



SECURITY AUDIT

BNB_FLASH

<https://bscscan.com/address/0xD7fFb47d6048DF0ddA79023a230C58B5e23c1592#code>



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 trustworthy.

Conclusion:

In the **BNB_FLASH** 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 **BNB_FLASH** Smart-Contract is safe for use in Binance Smart Chain main network.

BNB_FLASH
0xD7fFb47d6048DF0ddA7902
3a230C58B5e23c1592

Optimization suggestions

1- Loop on the dynamic variable (low severity)

If the user gets more parallel deposits his withdraw transaction going to cost more transaction fee, because the loop on the dynamic variable is used in the 'withdraw' function.

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

Note:

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

BNB_FLASH
0xD7fFb47d6048DF0ddA7902
3a230C58B5e23c1592



Independent description of the smart-contract functionality

The **BNB_FLASH** smart-contract provides the opportunity to invest any amount in BNB (from 0.05 BNB) in the contract and get 110% to 616% return on investment in 1 to 28 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 anytime
- Each subsequent Deposit is kept separately in the contract, in order to maintain the payment amount for each Deposit.

Contract Owners Fee

Project Fee: 10%

SIX INVESTMENT PLAN

Plans	Total Return	Daily Profit	Days	Withdraw Time
1	110%	110%	1	Any Time
2	120%	40%	3	Any Time
3	210%	30%	7	Any Time
4	364%	26%	14	Any Time
5	504%	24%	21	Any Time
6	616%	22%	28	Any Time

Minimum deposit amount is 0.05 BNB

BNB_FLASH

0xD7fFb47d6048DF0ddA7902

3a230C58B5e23c1592

Important: Plans return are float and daily profit for a new deposit will increase by 0.5% daily

```
function getPercent(uint8 plan) public view returns (uint256) {
    if (block.timestamp > startUNIX) {
        return plans[plan].percent.add(PERCENT_STEP.mul(block.timestamp.sub(startUNIX)).div(TIME_STEP));
    } else {
        return plans[plan].percent;
    }
}
```

Referral System (Match Bonus)

This contract paid referrals in three level totally 8%

- Level one: 5%
- Level two: 25%
- Level three: 05%

Notes:

- Referral should be an active user; it means referral address has at least one deposit

BNB_FLASH
0xD7fFb47d6048DF0ddA7902
3a230C58B5e23c1592



TRONLOCK Smart-Contract Functions

- Constructor: initial plans, owner address and start date
- invest: make a new deposit
- withdraw: transfer user profit to his wallet
- getPlaninfo: return plan info
- getPercent return calculated percent
- getResult return deposit calculated percent, profit and finish date
- getUserDividends: return user dividends
- getUserCheckpoint: return user checkpoint
- getUserReferrer: return user referrer
- getUserDownlineCount return referral amount in three level
- getUserReferralBonus: return referral bonus
- getUserReferralTotalBonus return total referrals
- getUserReferralWithdrawn: return total paid referrals
- getUserAvailable: return user available
- getUserAmountOfDeposits: return deposits amount
- getUserTotalDeposits: return total deposit
- getUserDepositinfo: return a deposit info
- isContract: check the address type

BNB_FLASH
0xD7fFb47d6048DF0ddA7902
3a230C58B5e23c1592



Disclaimer:

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

BNB_FLASH:

<https://bscscan.com/address/0xD7fFb47d6048DF0ddA79023a230C58B5e23c1592#code>

The audit makes no statements or warranties about the suitability or sustainability of the business model or regulatory regime for the business model. Do take in consideration that you are doing all financial actions & transactions at your own risk, especially if you are dealing with high-risk projects / Dapps.

DappKing Security

03/28/2021

All official info available:

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

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

Telegram: @dappking_official

Email: admin@dappking.net

