BLOCK SOLUTIONS

Smart Contract Code Review and Security Analysis Report for ALPHATERRA BEP20 Token Smart Contract

Request Date: 2022-11-19
Completion Date: 2022-11-21
Language: Solidity

Contents

Commission

Audited Project	ALPHATERRA BEP20 Token Smart Contract
Smart Contract Address	0x834eE470Ddb53b9337f07D909B10461C3035bb38
Owner Address	0x937cd31d806fc4ebd9a5a70c34809482e3166b6b
Creator Address	0x8B1935856467b0874EBfEa0Ef2F57173352D44fb
Blockchain Platform	Binance Smart Chain Mainnet

Block Solutions was commissioned by ALPHATERRA BEP20 Token Smart Contract owners to perform an audit of their main smart contract. The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

ALPHATERRA Properties

Contract Token name	ALPHATERRA
Total supply	1000000000 Alfat
Symbol	Alfat
Decimals	9
Pancake Swap V2 Router	0x10ed43c718714eb63d5aa57b78b54704e256024e
Pancake Swap Pair	0x9e3cc2b58e9dbc5f019280611bb3487ddb0c6c45
Marketing Wallet	0x7566726ea96c8da0ba6ec73009e86d514510102c
Tax Fee	1 %
Marketing Fee	1 %
Liquidity Fee	3 %
Burn Fee	1 %
Maximum Transaction Amount	1000000000
Smart Contract Address	0x834eE470Ddb53b9337f07D909B10461C3035bb38
Owner Address	0x937cd31d806fc4ebd9a5a70c34809482e3166b6b
Creator Address	0x8B1935856467b0874EBfEa0Ef2F57173352D44fb
Blockchain Platform	Binance Smart Chain Mainnet

Contract Functions

Executables

i. function approve(address spender, uint256 amount) public override returns (bool)
ii. function decreaseAllowance(address spender, uint256 subtractedValue) public virtual returns (bool)
iii. function deliver(uint256 tAmount) public
iv. function excludeFromReward(address account) public onlyOwner()
v. function excludeFromFee(address account) public onlyOwner
vi. function includeInFee(address account) public onlyOwner
vii. function increaseAllowance(address spender, uint256 addedValue) public virtual returns (bool)
viii. function includeInReward(address account) external onlyOwner()
ix. function lock(uint256 time) public virtual onlyOwner
x. function renounceOwnership() public virtual onlyOwner
xi. function setBurnFee(uint256 BurnFee) external onlyOwner()
xii. function setliquidityFee(uint256 liqFee) external onlyOwner()
xiii. function setmarketingFee(uint256 marketingFee) external onlyOwner()
xiv. function setmarketingWallet(address newAdd) external onlyOwner()
xv. function setMaxTxPercent(uint256 maxTxPercent) external onlyOwner()
xvi. function setSwapAndLiquifyEnabled(bool _enabled) public onlyOwner
xvii. function setTaxFee(uint256 taxFee) external onlyOwner()
xviii. function transfer(address recipient, uint256 amount) public override returns (bool)
xix. function transferFrom(address sender, address recipient, uint256 amount) public override returns (bool)
xx. function transferOwnership(address newOwner) public virtual onlyOwner
xxi. function unlock() public virtual

Checklist

Compiler errors.	Passed
Possible delays in data delivery.	Passed
Timestamp dependence.	Passed
Integer Overflow and Underflow.	Passed
Race Conditions and Reentrancy.	Passed
DoS with Revert.	Passed
DoS with block gas limit.	Passed
Methods execution permissions.	Passed
Economy model of the contract.	Passed
Private user data leaks.	Passed
Malicious Events Log.	Passed
Scoping and Declarations.	Passed
Uninitialized storage pointers.	Passed
Arithmetic accuracy.	Passed
Design Logic.	Passed
Impact of the exchange rate.	Passed
Oracle Calls.	Passed
Cross-function race conditions.	Passed
Fallback function security.	Passed

Safe Open Zeppelin contracts and implementation usage.	Passed
Whitepaper-Website-Contract correlation.	Not Checked
Front Running.	Not Checked

Owner's Functions

Alphaterra Contract

Owner of this contract renounces the ownership. New owner will be the Zero address.

```
function renounceOwnership() public virtual onlyOwner {
    emit OwnershipTransferred(_owner, address(0));
    _owner = address(0);
}
```

Transfers ownership of the contract to a new account (`newOwner`). Can only be called by the authorized address.

```
function transferOwnership(address newOwner) public virtual onlyOwner {
    require(newOwner != address(0), "Ownable: new owner is the zero address");
    emit OwnershipTransferred(_owner, newOwner);
    _owner = newOwner;
}
```

Owner of this contract locks the contract for self for specific "time".

```
function lock(uint256 time) public virtual onlyOwner {
    _previousOwner = _owner;
    _owner = address(0);
    _lockTime = now + time;
    emit OwnershipTransferred(_owner, address(0));
}
```

Owner of this contract excludes the "account" from fee payer list.

```
function excludeFromFee(address account) public onlyOwner {
    _isExcludedFromFee[account] = true;
}
```

Owner of this contract includes the "account" into fee payer List.

```
function includeInFee(address account) public onlyOwner {
    _isExcludedFromFee[account] = false;
}
```

Owner of this contract set the maximum value of token transfer per transaction.

```
function setMaxTxPercent(uint256 maxTxPercent) external onlyOwner() {
    _maxTxAmount = _tTotal.mul(maxTxPercent).div(
        10**2
    );
}
```

Owner of this contract updates the tax fee percentage.

```
function setTaxFee(uint256 taxFee) external onlyOwner() {
    _taxFee = _tTotal.mul(taxFee).div(
        10**2
    );
}
```

Owner of this contract updates the marketing fee percentage.

```
function setmarketingFee(uint256 marketingFee) external onlyOwner() {
    _marketingFee = _tTotal.mul(marketingFee).div(
        10**2
    );
}
```

Owner of this contract updates the liquidity fee percentage.

```
function setliquidityFee(uint256 liqFee) external onlyOwner() {
    _liquidityFee = _tTotal.mul(liqFee).div(
        10**2
    );
}
```

Owner of this contract updates the marketing wallet.

```
function setmarketingWallet(address newAdd) external onlyOwner() {
    marketingWallet = newAdd;
}
```

Owner of this contract updates the burn fee percentage.

```
function setBurnFee(uint256 BurnFee) external onlyOwner() {
    _burnFee = _tTotal.mul(BurnFee).div(
        10**2
    );
}
```

Owner of this contract flips the swap and liquify state.

```
function setSwapAndLiquifyEnabled(bool _enabled) public onlyOwner {
    swapAndLiquifyEnabled = _enabled;
    emit SwapAndLiquifyEnabledUpdated(_enabled);
}
```

Owner of this contract excludes the “account” from the reward list. Cannot exclude the router address which is “0x05fF2B0DB69458A0750badebc4f9e13aDd608C7F”.

```
function excludeFromReward(address account) public onlyOwner() {
    require(account != 0x05fF2B0DB69458A0750badebc4f9e13aDd608C7F,
    'We can not exclude Pancake router.');
    require(!_isExcluded[account], "Account is already excluded");
    if(_rOwned[account] > 0) {
        _tOwned[account] = tokenFromReflection(_rOwned[account]);
    }
    _isExcluded[account] = true;
    _excluded.push(account);
}
```

Owner of this contract includes the “account” into reward receivers list.

```
function includeInReward(address account) external onlyOwner() {
    require(_isExcluded[account], "Account is already excluded");
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (_excluded[i] == account) {
            _excluded[i] = _excluded[_excluded.length - 1];
            _tOwned[account] = 0;
            _isExcluded[account] = false;
            _excluded.pop();
            break;
        }
    }
}
```

Testing Summary

PASS

Block Solutions Believes
this smart contract security qualifications to passes listed be on digital asset exchanges.

21 November, 2022

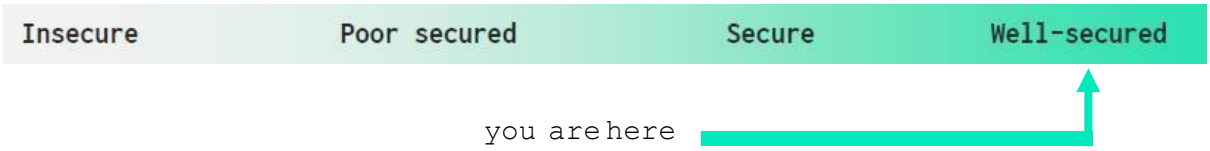
Quick Stats:

Main Category	Subcategory	Result
Contract Programming	Solidity version not specified	Passed
	Solidity version too old	Passed
	Integer overflow/underflow	Passed
	Function input parameters lack of check	Passed
	Function input parameters check bypass	Passed
	Function access control lacks management	Passed
	Critical operation lacks event log	Passed
	Human/contract checks bypass	Passed
	Random number generation/use vulnerability	Passed
	Fallback function misuse	Passed
	Race condition	Passed
	Logical vulnerability	Passed
	Other programming issues	Passed
Code Specification	Visibility not explicitly declared	Passed
	Var. storage location not explicitly declared	Passed
	Use keywords/functions to be deprecated	Passed
	Other code specification issues	Passed
Gas Optimization	Assert () misuse	Passed
	High consumption ‘for/while’ loop	Passed
	High consumption ‘storage’ storage	Passed
	“Out of Gas” Attack	Passed
Business Risk	The maximum limit for mintage not set	Passed
	“Short Address” Attack	Passed
	“Double Spend” Attack	Passed

Overall Audit Result: Passed

Executive Summary

According to the standard audit assessment, Customer`s solidity smart contract is Well-secured. Again, it is recommended to perform an Extensive audit assessment to bring a more assured conclusion.



We used various tools like Mythril, Slither and Remix IDE. At the same time this finding is based on critical analysis of the manual audit.
All issues found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the Quick Stat section.
We found 0 critical, 0 high, 0 medium and 0 low level issues.

Code Quality

The ALPHATERRA Smart Contract protocol consists of one smart contract. It has other inherited contracts like Context, IERC20, Ownable. These are compact and well written contracts. Libraries used in ALPHATERRA Smart Contract are part of its logical algorithm. They are smart contracts which contain reusable code. Once deployed on the blockchain (only once), it is assigned a specific address and its properties / methods can be reused many times by other contracts in protocol. The BLOCKSOLUTIONS team has **not** provided scenario and unit test scripts, which would help to determine the integrity of the code in an automated way. Overall, the code is not commented. Commenting can provide rich documentation for functions, return variables and more.

Documentation

As mentioned above, it's recommended to write comments in the smart contract code, so anyone can quickly understand the programming flow as well as complex code logic. We were given a ALPHATERRA Smart Contract smart contract code in the form of File.

Use of Dependencies

As per our observation, the libraries are used in this smart contract infrastructure that are based on well-known industry standard open-source projects. And even core code blocks are written well

and systematically. This smart contract does not interact with other external smart contracts.

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to token loss etc.
High	High-level vulnerabilities are difficult to exploit; however, they also have significant impact on smart contract execution, e.g. public access to crucial functions
Medium	Medium-level vulnerabilities are important to fix; however, they can't lead to tokens lose
Low	Low-level vulnerabilities are mostly related to outdated, unused etc. code snippets, that can't have significant impact on execution
Lowest / Code Style / Best Practice	Lowest-level vulnerabilities, code style violations and info statements can't affect smart contract execution and can be ignored.

Audit Findings

Critical

No Critical severity vulnerabilities were found.

High

No high severity vulnerabilities were found.

Medium

No Medium severity vulnerabilities were found.

Low

No Low severity vulnerabilities were found.

Conclusion

The Smart Contract code passed the audit. We were given a contract code. And we have used all possible tests based on given objects as files. Since possible test cases can be unlimited for such extensive smart contract protocol, hence we provide no such guarantee of future outcomes. We have used all the latest static tools and manual observations to cover maximum possible test cases to scan everything. Smart contracts within the scope were manually reviewed and analyzed with static analysis tools. Smart Contract's high-level description of functionality was presented in Quick Stat section of the report. Audit report contains all found security vulnerabilities and other issues in the reviewed code.
Security state of the reviewed contract is "Well Secured".

Our Methodology

We like to work with a transparent process and make our reviews a collaborative effort. The goals of our security audits are to improve the quality of systems we review and aim for sufficient remediation to help protect users. The following is the methodology we use in our security audit process.

Manual Code Review:

In manually reviewing all of the code, we look for any potential issues with code logic, error handling, protocol and header parsing, cryptographic errors, and random number generators. We also watch for areas where more defensive programming could reduce the risk of future mistakes and speed up future audits. Although our primary focus is on the in-scope code, we examine dependency code and behavior when it is relevant to a particular line of investigation.

Vulnerability Analysis:

Our audit techniques included manual code analysis, user interface interaction, and whitebox penetration testing. We look at the project's web site to get a high-level understanding of what functionality the software under review provides. We then meet with the developers to gain an appreciation of their vision of the software. We install and use the relevant software, exploring the user interactions and roles. While we do this, we brainstorm threat models and attack surfaces. We read design documentation, review other audit results, search for similar projects, examine source code dependencies, skim open issue tickets, and generally investigate details other than the implementation.

Documenting Results:

We follow a conservative, transparent process for analyzing potential security vulnerabilities and seeing them through successful remediation. Whenever a potential issue is discovered, we immediately create an Issue entry for it in this document, even though we have not yet verified the feasibility and impact of the issue. This process is conservative because we document our suspicions early even if they are later shown to not represent exploitable vulnerabilities. We generally, follow a process of first documenting the suspicion with unresolved questions, then

confirming the issue through code analysis, live experimentation, or automated tests. Code analysis is the most tentative, and we strive to provide test code, log captures, or screenshots demonstrating our confirmation. After this we analyze the feasibility of an attack in a live system.

Suggested Solutions:

We search for immediate mitigations that live deployments can take, and finally we suggest the requirements for remediation engineering for future releases. The mitigation and remediation recommendations should be scrutinized by the developers and deployment engineers, and successful mitigation and remediation is an ongoing collaborative process after we deliver our report, and before the details are made public.