SAYFER

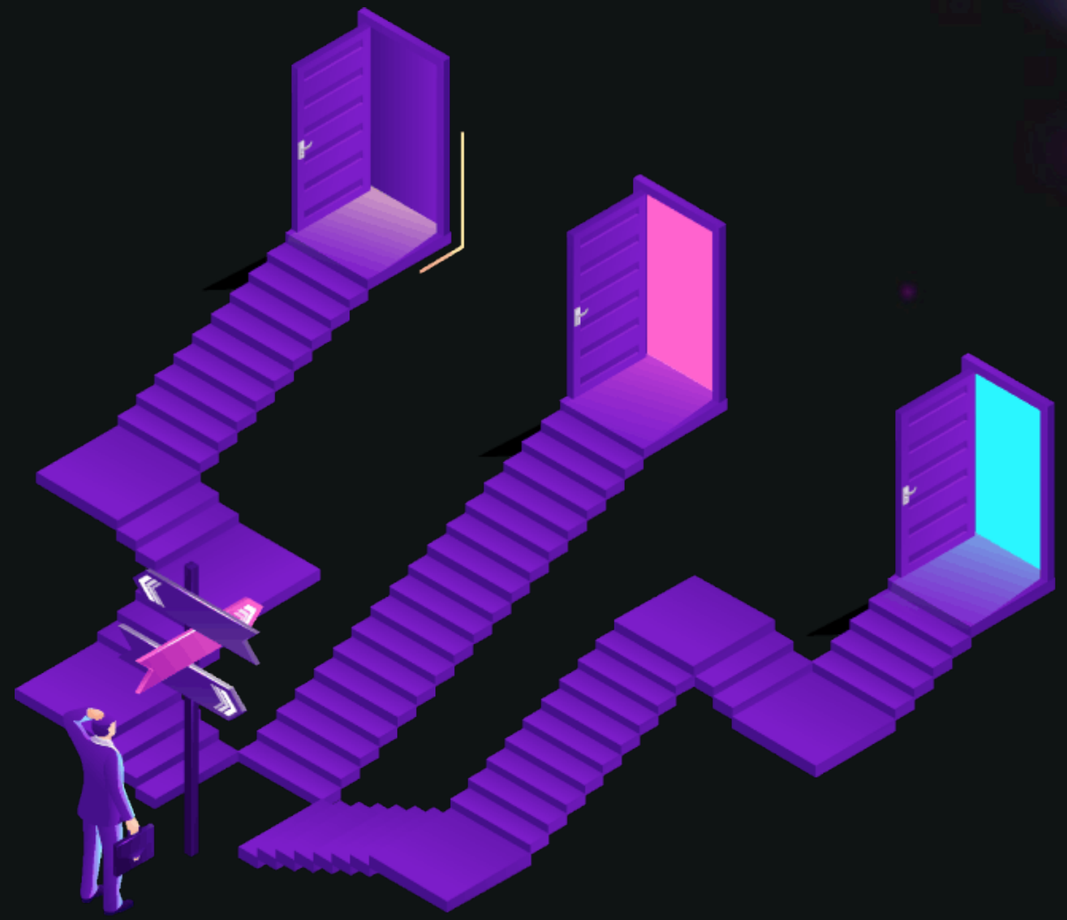
Tier-One Smart Contract Audit Firm

Sharing the Risk With You

sayfer.io

The Key to Success for Your Web3 Project - A Quality Smart Contract Audit

- Don't risk losing your hard-earned funds to **undetected vulnerabilities** in your smart contract.
- Smart contract audit it's a crucial investment in the **success of your web3 project**.
- With **Sayfer's** in-depth smart contract audit, you can have **peace of mind** knowing your project is secure and compliant with industry standards.



Get the Inside Scoop From Our Satisfied Customers

> Sayfer's team exceeded my expectations when they conducted a smart contract audit for our protocol. They went above and beyond to **uncover complex vulnerabilities** and provided valuable insights for ensuring the **security and integrity** of our contracts. I highly recommend Sayfer for any smart contract audit needs.

Hadar, CTO

Etoro (GoodDollar)

> The Sayfer team helped us with a structured project, a serious, smart contract audit and an **extremely clear report** with actionable findings. I **recommend them for web3 projects** which need any kind of security audit. Thank you, everyone.

Yoann, CTO

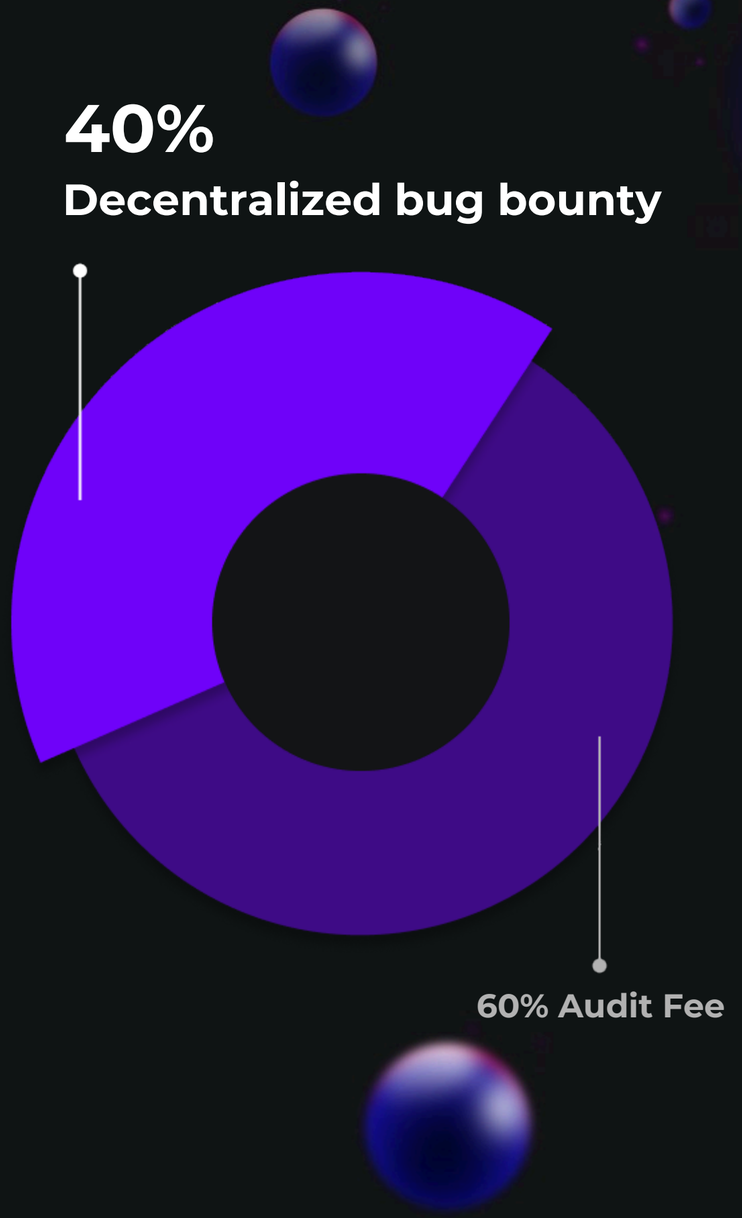
Request.Finance

Peace of Mind With Sayfer's Skin in the Game

At Sayfer, we understand that **trust is a key factor** in ensuring the security of blockchain projects.
To demonstrate our commitment to our clients' security, we have implemented a unique and first-of-its-kind approach to auditing.

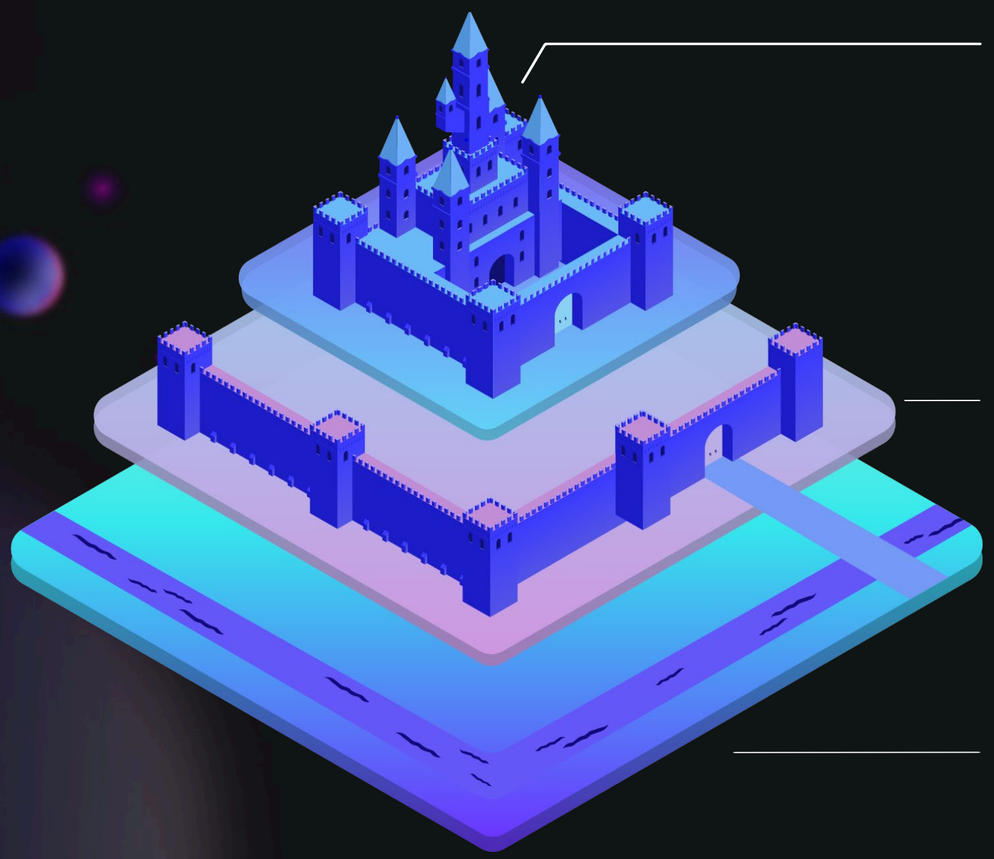
We stake 40% of the audit price as decentralized bug bounty collateral for any vulnerabilities we may have missed during our audit for 4 months.

This ensures that security vulnerabilities missed on our par **will be financially covered by us**, providing our clients with added peace of mind and assurance that their projects are **being protected to the highest standard in the industry.**



Trustworthy Web3 Security From Sayfer:

We Put Our Own Money on the Line



First Defense

Smart contract audits

Smart contract audit is a necessary process for securing, optimizing and ensuring compliance of your web3 project, making it a vital investment for its success.

Second Defense

A decentralized bug bounty

Program offers ongoing protection from top white hat hackers and includes a unique warranty staking of 40% of the audit price as collateral for any missed vulnerabilities.

Third Defense

AI hack protection

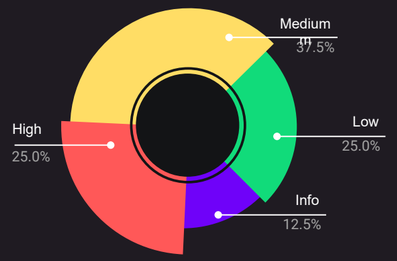
Is an additional layer to ensuring the security of smart contracts. This involves ongoing monitoring and protection against malicious transactions to ensure your protocol safety.

Setting the Standard for Smart Contract Audits

Management Summary

GoodDollar contacted Sayfer to perform a security audit on their smart contracts.
This report documents the research carried out by Sayfer targeting the selected resources defined under the research scope. Particularly, this report displays the security posture review for GoodDollar smart contracts.
Over the audit period of 4 weeks, we discovered 8 vulnerabilities in the contract. There are no critical vulnerabilities yet a couple of medium and high risks that can affect the protocol's financial funds.

Vulnerabilities by Severity



High – Direct threat to key business processes.

Medium– Indirect threat to key business processes or partial threat to business processes.

Low– No direct threat exists. The vulnerability may be exploited using other vulnerabilities.

Informational– This finding does not indicate vulnerability, but states a comment thatnotifies about design flaws and improper implementation that might cause a problem in thelong run.

Severity	High	Medium	Low	Informational
# of issues	2	3	2	1

Audit Findings

Unsafe Signature Verification Mechanism

Status	Fixed
Risk	Medium
Location	identity/IdentityV2.sol - function connectAccount
Tools	Manual testing

Description

Signature verification is the process of ensuring that a signed message was actually created by the claimed signer. This is done using cryptographic algorithms that generate a unique digital signature for each message, which can then be verified against the signer's public key.

The function uses untyped data signing and not using EIP712 which let the users see the data they are signing rather than the hex representation of it, which is a security concern because it can potentially be used in phishing campaigns.

Additionally, there is no replay protection, allowing an attacker to use a previously used signature to reconnect a disconnected account. This lack of replay protection increases the risk of unauthorized access and potential exploitation.

Mitigation

Implement the signature verification using EIP712 and add a mechanism to protect against replay attacks.

With You After the Audits

At Sayfer, we understand that protecting your protocols doesn't end with the completion of the audit. That's why we will provide **ongoing alerting of abnormal transactions** in your contracts using cutting-edge tech that detects on DeFi attacks in real time.

We also **provide consulting and code auditing after the final report**, as well as a free re-test of your fixes to ensure that the latest version of your deployed contract is completely covered.

Sayfer Plans

Book a free meeting

2 Weeks

Standard Audit

5,000 - 18,000 USD

Aim to Identifying All vulnerabilities, Smart Contract Security Verification Standard (SCSVS)

- ✓ Line-by-Line Auditing
- ✓ Retest Fixes
- ✓ Gas Optimizations
- ✓ PR + Website Badge
- ✓ 2 Auditors
- ✓ Additional Auditing After the Report - 100 100 Code Lines
- ✗ Warranty
- ✗ Bug Bounty
- ✗ AI Hack Protection
- ✗ In Depth Risk Assessment
- ✗ Contract Fuzzing
- ✗ Penetration Test
- ✗ Advance Phishing Simulation

3-4 Weeks

Premium Staked Audit

20,000 - 40,000 USD

Aim to Identifying All vulnerabilities, Smart Contract Contract Security Verification Standard (SCSVS)

- ✓ Line-by-Line Auditing
- ✓ Retest Fixes
- ✓ Gas Optimizations
- ✓ PR + Website Badge
- ✓ 3 Auditors
- ✓ Additional Auditing After the Report - 250 250 Code Lines
- ✓ Warranty - 40%, 4 Months
- ✓ Bug Bounty
- ✓ AI Hack Protection - 4 Months
- ✓ In Depth Risk Assessment
- ✗ Contract Fuzzing
- ✗ Penetration Test
- ✗ Advance Phishing Simulation

Every Month

Elite Warranty Audit

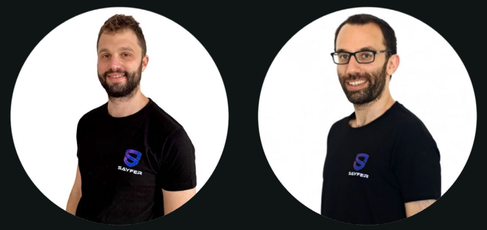
Talk to Us

Aim to Identifying All vulnerabilities, Smart Contract Contract Security Verification Standard (SCSVS)

- ✓ Line-by-Line Auditing
- ✓ Retest Fixes
- ✓ Gas Optimizations
- ✓ PR + Website Badge
- ✓ 3 Auditors
- ✓ Additional Auditing After the Report - 500 500 Lines a month
- ✓ Warranty - 40%, 4 Months
- ✓ Bug Bounty
- ✓ AI Hack Protection - Always
- ✓ In Depth Risk Assessment
- ✓ Contract Fuzzing
- ✓ Penetration Test
- ✓ Advance Phishing Simulation

Conducted by a Team of Industry-Leading Experts and Researchers

Highly skilled developers with years of military and hands-on research experience for building and scaling products



Deep understanding of the security risks that plague the web3 industry

Extensive experience finding vulnerabilities in national-level banks, telecommunications companies, DeFi, NFTs and more

Track record of providing groundbreaking and innovative solutions to supplement traditional security tools

Your Trusted Advisor in Web3 Security

At Sayfer, we understand the overwhelming feeling of **responsibility** that comes with launching a Web3 project.

That's why we're here to be your **trusted advisor and guide** you through the complex world of cyber security.

Our customized Web3 Cybersecurity strategy will **identify any weaknesses** in your framework and provide **tailored protocols** to ensure the protection of your project.

Secure Your Web3 Project

Rest easy knowing that your Web3 assets are protected by our unique tri-layered defense methodology:

Penetration Test

Sayfer researchers specialize in simulating real-life attacks and finding clients' specific vulnerabilities. When performing the penetration test, we use OWASP certified guidelines. Our reports are qualified for SOC2, ISO, and acceptable by major tech giants such as Google, Walmart, Samsung, and many more.

Cyber Product Consulting

Building a secure system isn't a one-time show, this is why Sayfer provides trusted advisors with over 10 years of experience in our client tech stack to attend architecture meetings and perform ongoing security advisory in the product's life cycle development to make sure everything is protected.

Discord Protection

Discord is a crucial platform for building web3 communities, however, millions of dollars are lost annually to phishing and fraud. Protect your discord server by ensuring it is audited and secure! By working with a leading provider of Discord security, you can rest assured that your server is protected from vulnerabilities.

Getting Started With Sayfer Is Quick & Hassle-Free!

We have devised a simple **6-step process** that delivers the expected results without compromising your project's operational integrity.

01 **Introductory** Meeting
To Identify Risk Points

02 Receive A Detailed **Price Quote & Expected Timelines**

03 We Conduct The Audit & Share Your Project's **Vulnerabilities & Proposed Fixes**

04 **We Help You Fix** the Weaknesses & Implement Security Protocols

05 **Double-Checking** the Fixes Plus 5 Hours Of Complimentary Consulting

06 Become **Sayfer Certified** & Show The Community Their Funds Are Safe!

Let’s Talk!

We invite you to book an obligation-free session with Nir our CEO

Book a free meeting

+972-559139416

info@sayfer.io

WhatsApp

Telegram

Twitter