Ensuring Security Integrity

AUDIT REPORT

BOND FLOW

Prepared by

BLOCKCHAIN GURDIAN

www.blockchaingurdian.com

Disclaimer

This audit is limited solely to the smart contract code at the specified address. Blockchain Guardian is an independent third-party auditing firm that conducts audits upon client request. As a professional auditing company, our review focuses exclusively on identifying potential vulnerabilities, backdoors, and/or malicious or scam-related scripts within the smart contract.
Accordingly:

- Blockchain Guardian does not provide financial advice and has no partnership or affiliation with the contract owners.
- All project operations, management, and website administration are fully controlled by the client.
- Blockchain Guardian has no influence over client decisions, including but not limited to website modifications, operational changes, or the enabling or disabling of withdrawal functions, which may be executed through the smart contract itself.
- Any concerns regarding the project, its team, or its operations should be directed to the project owners and not to Blockchain Guardian.
- Investors are not obligated, encouraged, or influenced by Blockchain Guardian to invest in any audited project.
- Blockchain Guardian does not assume responsibility for investor funds and does not guarantee profits or returns.
- Investors are strongly advised to conduct their own research (DYOR) and gain sufficient cryptocurrency knowledge before making any investment decisions.

To report suspected scams, malpractice, or irregular activities, please contact us through the official Blockchain Guardian communication channels for review and potential blacklisting.

Prepared by

BLOCKCHAIN GURDIAN www.blockchaingurdian.com

Conclusion & Project Overview

The **BONDFLOW** smart contract runs on the Arbitrum One main network and was found to contain no vulnerabilities, backdoors, or malicious scripts.

General Description of the Contract

The **BONDFLOW** smart contract enables users to invest arbitrary amounts of USDC in exchange for a predefined return on investment (ROI) ranging from 100.3% to 118%, depending on the selected plan duration, which spans 1 to 28 days. Payouts are subject to the availability of sufficient funds within the contract at the time of withdrawal.

Dividend amounts are calculated and fixed at the moment of deposit. These dividends become available for withdrawal only after the corresponding lock-up period has elapsed. Each deposit made by a user is stored and tracked independently within the contract to ensure accurate payout calculations for individual investments.

The protocol includes a daily lottery mechanism that allows participants to receive additional rewards in the form of lottery prizes.

A portion of each deposit is transferred to the PoolBondFlow contract, where project operators provide liquidity to the USDC/ETH trading pair on Uniswap V3. During the claimBond process, if the main BONDFLOW contract does not hold sufficient USDC to fulfill withdrawal requests, liquidity is sourced from the PoolBondFlow contract by utilizing the low and high liquidity positions opened by the system.

Deployment Information

- Launch Date: December 05, 2025, at 09:33:46 PM (UTC)

Contract Fees

- Buy Bond Fee: 10%
- Buy Bond with Name Fee: 10%

Conclusion & Project Overview

Owner Privileges and Access Control

The contract owner does not retain administrative control over the BONDFLOW contract nor access to privileged functions within the PoolBondFlow contract. Ownership of both contracts has been renounced, as confirmed by the following transactions:

- **BONDFLOW Ownership Renouncement:** 0x5e9f4fc1ca786810190cdec8ab4650bd167fab1cc82ac112e850d6622d4b300d
- **PoolBondFlow Ownership Renouncement:** 0x72996de21ab761f9cb43d39190349f353984124d8d86cb44695181dc0e83fb3c

High Issue – ROI-Based System (High Risk)

The contract operates on a return-on-investment (ROI) model and must be considered high risk. Users' principal deposits are not withdrawable. Participants may only receive dividends and referral commissions, which are funded by deposits from other users rather than from an external revenue source. Users are strongly advised to invest only with a full understanding of the risks involved and to conduct thorough due diligence before participation.

Medium Issue – NFT Transfer Can Break Claim Logic and Lock Funds

Each user deposit results in the minting of an NFT representing that specific deposit. During the claim process, profits associated with the deposit are transferred to the current owner of the NFT.

However, during the claim operation, the volumePersonal value of the NFT owner is reduced. If the owner's volumePersonal balance is less than the withdrawable profit amount, the transaction will revert, preventing the claim from being executed. As a result, profits from that deposit become permanently unclaimable.

Medium Issue – Off-Chain Management of PoolBondFlow Contract

Positions and swaps within the PoolBondFlow contract are managed entirely off-chain by the project operator. This approach significantly reduces transparency and introduces centralization risks. Additionally, reliance on off-chain management increases the risk of operational disruptions, which could potentially result in partial or complete loss of project funds.

Prepared by

BLOCKCHAIN GURDIAN www.blockchaingurdian.com

Contract Audit Checklist

S.NO	Vulnerability Description	Status
1	Visibility of functions and variables	Passed
2	Compiler error	Passed
3	ROI Investment Plan	Warning
4	Transfer Block	Passed
5	Floating pragma	Passed
6	Timestamp dependence	Passed
7	Deprecated solidity functions	Passed
8	Gas limit and loops	Passed
9	Front running	Passed
10	User balance manipulation	Passed
11	Dos with revert	Passed
12	Dos with block gas limit	Passed
13	Reentrancy security	Passed
14	Malicious libraries	Passed
15	Integer overflow/underflow	Warning
16	Using inline assembly	Passed
17	Missing event emission	Passed
18	Missing zero address validation	Passed
19	Use of tx.origin	Passed
20	Oracle security	Passed

Prepared by

BLOCKCHAIN GURDIAN www.blockchaingurdian.com

Contract Audit Checklist

S.NO	Vulnerability Description	Status
21	Outdated compiler version	Passed
22	Block values as a proxy for time	Passed
23	Presence of unused code	Passed
24	Data Consistency	Passed
25	Money giving bug	Passed
26	Unnecessary use of SafeMath	Passed
27	Self-destruct interaction	Passed
28	Signature unique id	Passed
29	Weak sources of randomness	Warning
30	Optimize code and efficient gas fee	Passed

Prepared by

BLOCKCHAIN GURDIAN www.blockchaingurdian.com