# ZenAudit

# Security Audit

**10/02/2022**

## BNBFish

**BINANCE**
SMART CHAIN

# Project Analysis

The BNBFish smart contract provides the opportunity to play a simple blockchain game investing a small BNB amount (0.025) , with the possibility to gain up to 4000% ROI as reward (calculated on the first prize). There is 20% of probability to win a prize. The total payout is 90% (10% reserved for referrals and maintenance)

- Nobody, even the authors of the game can know where the prizes are As any game there is no certainty of win.
- Do always invest with proper knowledge and investigation.
- Users deposits are used as jackpot pool. 5% is reserved for website maintenance and 5% is payed as referral reward. So, the total payout is 90%.
- Winners are made public only once all cells have been sold. At this point, players can check if they have won and can withdraw their prizes.
- The game is restarted manually, if winners haven't withdrawn their prizes, the amount is automatically sent to their wallet.

**Game Explanation**

- The board is composed by 100 cells (10x10 matrix)
- Every cell can be bought by selecting it and click on play button if not already sold to another player.
- Once all cells have been sold, every user can check if has won a prize by clicking on the cells identified with a bobber.
- If the cell selected contains a prize, the user can withdraw the prize amount.
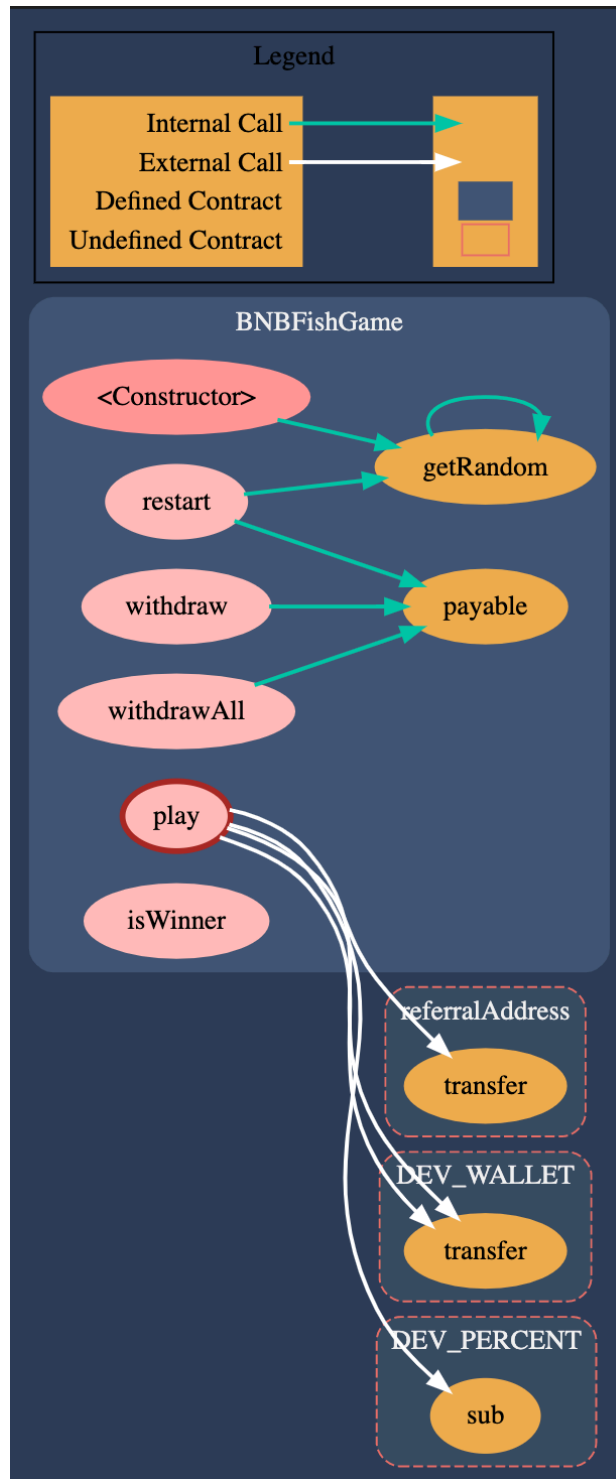
## Prizes:

| Prizes | Multiplier | ROI |
|--------|-----------|-----|
| 1 | x40 | 4000% |
| 2-3 | x10 | 1000% |
| 4-5 | x5 | 500% |
| 6-10 | x2 | 200% |
| 11-20 | x1 | 100% |

## Contract Owners Fee

- Devs Maintenance Fee: 5% (10% if no referrals)
- Referral Reward: 5%

# Smart Contract Analysis

## BNBFishGame

*Ownable*

📚 *SafeMath for uint256*

- ☐ **uint256** K
- ○ **uint256** gameId
- ○ **uint256** totalPlayed
- ○ **uint256** totalReferral
- ○ **uint256** PRICE
- ☐ **uint256** MAX_WINNERS
- ☐ **uint256** MAX_CELLS
- ☐ **address** DEV_WALLET
- ○ **uint256** DEV_PERCENT
- ○ **uint256** REF_PERCENT
- ○ **uint256** WINNERS_PERCENT
- ☐ **uint256** PERCENT_DIVIDER
- ○ **address** cells
- ○ **uint256** cellsSoldCount
- ☐ **address** winners
- ☐ **uint256** winnersIndexes
- ○ **address** lastGameWinners
- ○ **uint256** lastWinnersIndexes
- ○ **bool** withdrawn
- ○ **uint256=>null** winnersHistory

---

- ● **__constructor__()**
- ● 💰 play()
- ● withdraw()
- ● withdrawAll()
- ● restart()
- ● 🔍 isWinner()
- ■ getRandom()

**Ownable**

**SafeMath**

*for uint256*
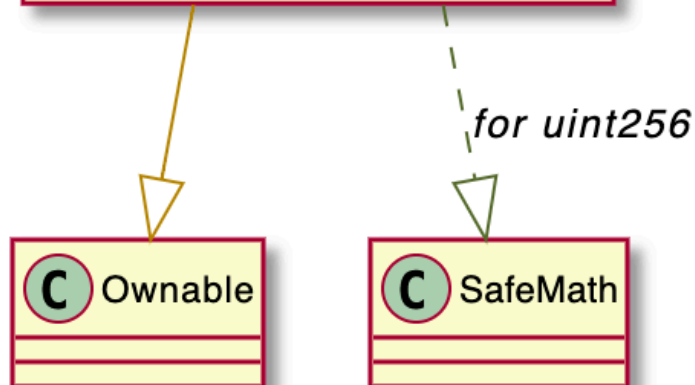
# Issues Analysis

**CRITICAL ISSUES** (critical, high severity): **0 - No Issues**

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 severity): **0 - No Issues**

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): **0 - No Issues**

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

**RECOMMENDATIONS** (very low severity): **0 - No Issues**

Hint and tips to improve contract functionality and trustworthiness.

■ Critical　　■ Medium　　■ Low　　■ Recommendations

4

3

2

1

0

Errors

# Conclusion

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

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

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

# Safe Harbor

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

ZenAudit is a 3rd party auditing company who works on audits based on client requests. Contracts are analyzed for any vulnerabilities, backdoors, and/or scam scripts.

We are not financial advisors nor our documents should be considered as financial advise.

Operations and website administration is fully managed by clients. We are not responsible for website changes or other function change.

Any concerns about the project must be raised directly to the project owners and not through ZenAudit.

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

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.