



# Security Audit

## CAKEVAULT

Website: <https://cakevault.net/>

Contract:

<https://bscscan.com/address/0xb28C485a96eD9506df0047Fc26e82866a27432D9#code>

**Haze Security**  
05/21/2021



## **CRITICAL ISSUES (critical, high severity): 0**

Critical and harmful access for owners, user block ability, Bugs, and vulnerabilities that enable theft of funds, lock access to funds without possibility to restore it or lead to any other loss of funds to be transferred to any party.

## **ERRORS, BUGS AND WARNINGS (medium, low severity): 0**

Bugs can negatively affect the usability of a program, errors that can trigger a contract failure, Lack of necessary security precautions, other warnings for owners and users, warning codes that are valid code but the compiler thinks are suspicious.

## **OPTIMIZATION (low severity): 1**

Methods to decrease the cost of transactions in Smart-Contract.

## **RECOMMENDATIONS (very low severity): 0**

Hint and tips to improve contract functionality and trustworthiness.

## **Conclusion:**

In the **CAKEVAULT** Smart-Contract were found no vulnerabilities, no backdoors, and no scam scripts.

The code was tested with compatible compilers and simulate manually reviewed for all commonly known and specific vulnerabilities.

So **CAKEVAULT** Smart-Contract is safe for use in the Binance Smart Chain main network.

## Optimization suggestions

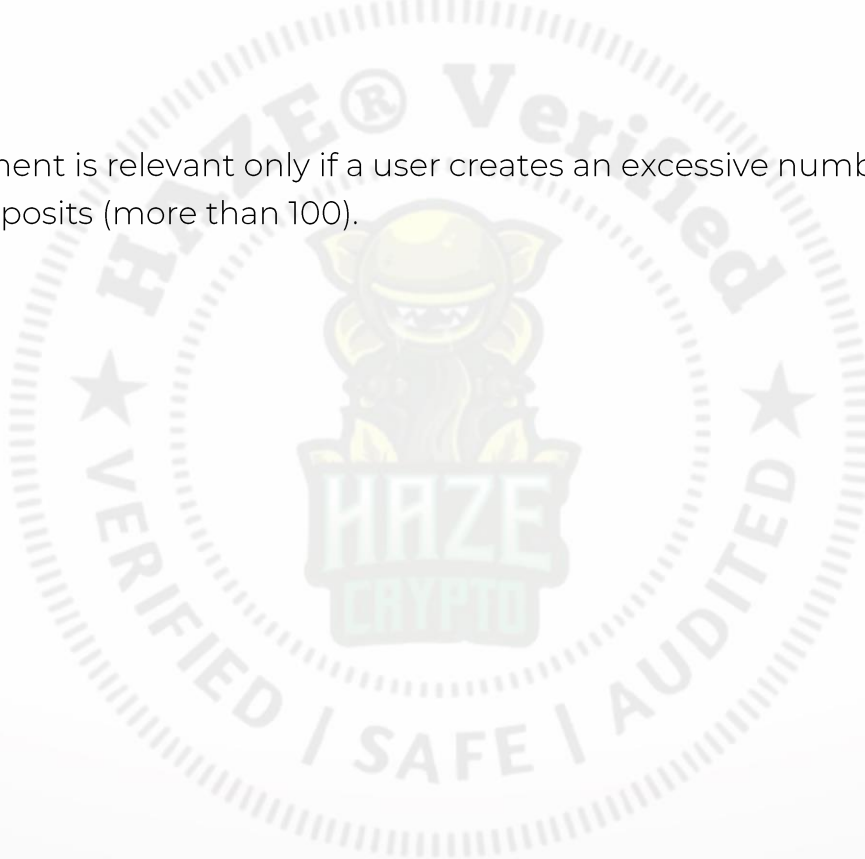
1- Loop on the dynamic variable (low severity).

If the user gets more parallel deposits his withdrawal transaction fee will cost more transaction fees because the loop on the dynamic variable is used in the 'withdraw' function.

In case of the GAS limit of exceeding the size of transaction withdraw is not possible.

Note:

This comment is relevant only if a user creates an excessive number of parallel deposits (more than 100).



## Independent description of the smart-contract functionality

The **CAKEVAULT** smart-contract provides the opportunity to invest any amount in CakeToken (from 0.25 Cake) in the contract and get 200% return on investment in 25 days if the contract balance has enough funds for payment.

- ❖ Dividends are paid from deposits of users.
- ❖ All dividends are calculated at the moment of request and available for withdrawal only once a day.
- ❖ Each subsequent Deposit is kept separately in the contract, in order to maintain the payment amount for each Deposit.

### Contract Owners Fee

On Invest: 12%

On Withdraw: 5%

On Reinvest: 10%

### INVESTMENT PLAN

Plans	Total Return	Daily Profit	Days	Withdraw time
1	200%	8%	25	Only Once a Day

- The Minimum deposit amount is 0.25 Cake
- The minimum withdrawable amount is 0.25 Cake
- Users can withdraw only once a day
- The contract has different bonus systems which daily profit can increase to the max 30% daily

### Referral System (Match Bonus)

The contract pays 8% referral commission over 3 levels

- Level one: 5%
- Level two: 2%
- Level three: 1%

#### Notes:

- Referral should be an active user; it means referral address has at least one deposit
- Referrer is specified once at the time of the first deposit and is assigned to the user without the possibility of changing. From each subsequent Deposit, the referrer will get his percent.

### Pool Bonus

The contract increases the daily profit by 0.1% for each 200 Cake in the balance of the contract

- ❖ The Maximum pool bonus is 8%.

### Hold Bonus

Users can get an extra 0.5% daily every 24h if you did not withdraw.

- The Maximum hold bonus is 6%.

### Community Bonus

New deposits get an extra 1% daily every day since the launch of the project.

- The Maximum community bonus is 8%.

### Withdraw and Reinvest

- ❖ Users can reinvest their dividends and the dividends of each deposit will be added to itself.
- ❖ Users can only withdraw or reinvest only once a day
- ❖ The minimum withdrawable amount is 0.25 Cake

### Contract features

- ❖ The contract is paused at the first initial and users can only invest in the contract
- ❖ The owner has access to unpause the contract and the start date of the contract will be set
- ❖ The owner can not pause the contract after unpauseing it

## Disclaimer:

This audit is only to the Smart-Contract code at the specified address.

### CAKEVAULT:

<https://bscscan.com/address/0xb28C485a96eD9506df0047Fc26e82866a27432D9#code>

Haze Security is a 3rd party auditing company who works on audits based on client requests. And as a professional auditing firm, we check on the contract for any vulnerabilities, backdoors, and/or scam scripts.

Therefore:

We are not financial advisors nor do we partner with the contract owners

Operations and website administration is fully on the client's side

We do not have influence over client operations, which can lead to website changes, withdrawal function closes, etc. One always has the option to do this through the contract.

Any concerns about the project themselves need to be raised directly to the project owners and not through Haze Security.

Investors are not in any way obliged, coerced or influenced to invest in projects audited by Haze Security.

We are not responsible for your funds or guarantee you profits.

We highly recommend that investors do their own research and gain crypto experience before investing

To report any scam, malpractices and irregularities, please send a message via Telegram to @Haze013 or @Sara\_Solidity for blacklisting.



# Haze Security

05/21/2021

If you are interested in developing/auditing of Smart-Contracts, please contact us.

Admin: [@Haze013](#)

Auditor: [@Sara\\_Solidity](#)

All official info available:

Website: <https://hazecrypto.net/cakevault>

Telegram Channel: [t.me/HazeCrypto](https://t.me/HazeCrypto)

Telegram Community: [t.me/HazecryptoCommunity](https://t.me/HazecryptoCommunity)

Twitter: [twitter.com/HazeCryptoTM](https://twitter.com/HazeCryptoTM)

Instagram: [instagram.com/HazeCryptoTM](https://www.instagram.com/HazeCryptoTM)

