



QuillAudits



Audit Report
April, 2021



BitBook

Contents

Audit Details and Target	01
Scope of Audit	03
Techniques and Methods	05
Issue Categories	06
Issues Found – Code Review/Manual Testing	08
Summary	09
Disclaimer	10

Audit Details and Target

1. Contract

<https://testnet.bscscan.com/address/0x44F85a0DAd0501A348bB21dcDa0422b9B3ED497F#code>

2. Audit Target

- To find the security bugs and issues regarding security, potential risks and critical bugs.
- Check gas optimization and check gas consumption.
- Check function reusability and code optimisation.
- Test the limit for token transfer and check the accuracy in decimals.
- Check the functions and naming conventions.
- Check the code for proper checks before every function call.
- Event trigger checks for security and logs.
- Checks for constant and function visibility and dependencies.
- Validate the standard functions and checks.
- Check the business logic and correct implementation.
- Automated script testing for multiple use cases including transfers, including values and multi transfer check.
- Automated script testing to check the validations and limit tests before every function call.
- Check the use of data type and storage optimisation.
- Calculation checks for different use cases based on the transaction, calculations and reflected values.

Functions list and audit details

1. Read Functions in Contract

- name()
- symbol()
- decimals()

- totalSupply()
- balanceOf()
- allowance()
- owner()

2. Write Function in Contract

- transfer()
- approve()
- transferFrom()
- increaseAllowance()
- decreaseAllowance()
- _transfer()
- _mint()
- _approve()
- renounceOwnership()
- transferOwnership()

Overview of BitDiamond

BitBook is a BEP20 compatible token with burn, mint, token transfer, hold token, check balance functionality. This contract follows all BEP20 Standard protocols. Smart contract checks all the balances, addresses before performing any operation.

This smart contract is designed with ownable functions to manage the owner of the smart contract.

Tokens are compatible with all types of BEP supporting wallets. These tokens can be used on all standard trading, staking or exchange platforms.

Smart contract have checks before sending, transfer, approve and burn the tokens for preventing any unexpected loss to the funds and minimize the chance of mistake during any transaction.

Gas usage is optimal and minimal for all the functions. Gas price depends on the complexity, time and blocks. This is checked in the BSC standard test net environment of BSC.

Tokenomics

As per the information provided, the tokens generated will be initially transferred to the contract owner and then further division will be done based on the business logic of the application.

Tokens cannot be directly purchased from the smart contract, so there will be an additional or third-party platform that will help users to purchase the tokens.

Tokens can be held, transferred and delegated freely. Contract owners can increase and decrease supply based on the business use case and supply management.

Scope of Audit

The scope of this audit was to analyse BitBook smart contracts codebase for quality, security, and correctness.

Checked Vulnerabilities

The smart contract is scanned and checked for multiple types of possible bugs and issues. This mainly focuses on issues regarding security, attacks, mathematical errors, logical and business logic issues. Here are some of the commonly known vulnerabilities that are considered:

- TimeStamp dependencies.
- Variable and overflow
- Calculations and checks
- SHA values checks
- Vulnerabilities check for use case
- Standard function checks
- Checks for functions and required checks
- Gas optimisations and utilisation
- Check for token values after transfer
- Proper value updates for decimals
- Array checks
- Safemath checks
- Variable visibility and checks
- Error handling and crash issues
- Code length and function failure check
- Check for negative cases
- D-DOS attacks
- Comments and relevance
- Address hardcoded
- Modifiers check
- Library function use check
- Throw and inline assembly functions
- Locking and unlocking (if any)
- Ownable functions and transfer ownership
- checksArray and integer overflow possibility checks
- Revert or Rollback transactions check

Techniques and Methods

- Manual testing for each and every test cases for all functions.
- Running the functions, getting the outputs and verifying manually for multiple test cases.
- Automated script to check the values and functions based on automated test cases written in JS frameworks.
- Checking standard function and check compatibility with multiple wallets and platforms
- <https://docs.google.com/document/d/1fivCY-Ib1DLj6GErriFP9R5DteBSTpPg2TuJ3pfcJyY/edit?usp=sharing>
Checks with negative and positive test cases.
- Checks for multiple transactions at the same time and checks d-dos attacks.
- Validating multiple addresses for transactions and validating the results in managed excel.
- Get the details of failed and success cases and compare them with the expected output.
- Verifying gas usage and consumption and comparing with other standard token platforms and optimizing the results.
Validate the transactions before sending and test the possibilities of attacks.

Structural Analysis

In this step we have analyzed the design patterns and structure of smart contracts. A thorough check was done to ensure the smart contract is structured in a way that will not result in future problems.
SmartCheck.

Code Review / Manual Analysis

Manual Analysis or review of code was done to identify new vulnerability or verify the vulnerabilities found during the static analysis. Contracts were completely manually analyzed, their logic was checked and compared with the one described in the whitepaper. Besides, the results of automated analysis were manually verified.

Static Analysis

Static Analysis of Smart Contracts was done to identify contract vulnerabilities. In this step a series of automated tools are used to test security of smart contracts.

Gas Consumption

In this step we have checked the behaviour of smart contracts in production. Checks were done to know how much gas gets consumed and possibilities of optimization of code to reduce gas consumption.

Tools and Platforms used for Audit

Remix IDE, Truffle, Truffle Team, Ganache, Solhint, Mythril, Slither, SmartCheck.

Issue Categories

High severity issues

Issues that must be fixed before deployment else they can create major issues.

Medium level severity issues

These issues will not create major issues in working but affect the performance of the smart contract.

Low level severity issues

These issues are more suggestions that should be implemented to refine the code in terms of gas, fees, speed and code accuracy

Informational

- Code is written in a very concise way which can be more informative and secure by more checks and modifier use.
- The use of variables and naming conventions can be minimized
- Gas use is proper and optimized as per the testing on the Ropsten test network and checking of the old transaction from this contract.
- **Suggestion:** There must be some locking function in case of any loss or security issue so that the admin can lock the contract in case of any security issue to the token.

Number of issues per severity

	High	Medium	Low	Total Issues
Open	0	0	0	0
Closed	2	2	0	4

Issues Found – Code Review / Manual Testing

High severity issues

- 1. Transfer and transferFrom functions failing due to use of owner only function inside public function.
Line number : 195
Line Number : 212
Testing Hash : <https://ropsten.etherscan.io/tx/0x0611b86089ebb160a853973ae01c406747e31f579d5460bc14efe983daf2a2af>

Resolved and Closed

```
ftrace | funcSig
95 function transfer(address recipient, uint256 amount) external ret
96     transfer(msgSender(), recipient, amount);
97     mint();
98     return true;
99 }
100
```

```
ftrace | funcSig
function transferFrom(address send
    transfer(sender, recipient, a
    approve(sender, msgSender(),
    mint();
    return true;
}
```


0x0611b86089ebb160a853973ae01c406747e31f579d5460bc14efe983daf2a2af ⓘ

❌ Fail with error 'Ownable: caller is not the owner'

10192254 2-Block Confirmations

Ⓢ 53 secs ago (May-07-2021 06:21:13 PM +UTC)

2. The above use case only passes for the smart contract owner. So this means only the contract owner can use this contract for token transfer functions. This is not recommended by the token standards of BEP20.

Resolved and Closed

Medium severity issues

1. Unused internal function at line 290, adding extra line of code, complexity to the smart contract.

Resolved and Closed

```
289  
290 ftrace | funcSig  
291 function burnFrom(address account, uint256 amount) internal {  
292     burn(account, amount);  
293     approve(account, msgSender(), allowances[account][msgSender()].sub(amount, "BEP20: burn amount exceeds allowance");  
294 }  
295
```

2. Burn function is open for all, this means anyone can burn their tokens and this will affect the supply. This is recommended that extra tokens should go to owner address else supply may be effected is function is open to everyone. **Line #241**

Resolved and Closed

```
240  
241 ftrace | funcSig  
242 function burn(uint256 amount) public returns (bool) {  
243     _burn(msgSender(), amount);  
244     return true;  
245 }
```

Low level severity issues

No low level issues found.

Closing Summary

All the major issues and suggestions are resolved. Contract is developed with a business logic for implementing mint and burn functions based on a specific business logic. Tokens are compatible with all type of supported wallets with the blockchain. Token can be hold, transfer and used freely as no further locking and restrictions on the use.

Disclaimer

QuillHash audit is not a security warranty, investment advice, or an endorsement of the BitBook platform. This audit does not provide a security or correctness guarantee of the audited smart contracts. The statements made in this document should not be interpreted as investment or legal advice, nor should its authors be held accountable for decisions made based on them. Securing smart contracts is a multistep process. One audit cannot be considered enough. We recommend that the BitBook Team put in place a bug bounty program to encourage further analysis of the smart contract by other third parties.



QuillAudits

📍 Canada, India, Singapore and United Kingdom

💻 audits.quillhash.com

✉️ hello@quillhash.com