



SOLIDProof

Bring trust into your projects

**Blockchain Security | Smart Contract Audits | KYC
Development | Marketing**

MADE IN GERMANY

Sakai Vault

AUDIT

SECURITY ASSESSMENT

03. September, 2023

FOR



[SolidProof.io](https://solidproof.io)



[@solidproof_io](https://t.me/solidproof_io)



Introduction	3
Disclaimer	3
Project Overview	4
Summary	4
Social Medias	4
Audit Summary	5
File Overview	6
Imported packages	6
Components	7
Exposed Functions	7
Capabilities	8
Inheritance Graph	9
Audit Information	10
Vulnerability & Risk Level	10
Auditing Strategy and Techniques Applied	11
Methodology	11
Overall Security	12
Upgradeability	12
Ownership	13
Ownership Privileges	14
Minting tokens	14
Burning tokens	15
Blacklist addresses	16
Fees and Tax	17
Lock User Funds	18
Centralization Privileges	19
Audit Results	20

Introduction

[SolidProof.io](#) is a brand of the officially registered company MAKE Network GmbH, based in Germany. We're mainly focused on Blockchain Security such as Smart Contract Audits and KYC verification for project teams.

Solidproof.io assess potential security issues in the smart contracts implementations, review for potential inconsistencies between the code base and the whitepaper/documentation, and provide suggestions for improvement.

Disclaimer

[SolidProof.io](#) reports are not, nor should be considered, an “endorsement” or “disapproval” of any particular project or team. These reports are not, nor should be considered, an indication of the economics or value of any “product” or “asset” created by any team. SolidProof.io do not cover testing or auditing the integration with external contract or services (such as Unicrypt, Uniswap, PancakeSwap etc'...)

SolidProof.io Audits do not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technology proprietors. SolidProof Audits should not be used in any way to make decisions around investment or involvement with any particular project. These reports in no way provide investment advice, nor should be leveraged as investment advice of any sort.

SolidProof.io Reports represent an extensive auditing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology. Blockchain technology and cryptographic assets present a high level of ongoing risk. SolidProof's position is that each company and individual are responsible for their own due diligence and continuous security. SolidProof in no way claims any guarantee of the security or functionality of the technology we agree to analyze.

Project Overview

Summary

Project Name	Sakai Vault
Website	https://sakaivault.io/
About the project	Sakai Vault is a decentralized spot and perpetual exchange that supports low swap fees and zero price impact trades. Trading is supported by a unique multi-asset pool that earns liquidity providers fees from market making, swap fees and leverage trading.
Chain	Binance Smart Chain(bsc)
Language	Solidity
Codebase	TheVaultTicker: https://bscscan.com/token/0x65d4cb29e0edaefb18246b22513483c21a8033f4#code SakaiVaultProtocol: https://bscscan.com/address/0xebb30b32e74ad446b00b6333c372c5a1ccabda7d#code
Commit	N/A
Unit Tests	Not Provided

Social Medias

Telegram	https://t.me/SakaiVault
Twitter	https://twitter.com/SakaiVault
Facebook	N/A
Instagram	N/A
GitHub	https://github.com/SakaiVault
Reddit	N/A
Medium	https://medium.com/@SakaiVault
Discord	https://discord.com/invite/HHq9uEXvr9
YouTube	N/A
TikTok	N/A
LinkedIn	N/A



Audit Summary

Version	Delivery Date	Change Log
v1.0	03. September 2023	<ul style="list-style-type: none"> · Layout Project · Automated/ Manual-Security Testing · Summary

Note - The following audit report presents a comprehensive security analysis of the smart contract utilized in the project. This analysis did not include functional testing (or unit testing) of the contract's logic. We cannot guarantee 100% logical correctness of the contract as it was not functionally tested by us.





File Overview

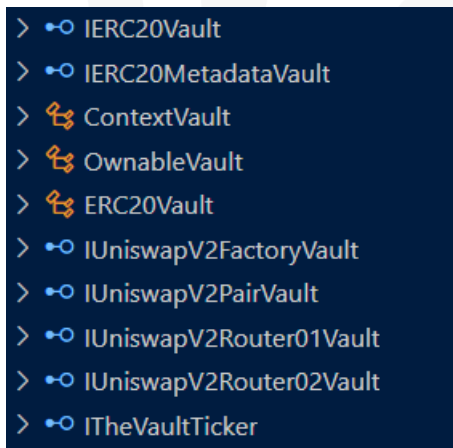
The Team provided us with the files that should be tested in the security assessment. This audit covered the following files listed below with an SHA-1 Hash.

File Name	SHA-1 Hash
contracts/SakaiVaultProtocol.sol	13ec2decc08bc8cb849b820bf58b95be652dadfa
contracts/TheVaultTicker.sol	6c3ef3d7918d5311fa57e284a8e405da62c691c9

Please note: Files with a different hash value than in this table have been modified after the security check, either intentionally or unintentionally. A different hash value may (but need not) be an indication of a changed state or potential vulnerability that was not the subject of this scan.

Imported packages.

Used code from other Frameworks/Smart Contracts.



Note for Investors: We only audited contracts mentioned in the scope above. All contracts related to the project apart from that are not a part of the audit, and we cannot comment on its security and are not responsible for it in any way.





External/Public functions

External/public functions are functions that can be called from outside of a contract, i.e., they can be accessed by other contracts or external accounts on the blockchain. These functions are specified using the function declaration's external or public visibility modifier.

State variables

State variables are variables that are stored on the blockchain as part of the contract's state. They are declared at the contract level and can be accessed and modified by any function within the contract. State variables can be needed within visibility modifier, such as public, private or internal, which determines the access level of the variable.

Components

 Contracts	 Libraries	 Interfaces	 Abstract
4	4	12	6


Exposed Functions

This section lists functions that are explicitly declared public or payable. Please note that getter methods for public stateVars are not included.












 Public	 Payable
155	5

External	Internal	Private	Pure	View
102	188	6	36	82

StateVariables

Total	 Public
51	30

Capabilities

Solidity Versions observed	 Experimental Features	 Can Receive Funds	 Uses Assembly	 Has Destroyable Contracts	
<code>^0.8.19</code>	<code>-----</code>	<code>yes</code>	<code>yes</code> <code>(9 asm blocks)</code>	<code>-----</code>	
 Transfers ETH	 Low-Level Calls	 Delegate Call	 Uses Hash Functions	 ECRecover	 New/Create/Create2
<code>Yes</code>		<code>Yes</code>	<code>Yes</code>		
 TryCatch	Σ Unchecked				
<code>yes</code>	<code>yes</code>				

Inheritance Graph

An inheritance graph is a graphical representation of the inheritance hierarchy among contracts. In object-oriented programming, inheritance is a mechanism that allows one class (or contract, in the case of Solidity) to inherit properties and methods from another class. It shows the relationships between different contracts and how they are related to each other through inheritance.



Audit Information

Vulnerability & Risk Level

Risk represents the probability that a certain source threat will exploit the vulnerability and the impact of that event on the organization or system. The risk level is computed based on CVSS version 3.0.

Level	Value	Vulnerability	Risk (Required Action)
Critical	9 - 10	A vulnerability that can disrupt the contract functioning in a number of scenarios, or creates a risk that the contract may be broken.	Immediate action to reduce risk level.
High	7 - 8.9	A vulnerability that affects the desired outcome when using a contract, or provides the opportunity to use a contract in an unintended way.	Implementation of corrective actions as soon as possible.
Medium	4 - 6.9	A vulnerability that could affect the desired outcome of executing the contract in a specific scenario.	Implementation of corrective actions in a certain period.
Low	2 - 3.9	A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective.	Implementation of certain corrective actions or accepting the risk.
Informational	0 - 1.9	A vulnerability that have informational character but is not effecting any of the code.	An observation that does not determine a level of risk



Auditing Strategy and Techniques Applied

Throughout the review process, care was taken to check the repository for security-related issues, code quality, and compliance with specifications and best practices. To this end, our team of experienced pen-testers and smart contract developers reviewed the code line by line and documented any issues discovered.

We check every file manually. We use automated tools only so that they help us achieve faster and better results.

Methodology

The auditing process follows a routine series of steps:

1. Code review that includes the following:
 - a. Reviewing the specifications, sources, and instructions provided to SolidProof to ensure we understand the size, scope, and functionality of the smart contract.
 - b. Manual review of the code, i.e., reading the source code line by line to identify potential vulnerabilities.
 - c. Comparison to the specification, i.e., verifying that the code does what is described in the specifications, sources, and instructions provided to SolidProof.
2. Testing and automated analysis that includes the following:
 - a. Test coverage analysis determines whether test cases cover code and how much code is executed when those test cases are executed.
 - b. Symbolic execution, which is analysing a program to determine what inputs cause each part of a program to execute.
3. Review best practices, i.e., review smart contracts to improve efficiency, effectiveness, clarity, maintainability, security, and control based on best practices, recommendations, and research from industry and academia.
4. Concrete, itemized and actionable recommendations to help you secure your smart contracts.



Overall Security Upgradeability

Contract is not an upgradable



Deployer cannot update the contract with new functionalities.

Description

The contract is not an upgradeable contract. The Deployer is not able to change or add any functionalities to the contract after deploying.

Comment

N/A



Ownership

The ownership is not renounced

✗ The ownership is not renounced

Description

The owner has not renounced the ownership that means that the owner retains control over the contract's operations, including the ability to execute functions that may impact the contract's users or stakeholders. This can lead to several potential issues, including:

- Centralizations
- The owner has significant control over contract's operations.

Example	N/A
Comment	N/A

Note – *The contract cannot be considered as renounced till it is not deployed or having some functionality that can change the state of the contract.*

Ownership Privileges

These functions can be dangerous. Please note that abuse can lead to financial loss. We have a guide where you can learn more about these Functions.

Minting tokens

Minting tokens refer to the process of creating new tokens in a cryptocurrency or blockchain network. This process is typically performed by the project's owner or designated authority, who has the ability to add new tokens to the network's total supply.

Contract owner can mint new tokens.

✗ The owner can mint new tokens.

Description

Owners who have the ability to mint new tokens can reward themselves or other stakeholders, who can then sell the newly minted tokens on a cryptocurrency exchange to raise funds. However, there is a risk that the owner may abuse this power, leading to a decrease in trust and credibility in the project or platform. If stakeholders perceive that the owner is using their power to mint new tokens unfairly or without transparency, it can result in decreased demand for the token and a reduction in its value.

Comment

The vault address can mint unlimited amount of tokens. It is recommended that there should not be an unlimited minting of tokens is possible, There must be a total supply added and the number of tokens should not be more than that minted in order to maintain the supply of the token.

File/Line(s): L1720-1736

Codebase: TheVaultTicker.sol

```
// Optional function to mint a new NFT
function mintNFT(address _to, uint256 _tokenId) public {
    require(msg.sender == vaultAddress, "Only the vault can mint");
    require(!_exists(_tokenId), "Token ID already exists");
    _mint(_to, _tokenId);
    uint256 id;
    assembly {
        id := chainid()
    }
    string memory uri = string(
        abi.encodePacked(
            Strings.toString(id),
            "/",
            Strings.toString(_tokenId)
        )
    );
    _setTokenURI(_tokenId, uri);
}
```



Burning tokens

Burning tokens is the process of permanently destroying a certain number of tokens, reducing the total supply of a cryptocurrency or token. This is usually done to increase the value of the remaining tokens, as the reduced supply can create scarcity and potentially drive up demand.

Contract owner cannot burn tokens



The owner cannot burn tokens

Description

The owner is not able burn tokens without any allowances.

Comment

N/A



Blacklist addresses

Blacklisting addresses in smart contracts is the process of adding a certain address to a blacklist, effectively preventing them from accessing or participating in certain functionalities or transactions within the contract. This can be useful in preventing fraudulent or malicious activities, such as hacking attempts or money laundering.

Contract owner cannot blacklist addresses

☒ The owner cannot blacklist addresses

Description

The owner is not able blacklist addresses to lock funds.

Comment

N/A



Fees and Tax

In some smart contracts, the owner or creator of the contract can set fees for certain actions or operations within the contract. These fees can be used to cover the cost of running the contract, such as paying for gas fees or compensating the contract's owner for their time and effort in developing and maintaining the contract.

Contract owner cannot set fees more than 25%.

 **The owner cannot set fees more than 25%.**

Description

The owner is not able to set any fees after initial deployment.

Comment

There is no functionality present to update any fees.

Lock User Funds

In a smart contract, locking refers to the process of restricting access to certain tokens or assets for a specified period of time. When token or assets are locked in a smart contract, they cannot be transferred or used until the lock-up period has expired or certain conditions have been met.

Contract owner can lock user funds.

✗ The owner can lock user funds.

Description

Locking the contract means that the owner is able to lock any funds of addresses that they are not able to transfer bought tokens anymore.

Comment

The owner can lock user funds by setting an arbitrary address for the nft. That causes the nft contract functions are not callable anymore. Also, It is recommended that the token address should not be changed after initial deployment to avoid these circumstances.

File,Line(s): L1714-1717

Codebase: TheVaultTicker.sol

```
function setVaultAddress(address _vaultAddress) external onlyOwner {
    require(_vaultAddress != address(0), "Invalid address");
    vaultAddress = _vaultAddress;
}
```

Centralization Privileges

Centralization can arise when one or more parties have privileged access or control over the contract's functionality, data, or decision-making. This can occur, for example, if the contract is controlled by a single entity or if certain participants have special permissions or abilities that others do not.

In the project, there are authorities that have access to the following functions:

File	Privileges
TheVaultTicker.sol	<ul style="list-style-type: none"> ➤ The owner can set the base URI. ➤ The owner can set the vault address in the contract. ➤ The owner can update the Token URI. ➤ By setting the vault address to an arbitrary address the owner can prevent the execution of mint and buyback functionality. Additionally, the owner can set the vaultAddress to an EOA address and mint new tokens to arbitrary addresses. ➤ The Vault address can mint unlimited number of tokens after the initial deployment of token. It is recommended that there must be a threshold or total supply so that the number of tokens will be fixed and cannot be more than that particular amount to avoid the manipulation of supply of the token.
SakaiVaultProtocol.sol	<ul style="list-style-type: none"> ➤ The owner can reset eligible if the current timestamp is greater than endingAt Time. ➤ The owner can stop eligible if the current timestamp is greater than endingAt Time. ➤ The owner can set any arbitrary value as price per ticket. ➤ The owner can toggle the isAutopickwinner to true and false which means he can enable and disable the auto picking winner functionality. ➤ The owner can set any arbitrary value as default eligible days. ➤ The owner can update the committed token address. ➤ The owner can update the staking address. ➤ The owner can update the charity address. ➤ The owner can update the router address.



- The owner can update the Busd address.
- The owner can update the NFT address.
- The owner can update the winner percentage and staking percentage.
- The owner can set the tax for the sum of staking and charity of not more than 25%.
- The owner can pick the winner manually.

Recommendations

To avoid potential hacking risks, it is advisable for the client to manage the private key of the privileged account with care. Additionally, we recommend enhancing the security practices of centralized privileges or roles in the protocol through a decentralized mechanism or smart-contract-based accounts, such as multi-signature wallets.

Here are some suggestions of what the client can do:

- Consider using multi-signature wallets: Multi-signature wallets require multiple parties to sign off on a transaction before it can be executed, providing an extra layer of security e.g. Gnosis Safe
- Use of a timelock at least with a latency of e.g. 48-72 hours for awareness of privileged operations
- Introduce a DAO/Governance/Voting module to increase transparency and user involvement
- Consider Renouncing the ownership so that the owner cannot modify any state variables of the contract anymore. Make sure to set up everything before renouncing.

Audit Result

#1 | Weak PRNG(weak-prng)

File	Severity	Location	Status
SakaiVaultProtocol.sol	Medium	L937-942	ACK

Description – Instead of implementing a random function in the contract which is predictable, use an external service like chainlink for randomness.

#2 | EligibleAmounts will be overridden.

File	Severity	Location	Status
SakaiVaultProtocol.sol	Medium	L885-890	ACK

Description – Instead of setting the amounts to the eligibleAmounts, add it to it because it is possible that the eligibleAmounts at index "x" didn't claim the winner amounts. If the same user is randomly chosen again, the eligibleAmounts will be overridden instead of added.

#3 | Floating pragma solidity version.

File	Severity	Location	Status
SakaiVaultProtocol.sol	Low	L6	Open
The vaultTicker.sol	Low	L6	Open

Description – Adding the constant version of solidity is recommended, as this prevents the unintentional deployment of a contract with an outdated compiler that contains unresolved bugs.

#4 | Missing events.

File	Severity	Location	Status
ThevaultTicker.sol	Low	L1714-1717	Open

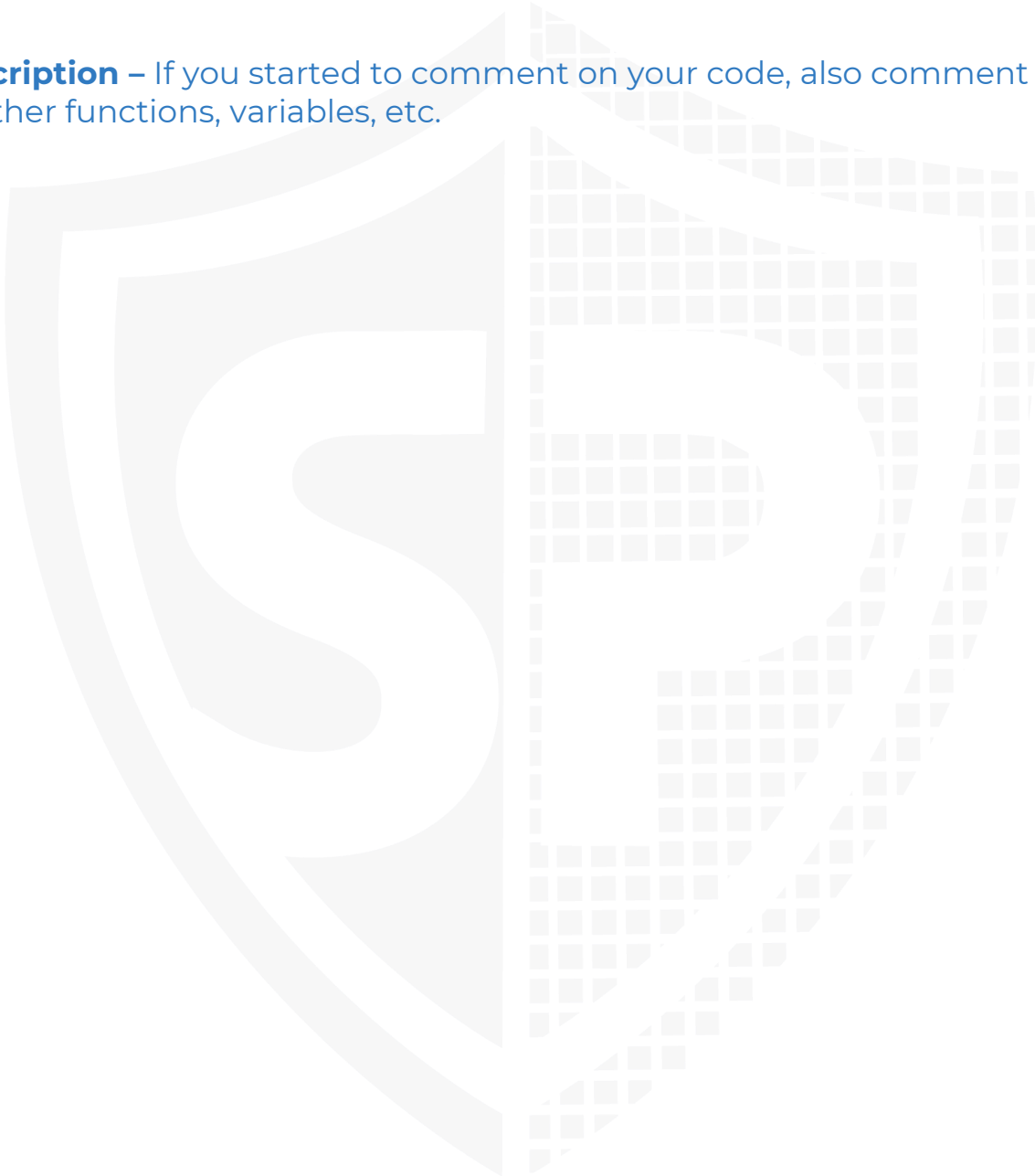
Description – Emit all the critical parameter changes.



#5 | NatSpec Documentation missing.

File	Severity	Location	Status
TheVaultTicker.sol	Informational	--	Open
SakaiVaultProtocol.sol	Informational	--	Open

Description – If you started to comment on your code, also comment on all other functions, variables, etc.





Legend for the Issue Status

Attribute or Symbol	Meaning
Open	The issue is not fixed by the project team.
Fixed	The issue is fixed by the project team.
Acknowledged(ACK)	The issue has been acknowledged or declared as part of business logic.





**Blockchain Security | Smart Contract Audits | KYC
Development | Marketing**

MADE IN GERMANY