

Audits & Security At zkSwap Finance, we place a paramount emphasis on the security of our code and the safety of user funds. We recognize the pivotal role these elements play in establishing trust and fostering a secure environment for our users. To achieve this objective, we have implemented a stringent approach encompassing multiple audits and robust security measures.

All contracts are VERIFIED on [zkSync Explorer](#) and [Era.zkSync.Network](#) All Audits: [zkSwap Finance Github](#) Certik Audit: [Report](#)

Audited by Certik

Our platform is undergone comprehensive audit conducted by [Certik](#), a renowned security auditing firm. The results of this meticulous evaluation gives us a code security category score of 95/100, positioned us in the top of audited projects, attesting to the high level of security we maintain.

[Certik](#)'s audit is widely acknowledged and esteemed in the blockchain and cryptocurrency industry. Their exhaustive review process involves a careful examination of our smart contracts, codebase, and overall system architecture. Through this rigorous assessment, we have showcased our unwavering commitment to upholding the highest standards of security and reliability for our users.

For more details: [Certik Audit Report](#) Certik Skynet: <https://skynet.certik.com/projects/zkswap-finance>

Audited by Cyberscope

zkSwap Finance underwent three comprehensive audits conducted by [Cyberscope.io](#), covering Token contracts, Farm Contracts, and DAO Staking Pool contracts. The audits yielded commendable results, with ZERO critical or medium findings, reflecting the robust security measures implemented by Zkswap Finance. This provides transparency and accessibility for stakeholders and shows our commitment to security, instilling confidence in users and the broader community about the safety and reliability of our decentralized finance (DeFi) platform.

For your information, Cyberscope is a prominent authority in blockchain security auditing, standing out as a leading service provider in the crypto industry. Renowned for its audits with launchpads such as PinkSale, Unicrypt, and DxSale. Cyberscope's commitment to thorough auditing reinforces its role as a key player in promoting the integrity and reliability of blockchain projects in general and zkSwap Finance in particular.

For more details: [Cyberscope Audit Report](#) Cyberscope security platform: <https://www.cyberscope.io/audits/zkswap-finance>

https://x.com/cyberscope_ann/status/1750435343289950341?s=20

Audited by Vital Block

[Vital Block](#) offers an extensive security evaluation for smart contracts and blockchain code, pinpointing vulnerabilities and suggesting effective solutions. The company also deliver a professional, thorough, swift, and easily comprehensible smart contract security audit. Vital Block's approach involves in-depth, penetrative analyses encompassing static, manual, automated, and intelligent methods to ensure comprehensive coverage.

Detailed Report: [Vital Block Github](#)

https://twitter.com/VB_Audit/status/1674643373574045696

Audited by MythX

MythX™ is a premier automatic security analysis service for Ethereum smart contracts by ConsenSys Software Inc™. Its mission is to ensure development teams avoid costly errors and make smart contracts more secure and trustworthy.

MythX™ passed badge:

- mainnet-contracts: <https://github.com/ZkSwapFinance/mainnet-contracts>
- zf-periphery: <https://github.com/ZkSwapFinance/zf-periphery>
-

Smart Contract Address Audit Report Router [0x18381c0f738146Fb694DE18D1106BdE2BE040Fa4 Report](#) ZF Token [0x31C2c031fDc9d33e974f327Ab0d9883Eae06cA4A Report](#) ZF Farm [0x9F9D043fB77A194b4216784Eb5985c471b979D67 Report](#) yZF [0x4Ca2aC3513739ceBF053B66a1d59C88d925f1987 Report](#) Governance Staking [0x4Ca2aC3513739ceBF053B66a1d59C88d925f1987 Report](#) Paymaster [0xABcA8CFDfa2a4285A4704BF960fb45E49821762F Report](#) Swap2Earn Rewarder [0xF4dAc6647f4c56DE2a8BE120e5a830B5bD5Aae91 Report](#) TGE Launchpad [0x723b715987b7E1B6C7872809b5B694dA153eAdD6 Report](#) Galxe Campaign Pool [0x3Cd6A09A60867643C80A2e6e22ab4D83368e0F89 Report](#)

Timelock Controllers & Multisig Wallets Security Mechanism

Utilized for safeguarding the platform's smart contracts, [Timelock Controllers](#) and [Multisig Wallets](#) serve to introduce delays in actions by the contract owner, showcasing commitment and mitigating risks within the realm of DeFi.

- [Timelock 24 hours](#)
- : Delay Transaction 24 hours. Utilized for the ZF Farm, Treasury, Team Fund, Operation & Marketing Fund, to manage any possible changes.
- [Timelock 48 hours](#)
- : Delay Transaction 48 hours. Utilized for the Factory, ZF Token, yZF DAO staking pool, ZF Contribution Reward Pool, TGE Participants Rewards Pool to manage any possible changes.
- [Timelock 7 days](#)
- : Delay Transaction 7 days. Utilized for the ZF/ETH Initial Liquidity contract to manage any possible changes.
- [Multisig Wallets](#)
- are used to control the above timelock controllers and mitigate the risk of any private key leakage.
-

[Previous Multisig Wallets Next Get Started](#) Last updated 1 month ago On this page * [Audited by Certik](#) * [Audited by Cyberscope](#) * [Audited by Vital Block](#) * [Audited by MythX](#) * [Timelock Controllers & Multisig Wallets Security Mechanism](#)