8Pay Token Audit

The BlockChain Auditor

Prepared by: Jorge Martinez

Version: 1
Date: April 7, 2021

Summary of Findings

This document expresses all security concerns of the 8Pay smart contract ecosystem as expressed by Jorge Martinez. I took care to attempt to find as many ways to improve the security, code efficiency, best practices, and overall function of the smart contracts.

Contract Status: Deployed at here 0xFeea0bDd3D07eb6FE305938878C0caDBFa169042

0 Critical Issue(s) were found.
0 Medium Issue(s) were found.
0 Low Issue(s) were found.
0 Informational Issue(s) were found.

Solidity Code Coverage

Jorge's Test Suite	8Pay	Industry Standard
87.16%	87.16%	95%

For this audit, I wasn't provided with a testing suite but as part of my audit methodology I developed a test suite to verify the functionality of the 8Pay contracts, check their security, and to help reveal any underlying issues.

This audit should be seen as one step in the development process with the intent of raising awareness on the meticulous work involved in secure development and making no material statements or guarantees to the operational state of the smart contract(s) once they are deployed. This document is not an endorsement of the reliability or effectiveness of the smart contracts. This is an assessment of the smart contract logic, implementation, and best practices. I cannot take responsibility for any potential consequences of the deployment or use of the smart contract(s) related to the audit.

Test Suite Results

Jorge’s Test Suite

```
  EightPayToken
    Deployment
      ✓ name should be 8PAY Network (589ms)
      ✓ symbol should be 8PAY
      ✓ deployer should be the owner
      ✓ should have 18 decimals
      ✓ total supply should be 88 888 888 tokens
      ✓ deployer should have the total initial supply
    allowance
      ✓ allowance works as expected (474ms)
    approve
      ✓ cannot approve the zero address to move your tokens
    transferFrom
      ✓ allows you transfer an address' tokens to another address (68ms)
    Ownership
      ✓ only the owner can transfer ownership to another address (102ms)
      ✓ owner cannot transfer ownership to the zero address
      ✓ the owner can renounce ownership of the contract (47ms)
    Whitelist
      ✓ creating the LGE whitelist requires duration and amountsMax of equal length (71ms)
      ✓ transferring tokens to the pair address begins the LGE (148ms)
      ✓ transferring tokens reverts if you're not on the whitelist (260ms)
      ✓ whitelisters cannot buy more than the specified amount max (107ms)
      ✓ whitelisted addresses can buy up to the specified max (201ms)
      ✓ whitelist admin can add whitelist addresses using modifyLGEWhitelist (148ms)
      ✓ whitelist admin can modify the whitelist duration (54ms)
      ✓ whitelist admin can modify the max tokens that can be bought during the whitelist (43ms)
      ✓ whitelist admin can call the modifyLGEWhitelist and not change anything (45ms)
      ✓ when the whitelist round is over, getLGEWhitelistRound returns 0 (40ms)
      ✓ whitelist admin cannot modify a whitelist that doesn't exist
      ✓ whitelist admin cannot set amountMax less than zero
      ✓ whitelist admin can renounce their whitelister permissions (39ms)
      ✓ whitelist admin can tranfer their whitelisting permission to another address
      ✓ whitelist admin cannot transfer their whitelisting permission to the zero address


  27 passing (3s)
```

File	% Stmts	% Branch	% Funcs	% Lines	Uncovered Lines
contracts/	87.16	72.41	85.37	86.73	
Context.sol	50	100	66.67	33.33	23,24
EightPayToken.sol	100	62.5	100	100	
IBEP20.sol	100	100	100	100	
LGEWhitelisted.sol	97.67	88.24	100	97.78	129
Ownable.sol	100	100	100	100	
SafeMath.sol	36.84	25	37.5	36.84	... 132,147,148
All files	87.16	72.41	85.37	86.73	

Table of Contents

Audit Methodology & Techniques

The BlockChain Auditor has the following auditing process:

1. Our audits include
   a. Review of the specifications, source code, and instructions provided to the TheBlockchainAuditor to clearly identify the desired functionality of the smart contract(s).
   b. Manual line by line review of contract code to spot potential vulnerabilities.
   c. Identification of deviations between desired functionality expressed to the TheBlockchainAuditor and what the smart contract(s) are doing.
2. Automated static and symbolic analysis, as well as verifying testing coverage using the provided test suite.
   a. Automated static and symbolic analysis help determine what inputs cause each part of the smart contract to execute. Analysis of how much of the code base is tested and comparison to industry standard.
3. Examination of smart contracts and development process as a whole, ensuring best practices are followed, allowing improved efficiency and security based on established industry and academic practices.
4. Specific, itemized, and actionable recommendations to assist in securing the smart contract(s) in question.

Contract Checklist

EightPayToken.sol

Contract Vulnerability	
Integer Overflow	Pass
Race Condition	Pass
Denial of Service	Pass
Logical Vulnerability	Pass
Hardcoded Address	Pass
Function Input Parameter Check	Pass
Function Access Control Check	Pass
Random Number Generation	N/A
Random Number Use	N/A
Contract Specification	
Solidity Compiler Version	Pass
Event Use	Pass
Fallback Function Use	N/A
Constructor Use	Pass
Function Visibility Declaration	Pass
Variable Storage Declaration	Pass
Deprecated Keyword Use	Pass
ERC20/223 Standard	Pass
ERC721 Standard	N/A
Business Risk	
Able to Arbitratrily Create Token	N/A
Able to Arbitrarily Destroy Token	N/A
Can Suspend Transactions	Pass
Short Address Attack	Pass
Gas Optimization	
assert()/require()/revert() misused	Pass
Loop Optimization	Pass
Storage Optimization	Pass

Executive Summary

Overall Thoughts

There are two subjects to address in this audit.

First, a thorough audit of the code provided for the 8Pay token. Second, a Medium article that has since been removed made claims regarding a backdoor and potential abuses possible. In short, my audit found no issues, and I will directly address the claims made in the medium article.

The 8Pay project was launched on both the Binance Smart Chain and the Ethereum network. After carefully testing the code, zero issues were found in the 8Pay ecosystem. The whitelist functionality that the EightPayToken utilized that was inherited from LGEWhitelisted.sol was thoroughly checked and no problems were found. This is the second time I've gone through LGEWhitelisted.sol and neither times did I find any exploits or security vulnerabilities. Overall, the codebase is solid and everything is working as intended and specified.

While external audits play an important role and can be very effective, the claims in the Medium article targeting 8Pay need to be in the correct context. They were analyzing a testnet contract that had to be reverse engineered before a difficult bytecode analysis could be done. The analysis was not done on the actual contract launched on BSC and Ethereum mainnets. We can see the contract they audited here on the BSC testnet https://testnet.bscscan.com/address/0x0d338e1a67966c995d754e06bd53fa5e59c1988b.

The live Ethereum Address is found here https://etherscan.com/address/0xFeea0bDd3D07eb6FE305938878C0caDBFa169042

Executive Summary

The live Ethereum Address is found here https://etherscan.com/address/0xFeea0bDd3D07eb6FE305938878C0caDBFa169042

And the BSC address is here https://bscscan.com/address/0xFeea0bDd3D07eb6FE305938878C0caDBFa169042

These are the contracts that users are actually interacting with and as such should be the contracts placed under scrutiny. One of the primary concerns raised was that the contracts could be upgraded to introduce malicious functions but the live contracts are not upgradable, and so are not vulnerable to the abuse.

In my analysis, I found no issues or security vulnerabilities.

Appendix A

File Fingerprints

Context.sol	dade3e179d32c478fbfb32a209d81253
EightPayToken.sol	a0008110aeb42667b4585009b2ac761b
IBEP20.sol	cbe2cda3e6550f981b43804ef400e410
LGEWhitelisted.sol	fda4ea6f0e1160ef72f845700ebb7efb
Ownable.sol	e72973724fb099e912ffd818b07df08f
SafeMath.sol	bb03ffbf17dd25a1cdc76579e034ece

The Blockchain Auditor is honored to have the opportunity to help verify the functionality of the 8Pay contract ecosystem. The communication with the 8Pay development team was excellent we were quickly able verify the functionality of the smart contracts. I look forward to working with 8Pay in the future and am excited about the promise projects launching on Binance Smart Chain show in the face of the multi-chain universe.

The BlockChain Auditor

- Jorge Martinez