

KISHIELD

Security Audit

BridgedECH Token

April 20, 2022





Table of Contents

1 Audit Summary

2 Project Overview

2.1 Token Summary

2.2 Main Contract Assessed

3 Smart Contract Vulnerability Checks

4 Contract Ownership

4.1 Privileged Functions

5 Important Notes To The Users

6 Findings Summary

6.1 Classification of Issues

6.1 Findings Table

01 Public function that could be declared external

02 Variables could be declared as constant

03 Unused Private Function

04 Boolean equality

7 Statistics

7.1 Liquidity

7.2 Token Holders

7.3 Liquidity Holders

8 Liquidity Ownership

9 Disclaimer



Audit Summary

This report has been prepared for BridgedECH Token on the Binance Chain network. KISHIELD provides both client-centered and user-centered examination of the smart contracts and their current status when applicable. This report represents the security assessment made to find issues and vulnerabilities on the source code along with the current liquidity and token holder statistics of the protocol.

A comprehensive examination has been performed, utilizing Cross Referencing, Static Analysis, In-House Security Tools, and line-by-line Manual Review.

The auditing process pays special attention to the following considerations:

- Ensuring contract logic meets the specifications and intentions of the client without exposing the user's funds to risk.
- Testing the smart contracts against both common and uncommon attack vectors.
- Inspecting liquidity and holders statistics to inform the current status to both users and client when applicable.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Verifying contract functions that allow trusted and/or untrusted actors to mint, lock, pause, and transfer assets.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Project Overview

Token Summary

Parameter	Result
Address	0x00EaFc9C1fb1b7f7889c7E91441ab62dE0259ad5
Name	BridgedECH
Token Tracker	BridgedECH (bECH)
Decimals	18
Supply	33,940,035
Platform	Binance Chain
compiler	v0.4.24+commit.e67f0147
Optimization	Yes with 200 runs
LicenseType	None
Language	Solidity
Codebase	https://bscscan.com/ address/0x00EaFc9C1fb1b7f7889c7E91441ab62dE0259ad5
Url	https://ech.network/

Main Contract Assessed

Name	Contract	Live
BridgedECH	0x00EaFc9C1fb1b7f7889c7E91441ab62dE0259ad5	Yes

Smart Contract Vulnerability Checks

Vulnerability	Automatic Scan	Manual Scan	Result
Unencrypted Private Data On-Chain	Complete	Complete	✓ Low / No Risk
Code With No Effects	Complete	Complete	✓ Low / No Risk
Message call with hardcoded gas amount	Complete	Complete	✓ Low / No Risk
Hash Collisions With Multiple Variable Length Arguments	Complete	Complete	✓ Low / No Risk
Unexpected Ether balance	Complete	Complete	✓ Low / No Risk
Presence of unused variables	Complete	Complete	✓ Low / No Risk
Right-To-Left-Override control character (U+202E)	Complete	Complete	✓ Low / No Risk
Typographical Error	Complete	Complete	✓ Low / No Risk
DoS With Block Gas Limit	Complete	Complete	✓ Low / No Risk
Arbitrary Jump with Function Type Variable	Complete	Complete	✓ Low / No Risk
Insufficient Gas Griefing	Complete	Complete	✓ Low / No Risk
Incorrect Inheritance Order	Complete	Complete	✓ Low / No Risk
Write to Arbitrary Storage Location	Complete	Complete	✓ Low / No Risk
Requirement Violation	Complete	Complete	✓ Low / No Risk
Missing Protection against Signature Replay Attacks	Complete	Complete	✓ Low / No Risk
Weak Sources of Randomness from Chain Attributes	Complete	Complete	✓ Low / No Risk

Vulnerability	Automatic Scan	Manual Scan	Result
Authorization through tx.origin	Complete	Complete	✓ Low / No Risk
Delegatecall to Untrusted Callee	Complete	Complete	✓ Low / No Risk
Use of Deprecated Solidity Functions	Complete	Complete	✓ Low / No Risk
Assert Violation	Complete	Complete	✓ Low / No Risk
Reentrancy	Complete	Complete	✓ Low / No Risk
Unprotected SELFDESTRUCT Instruction	Complete	Complete	✓ Low / No Risk
Unprotected Ether Withdrawal	Complete	Complete	✓ Low / No Risk
Unchecked Call Return Value	Complete	Complete	✓ Low / No Risk
Outdated Compiler Version	Complete	Complete	✓ Low / No Risk
Integer Overflow and Underflow	Complete	Complete	✓ Low / No Risk
Function Default Visibility	Complete	Complete	✓ Low / No Risk

Contract Ownership

The contract ownership of BridgedECH is not currently renounced. The ownership of the contract grants special powers to the protocol creators, making them the sole addresses that can call sensible ownable functions that may alter the state of the protocol.

The current owner is the address 0x5B38B90e4410bf71Aa6874913DAD74Ecbde857F1 which can be viewed from: [HERE](#)

The owner wallet has the power to call the functions displayed on the privileged functions chart below, if the owner wallet is compromised this privileges could be exploited.

We recommend the team to renounce ownership at the right timing if possible, or gradually migrate to a timelock with governing functionalities in respect of transparency and safety considerations.

Important Notes To The Users:

- The owner cannot stop Trading.
- The owner cannot change the max tx amount.
- There are no fees for buying, selling or sending tokens.
- Tokens are burned when users decide to bridge their tokens.
- Tokens are minted when the validators verification is passed, the tx hash has not used before, and the signatures are correct.
- The SignatureUtils contract was not verified as this falls outside the scope of the audit.
- Once the owner renounces ownership of the contract, none of the following are applicable.
- The owner can add validators.
- The owner can change the pair contract used to bridge tokens.
- No high-risk Exploits/Vulnerabilities Were Found in token Source Code.

Audit Passed



Findings Summary

Classification of Issues

Severity	Description
● High	Exploits, vulnerabilities or errors that will certainly or probabilistically lead towards loss of funds, control, or impairment of the contract and its functions. Issues under this classification are recommended to be fixed with utmost urgency
● Medium	Bugs or issues with that may be subject to exploit, though their impact is somewhat limited. Issues under this classification are recommended to be fixed as soon as possible.
● Low	Effects are minimal in isolation and do not pose a significant danger to the project or its users. Issues under this classification are recommended to be fixed nonetheless.
● Info	Consistency, syntax or style best practices. Generally pose a negligible level of risk, if any.

Findings

Severity	Found
● High	0
● Medium	0
● Low	0
● Info	4
Total	4

Findings

Public function that could be declared external

ID	Severity	Contract	Function
01	Informational	BridgedECH	Functions enter, exit, toEthPersonalSignedMessageHash, recoverAddress, addValidator

Description

Gas Optimization. Public function that could be declared external

Recommendation

Public functions that are never called by the contract should be declared external to save gas.

Variables could be declared as constant

ID	Severity	Contract	Function
02	Informational	BridgedECH	variables decimals, name, symbol

Description

Gas Optimization. Variables that are never changed could be declared as constant.

Recommendation

We recommend declaring those variables as constant.

Unused Private Function

ID	Severity	Contract	Function
03	Informational	BridgedECH	functions _burnFrom()

Description

These functions are private but never used by the contract logic.

Recommendation

We recommend deleting this function or setting the visibility to external if they are meant to be used.

Boolean equality

ID	Severity	Contract	Function
04	Informational	BridgedECH	Function exit()

Description

Statement 'require(bool,string)(contains(_txnHash) == false' Boolean constants can be used directly and do not need to be compare to true or false.

Recommendation

Remove the equality to the boolean constant. In case of comparing to false make use of '!'



Privileged Functions (onlyOwner)

Function Name	Parameters	Visibility
transferOwnership	address newOwner	default
addValidator	address _validator	public
pair	address _foreignContract	public

Statistics

Liquidity Info

Parameter	Result
Pair Address	0x793f8bcFD232843ac8d669f3682c15603463f5ec
bECH Reserves	0.00 bECH
BNB Reserves	0.00 BNB
Liquidity Value	\$0 USD

Token (bECH) Holders Info

Parameter	Result
bECH Percentage Burnt	0.00%
bECH Amount Burnt	0 bECH
Top 10 Percentage Own	100.00%
Top 10 Amount Owned	33,940,035 bECH
Top 10 Aprox Value	\$NaN USD

LP (bECH/BNB) Holders Info

Parameter	Result
bECH/BNB % Burnt	0.00%
bECH/BNB Amount Burnt	0 bECH
Top 10 Percentage Owned	0.00%
Top 10 Amount Owned	0 bECH
Locked Tokens Percentage	0.00%
Locked Tokens Amount	0 bECH

* All the data displayed above was taken on-chain at block 17119297

* The tokens on industry-standard burn wallets are not included on the top 10 wallets calculations

Liquidity Ownership

The token does not have liquidity at the moment of the audit, block 17119297

KISHIELD



Disclaimer

KISHIELD has conducted an independent audit to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the codes that were provided for the scope of this audit. This audit report does not constitute agreement, acceptance or advocacy for the Project that was audited, and users relying on this audit report should not consider this as having any merit for financial advice in any shape, form or nature. The contracts audited do not account for any economic developments that may be pursued by the Project in question, and that the veracity of the findings thus presented in this report relate solely to the proficiency, competence, aptitude and discretion of our independent auditors, who make no guarantees nor assurance that the contracts are completely free of exploits, bugs, vulnerabilities or deprecation of technologies.

All information provided in this report does not constitute financial or investment advice, nor should it be used to signal that any persons reading this report should invest their funds without sufficient individual due diligence regardless of the findings presented in this report. Information is provided 'as is', and KISHIELD is under no covenant to the completeness, accuracy or solidity of the contracts audited. In no event will KISHIELD or its partners, employees, agents or parties related to the provision of this audit report be liable to any parties for, or lack thereof, decisions and/or actions with regards to the information provided in this audit report.

The assessment services provided by KISHIELD 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.