CFG NINJA AUDITS

Security Assessment

BillzHub Token

July 28, 2022

Table of Contents

Audit Summary

This report has been prepared for BillzHub Token on the Binance smart chain network. CFGNINJA 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:

- 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.

Project Overview

Token Summary

Parameter	Result
Address	0x808D72347A802421d8F293E53D439a13eC547294
Name	BillzHub
Token Tracker	BillzHub (Billz)
Decimals	8
Supply	500,000,000,000
Platform	Binance smart chain
compiler	v0.8.6+commit.11564f7e
Contract Name	BillzHub
Optimization	Yes with 200 runs
LicenseType	Unlicensed
Language	Solidity
Codebase	https://bscscan.com/address/0x808D72347A802421d8F293E53D439a13eC547294#code
Payment Tx	0x9960229980b44009a6fa744aa51519b7914fc4d148164755115168cd873d11af

Project Overview

Risk Analysis Summary

Parameter	Result
Buy Tax	6%
Sale Tax	6%
Is honeypot?	Not Clean
Can edit tax?	Yes
Is anti whale?	Yes
Is blacklisted?	No
Is whitelisted?	No
Holders	Clean
Security Score	90/100
Auditor Score	90/100
Confidence Level	Medium

The following quick summary has been added to the project overview, however there are more details about the audit and their results please read every details.

Main Contract Assessed
Contract Name

Name	Contract	Live
BillzHub	0x808D72347A802421d8F293E53D439a13eC547294	Yes

TestNet Contract Assessed
Contract Name

Name	Contract	Live
BillzHub	0x6502323a19ec50e4cef3Efbe1571aa53A7D9a7EF	Yes

Solidity Code Provided

SolID	File Sha-1	FileName
billzhub	091f2efc0ff7c19e67d0dfb70d1b07e770577d2d	billzhub.sol
billzhub		
billzhub		

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

Mint Check

The Project Owners of BillzHub does not have a mint function in the contract, owner cannot mint tokens after initial deploy

. .

The Project has a Total Supply of 500,000,000,000 and cannot mint any more than the Max Supply.

.

Mint Notes:

Auditor Notes:

Project Owner Notes:

Owner can't mint new coins

Fees Check

The Project Onwers of BillzHub has the ability to set fees to 50%
We Recommend the team to create a new contract with fees restrictions to avoid any problems, as alternative the team can use multi signature wallet to ensure the project is safe from a potential fee increase.

Tax Fee Notes:

Auditor Notes: We asked Project owners: There is not a limit in Fees, how can you ensure the safety of holders and wont put tax to 100% and become a honeypot?

Project Owner Notes: There is no limit in fees because we want to upgrade with a dex. Where we have to change fee. We can't do a honeypot.

MaxTx Check

The Project Owners of BillzHub can set max tx amount.

The ability to set MaxTx can be used as bad actor, this can limit the ability of investors to sale their tokens at any given time if is set too low..

We recommend the project to set MaxTx to Total Supply or simiar to avoid swap or transfer from failures

MaxTX Notes:

Auditor Notes: We asked project owners: There is a MaxTX in the contract, why is that and how will you ensure the investors wont get lock and wont sale their asset

Project Owner Notes: MaxTX is to ensure every transaction works smoothly. It is to use to lock the asset. That is why it is unlimited.

Project Has MaxTX

Pause Trade Check

The Project Owners of BillzHub Owner can pause trading but he can move tokens.

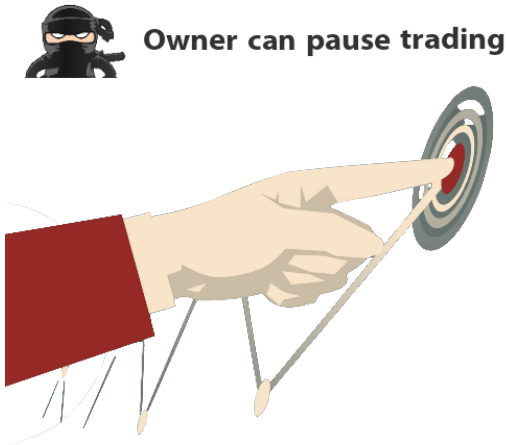
We recommend the team to only allow Open Trade and never use Stop Trade as this will be catastrofic for the project and investors.

We recommend the team to create a new contract without stop trade..

Pause Trade Notes:

Auditor Notes: We asked Project owners: There is a Start Trade, by default holders wont be able to sale or buy until you start trade. How will you ensure that after launch you will start trade?

Project Owner Notes: Start trade was to ensure token holders don't add liquidity and hijack our token by doing a rugpull.



Contract Ownership

The contract ownership of BillzHub 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 0x0b2607c0eac59e9d789eed03972761ff15b284b0 which can be viewed from:
HERE

The owner wallet has the power to call the functions displayed on the priviliged 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.

We recommend the team to use a Multisignature Wallet if contract is not going to be renounced, this will give the ability to the team to have more control over the contract.

Liquidity Ownership

The token does not have liquidity at the moment of the audit, block 17204169

KYC Information

The Project Owners of BillzHub is not KYC. .

The owner wallet has the power to call the functions displayed on the priviliged 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.

KYC Information Notes:

Auditor Notes: Asked project owner about KYC or Doxxed

Project Owner Notes:

Mythx Security Summary Checks

ID	Severity	Name	File	location
SWC-100	Pass	Function Default Visibility	billzhub.sol	L: 0 C: 0
SWC-101	Pass	Integer Overflow and Underflow.	billzhub.sol	L: 0 C: 0
SWC-102	Pass	Outdated Compiler Version file.	billzhub.sol	L: 0 C: 0
SWC-103	Low	A floating pragma is set.	billzhub.sol	L: 5 C: 0
SWC-104	Pass	Unchecked Call Return Value.	billzhub.sol	L: 0 C: 0
SWC-105	Pass	Unprotected Ether Withdrawal.	billzhub.sol	L: 0 C: 0
SWC-106	Pass	Unprotected SELFDESTRUCT Instruction	billzhub.sol	L: 0 C: 0
SWC-107	Pass	Read of persistent state following external call.	billzhub.sol	L: 0 C: 0
SWC-108	Low	State variable visibility is not set..	billzhub.sol	L: 0 C: 0
SWC-109	Pass	Uninitialized Storage Pointer.	billzhub.sol	L: 0 C: 0
SWC-110	Pass	Assert Violation.	billzhub.sol	L: 0 C: 0
SWC-111	Pass	Use of Deprecated Solidity Functions.	billzhub.sol	L: 0 C: 0
SWC-112	Pass	Delegate Call to Untrusted Callee.	billzhub.sol	L: 0 C: 0
SWC-113	Pass	Multiple calls are executed in the same transaction.	billzhub.sol	L: 0 C: 0

ID	Severity	Name	File	location
SWC-114	Pass	Transaction Order Dependence.	billzhub.sol	L: 0 C: 0
SWC-115	Low	Authorization through tx.origin.	billzhub.sol	L: 474 C: 15
SWC-116	Pass	A control flow decision is made based on The block.timestamp environment variable.	billzhub.sol	L: 0 C: 0
SWC-117	Pass	Signature Malleability.	billzhub.sol	L: 0 C: 0
SWC-118	Pass	Incorrect Constructor Name.	billzhub.sol	L: 0 C: 0
SWC-119	Pass	Shadowing State Variables.	billzhub.sol	L: 0 C: 0
SWC-120	Pass	Potential use of block.number as source of randonmness.	billzhub.sol	L: 0 C: 0
SWC-121	Pass	Missing Protection against Signature Replay Attacks.	billzhub.sol	L: 0 C: 0
SWC-122	Pass	Lack of Proper Signature Verification.	billzhub.sol	L: 0 C: 0
SWC-123	Pass	Requirement Violation.	billzhub.sol	L: 0 C: 0
SWC-124	Pass	Write to Arbitrary Storage Location.	billzhub.sol	L: 0 C: 0
SWC-125	Pass	Incorrect Inheritance Order.	billzhub.sol	L: 0 C: 0
SWC-126	Pass	Insufficient Gas Griefing.	billzhub.sol	L: 0 C: 0
SWC-127	Pass	Arbitrary Jump with Function Type Variable.	billzhub.sol	L: 0 C: 0
SWC-128	Pass	DoS With Block Gas Limit.	billzhub.sol	L: 0 C: 0

ID	Severity	Name	File	location
SWC-129	Pass	Typographical Error.	billzhub.sol	L: 0 C: 0
SWC-130	Pass	Right-To-Left-Override control character (U +202E).	billzhub.sol	L: 0 C: 0
SWC-131	Pass	Presence of unused variables.	billzhub.sol	L: 0 C: 0
SWC-132	Pass	Unexpected Ether balance.	billzhub.sol	L: 0 C: 0
SWC-133	Pass	Hash Collisions with Multiple Variable Length Arguments.	billzhub.sol	L: 0 C: 0
SWC-134	Pass	Message call with hardcoded gas amount.	billzhub.sol	L: 0 C: 0
SWC-135	Pass	Code With No Effects (Irrelevant/Dead Code).	billzhub.sol	L: 0 C: 0
SWC-136	Pass	Unencrypted Private Data On-Chain.	billzhub.sol	L: 0 C: 0

We scan the contract for additional security issues using MYTHX and industry standard security scanning tool

Security Check Details Page

SWC-103 - Floating Pragma.

CWE-664: Improper Control of a Resource Through its Lifetime.

Description:

Contracts should be deployed with the same compiler version and flags that they have been tested with thoroughly. Locking the pragma helps to ensure that contracts do not accidentally get deployed using, for example, an outdated compiler version that might introduce bugs that affect the contract system negatively.

Remediation:

Lock the pragma version and also consider known bugs (https://github.com/ethereum/solidity/releases) for the compiler version that is chosen.

Pragma statements can be allowed to float when a contract is intended for consumption by other developers, as in the case with contracts in a library or EthPM package. Otherwise, the developer would need to manually update the pragma in order to compile locally.

References:

Ethereum Smart Contract Best Practices - Lock pragmas to specific compiler version.

SWC-108 - State Variable Default Visibility

CWE-710: Improper Adherence to Coding Standards

Description:

Labeling the visibility explicitly makes it easier to catch incorrect assumptions about who can access the variable.

Remediation:

Variables can be specified as being public, internal or private. Explicitly define visibility for all state variables.

References:

Ethereum Smart Contract Best Practices - Explicitly mark visibility in functions and state variables

SWC-115 - Authorization through tx.origin

CWE-477: Use of Obsolete Function

Description:

tx.origin is a global variable in Solidity which returns the address of the account that sent the transaction. Using the variable for authorization could make a contract vulnerable if an authorized account calls into a malicious contract. A call could be made to the vulnerable contract that passes the authorization check since tx.origin returns the original sender of the transaction which in this case is the authorized account.

Remediation:

tx.origin should not be used for authorization. Use msg.sender instead.

References:

Solidity Documentation - tx.origin

Ethereum Smart Contract Best Practices - Avoid using tx.origin

SigmaPrime - Visibility.

SWC Information Notes:

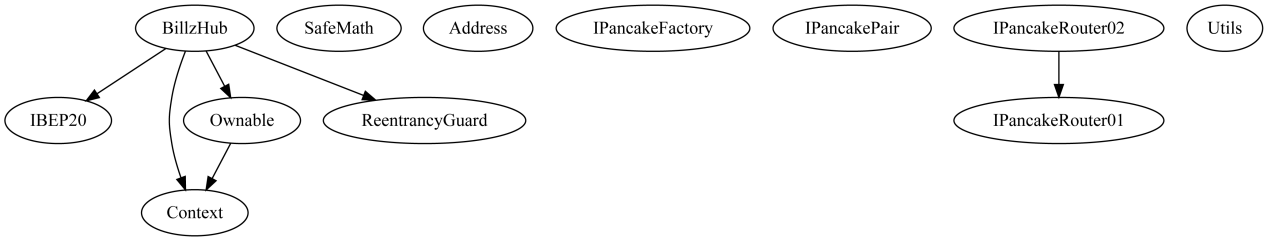
Auditor Notes:

Project Owner Notes:

Call Graph and Inheritance

The contract for BillzHub has the following call graph structure

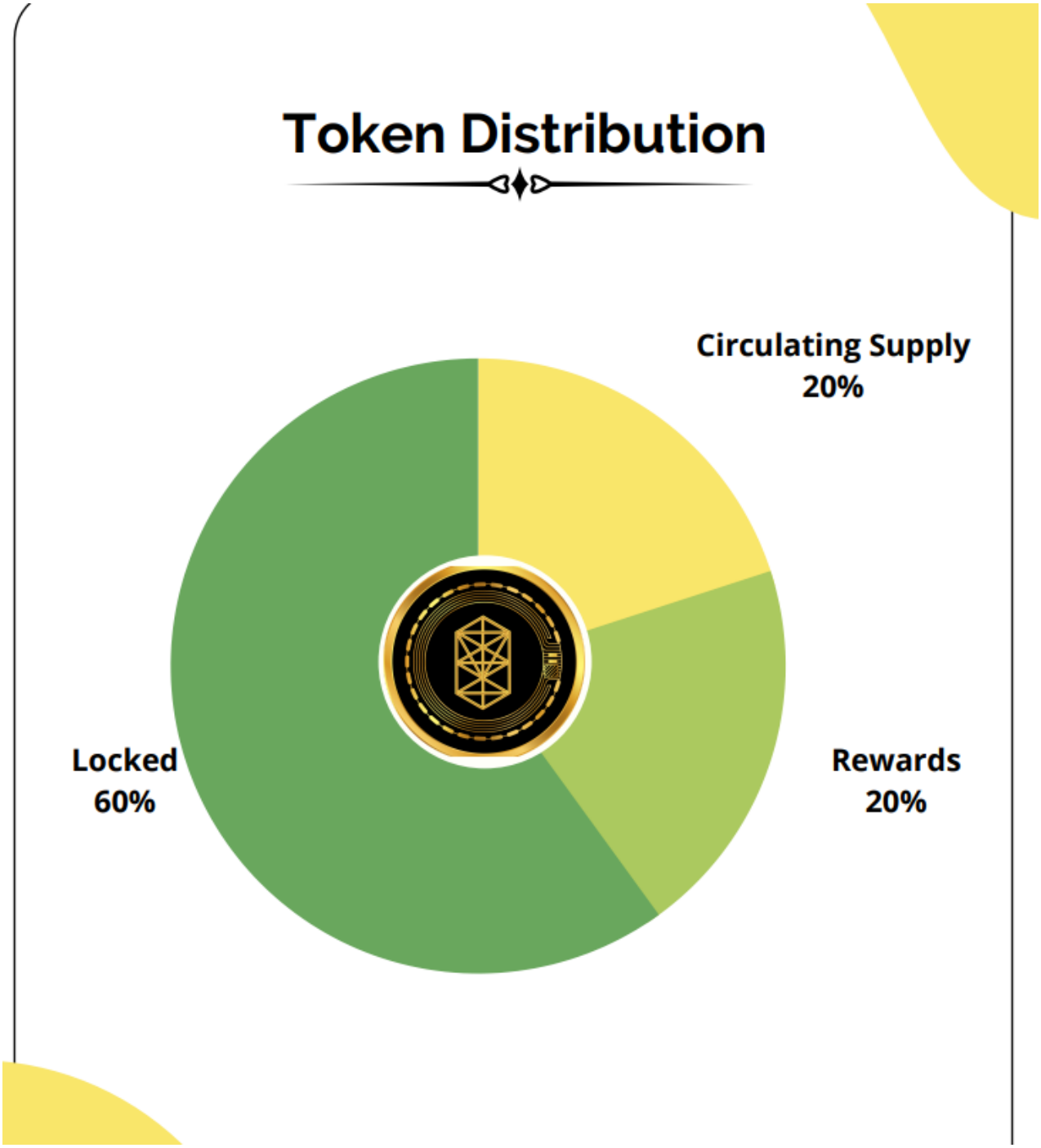
The Project has a Total Supply of 500,000,000,000 and has the following inheritance



Top Token Holders

The contract for BillzHub has the following top token holders

.



Priviliged Functions (onlyOwner)

Function Name	Parameters	Visibility
renounceOwnership		public
transferOwnership	address payable newOwner	public
Lock	uint256 time	public
startTrading		External
excludeFromreward	account (address)	public
IncludeInReward	account (address)	external
excludeFromFee	account (address)	public
includeInFee	account (address)	public
setMaxTxPercent	uint256 maxTxAmount	public
setMinTokenNumberToSell	uint256 _amount	public
setExcludeFromMaxTx	address _address, bool value	public
setTaxFeePercent	uint256 taxFee	external
setLiquidityFeePercent	uint256 liquidityFee	external
setMarketFeePercent	uint256 marketFee	external
setDevFeePercent	uint256 devFee	external
setSwapAndLiquifyEnabled	bool _state	public

Function Name	Parameters	Visibility
setReflectionFees	bool _state	external
setMarketAddress	address payable _marketAddress	external
setDevAddress	address payable _devAddress	external
setPancakeRouter	IPancakeRouter02 _pancakeRouter	external

Important Notes To The Users:

- Billzhub Team are a dedicated project team, they are looking to ensure the project is successful and are taking the necessary steps to do so.
- Owner can set fees up to 100%.
- Owner can set max tx amount.
- Owner can't pause trading, however is paused by default and they need to start trading.
- Some concerns over the fees, max tx has been channel to the project owners
- No high-risk Exploits/Vulnerabilities Were Found in the Source Code.

Audit Passed

Social Media Checks

Social Media	URL	Result
Twitter	https://twitter.com/billzhub	Pass
Reddit	https://instagram.com/billz.hub	Pass
Website	https://billzhub.world	Pass
Telegram	https://t.me/billzhubtalk	Pass

We recommend to have 3 or more social media sources including a completed working websites.

Social Media Information Notes:

Auditor Notes: undefined

Project Owner Notes: Project Owner states they also have a discord: https://discord.gg/xR3pMtb7jg .

Disclaimer

CFGNINJA 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 advocation 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 CFGNINJA is under no covenant to the completeness, accuracy or solidity of the contracts audited. In no event will CFGNINJA 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 CFGNINJA 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.