InterFi
NETWORK

SMART CONTRACT SECURITY AUDIT OF
PancakePoll

SMART CONTRACT AUDIT | TEAM KYC | PROJECT EVALUATION

RELENTLESSLY SECURING THE PUBLIC BLOCKCHAIN | MADE IN CANADA 🇨🇦

Summary

Auditing Firm	InterFi Network
Architecture	InterFi "Echelon" Auditing Standard
Smart Contract Audit Approved By	Chris	Blockchain Specialist at InterFi Network
Project Overview Approved BY	Albert	Project Specialist at InterFi Network
Platform	Solidity
Audit Check (Mandatory)	Static, Software, Auto Intelligent & Manual Analysis
Project Check (Optional)	KYC, Website & Socials Analysis (Not Applicable)
Consultation Request Date	October 20, 2021
Report Date	October 21, 2021 (24H fast-tracked)

Audit Summary

InterFi team has performed a line-by-line manual analysis and automated review of the smart contract. The smart contract was analyzed mainly for common smart contract vulnerabilities, exploits, and manipulation hacks. According to the smart contract audit:

❖ **PancakePoll's smart contract source code has LOW RISK SEVERITY.**

❖ **PancakePoll has PASSED the smart contract audit.**

For the detailed understanding of risk severity, source code vulnerability, and functional test, kindly refer to the audit.

Table Of Contents

Project Overview

InterFi was consulted by PancakePoll on October 20, 2021 to conduct a smart contract security audit of their token source code.

PancakePoll is the leading coin voting platform on Binance Smart Chain, with the highest unique visitors volume in the market. The most voted projects will stand out from the rest and allow it to unlock new features.

Project	PancakePoll
Blockchain	Binance Smart Chain
Language	Solidity
Contract	0xc29000A4b1eCD326b6DafAE17bDA636475FeA1e7
Website	https://app.pancakepoll.com/
Telegram	https://t.me/pancakepollbsc
Twitter	https://twitter.com/PancakePoll

Public logo

Solidity Source Code On Blockchain (EtherScan Verified Contract Source Code)

https://www.bscscan.com/address/0xc29000a4b1ecd326b6dafae17bda636475fea1e7#code

Contract Name: PancakePoll

Compiler Version: v0.8.9+commit.e5eed63a

Optimization Enabled: Yes with 200 runs

Solidity Source Code On InterFi GitHub

https://github.com/interfinetwork/audited-codes/blob/main/PancakePoll.sol

GitHub Commits

Solidity source code committed at: 0eb9e6ee0c2162729f2ef6033970fdde4f21b03a

Audit Scope & Methodology

The scope of this report is to audit the smart contract source code of PancakePoll. The source code can be viewed in its entirety on

https://www.bscscan.com/address/0xc29000a4b1ecd326b6dafae17bda636475fea1e7#code

InterFi has scanned the contract and reviewed the project for common vulnerabilities, exploits, hacks, and back-doors. Below is the list of commonly known smart contract vulnerabilities, exploits, and hacks:

Category

Smart Contract Vulnerabilities	❖ Re-entrancy (RE) ❖ Unhandled Exceptions (UE) ❖ Transaction Order Dependency (TO) ❖ Integer Overflow (IO) ❖ Unrestricted Action (UA)
Source Code Review	❖ Ownership Takeover ❖ Gas Limit and Loops ❖ Deployment Consistency ❖ Repository Consistency ❖ Data Consistency ❖ Token Supply Manipulation
Functional Assessment	❖ Access Control and Authorization ❖ Operations Trail and Event Generation ❖ Assets Manipulation ❖ Liquidity Access

InterFi's Echelon Audit Standard

The aim of InterFi's "Echelon" standard is to analyze the smart contract and identify the vulnerabilities and the hacks in the smart contract. Mentioned are the steps used by ECHELON-1 to assess the smart contract:

1. Solidity smart contract source code reviewal:
   - ❖ Review of the specifications, sources, and instructions provided to InterFi to make sure we understand the size, scope, and functionality of the smart contract.
   - ❖ Manual review of code, which is the process of reading source code line-byline to identify potential vulnerabilities.

2. Static, Manual, and Automated AI analysis:
   - ❖ Test coverage analysis, which is the process of determining whether the test cases are covering the code and how much code is exercised when we run those test cases.
   - ❖ Symbolic execution, which is analysing a program to determine what inputs causes each part of a program to execute.

3. Best practices review, which is a review of the smart contracts to improve efficiency, effectiveness, clarify, maintainability, security, and control based on the established industry and academic practices, recommendations, and research.

4. Specific, itemized, actionable recommendations to help you take steps to secure your smart contracts

Automated 3P frameworks used to assess the smart contract vulnerabilities

- ❖ Slither
- ❖ Consensys MythX
- ❖ Consensys Surya
- ❖ Open Zeppelin Code Analyzer
- ❖ Solidity Code Complier

InterFi's Risk Classification

Smart contracts are generally designed to manipulate and hold funds denominated in ETH/BNB. This makes them very tempting attack targets, as a successful attack may allow the attacker to directly steal funds from the contract. Below are the typical risk levels of a smart contract:

Vulnerable: A contract is vulnerable if it has been flagged by a static analysis tool as such. As we will see later, this means that some contracts may be vulnerable because of a false-positive.

Exploitable: A contract is exploitable if it is vulnerable and the vulnerability could be exploited by an external attacker. For example, if the "vulnerability" flagged by a tool is in a function which requires to own the contract, it would be vulnerable but not exploitable.

Exploited: A contract is exploited if it received a transaction on the main network which triggered one of its vulnerabilities. Therefore, a contract can be vulnerable or even exploitable without having been exploited.

Risk severity	Meaning
! Critical	This level vulnerabilities could be exploited easily, and can lead to asset loss, data loss, asset manipulation, or data manipulation. They should be fixed right away.
! High	This level vulnerabilities are hard to exploit but very important to fix, they carry an elevated risk of smart contract manipulation, which can lead to critical risk severity
! Medium	This level vulnerabilities are should be fixed, as they carry an inherent risk of future exploits, and hacks which may or may not impact the smart contract execution.
! Low	This level vulnerabilities can be ignored. They are code style violations, and informational statements in the code. They may not affect the smart contract execution

Smart Contract – Overview

Contract information

Query	Result
Name	PancakePoll
Symbol	PPOLL
Decimals	9
Total Supply	1,000,000,000,000
Total Fees	8
Owner	0x889d7483ab3f16e5fa0b0a5141bd08770a7cd1d6
Liquidity Wallet	0xbb84abfdd2d4d3fec5d0fd48fa752dbd307ef3d7
Dividend Tracker	0x5a572ea8e5850afc0f40501c1079697bcbb73151
Operations Wallet	0x01abf38e346781216c06df8402d0ad1a8b0e6aad
Pair	0xe5ceb5e3612b8f7ef06f98f40edc5e00f5c9f26b
Router	0x10ed43c718714eb63d5aa57b78b54704e256024e

Smart Contract – Static Analysis

Symbol	Meaning
🛑	Function can be modified
💵	Function is payable
🔒	Function is locked
🔓	Function can be accessed
❗	Important functionality

```
| **Context** | Implementation |  |||
| └ | _msgSender | Internal 🔒 |   | |
| └ | _msgData | Internal 🔓 |   | |
||||||
| **Ownable** | Implementation | Context |||
| └ | <Constructor> | Public ❗ | 🛑  |NO❗ |
| └ | owner | Public ❗ |    |NO❗ |
| └ | renounceOwnership | Public ❗ | 🛑 | onlyOwner |
| └ | transferOwnership | Public ❗ | 🛑 | onlyOwner |
||||||
| **IERC20** | Interface |  |||
| └ | totalSupply | External ❗ |   |NO❗ |
| └ | balanceOf | External ❗ |   |NO❗ |
| └ | transfer | External ❗ | 🛑 |NO❗ |
| └ | allowance | External ❗ |   |NO❗ |
| └ | approve | External ❗ | 🛑 |NO❗ |
| └ | transferFrom | External ❗ | 🛑 |NO❗ |
||||||
| **IERC20Metadata** | Interface | IERC20 |||
| └ | name | External ❗ |   |NO❗ |
| └ | symbol | External ❗ |   |NO❗ |
| └ | decimals | External ❗ |   |NO❗ |
||||||
| **DividendPayingTokenOptionalInterface** | Interface |  |||
| └ | withdrawableDividendOf | External ❗ |   |NO❗ |
| └ | withdrawnDividendOf | External ❗ |   |NO❗ |
| └ | accumulativeDividendOf | External ❗ |   |NO❗ |
||||||
| **DividendPayingTokenInterface** | Interface |  |||
| └ | dividendOf | External ❗ |   |NO❗ |
| └ | distributeDividends | External ❗ | 💵 |NO❗ |
```

```
| └ | withdrawDividend | External ❗ | 🔴 |NO❗ |
||||||
| **SafeMathInt** | Library | |||
| └ | mul | Internal 🔒 | | |
| └ | div | Internal 🔒 | | |
| └ | sub | Internal 🔒 | | |
| └ | add | Internal 🔒 | | |
| └ | abs | Internal 🔒 | | |
| └ | toUint256Safe | Internal 🔒 | | |
||||||
| **SafeMathUint** | Library | |||
| └ | toInt256Safe | Internal 🔒 | | |
||||||
| **SafeMath** | Library | |||
| └ | add | Internal 🔒 | | |
| └ | sub | Internal 🔒 | | |
| └ | sub | Internal 🔒 | | |
| └ | mul | Internal 🔒 | | |
| └ | div | Internal 🔒 | | |
| └ | div | Internal 🔒 | | |
| └ | mod | Internal 🔒 | | |
| └ | mod | Internal 🔒 | | |
||||||
| **ERC20** | Implementation | Context, IERC20, IERC20Metadata |||
| └ | <Constructor> | Public ❗ | 🔴 |NO❗ |
| └ | name | Public ❗ | |NO❗ |
| └ | symbol | Public ❗ | |NO❗ |
| └ | decimals | Public ❗ | |NO❗ |
| └ | totalSupply | Public ❗ | |NO❗ |
| └ | balanceOf | Public ❗ | |NO❗ |
| └ | transfer | Public ❗ | 🔴 |NO❗ |
| └ | allowance | Public ❗ | |NO❗ |
| └ | approve | Public ❗ | 🔴 |NO❗ |
| └ | transferFrom | Public ❗ | 🔴 |NO❗ |
| └ | increaseAllowance | Public ❗ | 🔴 |NO❗ |
| └ | decreaseAllowance | Public ❗ | 🔴 |NO❗ |
| └ | _transfer | Internal 🔒 | 🔴 | |
| └ | _mint | Internal 🔒 | 🔴 | |
| └ | _burn | Internal 🔒 | 🔴 | |
| └ | _approve | Internal 🔒 | 🔴 | |
| └ | _beforeTokenTransfer | Internal 🔒 | 🔴 | |
||||||
| **DividendPayingToken** | Implementation | ERC20, DividendPayingTokenInterface,
DividendPayingTokenOptionalInterface, Ownable |||
| └ | updateDividendUniswapV2Router | External ❗ | 🔴 | onlyOwner |
| └ | <Constructor> | Public ❗ | 🔴 | ERC20 |
| └ | <Receive Ether> | External ❗ | 💵 |NO❗ |
| └ | swapETHForTokens | Private 🔐 | 🔴 | |
| └ | setIgnoreToken | External ❗ | 🔴 | onlyOwner |
| └ | isIgnoredToken | Public ❗ | |NO❗ |
```

```
| └ | getRawBNBDividends | External ❗ |    |NO❗ |
| └ | setWhiteListAMM | External ❗ | 🔴 | onlyOwner |
| └ | setRewardToken | External ❗ | 🔴 | onlyOwner |
| └ | unsetRewardToken | External ❗ | 🔴 | onlyOwner |
| └ | distributeDividends | Public ❗ | 💰 |NO❗ |
| └ | withdrawDividend | Public ❗ | 🔴 |NO❗ |
| └ | _withdrawDividendOfUser | Internal 🔒 | 🔴 | |
| └ | dividendOf | Public ❗ |    |NO❗ |
| └ | withdrawableDividendOf | Public ❗ |    |NO❗ |
| └ | withdrawnDividendOf | Public ❗ |    |NO❗ |
| └ | accumulativeDividendOf | Public ❗ |    |NO❗ |
| └ | _transfer | Internal 🔒 | 🔴 | |
| └ | _mint | Internal 🔒 | 🔴 | |
| └ | _burn | Internal 🔒 | 🔴 | |
| └ | _setBalance | Internal 🔒 | 🔴 | |
||||||
| **PancakePoll** | Implementation | ERC20, Ownable |||
| └ | <Constructor> | Public ❗ | 🔴 | ERC20 |
| └ | <Receive Ether> | External ❗ | 💰 |NO❗ |
| └ | setWhiteListAMM | External ❗ | 🔴 | onlyOwner |
| └ | updateSwapTokensAtAmount | External ❗ | 🔴 | onlyOwner |
| └ | disableTransferDelay | External ❗ | 🔴 | onlyOwner |
| └ | updateDividendTracker | Public ❗ | 🔴 | onlyOwner |
| └ | updateMaxTxn | External ❗ | 🔴 | onlyOwner |
| └ | updateDividendTokensMinimum | External ❗ | 🔴 | onlyOwner |
| └ | updateUniswapV2Router | External ❗ | 🔴 | onlyOwner |
| └ | updateDividendUniswapV2Router | External ❗ | 🔴 | onlyOwner |
| └ | updateTradingStatus | External ❗ | 🔴 | onlyOwner |
| └ | excludeFromFees | Public ❗ | 🔴 | onlyOwner |
| └ | excludeMultipleAccountsFromFees | External ❗ | 🔴 | onlyOwner |
| └ | addToWhitelist | External ❗ | 🔴 | onlyOwner |
| └ | setIsBot | External ❗ | 🔴 | onlyOwner |
| └ | excludeFromDividends | External ❗ | 🔴 | onlyOwner |
| └ | includeInDividends | External ❗ | 🔴 | onlyOwner |
| └ | setAutomatedMarketMakerPair | External ❗ | 🔴 | onlyOwner |
| └ | updateLiquidityWallet | External ❗ | 🔴 | onlyOwner |
| └ | updateOperationsWallet | External ❗ | 🔴 | onlyOwner |
| └ | updateBuyBackWallet | External ❗ | 🔴 | onlyOwner |
| └ | updateFees | External ❗ | 🔴 | onlyOwner |
| └ | updateGasForProcessing | External ❗ | 🔴 | onlyOwner |
| └ | updateClaimWait | External ❗ | 🔴 | onlyOwner |
| └ | setIgnoreToken | External ❗ | 🔴 | onlyOwner |
| └ | isAMMWhitelisted | Public ❗ |    |NO❗ |
| └ | isContract | Internal 🔒 |    | |
| └ | getUserCurrentRewardToken | Public ❗ |    |NO❗ |
| └ | getUserHasCustomRewardToken | Public ❗ |    |NO❗ |
| └ | getRewardTokenSelectionCount | Public ❗ |    |NO❗ |
| └ | getLastProcessedIndex | External ❗ |    |NO❗ |
| └ | getNumberOfDividendTokenHolders | External ❗ |    |NO❗ |
| └ | getHolderSellFactor | Public ❗ |    |NO❗ |
```

```
| └ | getDividendTokensMinimum | External ❗ |   |NO❗ |
| └ | getClaimWait | External ❗ |   |NO❗ |
| └ | getTotalDividendsDistributed | External ❗ |   |NO❗ |
| └ | isExcludedFromFees | Public ❗ |   |NO❗ |
| └ | withdrawableDividendOf | Public ❗ |   |NO❗ |
| └ | dividendTokenBalanceOf | Public ❗ |   |NO❗ |
| └ | getAccountDividendsInfo | External ❗ |   |NO❗ |
| └ | getAccountDividendsInfoAtIndex | External ❗ |   |NO❗ |
| └ | getRawBNBDividends | Public ❗ |   |NO❗ |
| └ | getBNBAvailableForHolderBuyBack | Public ❗ |   |NO❗ |
| └ | isIgnoredToken | Public ❗ |   |NO❗ |
| └ | setRewardToken | Public ❗ | 🔴 |NO❗ |
| └ | setRewardTokenWithCustomAMM | Public ❗ | 🔴 |NO❗ |
| └ | unsetRewardToken | Public ❗ | 🔴 |NO❗ |
| └ | activateContract | Public ❗ | 🔴 | onlyOwner |
| 🔐 | 🔴 | |
| └ | _transfer | Internal 🔒 | 🔴 | |
| └ | swapAndLiquify | Private 🔐 | 🔴 | |
| └ | swapTokensForEth | Private 🔐 | 🔴 | |
| └ | addLiquidity | Private 🔐 | 🔴 | |
| └ | swapAndSendDividends | Private 🔐 | 🔴 | |
| └ | recoverContractBNB | Public ❗ | 🔴 | onlyOwner |
| └ | sendToOperationsWallet | Private 🔐 | 🔴 | |
| └ | setMaxSellPercent | Public ❗ | 🔴 | onlyOwner |
||||||
| **IterableMapping** | Library |   |||
| └ | get | Public ❗ |   |NO❗ |
| └ | getIndexOfKey | Public ❗ |   |NO❗ |
| └ | getKeyAtIndex | Public ❗ |   |NO❗ |
| └ | size | Public ❗ |   |NO❗ |
| └ | set | Public ❗ | 🔴 |NO❗ |
| └ | remove | Public ❗ | 🔴 |NO❗ |
||||||
| **PPOLLDividendTracker** | Implementation | DividendPayingToken |||
| └ | <Constructor> | Public ❗ | 🔴 | DividendPayingToken |
| └ | _transfer | Internal 🔒 |   | |
| └ | withdrawDividend | Public ❗ |   |NO❗ |
| └ | excludeFromDividends | External ❗ | 🔴 | onlyOwner |
| └ | includeInDividends | External ❗ | 🔴 | onlyOwner |
| └ | updateDividendMinimum | External ❗ | 🔴 | onlyOwner |
| └ | updateClaimWait | External ❗ | 🔴 | onlyOwner |
| └ | getLastProcessedIndex | External ❗ |   |NO❗ |
| └ | getNumberOfTokenHolders | External ❗ |   |NO❗ |
| └ | getAccount | Public ❗ |   |NO❗ |
| └ | getAccountAtIndex | Public ❗ |   |NO❗ |
| └ | canAutoClaim | Private 🔐 |   | |
| └ | setBalance | External ❗ | 🔴 | onlyOwner |
| └ | process | Public ❗ | 🔴 |NO❗ |
| └ | processAccount | Public ❗ | 🔴 | onlyOwner |
```

Smart Contract – Software Analysis

Function Signatures

```
16279055  =>  isContract(address)
39509351  =>  increaseAllowance(address,uint256)
43509138  =>  div(int256,int256)
119df25f  =>  _msgSender()
8b49d47e  =>  _msgData()
8da5cb5b  =>  owner()
715018a6  =>  renounceOwnership()
f2fde38b  =>  transferOwnership(address)
18160ddd  =>  totalSupply()
70a08231  =>  balanceOf(address)
a9059cbb  =>  transfer(address,uint256)
dd62ed3e  =>  allowance(address,address)
095ea7b3  =>  approve(address,uint256)
23b872dd  =>  transferFrom(address,address,uint256)
06fdde03  =>  name()
95d89b41  =>  symbol()
313ce567  =>  decimals()
a8b9d240  =>  withdrawableDividendOf(address)
aafd847a  =>  withdrawnDividendOf(address)
27ce0147  =>  accumulativeDividendOf(address)
91b89fba  =>  dividendOf(address)
03c83302  =>  distributeDividends()
6a474002  =>  withdrawDividend()
bbe93d91  =>  mul(int256,int256)
adefc37b  =>  sub(int256,int256)
a5f3c23b  =>  add(int256,int256)
1b5ac4b5  =>  abs(int256)
744f7c7d  =>  toUint256Safe(int256)
e823b9bf  =>  toInt256Safe(uint256)
771602f7  =>  add(uint256,uint256)
b67d77c5  =>  sub(uint256,uint256)
e31bdc0a  =>  sub(uint256,uint256,string)
c8a4ac9c  =>  mul(uint256,uint256)
a391c15b  =>  div(uint256,uint256)
b745d336  =>  div(uint256,uint256,string)
f43f523a  =>  mod(uint256,uint256)
71af23e8  =>  mod(uint256,uint256,string)
a457c2d7  =>  decreaseAllowance(address,uint256)
30e0789e  =>  _transfer(address,address,uint256)
4e6ec247  =>  _mint(address,uint256)
6161eb18  =>  _burn(address,uint256)
104e81ff  =>  _approve(address,address,uint256)
cad3be83  =>  _beforeTokenTransfer(address,address,uint256)
8021974b  =>  updateDividendUniswapV2Router(address)
51422e97  =>  swapETHForTokens(address,uint256)
```

```
a47e9917  =>  setIgnoreToken(address,bool)
3d01b8a7  =>  isIgnoredToken(address)
e1272992  =>  getRawBNBDividends(address)
cd06ab73  =>  setWhiteListAMM(address,bool)
065c981a  =>  setRewardToken(address,address,address)
e8f8fe39  =>  unsetRewardToken(address)
373de4aa  =>  _withdrawDividendOfUser(address)
ab86e0a6  =>  _setBalance(address,uint256)
c45a0155  =>  factory()
ad5c4648  =>  WETH()
e8e33700  =>  addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256)
f305d719  =>  addLiquidityETH(address,uint256,uint256,uint256,address,uint256)
baa2abde  =>  removeLiquidity(address,address,uint256,uint256,uint256,address,uint256)
02751cec  =>  removeLiquidityETH(address,uint256,uint256,uint256,address,uint256)
2195995c  =>
removeLiquidityWithPermit(address,address,uint256,uint256,uint256,address,uint256,bool,uint8,bytes3
2,bytes32)
ded9382a  =>
removeLiquidityETHWithPermit(address,uint256,uint256,uint256,address,uint256,bool,uint8,bytes32,byt
es32)
38ed1739  =>  swapExactTokensForTokens(uint256,uint256,address[],address,uint256)
8803dbee  =>  swapTokensForExactTokens(uint256,uint256,address[],address,uint256)
7ff36ab5  =>  swapExactETHForTokens(uint256,address[],address,uint256)
4a25d94a  =>  swapTokensForExactETH(uint256,uint256,address[],address,uint256)
18cbafe5  =>  swapExactTokensForETH(uint256,uint256,address[],address,uint256)
fb3bdb41  =>  swapETHForExactTokens(uint256,address[],address,uint256)
ad615dec  =>  quote(uint256,uint256,uint256)
054d50d4  =>  getAmountOut(uint256,uint256,uint256)
85f8c259  =>  getAmountIn(uint256,uint256,uint256)
d06ca61f  =>  getAmountsOut(uint256,address[])
1f00ca74  =>  getAmountsIn(uint256,address[])
af2979eb  =>
removeLiquidityETHSupportingFeeOnTransferTokens(address,uint256,uint256,uint256,address,uint256)
5b0d5984  =>
removeLiquidityETHWithPermitSupportingFeeOnTransferTokens(address,uint256,uint256,uint256,address,u
int256,bool,uint8,bytes32,bytes32)
5c11d795  =>
swapExactTokensForTokensSupportingFeeOnTransferTokens(uint256,uint256,address[],address,uint256)
b6f9de95  =>  swapExactETHForTokensSupportingFeeOnTransferTokens(uint256,address[],address,uint256)
791ac947  =>
swapExactTokensForETHSupportingFeeOnTransferTokens(uint256,uint256,address[],address,uint256)
017e7e58  =>  feeTo()
094b7415  =>  feeToSetter()
e6a43905  =>  getPair(address,address)
1e3dd18b  =>  allPairs(uint256)
574f2ba3  =>  allPairsLength()
c9c65396  =>  createPair(address,address)
f46901ed  =>  setFeeTo(address)
a2e74af6  =>  setFeeToSetter(address)
3644e515  =>  DOMAIN_SEPARATOR()
```

```
30adf81f  =>  PERMIT_TYPEHASH()
7ecebe00  =>  nonces(address)
d505accf  =>  permit(address,address,uint256,uint256,uint8,bytes32,bytes32)
ba9a7a56  =>  MINIMUM_LIQUIDITY()
0dfe1681  =>  token0()
d21220a7  =>  token1()
0902f1ac  =>  getReserves()
5909c0d5  =>  price0CumulativeLast()
5a3d5493  =>  price1CumulativeLast()
7464fc3d  =>  kLast()
6a627842  =>  mint(address)
89afcb44  =>  burn(address)
022c0d9f  =>  swap(uint256,uint256,address,bytes)
bc25cf77  =>  skim(address)
fff6cae9  =>  sync()
485cc955  =>  initialize(address,address)
d257b34f  =>  updateSwapTokensAtAmount(uint256)
e884f260  =>  disableTransferDelay()
88bdd9be  =>  updateDividendTracker(address)
2bc4d48b  =>  updateMaxTxn(uint256)
d4064503  =>  updateDividendTokensMinimum(uint256)
65b8dbc0  =>  updateUniswapV2Router(address)
870000e1  =>  updateTradingStatus(bool)
c0246668  =>  excludeFromFees(address,bool)
c492f046  =>  excludeMultipleAccountsFromFees(address[],bool)
bc93233f  =>  addToWhitelist(address,bool)
03c0f5d4  =>  setIsBot(address,bool)
31e79db0  =>  excludeFromDividends(address)
c0f306ef  =>  includeInDividends(address)
9a7a23d6  =>  setAutomatedMarketMakerPair(address,bool)
e37ba8f9  =>  updateLiquidityWallet(address)
30d5d18d  =>  updateOperationsWallet(address)
06e7b14d  =>  updateBuyBackWallet(address)
c6616ba1  =>  updateFees(uint256,uint256,uint256,uint256)
871c128d  =>  updateGasForProcessing(uint256)
e98030c7  =>  updateClaimWait(uint256)
2501ff16  =>  isAMMWhitelisted(address)
d2bbdac2  =>  getUserCurrentRewardToken(address)
d5de7e9d  =>  getUserHasCustomRewardToken(address)
dfb6d223  =>  getRewardTokenSelectionCount(address)
e7841ec0  =>  getLastProcessedIndex()
64b0f653  =>  getNumberOfDividendTokenHolders()
1a8dd2f7  =>  getHolderSellFactor(address)
479c5266  =>  getDividendTokensMinimum()
a26579ad  =>  getClaimWait()
30bb4cff  =>  getTotalDividendsDistributed()
4fbee193  =>  isExcludedFromFees(address)
6843cd84  =>  dividendTokenBalanceOf(address)
ad56c13c  =>  getAccountDividendsInfo(address)
f27fd254  =>  getAccountDividendsInfoAtIndex(uint256)
```

```
bc728a6f  =>  getBNBAvailableForHolderBuyBack(address)
8aee8127  =>  setRewardToken(address)
d32cf929  =>  setRewardTokenWithCustomAMM(address,address)
f9fbb138  =>  unsetRewardToken()
8fda356d  =>  activateContract()
dad80fc4  =>  buyBackTokensWithNoFees()
4e71d92d  =>  claim()
700bb191  =>  processDividendTracker(uint256)
a7f7b36f  =>  _setAutomatedMarketMakerPair(address,bool)
173865ad  =>  swapAndLiquify(uint256)
b28805f4  =>  swapTokensForEth(uint256)
9cd441da  =>  addLiquidity(uint256,uint256)
818c19dc  =>  swapAndSendDividends(uint256)
68fc7415  =>  recoverContractBNB(uint256)
0a535b58  =>  sendToOperationsWallet(uint256)
59992dbc  =>  setMaxSellPercent(uint256)
268d8e2e  =>  get(Map,address)
b45dad3d  =>  getIndexOfKey(Map,address)
7596720f  =>  getKeyAtIndex(Map,uint256)
b1b533f3  =>  size(Map)
6b06f325  =>  set(Map,address,uint256)
0eac8729  =>  remove(Map,address)
f9e2f5fb  =>  updateDividendMinimum(uint256)
09bbedde  =>  getNumberOfTokenHolders()
fbcbc0f1  =>  getAccount(address)
5183d6fd  =>  getAccountAtIndex(uint256)
77fdb837  =>  canAutoClaim(uint256)
e30443bc  =>  setBalance(address,uint256)
ffb2c479  =>  process(uint256)
bc4c4b37  =>  processAccount(address,bool)
```

Inheritance Graph
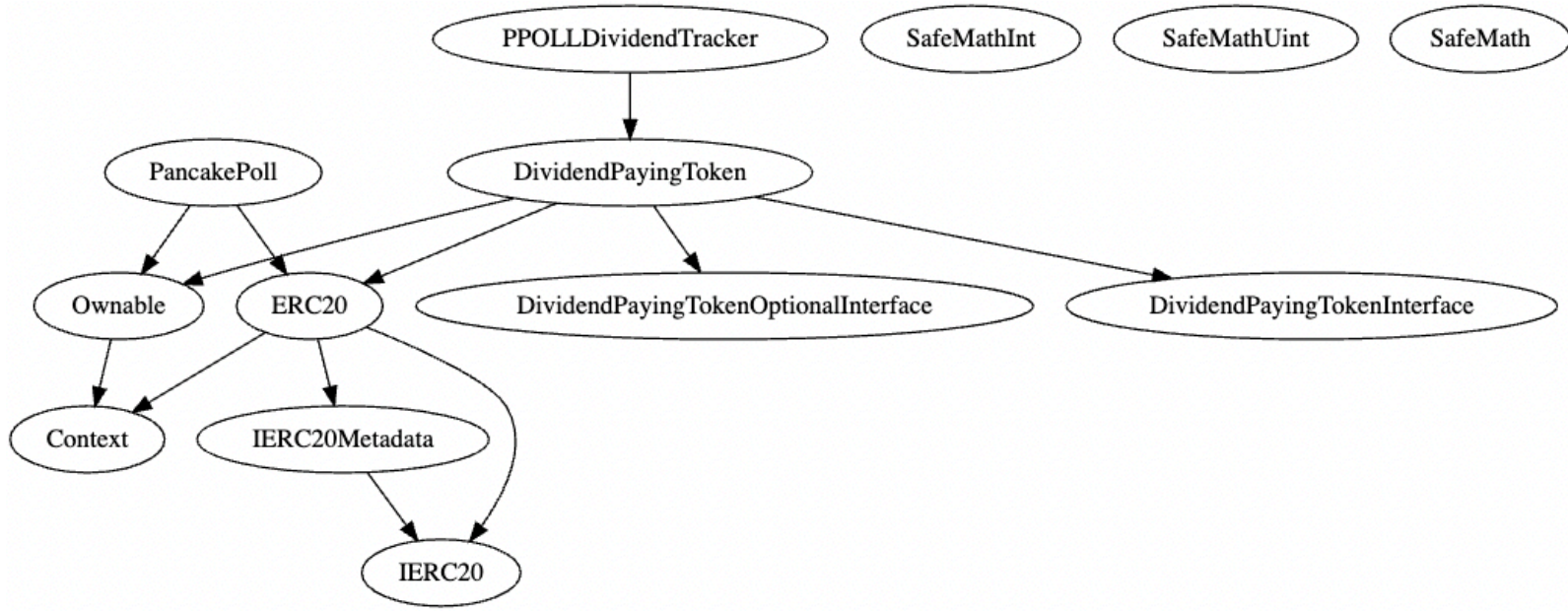
Smart Contract – Manual Analysis

Function	Description	Tested	Verdict
TotalSupply	provides information about the total token supply	Yes	**Passed**
BalanceOf	provides account balance of the owner's account	Yes	**Passed**
Transfer	executes transfers of a specified number of tokens to a specified address	Yes	**Passed**
Approve	allow a spender to withdraw a set number of tokens from a specified account	Yes	**Passed**
Allowance	returns a set number of tokens from a spender to the owner	Yes	**Passed**
burn	executes transfers of a specified number of tokens to a burn address	Yes	**Passed**
Rebase	circulating token supply adjusts (increases or decreases) automatically according to a token's price fluctuations	NA	NA

Note

❖ Active Owner: **0x889d7483ab3f16e5fa0b0a5141bd08770a7cd1d6**

❖ When the smart contract has an active owner address, some of the smart contract functions can be edited, modified or altered.

❖ Owner can mint tokens at token launch.

❖ Owner can-not lock or burn user assets.

❖ Owner can-not stop or pause the smart contract.

Important Information

1. **PancakePoll Smart Contract utilizes "SafeMath" function to avoid common smart contract vulnerabilities.**

```
library SafeMath {
function add(uint256 a, uint256 b) internal pure returns (uint256) {
    uint256 c = a + b;
    require(c >= a, 'SafeMath: addition overflow');

    return c;
  }
  function sub(uint256 a, uint256 b) internal pure returns (uint256) {
    return sub(a, b, 'SafeMath: subtraction overflow');
  }
uint256 c = a * b;
    require(c / a == b, 'SafeMath: multiplication overflow');

    return c;
  }
```

2. **PancakePoll smart contract has 1 low severity issue which may or may not create any functional vulnerability.**

```
{

        "resource": " /PancakePoll.sol",

        "owner": "_generated_diagnostic_collection_name_#0",

        "severity": 8, (! Low Severity)

        " Expected pragma, import directive or contract/interface/library definition",

        "source": "solc",

}
```

Smart Contract – SWC Attacks

| SWC ID	Description	Verdict
SWC-101	Integer Overflow and Underflow	Passed
SWC-102	Outdated Compiler Version	Passed
SWC-103	Floating Pragma	! Low
SWC-104	Unchecked Call Return Value	Passed
SWC-105	Unprotected Ether Withdrawal	Passed
SWC-106	Unprotected SELFDESTRUCT Instruction	Passed
SWC-107	Re-entrancy	Passed
SWC-108	State Variable Default Visibility	Passed
SWC-109	Uninitialized Storage Pointer	Passed
SWC-110	Assert Violation	Passed
SWC-111	Use of Deprecated Solidity Functions	Passed
SWC-112	Delegate Call to Untrusted Callee	Passed
SWC-113	DoS with Failed Call	Passed
SWC-114	Transaction Order Dependence	Passed
SWC-115	Authorization through tx.origin	Passed
SWC-116	Block values as a proxy for time	Passed
SWC-117	Signature Malleability	Passed
SWC-118	Incorrect Constructor Name	Passed

SWC-119	Shadowing State Variables	Passed
SWC-120	Weak Sources of Randomness from Chain Attributes	Passed
SWC-121	Missing Protection against Signature Replay Attacks	Passed
SWC-122	Lack of Proper Signature Verification	Passed
SWC-123	Requirement Violation	Passed
SWC-124	Write to Arbitrary Storage Location	Passed
SWC-125	Incorrect Inheritance Order	Passed
SWC-126	Insufficient Gas Griefing	Passed
SWC-127	Arbitrary Jump with Function Type Variable	Passed
SWC-128	DoS With Block Gas Limit	Passed
SWC-129	Typographical Error	Passed
SWC-130	Right-To-Left-Override control character (U+202E)	Passed
SWC-131	Presence of unused variables	Passed
SWC-132	Unexpected Ether balance	Passed
SWC-133	Hash Collisions With Multiple Variable Length Arguments	Passed
SWC-134	Message call with hardcoded gas amount	Passed
SWC-135	Code With No Effects (Irrelevant/Dead Code)	! Low
SWC-136	Unencrypted Private Data On-Chain	Passed

Smart Contract - Risk Status & Radar Chart

Risk Severity	Status
! Critical	None critical severity issues identified
! High	None high severity issues identified
! Medium	None medium severity issues identified
! Low	**1 low severity issue identified**
Passed	**41 functions and instances verified and passed**

Score out of 100
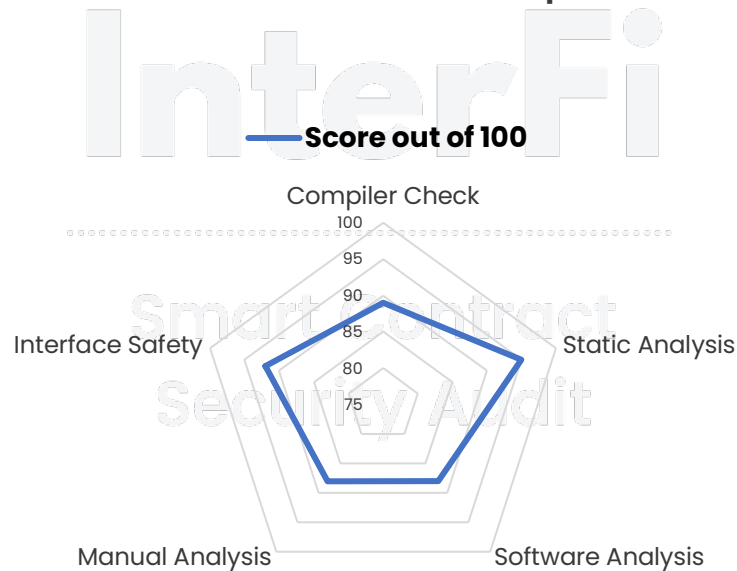
Compiler Check	89
Static Analysis	95
Software Analysis	88
Manual Analysis	88
Interface Safety	92

Auditor's Verdict

InterFi team has performed a line-by-line manual analysis and automated review of the smart contract. The smart contract was analyzed mainly for common smart contract vulnerabilities, exploits, and manipulation hacks.

PancakePoll's smart contract source code has LOW RISK SEVERITY.

PancakePoll has PASSED the smart contract audit.

Auditor's Note:

❖ Be aware that active smart contract owner privileges constitute an elevated impact to smart contract's safety and security.

❖ Owner or developer KYC isn't checked and verified due to out of scope.

❖ Project's liquidity pair isn't checked and verified due to out of scope.

❖ Project website is not checked due to out of scope. The website hasn't been reviewed for SSL and lighthouse report.

Important Disclaimer

InterFi Network provides contract auditing and project verification services for blockchain projects. The purpose of the audit is to analyse the on-chain smart contract source code, and to provide basic overview of the project. **This report should not be transmitted, disclosed, referred to, or relied upon by any person for any purposes without InterFi's prior written consent.**

InterFi provides the easy-to-understand assessment of the project, and the smart contract (otherwise known as the source code). The audit makes no statements or warranties on the security of the code. It also cannot be considered as an enough assessment regarding the utility and safety of the code, bug-free status, or any other statements of the contract. While we have used all the data at our disposal to provide the transparent analysis, it is important to note that you should not rely on this report only — we recommend proceeding with several independent audits and a public bug bounty program to ensure the security of smart contracts. **Be aware that smart contracts deployed on a blockchain aren't resistant from external vulnerability, or a hack. Be aware that active smart contract owner privileges constitute an elevated impact to smart contract's safety and security. Therefore, InterFi does not guarantee the explicit security of the audited smart contract.**

The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.

This report should not be considered as an endorsement or disapproval of any project or team. The information provided on this report does not constitute investment advice, financial advice, trading advice, or any other sort of advice and you should not treat any of the report's content as such. Do conduct your own due diligence and consult your financial advisor before making any investment decisions.

About InterFi Network

InterFi Network provides intelligent blockchain solutions. InterFi is developing an ecosystem that is seamless and responsive. Some of our services: Blockchain Security, Token Launchpad, NFT Marketplace, etc. **InterFi's mission is to interconnect multiple services like Blockchain Security, DeFi, Gaming, and Marketplace under one ecosystem that is seamless, multi-chain compatible, scalable, secure, fast, responsive, and easy-to-use.**

InterFi is built by a decentralized team of UI experts, contributors, engineers, and enthusiasts from all over the world. Our team currently consists of 6+ core team members, and 10+ casual contributors. **InterFi provides manual, static, and automatic smart contract analysis, to ensure that project is checked against known attacks and potential vulnerabilities.**

To learn more, visit https://interfi.network

To view our audit portfolio, visit https://github.com/interfinetwork

To book an audit, message https://t.me/interfiaudits

@INTERFINETWORK

RELENTLESSLY SECURING THE PUBLIC BLOCKCHAIN | MADE IN CANADA 🇨🇦