CERTIK

Security Assessment

Gotabit

CertiK Verified on Dec 28th, 2022

CertiK Verified on Dec 28th, 2022

Gotabit

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

Executive Summary

TYPES	ECOSYSTEM	METHODS
DeFi	Cosmos (ATOM)	Manual Review, Static Analysis
LANGUAGE	**TIMELINE**	**KEY COMPONENTS**
Golang	Delivered on 12/28/2022	N/A

CODEBASE
https://github.com/gotabit/gotabit/tree/6d4cb352a23bb6ec337af0b35d4d4aeaf126ab8b
...View All

COMMITS
6d4cb352a23bb6ec337af0b35d4d4aeaf126ab8b
...View All

Vulnerability Summary

6	0	0	0	6	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 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.
1	Medium	1 Acknowledged	Medium risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform.
2	Minor	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.
2	Informational	2 Acknowledged	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 | GOTABIT

CODEBASE | GOTABIT

Repository

https://github.com/gotabit/gotabit/tree/6d4cb352a23bb6ec337af0b35d4d4aeaf126ab8b

Commit

6d4cb352a23bb6ec337af0b35d4d4aeaf126ab8b

AUDIT SCOPE | GOTABIT

38 files audited ● 5 files with Acknowledged findings ● 33 files without findings

ID	File	SHA256 Checksum
APP	app/app.go	6916aa6aa01f8255507b2b5e7d031cc9eaa07db18657aa72617d2f73672e3977
HOK	x/epochs/types/hooks.go	80402e18f7598ef3c7d9313eb09819299604665410093c7a13a576c561bacb91
HOT	x/mint/types/hooks.go	4f29a632b0362f1f949f2385497d9bded47b264e6da60276a864636d6d8aaa6f
MIT	x/mint/types/minter.go	c24c74c654fc8e8e2c1c1fb33f54e2e762dae712d4f8fb3d8cd76bfd7ae1648c
PAR	x/mint/types/params.go	8edc2f68476afaef7b5ca846727ff948302cea5adf7876e113dec06c6e5d26b0
ANT	app/ante.go	82ab7be9101619620ea4edce262e33928b3a8a2e03f1692f2d0a9ff460de57f9
EXP	app/export.go	75ed7cb717265cbc146ad4e9d090a2c34bfd27a4c90b811d7bc8135363c42f52
GEN	app/genesis.go	fa720055e77331d79edf6ea877ea4cc3ab4cbee282681b10f77143e77f82b2c4
UPG	app/upgrades.go	d872085b59332e542c9c3e21c88ee727f8bc7533437327552436d8d47f13b3f1
WAS	app/wasm_config.go	71003ef47e0b1979d2eba3b0f6b1b354d841b6de7b0e36a196e087079fc08d07
QUE	x/epochs/client/cli/query.go	5a59349f045fbd0fe9db00c17205c00d6c3cd8adb0be759bf7e29a346629844f
TXC	x/epochs/client/cli/tx.go	435f39592ba4ad45f362c34985e3a4d9e1580c3ebe254c50a047542b7d934946
ABC	x/epochs/keeper/abci.go	6881cac6a33dbef6b5de27343375bb16ef92173e1429736977c608628b0ce0d4
EPO	x/epochs/keeper/epoch.go	9aecffb38b7a6faa79a218904bf7955aab7c66b293b504021b9165ceabd93c1e

ID	File	SHA256 Checksum
GEE	x/epochs/keeper/genesis.go	76e2052ac2c61ddf6dbb0e5914104358f854b59a33b72d137e07b490b3eeacf9
GRP	x/epochs/keeper/grpc_query.go	8a14893844011adac5dcceb02eadbe6388baca10326d1e5c059b33b5604c39fb
HOO	x/epochs/keeper/hooks.go	6befe03d4a47a5a7bd9a74f4608f51abf64ed95d3e86eeb787572e2124f9f5ed
KEP	x/epochs/keeper/keeper.go	c4886ce6b5add52a7884c97ea229b8a9043df4e7d81fd1c7ead9d482ae1ea5c8
MOD	x/epochs/module.go	e9787fe86b7cc46f686303559665c7231da84996bd589863f3a3761a7e4ef06a
DOC	x/epochs/types/doc.go	5ae31fc2ce8d08cde7ab47809cdfdb8f5ceedc9bd135458bc8ec89d27421fcc5
EVE	x/epochs/types/events.go	f8d4377c3cbb493a531673f549e7a9e3b03f3dd453ff31ec9181aca2283d6cfb
GES	x/epochs/types/genesis.go	270936f9be87802f0855b354ceca2ab96101a2c06235bdaf7653165e7dd2b7bc
IDE	x/epochs/types/identifier.go	030c5ffac1ee5145e442943ee944dae56c33bc30f05142ee84f92bc4c463971c
KEY	x/epochs/types/keys.go	44b33a8c93893a5a77893b37e644d48cc9431c17919b5e11ad01669861b918a6
QUR	x/mint/client/cli/query.go	8a83382c66070516319f4aaa96a71fafe0449eb180f3397cb6e92aa3891c67f0
QUY	x/mint/client/rest/query.go	f12c0c9c23a3654f52bcef077eec7b3296397eb0883705c6ebd38d7fbc7adcd3
RES	x/mint/client/rest/rest.go	bfc971f9950d2a908bcab2da856172e447de2eaa16211eef334e9592ca3f92fb
GEI	x/mint/keeper/genesis.go	4c41660d1c30813545c26c28ef3e5d76e16b9971c2d8fdf405b304c5990e3841
GRC	x/mint/keeper/grpc_query.go	c0c8f75c3b1df82e6a19fa01982f70a4be7a8ec58a9ce051970a2aa6eaa5c811
HOS	x/mint/keeper/hooks.go	fe205d0377fa773b7ffab68ef8126f71fabf343c954df57c2dd77922eead4af4
KEK	x/mint/keeper/keeper.go	28d6b9997881dab587928d9cb148b1101271a266ae42ccf6a02f3b4e271a57fc

ID	File	SHA256 Checksum
MOU	x/mint/module.go	cc4d937d963924e2a0bbb114410b4c98ef0391a35dbf0eccc0073c7637aa95f4
COD	x/mint/types/codec.go	e7f2bed92b9c0d4eb4044ec520190ae5f744d4efca3d5c09d1dcbe95b50bac19
EVN	x/mint/types/events.go	20641bd2199985f0bbc054a473765748811034960a8bd1e584f7fb681ab0486a
EXE	x/mint/types/expected_keepers.go	51215ecf7c15e63b14652813e3eabac4a72105c1662b5b5c7ebd1dede9fea837
GET	x/mint/types/genesis.go	a903130a761b630b3f790a26dc0e1f8ec89e9f5080052a7cdefc839d1c9152f6
KES	x/mint/types/keys.go	f9c808de4e0ccef322c2e0aa24e351ea1739ab3cf918f2442004ebc94de2ee64
MIN	x/mint/types/mint.pb.go	9214a5ec70026590797fae7d2d8bcb869aef9cb6f4d6ef3a181c9a6b859329c5

APPROACH & METHODS | GOTABIT

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

FINDINGS | GOTABIT

6	0	1	1	2	2
Total Findings	Critical	Major	Medium	Minor	Informational

This report has been prepared to discover issues and vulnerabilities for Gotabit. Through this audit, we have uncovered 6 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
TYP-01	Possible Issue With 0 `ReductionFactor`	Logical Issue	Major	Acknowledged
PAR-01	Incorrect Check Of 'Reductionfactor'	Logical Issue	Medium	Acknowledged
APP-01	Redundant Code	Logical Issue	Minor	Acknowledged
PAR-02	Wrong Error Message	Inconsistency	Minor	Acknowledged
6D4-01	Unused Function	Coding Style	Informational	Acknowledged
HOK-01	The `TODO` Comment	Coding Style	Informational	Acknowledged

TYP-01 | POSSIBLE ISSUE WITH 0 `ReductionFactor`

Category	Severity	Location	Status
Logical Issue	Major	x/mint/types/minter.go: 45~47; x/mint/types/params.go: 180~182	Acknowledged

Description

```
if v.IsNegative() {
    return fmt.Errorf("reduction factor cannot be negative")
}
```

x/mint/type/minter

```
func (m Minter) NextEpochProvisions(params Params) sdk.Dec {
    return m.EpochProvisions.Mul(params.ReductionFactor)
}
```

The code in the `NextEpochProvisions` method of the `Minter` type in the `x/mint/type` package calls the `Mul` method of the `EpochProvisions` field. If the `ReductionFactor` parameter passed to this method is set to 0, the chain will not be able to mint new coins after a reduction has occurred. This is because a `ReductionFactor` of 0 means that no new coins can be created, and the total number of coins in circulation will not increase. It is important to ensure that the `ReductionFactor` is set to a positive value in order to allow the chain to continue minting new coins.

Recommendation

We recommend verifying that the value of the `v` variable is greater than 0.

Alleviation

[Gotabit Team]: The current design is multiplication, and the specifics can be determined by the upper layer. So there's no problem here.

PAR-01 | INCORRECT CHECK OF 'REDUCTIONFACTOR'

Category	Severity	Location	Status
Logical Issue	Medium	x/mint/types/params.go: 176	Acknowledged

Description

The total supply is calculated using the following formula, based on the code:

$$TotalSupply = InitialSupply + EpochsPerPeriod * \frac{InitialRewardsPerEpoch}{1 - ReductionFactor}$$

It is important to note that the value of `ReductionFactor` must be less than 1. Therefore, the check shown below is incorrect:

```
176 if v.GT(sdk.NewDec(1)) {
177   return fmt.Errorf("reduction factor cannot be greater than 1")
178 }
```

This check determines if the value of `v` is greater than 1, but it does not consider the possibility that `v` may be equal to 1. It is important to note that the value of `ReductionFactor` must be less than 1.

Recommendation

We recommend validating that the variable `v` should be greater than or equal to `sdk.NewDec(1)`.

Alleviation

[Gotabit Team]: The current design is multiplication, and the specifics can be determined by the upper layer. So there's no problem here.

APP-01 | REDUNDANT CODE

Category	Severity	Location	Status
Logical Issue	Minor	app/app.go: 473	Acknowledged

Description

The following code is unnecessary because the `hooks[]` array is always empty:

```
473    app.MintKeeper.SetHooks(minttypes.MultiMintHooks{})
```

This code is redundant because the `mint` module's hook has already been initialized in the `EpochsKeeper` as shown here:

```
477 app.EpochsKeeper.SetHooks(
478     epochstypes.NewMultiEpochHooks(
479         // insert epoch hooks receivers here
480         app.MintKeeper.Hooks(),
481     ),
482 )
```

Recommendation

Please review the code to ensure that it meets the intented design.

Alleviation

The team acknowledged the finding.

PAR-02 | WRONG ERROR MESSAGE

Category	Severity	Location	Status
Inconsistency	Minor	x/mint/types/params.go: 164	Acknowledged

Description

The `validateReductionPeriodInEpochs` function is used to ensure that the value of `ReductionPeriodInEpochs` is valid, and it is called whenever this value needs to be checked. This function has no connection to the `validators` in the system, and it performs a separate set of checks on the value of `ReductionPeriodInEpochs` to ensure that it is valid.

Recommendation

The error message should be as follows:

```
164    return fmt.Errorf("ReductionPeriodInEpochs must be positive: %d", v)
```

We recommend correcting this information in order to improve the maintainability of the system.

Alleviation

The team acknowledged the finding.

6D4-01 | UNUSED FUNCTION

Category	Severity	Location	Status
Coding Style	Informational	app/app.go: 882~888; x/mint/types/hooks.go: 19~21	Acknowledged

Description

The following functions are not being used:

- `GetMaccPerms` in `app.go`
- `NewMultiMintHooks` in `hooks.go`

Recommendation

It is recommended to delete the unsed code in order to maintain a clean and organized codebase.

Alleviation

The team acknowledged the finding.

HOK-01 | THE `TODO` COMMENT

Category	Severity	Location	Status
Coding Style	Informational	x/epochs/types/hooks.go: 52	Acknowledged

Description

There is a TODO comment on the aforementioned line. It appears that there is an unfinished function based on the comment. If this is not the case, it is recommended to remove the unnecessary TODO comment. As a best practice, product code should not contain TODO comments.

Recommendation

Please review this code to ensure that it meets the intended design and that all necessary functions are completed.

Alleviation

The team acknowledged the finding.

APPENDIX | GOTABIT

Finding Categories

Categories	Description
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.
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.

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.