f0c9bb2308bf93729c4e57f9f66bd15156441646787f3da8064d0bb1af58
● ACE	maalchain/maalchain_l1	 x/evm/types/access_list.go	38f395d40fdd405ca8467a8f0ddb58937f0f6511f1ce92d542942011a672d259
● ACS	maalchain/maalchain_l1	 x/evm/types/access_list_tx.go	dcbd997268cd7e91cb1f56cdd784653156685988a6ea46d7bae6cf454e369bf2
● CHA	maalchain/maalchain_l1	 x/evm/types/chain_config.go	f2519bc3df70dc71a2979d0dd4e03b01026f4b364e1f9b590cfca323f0eb09da
● COD	maalchain/maalchain_l1	 x/evm/types/codec.go	285fb4374a96083611ceed766e43517e2e0b546b60b8b478f0254e6dba1bc3c8
● COM	maalchain/maalchain_l1	 x/evm/types/compiled_contract.go	dcd8d7ba8989dc5306adad899b2f6c59248099847678643091012f1d083b5332
● DYN	maalchain/maalchain_l1	 x/evm/types/dynamic_fee_tx.go	70005d29958c7b3e0ddd9acae50de10e7332f33c9a1c03116716cabf9adddede

ID	Repo	File	SHA256 Checksum
● ERR	maalchain/maalchain_l1	 x/evm/types/errors.go	6d51aff9cbfd9de003a12748e669456424 4281b61bead64de1966dc65207caa0
● EVE	maalchain/maalchain_l1	 x/evm/types/events.go	b2c54b9cc98b0054d6fbc24e6799bd573 687ecd75e449708f65b85d36bd642e
● GEE	maalchain/maalchain_l1	 x/evm/types/genesis.go	791b18ad109709c7959a4e17b2e392ec3 0e6d531942d1c8bfc0c5c661f17e62d
● INE	maalchain/maalchain_l1	 x/evm/types/interfaces.go	2ae3a018969780d9a09f6b2cacbdfcbff9c 509abc0d942c8237903b73fb1850a
● KEY	maalchain/maalchain_l1	 x/evm/types/key.go	ab665711d8081f6b3e0022c61bddb9f084 e9337cedf7ab3460418a60863840bf
● LEG	maalchain/maalchain_l1	 x/evm/types/legacy_tx.go	16560a002da9e28e3552bea95ffbc9fab4 e6dc5e993d029dad5cb03a238248a5
● LOG	maalchain/maalchain_l1	 x/evm/types/log.pb.go	7e86252553f7dc6307f10f6a1f2a594aeaa da7b8591194e0b71a8add58c694b8
● LOS	maalchain/maalchain_l1	 x/evm/types/logs.go	05806cee9a82ba54f2b6bcf858c6139d6f ba1dada21b2499b25835340a03b142
● MST	maalchain/maalchain_l1	 x/evm/types/msg.go	7083b737ad2b104ef1d7ad0c99ae55e21 62a5abfcec8ab0ba4cc4c9ee32f84c2
● PAM	maalchain/maalchain_l1	 x/evm/types/params.go	f9c6b019e38290f26124191eff3a17f31da 7b1203bc93279ed09b599488a2855
● QUE	maalchain/maalchain_l1	 x/evm/types/query.go	642261769f90965a79cdd57d5a1948fbbf 96cbd45fc169683d1c340b077952f8
● STO	maalchain/maalchain_l1	 x/evm/types/storage.go	6c7f2245a007dc6caca7d1685b1586566 5f1d578313fc523ef333a6f2d50cf24
● TRC	maalchain/maalchain_l1	 x/evm/types/tracer.go	f62929ba89edc7f557198bdc0081003e6d b7e6ea731b0b182c2ad5c1783a6763
● TXT	maalchain/maalchain_l1	 x/evm/types/tx.go	3c0e92144d4bcd52494f940a05ac11af54 0f595f02d9648da173d4197f7b84db
● TXA	maalchain/maalchain_l1	 x/evm/types/tx_args.go	cf617908e2e330f0a7f35d1dd074850621 67e2d4d8a7a229fe2518356429e9ef
● TXD	maalchain/maalchain_l1	 x/evm/types/tx_data.go	fcae20c04a1b64ffa1abe12f2af997b957f7 1000f2a7c85d132b1c08035a747c
● UTL	maalchain/maalchain_l1	 x/evm/types/utils.go	10fafc60216f8bc0dd919cc15f485ba19c2 67e9b6b7e6d3625600f171fbd301d

ID	Repo	File	SHA256 Checksum
● QUR	maalchain/maalchain_l1	 x/evm/client/cli/query.go	7cc997c46a5989018dfb08a696c3b55efe3596dfdcd5e0b02dd5fa54dc938b82
● UTS	maalchain/maalchain_l1	 x/evm/client/cli/utlis.go	38a904e86d5fa73c959106d336227ee69cb3a8d3333c37e3acc49902e695c611
● QUY	maalchain/maalchain_l1	 x/feemarket/client/cli/query.go	2fdaf52e09ef5deb3e1c7b32039b28da7925797eacc120120c86ae2f8cfd3f9
● GES	maalchain/maalchain_l1	 x/feemarket/genesis.go	24efae21bb857fac398d04b984802f05e85a4e1fdb9ad863389c047ef4ceb1b0
● HAD	maalchain/maalchain_l1	 x/feemarket/handler.go	5ed260e8a50d96862d14414fe5ac8c4e64901117cc1ce8cc874420dcfdaf9cd8
● MOU	maalchain/maalchain_l1	 x/feemarket/module.go	5e1701b27bdf043f938d18c3232354ebf9f3e0d68544abb7b12212b85a6082ef
● ABI	maalchain/maalchain_l1	 x/feemarket/keeper/abci.go	b72130dbfa8062bd0a475d79c490ab37c0cc242f2da8931d723642012cb725d7
● EIP	maalchain/maalchain_l1	 x/feemarket/keeper/eip1559.go	640a43371970dedad2ec8a428399a6c97f2f5d455c4f8de19f1b9a5babd42b06
● GRC	maalchain/maalchain_l1	 x/feemarket/keeper/grpc_query.go	a38bccabd7c8c1b6f8935db574c75c764796d07f0c81916fc8d722f3e5bd15d4
● KEP	maalchain/maalchain_l1	 x/feemarket/keeper/keeper.go	02a00023e5be30928300c6ee26137c71c4b3ebe7397cde2fdbf7dabf7f1f6ddd
● MIR	maalchain/maalchain_l1	 x/feemarket/keeper/migrations.go	75795a54762101e63ddb8e0aa89459953747c09bde39bc341577ac60fab8ec45
● MSS	maalchain/maalchain_l1	 x/feemarket/keeper/msg_server.go	8044ef20fbd5ec05a86b25b7abcf9d089ef78c18b3174f50bdba5699a08d4b63
● PAS	maalchain/maalchain_l1	 x/feemarket/keeper/params.go	0334692d272c11ad90f74cb64df5987b3703c2067eda1cdf87ff47cbd3e7fc83
● COE	maalchain/maalchain_l1	 x/feemarket/types/codec.go	096112389de9815f02cf990ea8f3a5189115d77571b98411cdd5033573f3222c
● EVN	maalchain/maalchain_l1	 x/feemarket/types/events.go	b3b30534fa839c0b164e36da2efce322bad1ff687bceb7805c185b63a13c4538
● GEI	maalchain/maalchain_l1	 x/feemarket/types/genesis.go	1881963440bebc4744393ea6b3b4ef4514931e7f6f6153e77eef96b18bf96ece
● INR	maalchain/maalchain_l1	 x/feemarket/types/interfaces.go	33f44544d57b14f82e5375bafd516b5c17a81bf4d41d356e3b89f7e0cba953b2

ID	Repo	File	SHA256 Checksum
● KES	maalchain/maalchain_l1	 x/feemarket/types/keys.go	1c42358c94bd078510ce5d7d497792f38 231867b48567feb8dfb15022c31fbec
● MSY	maalchain/maalchain_l1	 x/feemarket/types/msg.go	d3d946db3da35802ced489137e56c3e50 7519df427d05b3cedd1c68835e82300
● PAT	maalchain/maalchain_l1	 x/feemarket/types/params.go	81b1b60df50d4fddeab81f41bb1fe90818 aedec7fa077b7c0d15f511c3dfd255

APPROACH & METHODS | MAALCHAIN

This report has been prepared for Maalchain to discover issues and vulnerabilities in the source code of the Maalchain 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.

SYSTEM OVERVIEW | MAALCHAIN

Maalchain is a Layer 1 chain based on the Cosmos SDK, so run by the CometBFT consensus engine. The main functionality of the blockchain is to provide an Ethereum Virtual Machine runtime for smart contracts execution.

The main custom Cosmos SDK module is the `x/evm` one which makes available all the EVM functionalities. Then, the `x/feemarket` module defines the basic economics for transaction fees. Both modules are derived from Evmos.

REVIEW NOTES | MAALCHAIN

The audit was conducted on a diff base, taking the following commit as reference

[45cd70ab6f50d04a5ddb60e3043fb83657c1c15a](#). Also, majority of the code is taken from [Crypto.org chain](#)

Known Issues

The following issues are known to be present in specific version of Evmos, parent codebase of Maalchain.

Title	Severity	Applicable	Comment
Patch incorrect balance update & DoS attack vector	Critical	NO	Maalchain does not provide any EVM custom precompiled contract
Precompiles exploit of smart contract account and vesting	Critical	NO	Maalchain does not provide any EVM custom precompiled contract
Contract balance not updating correctly after interchain transaction	Critical	NO	There is not any ICS20 module in Maalchain
Transaction execution not accounting for all state transition after interaction with precompiles	Critical	NO	Maalchain does not provide any EVM custom precompiled contract
Transferring unvested tokens after delegations	Minor	NO	No vesting in configured in Maalchain
Unauthorized accounts creation with vesting module	Medium	NO	No vesting module in Maalchain
Unvested token delegations	Medium	NO	No vesting module in Maalchain
DOS and transaction fee expropriation through Authz exploit	Critical	NO	Fix is present
Malicious Migration of Claimable Amount through IBC	Critical	NO	There is not x/claim module in Maalchain

■ System Configuration

The audit scope is limited to the modules indicated in this report section. The network behavior may vary according to the network deployment configuration and its genesis state, which impact key business parameters like, including but not limited to, initial token distribution and centralization of the system. We recommend the team publishing such detailed information in a transparent and verifiable manner and any user reviewing such data before interacting with the Maalchain blockchain.

FINDINGS | MAALCHAIN



2

Total Findings

0

Critical

0

Major

0

Medium

1

Minor

1

Informational

This report has been prepared to discover issues and vulnerabilities for Maalchain. Through this audit, we have uncovered 2 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
FEE-01	Missing Validation Of GasWanted Against Block Gas Limit	Logical Issue	Minor	● Resolved
TXC-01	Offline Transaction Creation From Raw Data	Logical Issue	Informational	● Resolved

FEE-01 | MISSING VALIDATION OF GASWANTED AGAINST BLOCK GAS LIMIT

Category	Severity	Location	Status
Logical Issue	Minor	app/ante/fee_market.go: 45	Resolved

Description

In the ante handler in `fee_market.go`, the `Maalchain` project does not validate `gasWanted` per tx against the max block gas limit.

```
45 func (gwd GasWantedDecorator) AnteHandle(ctx sdk.Context, tx sdk.Tx, simulate
bool, next sdk.AnteHandler) (newCtx sdk.Context, err error) {
46     blockHeight := big.NewInt(ctx.BlockHeight())
47     isLondon := gwd.ethCfg.IsLondon(blockHeight)
48
49     feeTx, ok := tx.(sdk.FeeTx)
50     if !ok || !isLondon {
51         return next(ctx, tx, simulate)
52     }
53
54     gasWanted := feeTx.GetGas()
55     isBaseFeeEnabled := gwd.feeMarketKeeper.GetBaseFeeEnabled(ctx)
56
57
58     // Add total gasWanted to cumulative in block transientStore in FeeMarket module
59     if isBaseFeeEnabled {
60         if _, err := gwd.feeMarketKeeper.AddTransientGasWanted(ctx, gasWanted);
err != nil {
61             return ctx, errorsmod.Wrapf(err,
"failed to add gas wanted to transient store")
62         }
63
64         return next(ctx, tx, simulate)
65     }
```

If a transaction with too much `gasWanted` is sent, it will not be directly discarded but will cause a time-out.

Note: While this section of the code was outside the audit's scope, CertiK promptly informed the client, enabling them to address the problem quickly and efficiently.

Recommendation

We recommend checking if the total `gasWanted` is within the max block gas limit.

■ Alleviation

[Certik, 12/06/2024]: The team heeded the advice and resolved the issue by checking the gasWanted does not go over the max block gas limit in commit [a577397716d687f4716896ceda7e5b6e0e9f8a45](#).

TXC-01 | OFFLINE TRANSACTION CREATION FROM RAW DATA

Category	Severity	Location	Status
Logical Issue	● Informational	x/evm/client/cli/tx.go: 79~82	● Resolved

Description

The cli `raw` command constructs a Cosmos transaction from an EVM transaction encoded in hexadecimal. In order to do that, the denomination of the EVM currency is needed and requested with a remote call to a node. For this reason the command cannot execute in an offline scenario.

Since the denomination information is constant and known, it could be gathered from the user rather than being requested from an active node, so removing the online requirement.

Recommendation

We recommend accepting the denomination as an optional cli parameter to enable the offline usage of the command.

A reference fix can be found in [PR#524](#).

Alleviation

[[Certik](#), 10/09/2024]: The team acknowledged the finding and solved the issue in commit

[d17c7e94c212507dde90c3d1ebb6eb5e531751d0](#) by adding an optional flag to provide the token denomination.

APPENDIX | MAALCHAIN

Finding Categories

Categories	Description
Logical Issue	Logical Issue findings indicate general implementation issues related to the program logic.

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.

