DeFi Yield.info

VIKING SWAP

SMART CONTRACT SECURITY ANALYSIS

FEBRUARY 25th, 2021

Project Summary

Project Name	Viking Swap
Scope	A next generation decentralized exchange that is based on a deflationary governance token model.
Platform	Binance, Solidity

Executive Summary

- Three smart contracts were analyzed to check the availability of code vulnerabilities associated with the process of funds staking: **VIKING**, **MasterChef** and **Timelock**.
- No significant security issues were revealed in the aforementioned contracts.

Smart Contract Ownership	Team Reward	Total Supply	Minting Function	Migration Function	Funds Lock Period	Contract Pause	Suspicious Functions
EOA over Timelock	10% of user **VIKING** rewards	Variable	Available	Not available	None	Not available	Not found

External Smart Contract Audits:

- No external audits were found.

Manual Check Results

Ownership structure:

Smart contract	Owner	Description

VIKING	MasterChef	• The owner, the MasterChef smart contract, can call:
		  • the **mint** function
		  • **renounceOwnership** / **transferOwnership**
		• 22% of the token total supply is held by MasterChef
		• 5% of the token total supply is held by VikingTopHolder

MasterChef	Timelock	• The owner can call the following functions:
		  • add adds new LP tokens to the pools
		  • set changes deposit fee and allocation points for the pools
		  • updateEmissionRate sets minting rate of VIKING per block
		• The contract:
		  • mints team rewards and sends them to the DEV address
		  • transfers up to 100% of the deposit fee to FEE_ADDR. The current deposit fee across all pools is up to 4%

Timelock	Viking Swap: Deployer	• The minimum delay is 6h • The maximum delay is 30d • The current delay is set to 24h • The admin is the Viking Swap: Deployer

Total supply:
- Variable

Team reward:
- 10% of user VIKING rewards are additionally minted to the DEV address

Minting function:
- Available only for reward generation

Migration function:
- Not available, unlike in other PancakeSwap clones

Funds lock period:
- None

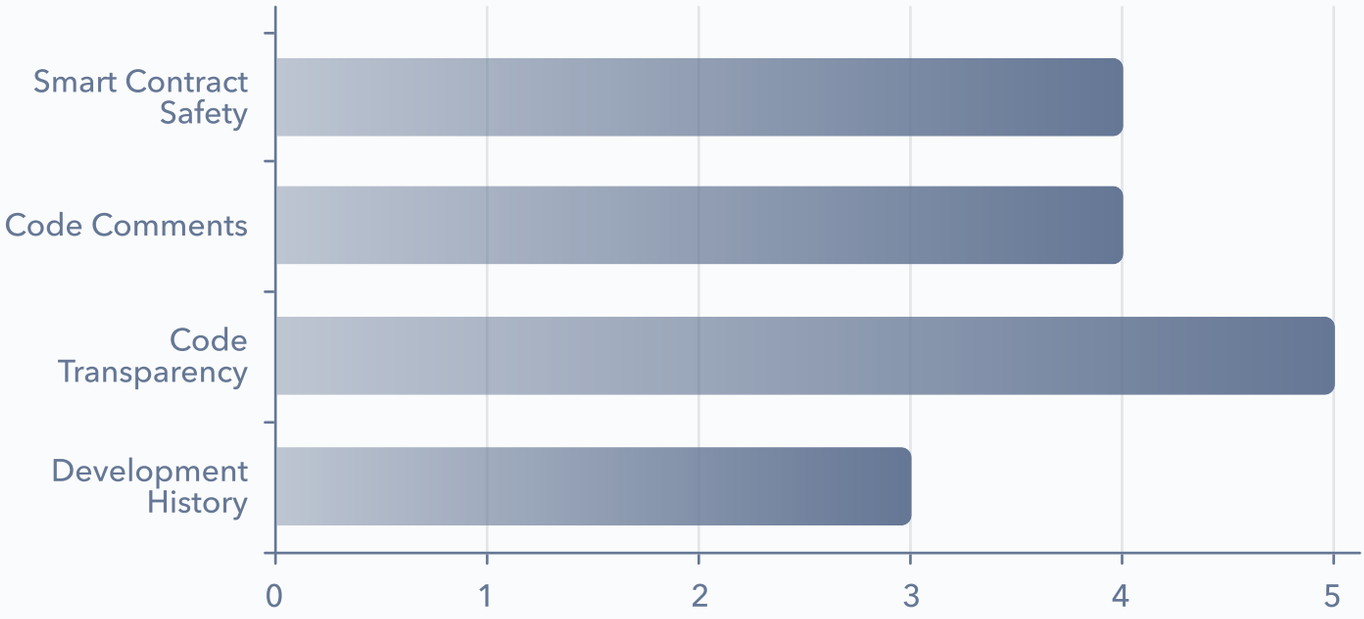
Possibility to pause the Smart Contracts:
- Not available

Suspicious functions:
- Not found

Tornado cash connections:
- Not found

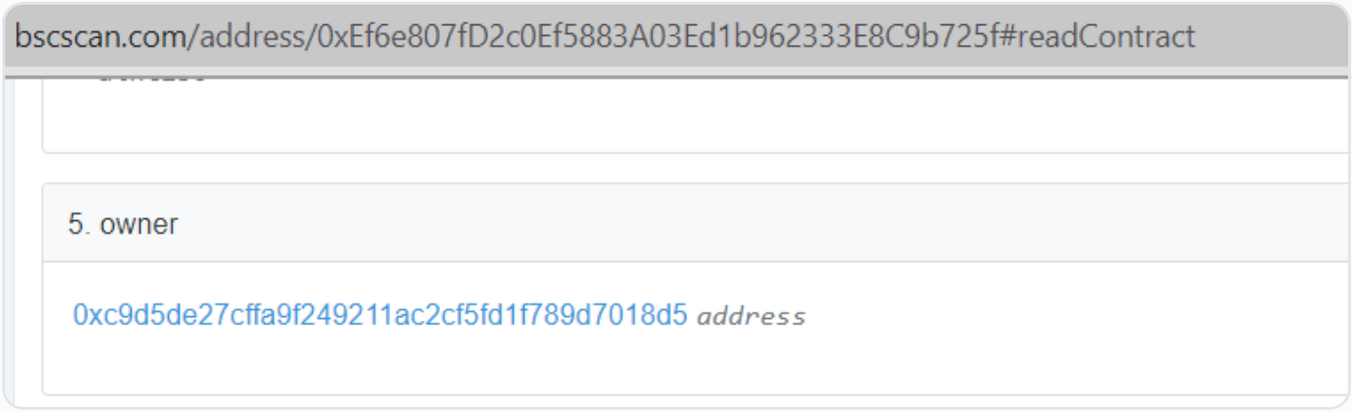
⚠ Risk Level LOW

Smart Contracts

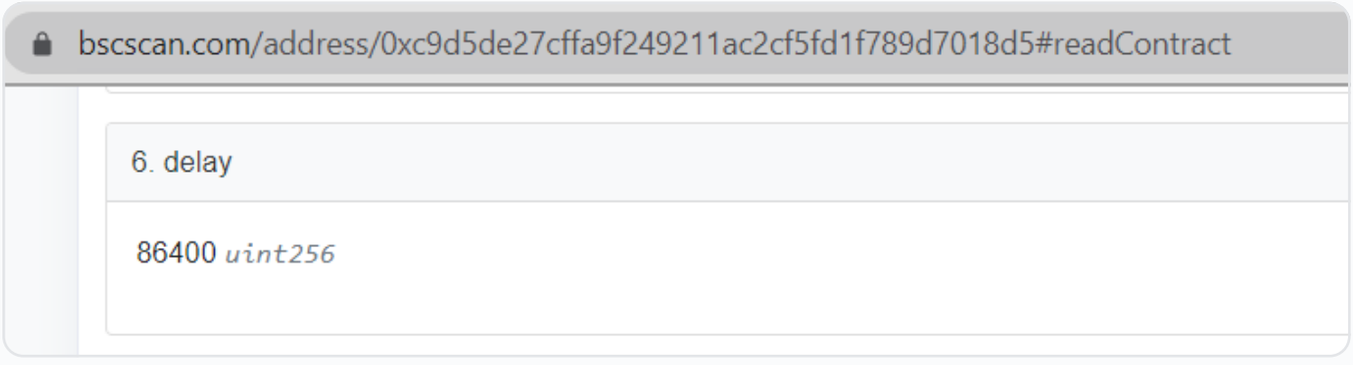


Conclusion

Viking Swap is a decentralized exchange built as a clone of PancakeSwap.
One of the main distinguishing features of the project is a deflationary mechanics of its token VIKING.
Total supply of the token is variable and is controlled by the **MasterChef** contract, which in its turn is owned by the **Timelock** contract:



22% of the token total supply is held by **MasterChef** and 5% of the token total supply is held by **VikingTopHolder**.
Through Timelock, **MasterChef** adds new LP tokens to the pools, manages deposit fee, allocation points for the pools and team rewards. Any smart contract changes related to these processes and terms proceed with a 24-hour delay:



The maximum and minimum delays are 6 and 30 days, respectively:

bscscan.com/address/0xc9d5de27cffa9f249211ac2cf5fd1f789d7018d5#code

Contract Source Code (Solidity Standard Json-Input format)

File 1 of 2 : Timelock.sol

```
21
22      event NewAdmin(address indexed newAdmin);
23      event NewPendingAdmin(address indexed newPendingAdmin);
24      event NewDelay(uint indexed newDelay);
25      event CancelTransaction(bytes32 indexed txHash, address indexed t
26      event ExecuteTransaction(bytes32 indexed txHash, address indexed
27      event QueueTransaction(bytes32 indexed txHash, address indexed ta
28
29      uint public constant GRACE_PERIOD = 14 days;
30      uint public constant MINIMUM_DELAY = 6 hours;
31      uint public constant MAXIMUM_DELAY = 30 days;
32
33      address public admin;
34      address public pendingAdmin;
35      uint public delay;
```

The minting is available only for reward generation.

bscscan.com/address/0xEf6e807fD2c0Ef5883A03Ed1b962333E8C9b725f#code

File 1 of 9 : MasterChef.sol

```
147     // Update reward variables of the given pool to be up-to-date.
148     function updatePool(uint256 _pid) public {
149         PoolInfo storage pool = poolInfo[_pid];
150         if (block.number <= pool.lastRewardBlock) {
151             return;
152         }
153         uint256 lpSupply = pool.lpToken.balanceOf(address(this));
154         if (lpSupply == 0 || pool.allocPoint == 0) {
155             pool.lastRewardBlock = block.number;
156             return;
157         }
158         uint256 multiplier = getMultiplier(pool.lastRewardBlock, block.number);
159         uint256 vikingReward = multiplier.mul(vikingPerBlock).mul(pool.allocPoint).div(totalAllocPoint);
160         viking.mint(devaddr, vikingReward.div(10));
161         viking.mint(address(this), vikingReward);
162         pool.accEggPerShare = pool.accEggPerShare.add(vikingReward.mul(1e12).div(lpSupply));
163         pool.lastRewardBlock = block.number;
164     }
165
```

This screenshot also shows the 10% hardcoded fee sent to the developer's address as team reward.
In contrast to other PancakeSwap clones, the smart contracts of Viking Swap don't have migration functionality.

The risk of a quick token dump initiated by the team is **2**/10.
No suspicious functions were detected.
No funds lock period is defined in the smart contracts analyzed, and there is no possibility to pause the contracts, meaning liquidity providers have constant access to their funds.
Considering the above mentioned facts, the risk level of the project can be estimated as low.

Audit recommendations

As developers point out in their **docs**:

- "4% burn fee will be charged at staking;
- 80% of the burn fee will be used to buyback VIKING and burn it;
- 10% will be sent to the developer's address;
- 10% will be held in escrow for Viking Swap, for future projects."

The actual **receiver** of the fees is an EOA, so fee utilization described above rather executes manually.
Defi Yield recommends either to describe this fact in the docs, or replace **the fee receiver address** with a brand new contract that would manage the fees in a decentralized way or, at least, publically.
In addition, the docs don't contain info about the hardcored dev rewards that amount to 10% of **VIKING** rewards.