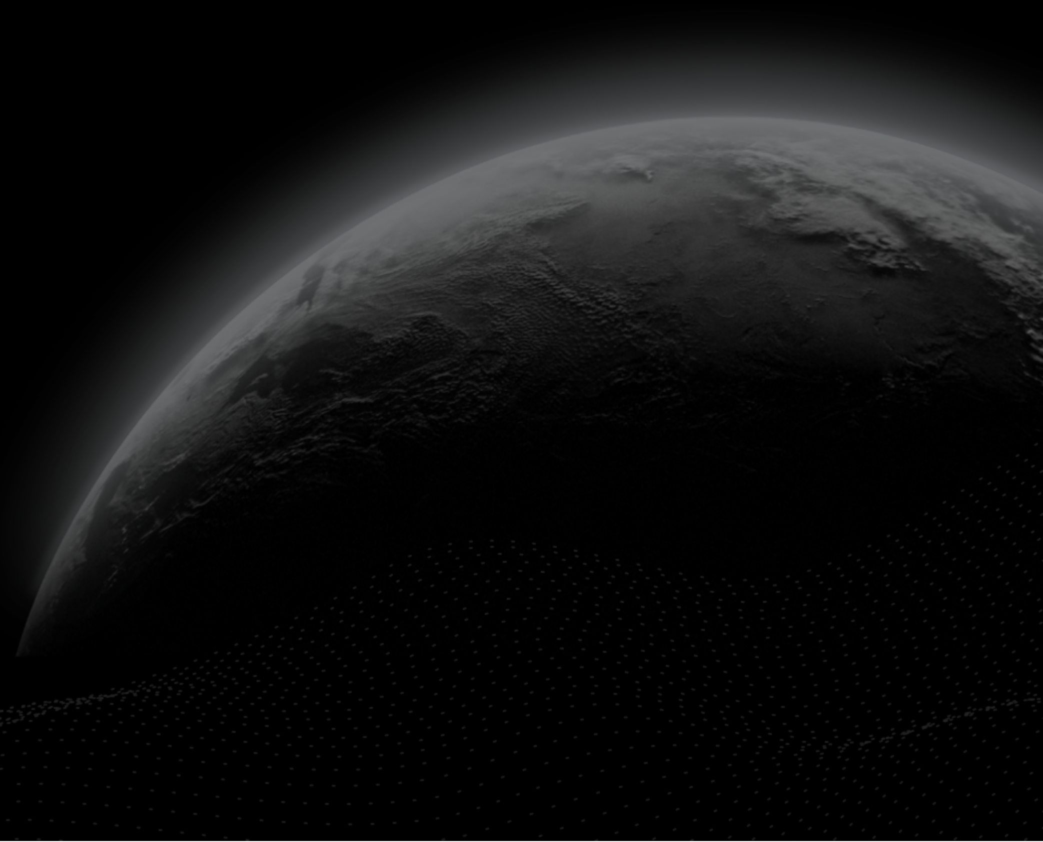
CERTIK

Security Assessment

Hanchain

CertiK Assessed on Feb 17th, 2023



CertiK Assessed on Feb 17th, 2023

Hanchain

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

Executive Summary

TYPES	ECOSYSTEM	METHODS
DeFi	Ethereum (ETH)	Manual Review, Static Analysis

LANGUAGE	TIMELINE	KEY COMPONENTS
Solidity	Delivered on 02/17/2023	N/A

CODEBASE

https://github.com/hanchain-paykhan/hanchain

...View All

COMMITS

base1: c9246c9e9f49d0da7cc93f40ed93fdafe7a61f83

base2: f8f6cc6a0917f1f4cd665780d964ef20f67e086d

...View All

Vulnerability Summary

6	3	2	0	1	0
Total Findings	Resolved	Mitigated	Partially Resolved	Acknowledged	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.
🟧	3	Major	2 Mitigated, 1 Acknowledged	Major risks can include centralization issues and logical errors. Under specific circumstances, these major risks can lead to loss of funds and/or control of the project.
🟨	0	Medium		Medium risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform.
🟨	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.
🟦	2	Informational	2 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 | HANCHAIN

CODEBASE | HANCHAIN

Repository

https://github.com/hanchain-paykhan/hanchain

Commit

base1: c9246c9e9f49d0da7cc93f40ed93fdafe7a61f83

base2: f8f6cc6a0917f1f4cd665780d964ef20f67e086d

AUDIT SCOPE | HANCHAIN

2 files audited ● 1 file with Mitigated findings ● 1 file without findings

ID	File	SHA256 Checksum
● TTB	contracts/TokenTimelock.sol	261591c77b8ad03ec3b11b57009926c82ae1bda3b2ffa1cbf977dd0227028cff
● HCU	contracts/HanChain.sol	871bcc62c468a291d47d0f0c230bdd780ee7ce4f0853e5a342a3f2d37970b12c

APPROACH & METHODS | HANCHAIN

This report has been prepared for Hanchain to discover issues and vulnerabilities in the source code of the Hanchain 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 | HANCHAIN

6	0	3	0	1	2
Total Findings	Critical	Major	Medium	Minor	Informational

This report has been prepared to discover issues and vulnerabilities for Hanchain. 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:

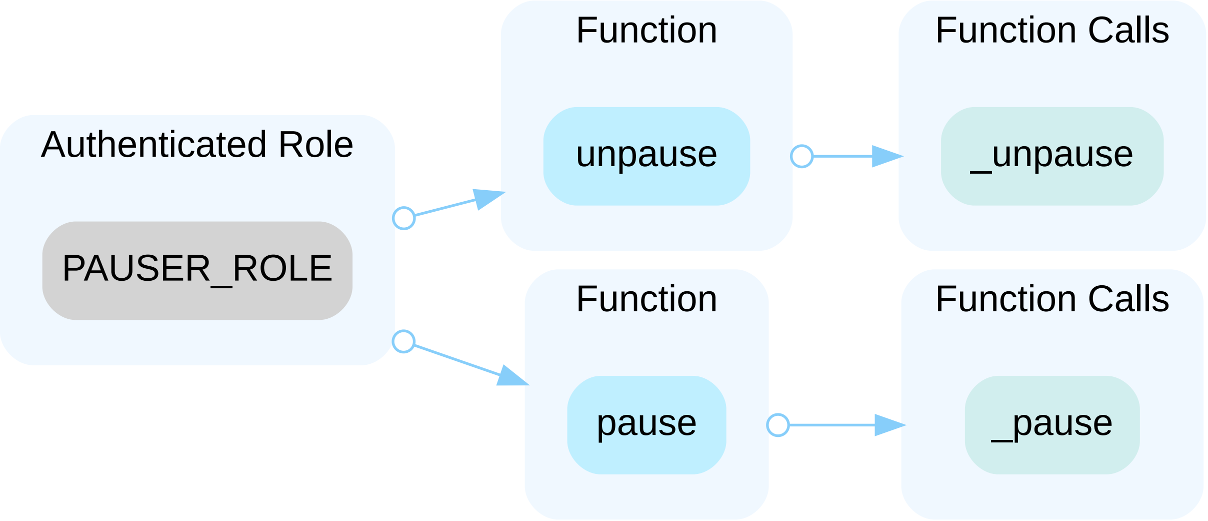
ID	Title	Category	Severity	Status
HCB-01	**Centralization Risks In HanChain.Sol**	**Centralization / Privilege**	**Major**	● **Mitigated**
HCB-02	**Initial Token Distribution**	**Centralization / Privilege**	**Major**	● **Acknowledged**
TTB-01	**Centralization Risks In TokenTimelock.Sol**	**Centralization / Privilege**	**Major**	● **Mitigated**
TTB-02	Potential Duplicate Beneficiaries	Data Flow	Minor	● Resolved
HCB-03	Too Many Digits	Coding Style	Informational	● Resolved
TTB-03	Missing Emit Events	Coding Style	Informational	● Resolved

HCB-01 | CENTRALIZATION RISKS IN HANCHAIN.SOL

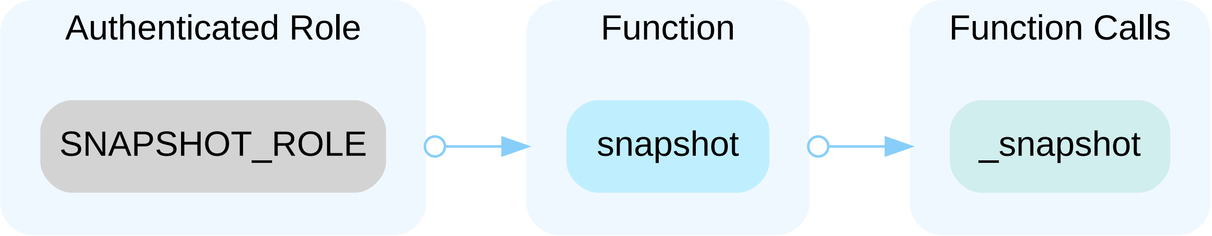
Category	Severity	Location	Status
Centralization / Privilege	● **Major**	**contracts/HanChain.sol (base): 23, 27, 31**	● **Mitigated**

Description

In the contract `HanChain` the role `PAUSER_ROLE` has authority over the functions shown in the diagram below. Any compromise to the `PAUSER_ROLE` account may allow the hacker to take advantage of this authority.



In the contract `HanChain` the role `SNAPSHOT_ROLE` has authority over the functions shown in the diagram below. Any compromise to the `SNAPSHOT_ROLE` account may allow the hacker to take advantage of this authority.



Recommendation

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

Short Term:

Timelock and Multi sign (⅔, ⅗) combination *mitigate* by delaying the sensitive operation and avoiding a single point of key management failure.

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

Long Term:

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

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

Permanent:

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

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

Alleviation

[`HanChain`]: As recommended, Short-Term measures were completed with a combination of Timelock and Multi-sign, all private keys are stored in hardware wallets, and are stored and managed in each fireproof safe according to the Information Security Management System. In the Long-Term, we plan to switch to a combination of Timelock and DAO. We also permanently relinquish ownership once the token distribution is complete.

[`CertiK`]: The team acknowledged the issue and adopted the timelock solution to delay-sensitive operations at the current stage. The `HanChain` contract has transferred the ownership to a Timelock contract with a minimal 48 hours delay.

HanChain contract address:

- https://etherscan.io/address/0x0c90C57aaf95A3A87eadda6ec3974c99D786511F

Timelock contract address:

- https://etherscan.io/address/0x1FF7652E80ab0Ee42Ba6fAD132a1e8A334384F4c

Grant Role transaction hash for the Timelock contract:

- https://etherscan.io/tx/0x641f90488ac0803f8515afb937cc612c0b59b52599af6a850d78e8c8644507ee

The team also adopted the multisign solution to ensure the private key management process at the current stage. The Timelock contract has transferred the PROPOSER_ROLE and CANCELLER_ROLE to a Gnosis Safe contract with 2/3 signers in the sensitive function signing process.

Multi-sign proxy address:

- https://etherscan.io/address/0xfc0e60F7B7AEe268d7492F7075ED9dD23E48F7cE

Grant Role transaction hash for Gnosis Safe:

- https://etherscan.io/tx/0x66381f8cabdcec8a45ed8258b6241243e186ed0c92bd999527b02b12c371821a

The 3 multisign addresses:

1. EOA: 0x60A3fc3f8E68C3561d52697cD14f9C0c4fBa4b9A
2. EOA: 0xfDB509381b0dEdde0599607aFd92C935CAdC3Ef7
3. EOA: 0xA137120BCC903638CF156c6F66b5c24997630722

HCB-02 | INITIAL TOKEN DISTRIBUTION

Category	Severity	Location	Status
Centralization / Privilege	● **Major**	**contracts/HanChain.sol (base): 20**	● **Acknowledged**

Description

All **HanChain** tokens are sent to the contract deployer when deploying the contract. This is a potential centralization risk as the deployer can distribute **HanChain** tokens without the consensus of the community.

Recommendation

We recommend transparency through providing a breakdown of the intended initial token distribution in a public location. We also recommend the team make an effort to restrict the access of the corresponding private key.

Alleviation

[`HanChain`]: The distributed tokens are stored in 5 multisig wallets according to each distribution plan, and when the tokentimelock contract audit is completed, the planned distribution amount to the founders and team members is sent to the tokentimelock address.

In addition, detailed plans for token distribution will be officially announced as soon as tokentimelock's audit is completed.

And all private keys related to multisig are stored in hardware wallets and stored and managed in each fire safe in accordance with the Information Security Management System.

Multisig address list

reward_multisigColdWallet : 0x3811F5674ABbC216AD29a1EDcDd0B05172A9f123

HANeP_multisigColdWallet : 0x495FCD7f56A0bf8BE1F29BE02D1aA5F492F2ff66

partner_multisigColdWallet : 0x19681F34aFCe6B7fadfb07cd34C8f20DcF0A4F2A

founder_multisigColdWallet : 0x90A692e0819075C49100F9F5f2724E75d8a34711

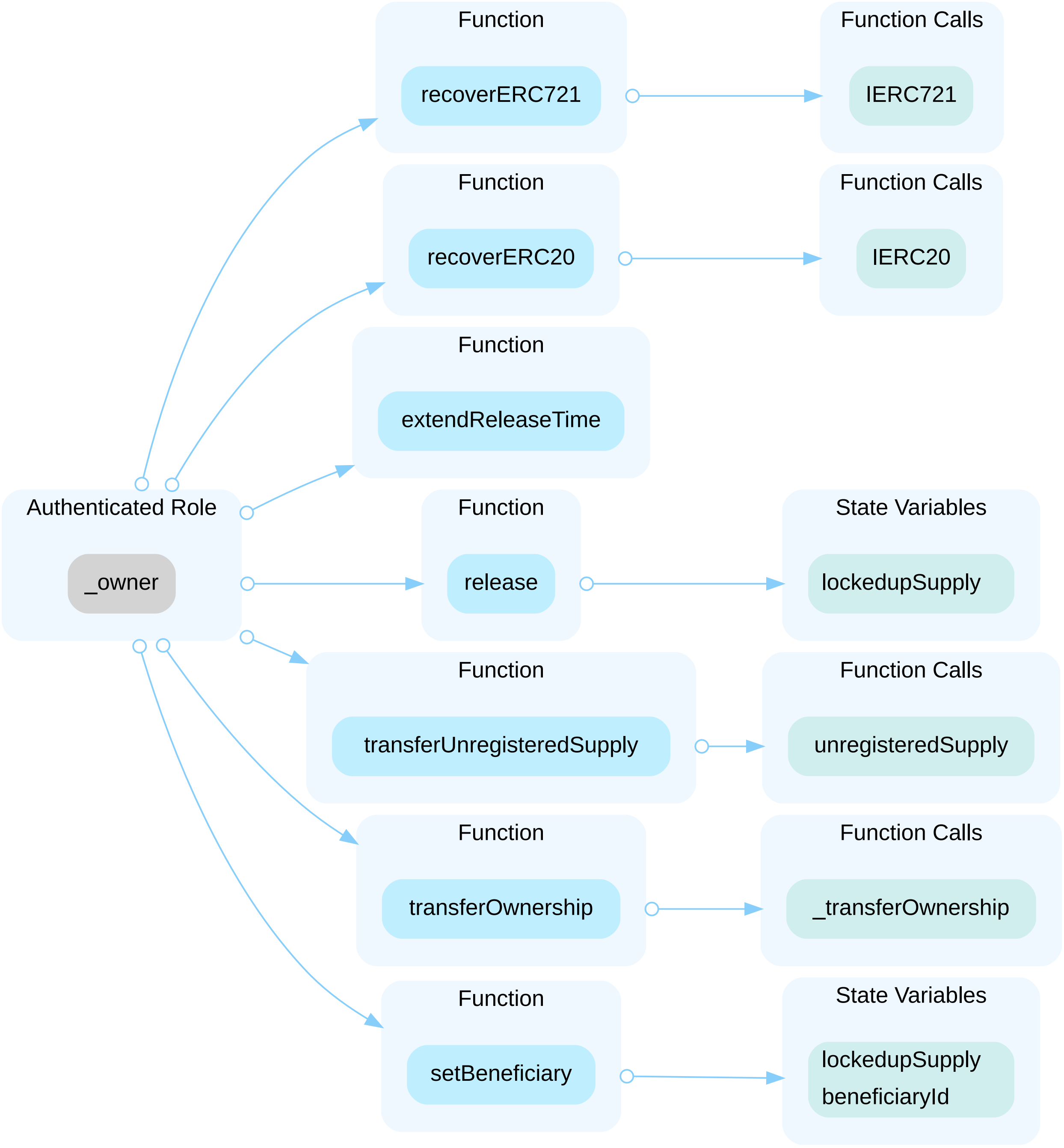
team_multisigColdWallet : 0xC7BdBCda0B8162427868aC41713d2559a9e2281c

TTB-01 | CENTRALIZATION RISKS IN TOKENTIMELOCK.SOL

Category	Severity	Location	Status
Centralization / Privilege	● **Major**	**contracts/TokenTimelock.sol: 46, 57, 86, 111, 116, 122, 168**	● **Mitigated**

Description

In the contract `TokenTimelock` the role `_owner` has authority over the functions shown in the diagram below. Any compromise to the `_owner` account may allow the hacker to take advantage of this authority.



Recommendation

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

Short Term:

Timelock and Multi sign (⅔, ⅗) combination *mitigate* by delaying the sensitive operation and avoiding a single point of key management failure.

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

Long Term:

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

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

Permanent:

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

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

Alleviation

[`HanChain`]: As recommended, Short-Term measures were completed with a combination of Timelock and Multi-sign, all private keys are stored in hardware wallets, and are stored and managed in each fireproof safe according to the Information Security Management System.

[`CertiK`]: The team acknowledged the issue and adopted the timelock solution to delay-sensitive operations at the current stage. The `TokenTimelock` contract has transferred the ownership to a Timelock contract with a minimal 48 hours delay.

TokenTimelock contract address:

- https://etherscan.io/address/0xfA2B470cac8b79A56B9486e029fef07DC634826B

Timelock contract address:

- https://etherscan.io/address/0x1FF7652E80ab0Ee42Ba6fAD132a1e8A334384F4c

Grant Role transaction hash for the Timelock contract:

- https://etherscan.io/tx/0x06bbd70c8c14ec7734a4ddb21d2f147cfb327093a79e2e480ccb29ea3c9af50c

The team also adopted the multisign solution to ensure the private key management process at the current stage. The Timelock contract has transferred the PROPOSER_ROLE and CANCELLER_ROLE to a Gnosis Safe contract with 2/3 signers in the sensitive function signing process.

Multi-sign proxy address:

- https://etherscan.io/address/0xfc0e60F7B7AEe268d7492F7075ED9dD23E48F7cE

Grant Role transaction hash for Gnosis Safe:

- https://etherscan.io/tx/0x66381f8cabdcec8a45ed8258b6241243e186ed0c92bd999527b02b12c371821a

The 3 multisign addresses:

1. EOA: 0x60A3fc3f8E68C3561d52697cD14f9C0c4fBa4b9A
2. EOA: 0xfDB509381b0dEdde0599607aFd92C935CAdC3Ef7
3. EOA: 0xA137120BCC903638CF156c6F66b5c24997630722

TTB-02 | POTENTIAL DUPLICATE BENEFICIARIES

Category	Severity	Location	Status
Data Flow	● Minor	contracts/TokenTimelock.sol: 66~73	● Resolved

Description

Because there is no prohibition on adding beneficiaries repeatedly after release, this function `getAllBeneficiary()` may return the duplicate values.

Scenario

1. The owner calls `setBeneficiary()` to set Alice as beneficiary.
2. The owner calls `setBeneficiary()` to set Bob as beneficiary.
3. It is time for Alice's release, the owner calls `release()` to release token for Alice.
4. If the owner calls `setBeneficiary()` to set Alice as beneficiary again. Now the beneficiary array returned by `getAllBeneficiary()` will be `[Alice's address, Bob's address, Alice's address]` . We are not sure if Alice appears twice would cause a problem or not.

Recommendation

We recommend the client to ensure if or not this design is correct. If the `getAllBeneficiary()` is only used to return all beneficiary addresses, we recommend refactoring the code and removing the duplicate addresses.

Alleviation

[`CertiK`]: The team resolved this issue in the commit hash: 93eccd7e758701a11e7caa109b25f4f15115fd40.

HCB-03 | TOO MANY DIGITS

Category	Severity	Location	Status
Coding Style	● Informational	contracts/HanChain.sol (base): 20	● Resolved

Description

Literals with many digits are difficult to read and review.

```
20          _mint(msg.sender, 1500000000 * 10 ** decimals());
```

Recommendation

We advise the client to use the scientific notation to improve readability.

Alleviation

[`CertiK`]: The client has added comment on the digits to improve readability. Changes have been reflected in the commit hash:38b8e3ebae88007c5171c8147b31b0b6777de7bd.

TTB-03 | MISSING EMIT EVENTS

Category	Severity	Location	Status
Coding Style	● Informational	contracts/TokenTimelock.sol: 46, 57, 111	● Resolved

Description

There should always be events emitted in the sensitive functions that are controlled by centralization roles.

Recommendation

It is recommended emitting events for the sensitive functions that are controlled by centralization roles.

Alleviation

[`CertiK`]: The team resolved this issue in the commit hash: 93eccd7e758701a11e7caa109b25f4f15115fd40.

APPENDIX | HANCHAIN

Finding Categories

Categories	Description
Centralization / Privilege	Centralization / Privilege findings refer to either feature logic or implementation of components that act against the nature of decentralization, such as explicit ownership or specialized access roles in combination with a mechanism to relocate funds.
Data Flow	Data Flow findings describe faults in the way data is handled at rest and in memory, such as the result of a struct assignment operation affecting an in-memory struct rather than an in-storage one.
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.

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.