INTERFI

SMART CONTRACT SECURITY ASSESSMENT

PREPARED FOR

BLOCK HUB COIN (BHC)

hello@interfi.network

interfinetwork

www.interfi.network

FOR BLOCK HUB COIN

Date of Report	November 06, 2025
Live Code	0xb1dF24F72C3D4962581C80aa543C95dEfdF6DAa1
Platform	Ethereum Chain
Website	https://blockhubcoin.com
Telegram Channel	https://t.me/BHCToken_Official
Telegram Chat	https://t.me/blockhubcoin
Liquidity Lock	
Language	Solidity
Methodology	Automated Review, Unit Tests, Manual Review
Auditor	InterFi

Disclaimer: Smart contracts deployed on blockchains are inherently exposed to potential exploits, vulnerabilities, and security risks. Blockchain and cryptographic technologies are emerging and carry ongoing uncertainties. Please review the full audit report for detailed insights into risk severity, vulnerabilities, and audit scope limitations.

Centralization Warning: Centralized privileges—regardless of intent or access control—introduce elevated risks to contract security and user trust.

KYC Advisory: The project lacks verified third-party KYC of its owners, team, or deployers. Without independent KYC, transparency and accountability are reduced, increasing the risk of fraud or rug pulls.

Verification: Verify this report: https://www.github.com/interfinetwork

TABLE OF CONTENTS

1. SUMMARY

The audit resulted in the identification of issues across a range of severity levels, including logic flaws, access control oversights, and design inconsistencies. All high-impact findings were communicated to the development team with clear recommendations for remediation. Where applicable, the team has confirmed implementation of fixes or provided justifications for design choices.

1.1 Summary of Findings

Severity	Count
Critical	0
Major	0
Medium	0
Minor	2
Unknown	1
Centralization	1

1.2 Resolution Status

Status	Count
Fixed	1
Partially Fixed	0
Acknowledged	3
Pending	0

1.3 System Overview

This system is a decentralized protocol comprising a suite of smart contracts. These contracts collectively define the rules, permissions, and operational workflows for managing on-chain assets, executing user interactions, and enforcing protocol-level logic. Smart contracts in this context are self-executing code units that autonomously manage the state and behavior of digital assets based on predefined conditions. The protocol utilizes these contracts to enable key functionalities such as:

- Ownership and access control enforcement
- Permission and role-based actions
- Data storage and updates
- Event logging and auditability
- Batch processing and collection management

1.4 Files in Scope

InterFi was engaged by `BLOCK HUB COIN` to perform a security audit of the smart contracts. The audit scope was strictly limited to the files explicitly listed under the “Files in Scope” section. No other files or components were reviewed unless otherwise stated.

File	Path	Notes
ERC-20: Block Hub Coin (BHC)	`BHC.sol`	

1.5 Out-of-Scope Assumptions

The following components and assumptions were explicitly excluded from this audit:

- Frontend or backend integration logic.
- Off-chain components, scripts, or oracles.
- External contracts or libraries unless explicitly stated.
- Compiler-level or EVM-specific behavior outside the contract's scope.
- Governance or tokenomics-related decisions not implemented in code.
- All third-party dependencies as discussed in findings.

2. METHODOLOGY

2.1 Audit Objectives

This audit aims to ensure that the smart contract system is predictable, and behaves as intended under normal conditions. Primary audit objectives are to:

- Identify potential vulnerabilities or logic errors in the implementation.
- Evaluate adherence to best practices in smart contract development.
- Assess the correctness of access controls and permission systems.
- Recommend remediations or enhancements for improved security and performance.

2.2 Methodologies

The audit follows a layered security approach using both automated tools and manual techniques. We review the contracts for functional correctness, exploitability, and adherence to smart contract best practices:

Type	Tools & Techniques
Manual Code Review	Line-by-line analysis to check logic, permissions, and edge cases
Automated Analysis	Tools like Slither, MythX, or custom linters to catch known patterns
Static Analysis	Identification of bugs without executing the code (compile-time checks)
Unit Test Inspection	Evaluation of existing test coverage, assumptions, and potential false positives/negatives (if applicable)
Architecture Review	Mapping of privileged roles, callable paths, and contract interdependencies (if applicable)

2.3 Risk Categorization

Each issue identified during the audit is assigned a severity level based on its potential impact, exploitability, and likelihood of real-world abuse. These categories help prioritize remediation efforts:

Risk Severity	Definition
Critical	Represents a severe vulnerability that may result in complete contract compromise, such as asset theft, permanent loss of functionality, or unrestricted access. These issues are often easily exploitable and require immediate resolution.
Major	Indicates significant risk that can affect core contract behavior, enable unauthorized operations, or create unintended financial exposure. While not as urgent as critical risks, they should be remediated promptly.
Medium	These are moderate-level risks that may become exploitable under specific conditions. They often relate to logic errors, insufficient validation, or architectural oversights that could escalate over time.
Minor	Denotes issues that have low security impact but may degrade code quality, performance, or maintainability. These include inefficiencies, style violations, or redundant logic. Fixes are recommended for robustness.
Unknown	Risks where the severity cannot be confidently determined due to limited context, external dependencies, or ambiguous design intent. It is advised to treat these conservatively and address them proactively.
Centralization	Any function controlled by a single privileged role is treated as a critical risk, regardless of its purpose, due to the potential for misuse, override, or total asset control.

2.4 Resolution Status Definitions

All identified issues are also assigned a resolution status, indicating the current handling and response from the development team:

Status	Definition
Fixed	The issue has been remediated and verified as resolved during the re-audit or final check.
Partially Fixed	The issue has been partially mitigated, but remnants or related concerns may still exist. Further attention may be required.
Acknowledged	The development team has accepted the finding but opted not to implement a fix.
Pending	The issue remains unresolved at the time of publication. It poses a potential risk and should be addressed.

3. FINDINGS

01	ERC-20 Allowance Race (Approve Front-Running)
Severity	Minor
Description	Standard ERC-20 race: If a holder changes an allowance from a non-zero to another non-zero amount, a spender can front-run to consume the old allowance just before it's updated, potentially spending old + new in aggregate.
Recommendation	Add `increaseAllowance/decreaseAllowance` helpers, or implement *EIP-2612* `permit` to reduce approval transactions.
Status	Acknowledged
Comment	This is a well-known pattern; commonly exploitable in practice when users "top up" approvals.

02	Transfer to Zero Address Allowed
Severity	Minor
Description	Sending tokens to `address(0)` is permitted and will credit `balanceOf[address(0)]` while not decreasing `totalSupply` (declared constant). This is a soft burn that: ▪ Permanently locks tokens at the zero address, and ▪ Leaves `totalSupply` overstated relative to circulating supply
Recommendation	Add `require(to != address(0), "transfer to zero")` in `transfer/transferFrom`
Status	Acknowledged
Comment	Design choice. No exploitable surface.

03	Direct & Indirect Dependencies
Severity	Unknown
Description	Smart contract is interacting with third party protocols e.g., Market Makers, External Contracts, Web 3 Applications, *OpenZeppelin* tools. The scope of the audit treats these entities as black boxes and assumes their functional correctness. However, in the real world, all of them can be compromised, and exploited. Moreover, upgrades in these entities can create severe impacts, e.g., increased transactional fees, deprecation of previous routers, etc.
Recommendation	Inspect third party dependencies regularly, and mitigate severe impacts whenever necessary.
Status	Acknowledged
Comment	Team will review dependencies periodically and push updates if required

4. CENTRALIZATION

Centralization is one of the leading causes of smart contract-related asset losses. When a contract assigns critical powers to a privileged role- such as an `owner`, `admin`, or designated `controller` - the associated risk becomes elevated, especially if that role is tied to a single externally owned account (EOA). In many cases, privileged roles serve operational or safety functions:

4.1 Noteworthy Privileged Functions

None

01	Token Distribution
Severity	Centralization
Description	Entire supply is minted to `msg.sender` during contract deployment. This hardcodes full token control to the deployer at genesis. The initial supply has been subsequently distributed across multiple wallets.
Recommendation	Implement vesting, time locks, or controlled distribution logic to mitigate single-party control.
Status	Fixed
Comment	Team has implemented an off-chain token distribution strategy aligned with the published tokenomics plan (see “Tokenomics & Supply Management” table in Block Hub Coin whitepaper). Although the smart contract still mints the full supply to the deployer at genesis, the project has manually distributed allocations across multiple wallets corresponding to the designated categories (Private Sale, Presale, CEX, Marketing, Operations, R&D, and Reserve). Reserve and founder-related allocations are reportedly locked via multi-year smart contracts and vesting schedules as per the vesting policy (10-year and 5-year releases). This mitigates the original centralization concern, provided these locking mechanisms are on-chain and verifiable. ✓ Verified fix at distribution level; recommend public disclosure of vesting contract addresses for transparency.

5. DISCLAIMER

InterFi Network provides professional smart contract audits for blockchain-based codebases (commonly known as smart contracts). This audit assessed the reviewed contract(s) for common vulnerabilities, centralization risks, and logic flaws. However, no audit can guarantee the complete absence of bugs or vulnerabilities. This report does not constitute a security guarantee, endorsement, or assurance of business model soundness or legal compliance.

The review is limited strictly to the source code and its logic as provided, and does not extend to compiler behavior, off-chain components, or external integrations. Due to the evolving nature of blockchain technology and associated risks, users should understand that all materials, including this audit report, are provided strictly on an “as is”, “as available”, and “with all faults” basis.

5.1 Confidentiality

This report is confidential and intended solely for the client. It may not be disclosed, reproduced, or relied upon by third parties without prior written consent from InterFi Network. All terms, including confidentiality, liability limitations, and scope, are governed by the audit agreement.

5.2 No Financial Advice

This report is not financial, investment, tax, legal, or regulatory advice. It should not be relied upon for making investment decisions or assessing the value, viability, or safety of any token, product, or platform. No part of this document should be interpreted as an endorsement or recommendation. InterFi Network accepts no liability for any actions taken based on this report.

5.3 Technical Disclaimer

InterFi disclaims all warranties—express, implied, or statutory—including merchantability, fitness for a particular purpose, title, and non-infringement. We do not guarantee that the reviewed contracts are error-free, fully secure, or meet any specific requirements. Audit results may contain false positives or negatives, and findings are subject to the context and limitations of the review scope.

5.4 Timeliness & Accuracy

Audit results reflect the state of the code at the time of review. InterFi makes no commitment to update findings after publication. We do not warrant the accuracy, completeness, or timeliness of information delivered via this report.

5.5 Third-Party Links

This report may contain references or links to external websites and social media accounts. InterFi Network is not responsible for the content or operation of third-party platforms and assumes no liability for actions taken based on their content.

6. ABOUT

InterFi Network is a leading provider of intelligent blockchain solutions, offering secure, scalable, and production-ready smart contract services. Our team specializes in the development, testing, and auditing of smart contracts across a wide range of blockchain ecosystems.

We have delivered:

- 300+ smart contract systems developed
- 2,000+ smart contracts audited
- 500,000+ lines of code reviewed and analyzed

Our technical expertise spans multiple languages including:

- Solidity for EVM-compatible chains (Ethereum, BNB Chain, Polygon, Avalanche, Cronos, Fantom, Velas, Metis, and more)
- Move for next-generation platforms such as Sui and Aptos
- Rust for advanced ecosystems like Solana, Near, and Cosmos SDK-based chains

6.1 Connect with Us

InterFi Network is driven by a multidisciplinary team of engineers, developers, UI/UX specialists, and blockchain researchers. The core team consists of 3 senior members supported by 4+ expert contributors across code auditing, tooling, and protocol design.

- Website: interfi.network
- Email: hello@interfi.network
- GitHub: github.com/interfinetwork
- Telegram (Engineering): @interfiaudits
- Telegram (Onboarding): @interfisupport

THANK YOU