SHERLOCK

Security Review For Centrifuge

Collaborative Audit Prepared For: **Centrifuge**
Lead Security Expert(s): **0x52**
Date Audited: **January 29 - January 30, 2026**

Introduction

The following report focuses on the deployment check/verification of the contracts described herein.

Scope

Repository: centrifuge/protocol

Audited Commit: 6b9d36eabee48728486f377ea2766a5cd233c555

Final Commit: 6b9d36eabee48728486f377ea2766a5cd233c555

Files:

- src/adapters/AxelarAdapter.sol
- src/adapters/LayerZeroAdapter.sol
- src/admin/OpsGuardian.sol
- src/admin/ProtocolGuardian.sol
- src/admin/TokenRecoverer.sol
- src/core/hub/Accounting.sol
- src/core/hub/Holdings.sol
- src/core/hub/HubHandler.sol
- src/core/hub/HubRegistry.sol
- src/core/hub/Hub.sol
- src/core/hub/ShareClassManager.sol
- src/core/messaging/GasService.sol
- src/core/messaging/Gateway.sol
- src/core/messaging/MessageDispatcher.sol
- src/core/messaging/MessageProcessor.sol
- src/core/messaging/MultiAdapter.sol
- src/core/spoke/BalanceSheet.sol
- src/core/spoke/factories/PoolEscrowFactory.sol
- src/core/spoke/factories/TokenFactory.sol
- src/core/spoke/PoolEscrow.sol
- src/core/spoke/ShareToken.sol
- src/core/spoke/Spoke.sol

- src/core/spoke/VaultRegistry.sol
- src/core/utils/BatchedMulticall.sol
- src/core/utils/ContractUpdater.sol
- src/hooks/BaseTransferHook.sol
- src/hooks/FreelyTransferable.sol
- src/hooks/FreezeOnly.sol
- src/hooks/FullRestrictions.sol
- src/hooks/RedemptionRestrictions.sol
- src/managers/hub/NAVManager.sol
- src/managers/hub/SimplePriceManager.sol
- src/managers/spoke/decoders/BaseDecoder.sol
- src/managers/spoke/decoders/CircleDecoder.sol
- src/managers/spoke/decoders/VaultDecoder.sol
- src/managers/spoke/MerkleProofManager.sol
- src/managers/spoke/OnOfframpManager.sol
- src/managers/spoke/QueueManager.sol
- src/utils/RefundEscrowFactory.sol
- src/utils/RefundEscrow.sol
- src/utils/SubsidyManager.sol
- src/valuations/IdentityValuation.sol
- src/valuations/OracleValuation.sol
- src/vaults/AsyncRequestManager.sol
- src/vaults/AsyncVault.sol
- src/vaults/BaseVaults.sol
- src/vaults/BatchRequestManager.sol
- src/vaults/factories/AsyncVaultFactory.sol
- src/vaults/factories/SyncDepositVaultFactory.sol
- src/vaults/SyncDepositVault.sol
- src/vaults/SyncManager.sol
- src/vaults/VaultRouter.sol

Findings

Issues Found

High	Medium	Low/Info
0	0	0

Issues Not Fixed and Not Acknowledged

High	Medium	Low/Info
0	0	0

Deployment Verification

Project: Centrifuge Protocol v3.1

Date: 2026-01-30

Commit: `6b9d36eabee48728486f377ea2766a5cd233c555`

---

1. Executive Summary

Centrifuge engaged an independent verification of the v3.1 protocol deployment across 8 blockchain networks. The verification confirmed that deployed smart contracts match the audited source code at commit `6b9d36ea`.

Verification Type	Contracts	Status
Bytecode	46	Passed
Factory	7	Passed
Ownership	46	Passed
Constructor	35	Passed

---

2. Scope

All contracts have identical addresses across all networks, except where noted.

Core

Contract	Address
Hub	`0xA4A7Bb3831958463b3FE3E27A6a160F764341953`
Hub Registry	`0x19f46D8130e610C6C0f0116EA40Fb781dEFaDE93`
Accounting	`0x050206c38f06e4710C4a37D39F75Ddc5c16a7396`
Holdings	`0x3f0c8D8d2637881c3f6d8531F51a47c2094C918d`

Contract	Address
Share Class Manager	0xaFFC269c8fe18EE9C7DDb22301AC2c2507d69BEf
Hub Handler	0x0dEFb429B1663698da4bAe3278393F6844c3392C
Spoke	0xEC3582fcDc34078a4B7a8c75a5a3AE46f48525aB
Balance Sheet	0x12a110cE5f0FC871cC72Bc7ECaF35cf39DD0f43e
Token Factory	0xcE1616505F93215751FBb41Efac618b631997c38
Vault Registry	0xd9531AC47928c3386346f82d9A2478960bf2CA7B
Pool Escrow Factory	0x5187A505c485E22f0b8a5FBdF69eF1c29C478CE3
Gateway	0x19a524D03aA94ECEe41a80341537BCFCb47D3172
Multi Adapter	0x35C837F0A54B715a23D193E1476BFC9BC30073BE
Message Processor	0x97cc7e9Dafdd725Cc23B25eeBC93c4384B4Fe30A
Message Dispatcher	0xf837a22883e004f705E0D7e1deE08e295Df30B27
Gas Service	0xbEbef21D686a957decECCe6a58455fA0F16754Be
Contract Updater	0x3B150B19245D2C366bc8f18c775b725DFB298F71

Adapters

Contract	Address
LayerZero Adapter	0xD517BC7ba17271a8D87BE7355B2523bF5c750295
Chainlink Adapter	0x39CF679Eb0Ac9075CFb5f94930A367Ba1557D955
Axelar Adapter	0x34e904237341C3de02D4447C3fF0ca8880ca6484
Wormhole Adapter	0x4BE430401760075315E931dD34b892DFdfc706A7 (ETH, Base, Arb, AVAX, Plume, BSC)

Admin

Contract	Address
Root	0x7Ed48C31f2fdC40d37407cBaBf0870B2b688368f
	(ETH, Base, Arb, AVAX, Plume, BSC)
Root	0xdc9456e7e20f15029C8231Ec433a20F404b7235E (Optimism, HyperEVM)
Protocol Guardian	0xCEb7eD5d5B3bAD3088f6A1697738B60d829635c6
Ops Guardian	0x055589229506Ee89645EF08ebE9B9a863486d0dE
Token Recoverer	0x1E70530e9555711f8DF4838Ab940b97c039B4037

Hooks

Contract	Address
Freeze Only Hook	0xd5B243F05b2906F1f6C80c6096945faADa0731C1
Full Restrictions Hook	0x8E680873b4C77e6088b4Ba0aBD59d100c3D224a4
Freely Transferable Hook	0x2a9B9C14851Baf7AD19f26607C9171CA1E7a1A61
Redemption Restrictions Hook	0xE5423eD8602Fa0F263e17b6212d88Efe42317f06

Managers (Hub)

Contract	Address
Simple Price Manager	0x280C94eB440A8a75c2F8f6cA8c6FaFf907000823
NAV Manager	0x493b6C8ccC7BfD43c5a20C4F2C648701f74E9130

Managers (Spoke)

Contract	Address
On/Offramp Manager Factory	0x2539e60B0B50D7BD004A09e9D2b7E8c86EB0AaF6

Contract	Address
Merkle Proof Manager Factory	0xc5243bdEa2d86eA7541AC69084dF3EDdc137a18b
Queue Manager	0x971ACA9b4AB4895F400bA042Fd10A31c7918D220
Vault Decoder	0x8Ca5372A5613A6Df75fD5fbC43216e68c1bE6D38
Circle Decoder	0xd40871a6336fD19A25a7bd96c0C0dd66Ed60931D

Valuation

Contract	Address
Identity Valuation	0x05e22C20B21c1314a0c93d34855358B9B96133CF
Oracle Valuation	0xCBdb6EFFC9b954D05dF89c747eCaa8A143c26E6D

Vault

Contract	Address
Async Vault Factory	0x55cde53B7dbc24336E34FFE233AF8DF10f72F0Be
Sync Deposit Vault Factory	0xdb9C27762045Addd713182521C0580C68BDF700A
Vault Router	0xF684014771C01e50B8B526968B3a1e33acDA63f6
Async Request Manager	0xF48256AbDDf96EcDDc4B3DbD23E8C1921f9761Ae
Sync Manager	0xFf8Ed1862f6aC3a8e89B81C75507c225E36e273D
Batch Request Manager	0xc52Bd1Bdfa0135147D3F01a0B6D6cd0A831dFe77
Refund Escrow Factory	0xC4f9A1DCF2E05eb55AbB30BaA7070838D3Fd3D5B
Subsidy Manager	0xBFC7B60684880457030C08AceE2E675CbcB9d646

3. Bytecode Verification

Deployed contract bytecode was compared against locally compiled bytecode from commit `6b9d36eabee48728486f377ea2766a5cd233c555`.

Category	Status
Core	17/17 Passed
Adapters	3/4 Passed
The Wormhole adapter is not deployed on Optimism, HyperEVM and Monad.	
Admin	3/4 Passed
The v3.0.0 Root contract is used on Eth, Base, Arb, Avalanche, BNB and Plume.	
Hooks	4/4 Passed
Managers (Hub)	2/2 Passed
Managers (Spoke)	5/5 Passed
Valuation	2/2 Passed
Vault	8/8 Passed

---

4. Factory Implementation Verification

Factory contracts were verified to have correct dependency addresses configured.

Factory Contract	Verification Status
Token Factory	Passed
Pool Escrow Factory	Passed
On/Offramp Manager Factory	Passed
Merkle Proof Manager Factory	Passed
Async Vault Factory	Passed

Factory Contract	Verification Status
Sync Deposit Vault Factory	Passed
Refund Escrow Factory	Passed

---

5. Ownership Verification

All contracts use the `Auth` pattern with a `wards` mapping for access control. The Root contract (`0x7Ed48C31f2fdC40d37407cBaBf0870B2b688368f`) is the primary administrator.

Category	Status
Core	17/17 Passed
Adapters	4/4 Passed
Admin	4/4 Passed
Hooks	4/4 Passed
Managers (Hub)	2/2 Passed
Managers (Spoke)	5/5 Passed
Valuation	2/2 Passed
Vault	8/8 Passed

Deployer Access: The deployer address has been properly removed from all contracts. No contracts retain deployer ward permissions.

---

6. Deployment Script Compliance

Constructor parameters were verified by reading immutable values from deployed contracts.

Category	Status
Core	12/12 Passed

Category	Status
Adapters	4/4 Passed
Admin	3/3 Passed
Hooks	4/4 Passed
Managers (Hub)	2/2 Passed
Managers (Spoke)	3/3 Passed
Valuation	2/2 Passed
Vault	4/4 Passed

Disclaimers

Sherlock does not provide guarantees nor warranties relating to the security of the project.

Usage of all smart contract software is at the respective users' sole risk and is the users' responsibility.