SMART CONTRACT
SECURITY AUDIT

Futura Finance

October, 2021

Table of Contents

Disclaimer

This is a comprehensive report based on our automated and manual examination of cybersecurity vulnerabilities and framework flaws. We took into consideration smart contract based algorithms, as well. Reading the full analysis report is essential to build your understanding of project's security level. It is crucial to take note, though we have done our best to perform this analysis and report, that you should not rely on the our research and cannot claim what it states or how we created it. Before making any judgments, you have to conduct your own independent research. We will discuss this in more depth in the following disclaimer - please read it fully.

DISCLAIMER: You agree to the terms of this disclaimer by reading this report or any portion thereof. Please stop reading this report and remove and delete any copies of this report that you download and/or print if you do not agree to these conditions. This report is for non-reliability information only and does not represent investment advice. No one shall be entitled to depend on the report or its contents, and Soken and its affiliates shall not be held responsible to you or anyone else, nor shall Soken provide any guarantee or representation to any person with regard to the accuracy or integrity of the report. Without any terms, warranties or other conditions other than as set forth in that exclusion and Soken excludes hereby all representations, warrants, conditions and other terms (including, without limitation, guarantees implied by the law of satisfactory quality, fitness for purposes and the use of reasonable care and skills). The report is provided as "as is" and does not contain any terms and conditions. Except as legally banned, Soken disclaims all responsibility and responsibilities and no claim against Soken is made to any amount or type of loss or damages (without limitation, direct, indirect, special, punitive, consequential or pure economic loses or losses) that may be caused by you or any other person, or any damages or damages, including without limitations (whether innocent or negligent).

Security analysis is based only on the smart contracts. No applications or operations were reviewed for security. No product code has been reviewed.

Procedure

Our analysis contains following steps:

1. Project Analysis;

2. Manual analysis of smart contracts:
- Deploying smart contracts on any of the network(Ropsten/Rinkeby) using Remix IDE
- Hashes of all transaction will be recorded
- Behaviour of functions and gas consumption is noted, as well.

3. Unit Testing:
- Smart contract functions will be unit tested on multiple parameters and under multiple conditions to ensure that all paths of functions are functioning as intended.
- In this phase intended behaviour of smart contract is verified.
- In this phase, we would also ensure that smart contract functions are not consuming unnecessary gas.
- Gas limits of functions will be verified in this stage.

4. Automated Testing:
- Mythril
- Oyente
- Manticore
- Solgraph

Terminology

We categorize the finding into 4 categories based on their vulnerability:

• Low-severity issue — less important, must be analyzed
• Medium-severity issue — important, needs to be analyzed and fixed
• High-severity issue —important, might cause vulnerabilities, must be analyzed and fixed
• Critical-severity issue —serious bug causes, must be analyzed and fixed.

Limitations

The security audit of Smart Contract cannot cover all vulnerabilities. Even if no vulnerabilities are detected in the audit, there is no guarantee that future smart contracts are safe. Smart contracts are in most cases safeguarded against specific sorts of attacks. In order to find as many flaws as possible, we carried out a comprehensive smart contract audit. Audit is a document that is not legally binding and guarantees nothing.

Token Contract Details for 16.10.2021

Contract Name: **FuturaFinance**

Deployed address: **0x183B2c147fE11788b73BC0D6A7E0186aA5464BfA**

Total Supply: **1,000,000,000,000**

Token Tracker: **FFT**

Decimals: **9**

Token holders: **2,288**

Transactions count: **9,186**

Top 100 holders dominance: **78.04%**

Audit Details

Project Name: **Futura Finance**

Language: **Solidity**

Compiler version: **v.0.8.5**
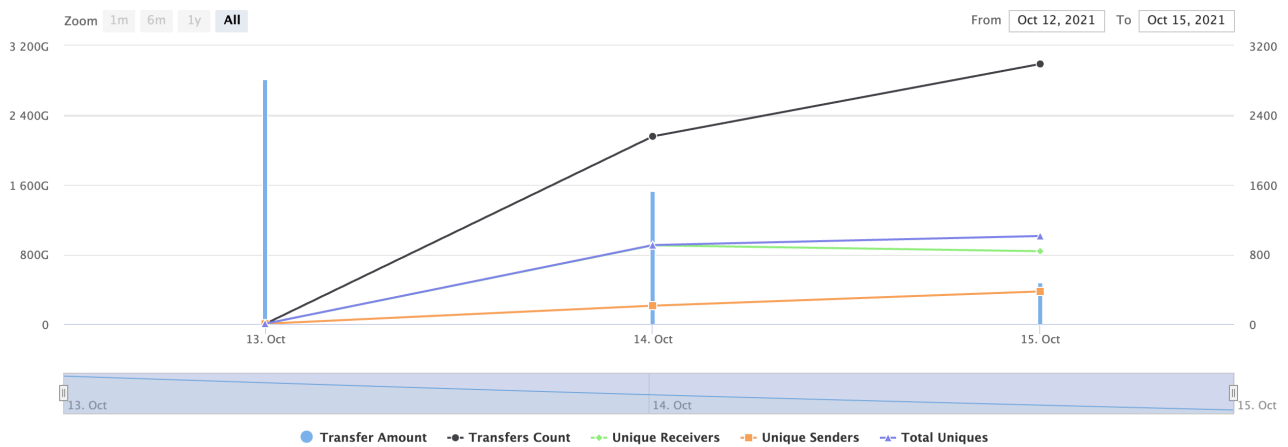
Blockchain: **BSC**
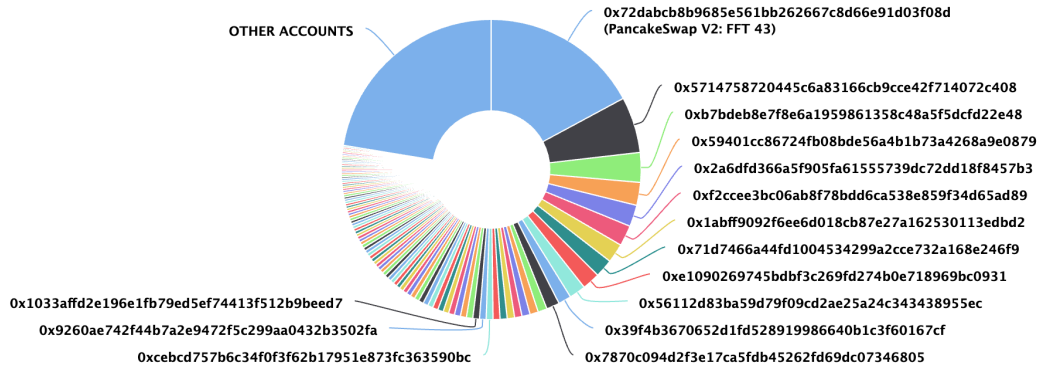
Social Profiles

Project Website: **futurafinance.io/**

Project Twitter: **@futurabsc**

Project Telegram: **FuturaBSC**

Token Contract Overview

FFT Token Distribution

OTHER ACCOUNTS

0x72dabcb8b9685e561bb262667c8d66e91d03f08d
(PancakeSwap V2: FFT 43)

0x5714758720445c6a83166cb9cce42f714072c408
0xb7bdeb8e7f8e6a1959861358c48a5f5dcfd22e48
0x59401cc86724fb08bde56a4b1b73a4268a9e0879
0x2a6dfd366a5f905fa61555739dc72dd18f8457b3
0xf2ccee3bc06ab8f78bdd6ca538e859f34d65ad89
0x1abff9092f6ee6d018cb87e27a162530113edbd2
0x71d7466a44fd1004534299a2cce732a168e246f9
0xe1090269745bdbf3c269fd274b0e718969bc0931
0x56112d83ba59d79f09cd2ae25a24c343438955ec
0x39f4b3670652d1fd528919986640b1c3f60167cf
0x7870c094d2f3e17ca5fdb45262fd69dc07346805

0x1033affd2e196e1fb79ed5ef74413f512b9beed7
0x9260ae742f44b7a2e9472f5c299aa0432b3502fa
0xcebcd757b6c34f0f3f62b17951e873fc363590bc

FFT Top 10 Holders

Rank	Address	Quantity	Percentage
1	PancakeSwap V2: FFT 43	171,508,353,516.930948377	17.1508%
2	0x5714758720445c6a83166cb9cce42f714072c408	60,388,107,686.560216756	6.0388%
3	0xb7bdeb8e7f8e6a1959861358c48a5f5dcfd22e48	31,988,253,778.247056569	3.1988%
4	0x59401cc86724fb08bde56a4b1b73a4268a9e0879	24,648,500,656.193340985	2.4649%
5	0x2a6dfd366a5f905fa61555739dc72dd18f8457b3	23,185,819,860.743618934	2.3186%
6	0xf2ccee3bc06ab8f78bdd6ca538e859f34d65ad89	22,335,723,879.047347888	2.2336%
7	0x1abff9092f6ee6d018cb87e27a162530113edbd2	20,659,765,622.213326401	2.0660%
8	0x71d7466a44fd1004534299a2cce732a168e246f9	19,634,049,735.397486223	1.9634%
9	0xe1090269745bdbf3c269fd274b0e718969bc0931	19,168,080,309.214760658	1.9168%
10	0x56112d83ba59d79f09cd2ae25a24c343438955ec	17,826,732,254.757744782	1.7827%

Vulnerabilities checking

Issue Description	Checking Status
Compiler Errors	Completed
Delays in Data Delivery	Completed
Re-entrancy	Completed
Transaction-Ordering Dependence	Completed
Timestamp Dependence	Completed
Shadowing State Variables	Completed
DoS with Failed Call	Completed
DoS with Block Gas Limit	Completed
Outdated Complier Version	Completed
Assert Violation	Completed
Use of Deprecated Solidity Functions	Completed
Integer Overflow and Underflow	Completed
Function Default Visibility	Completed
Malicious Event Log	Completed
Math Accuracy	Completed
Design Logic	Completed
Fallback Function Security	Completed
Cross-function Race Conditions	Completed
Safe Zeppelin Module	Completed

Security Issues

1) Owner privileges:

The contract contains ownership functionality and ownership is not renounced which allows the creator or current owner to modify contract behavior (for example, disable selling or mint new tokens).

2) Volatile Code:

The return values of functions *swapExactTokensForETHSupportingFeeOnTransferTokens* and *addLiquidityETH* are not properly handled.

Conclusion

Low-severity issues exist within smart contracts. Smart contracts are free from any critical or high-severity issues.

NOTE: Please check the disclaimer above and note, that audit makes no statements or warranties on business model, investment attractiveness or code sustainability.

Audited by soken

Soken Contact Info

Website: www.soken.io

Mob: (+1)416-875-4174

32 Britain Street, Toronto, Ontario, Canada

Telegram: @team_soken

GitHub: sokenteam

Twitter: @soken_team