soken

SMART CONTRACT SECURITY AUDIT

BitcoMine

November, 2021

Website: soken.io

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 19.11.2021

Contract Name: **BME**

Deployed address: **0xbcba01f7d6cc0a950464a4b98ba8358c4f6b69a0**

Total Supply: **900,000,000,000**

Token Tracker: **BME**

Decimals: **9**

Token holders: **53,140**

Transactions count: **110,052**

Top 100 holders dominance: **96.47%**

Audit Details

Project Name: **BitcoMine**

Language: **Solidity**

Compiler version: **v0.6.12**

Blockchain: **BSC**

Social Profiles

Project Website: **bitcominetoken.com**

Project Twitter: **bitcominetoken**

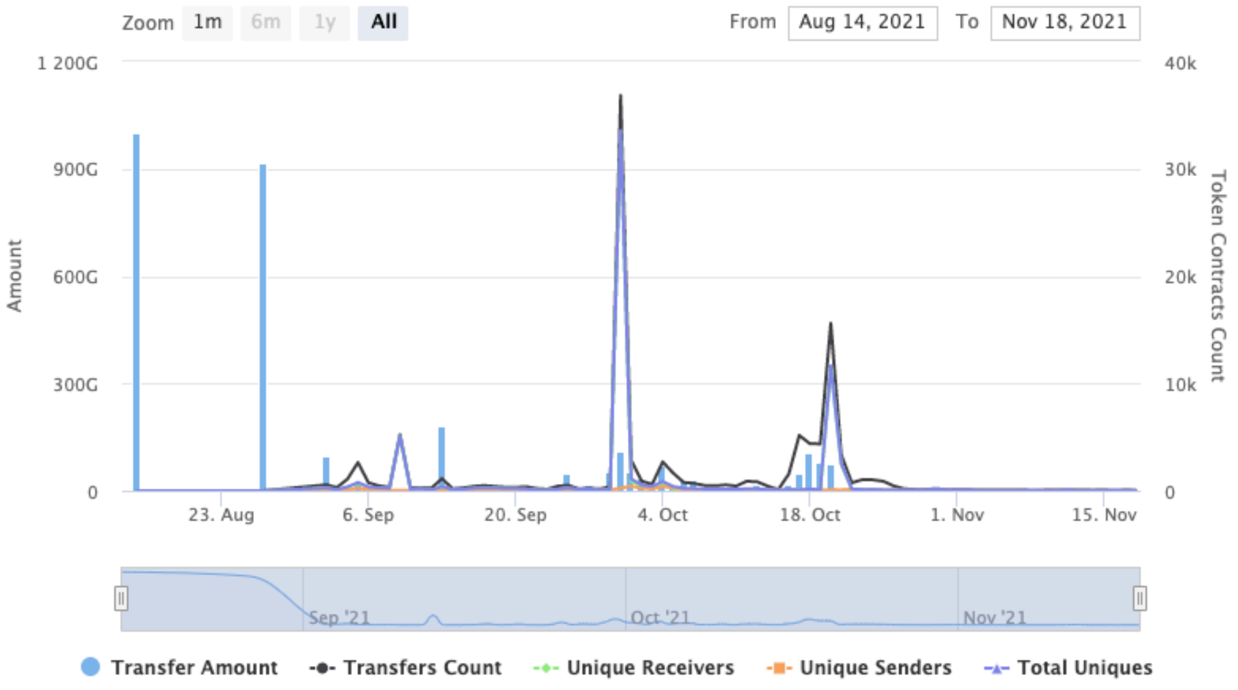
Project Announcement Telegram: **BitcoMineToken**

Project Medium: **https://bitcomine.medium.com/**

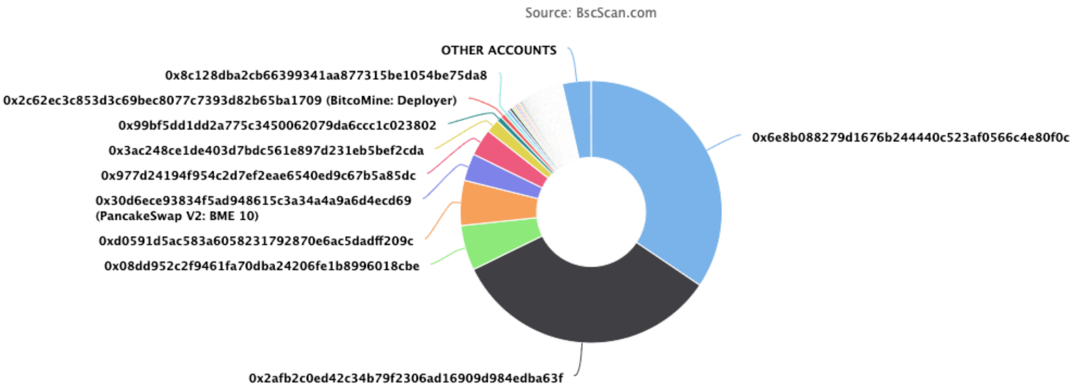
KYC Passed

CEO and CFO of Bitcomine project have passed KYC verification on behalf of Soken team. All personal data received from audited company will remain private until any fraudulent activity will happen.

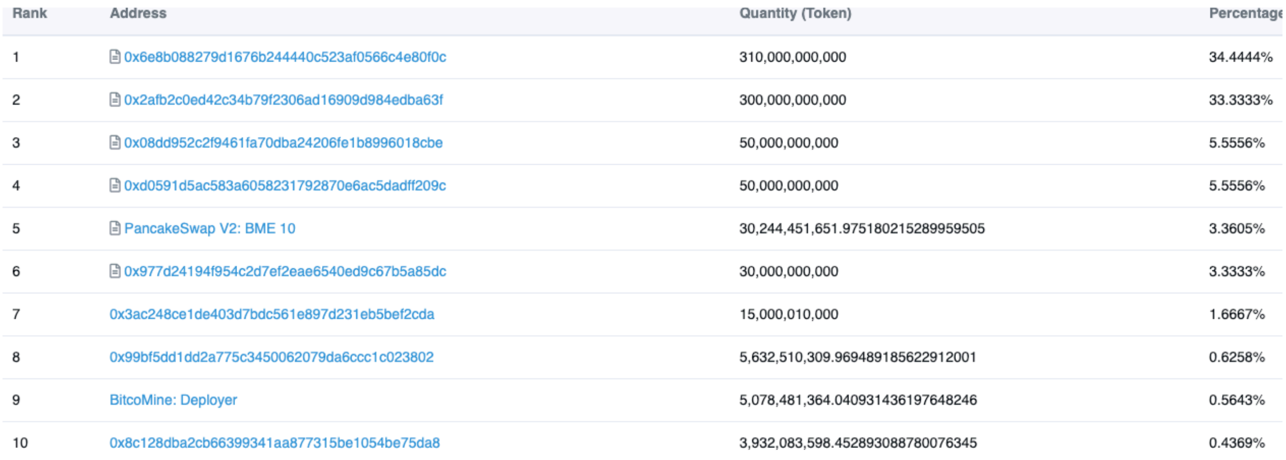
Token Contract Overview



BME Token Distribution



BME Top 10 Holders



Rank	Address	Quantity (Token)	Percentage
1	📄 0x6e8b088279d1676b244440c523af0566c4e80f0c	310,000,000,000	34.4444%
2	📄 0x2afb2c0ed42c34b79f2306ad16909d984edba63f	300,000,000,000	33.3333%
3	📄 0x08dd952c2f9461fa70dba24206fe1b8996018cbe	50,000,000,000	5.5556%
4	📄 0xd0591d5ac583a6058231792870e6ac5dadff209c	50,000,000,000	5.5556%
5	📄 PancakeSwap V2: BME 10	30,244,451,651.975180215289959505	3.3605%
6	📄 0x977d24194f954c2d7ef2eae6540ed9c67b5a85dc	30,000,000,000	3.3333%
7	0x3ac248ce1de403d7bdc561e897d231eb5bef2cda	15,000,010,000	1.6667%
8	0x99bf5dd1dd2a775c3450062079da6ccc1c023802	5,632,510,309.969489185622912001	0.6258%
9	BitcoMine: Deployer	5,078,481,364.040931436197648246	0.5643%
10	0x8c128dba2cb66399341aa877315be1054be75da8	3,932,083,598.452893088780076345	0.4369%

Swap Analysis

✔ Token is sellable (not a honeypot)

✔ Buy fee is less than 5% (0%)

✔ Sell fee is less than 5% (0%)

Contract Analysis

✔ Verified contract source

✔ No prior similar token contracts

✔ Source does not contain a proxy contract

✔ Source does not contain a pausable contract

✘ Ownership renounced or source does not contain an owner contract.

✔ Owner wallet contains less than 5% of token supply (1.67%)

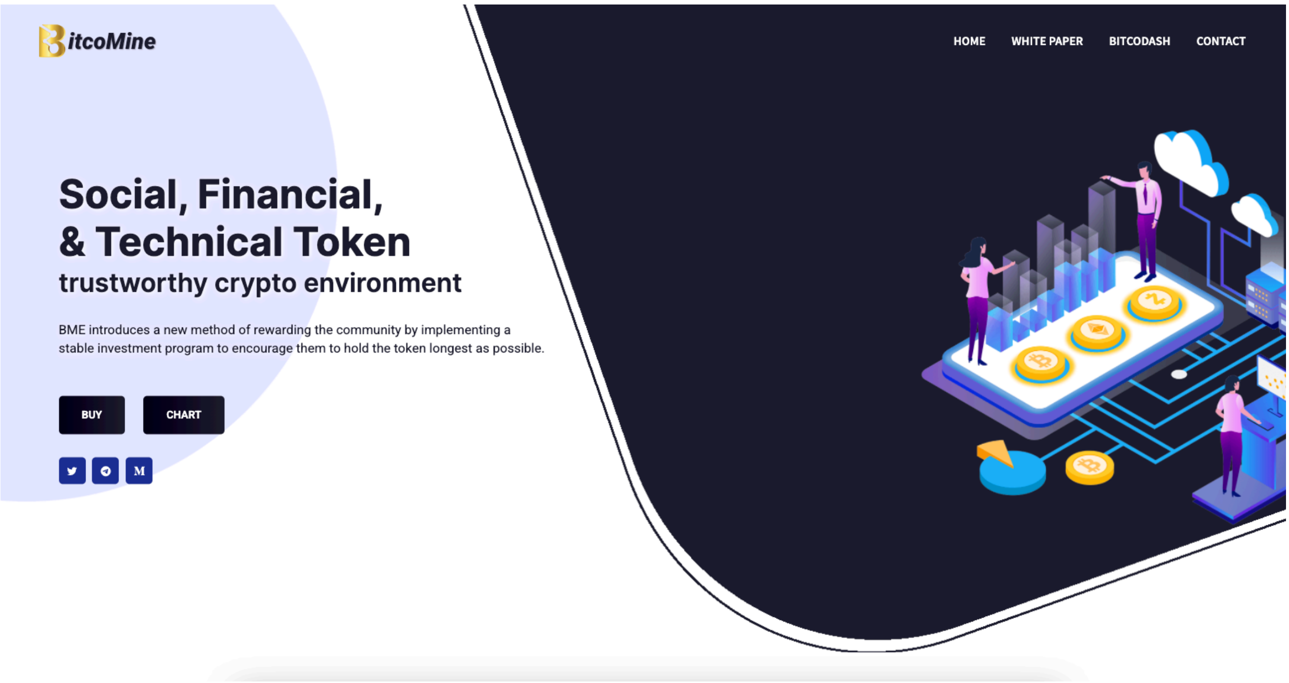
✔ Creator wallet contains less than 5% of token supply (0.56%)

✘ All other holders possess less than 5% of token supply

✔ Adequate liquidity present (336.34 BNB)

✔ At least 95% of liquidity burned/locked (98.68%)

Project Website Overview



BitcoMine

HOME WHITE PAPER BITCODASH CONTACT

Social, Financial, & Technical Token

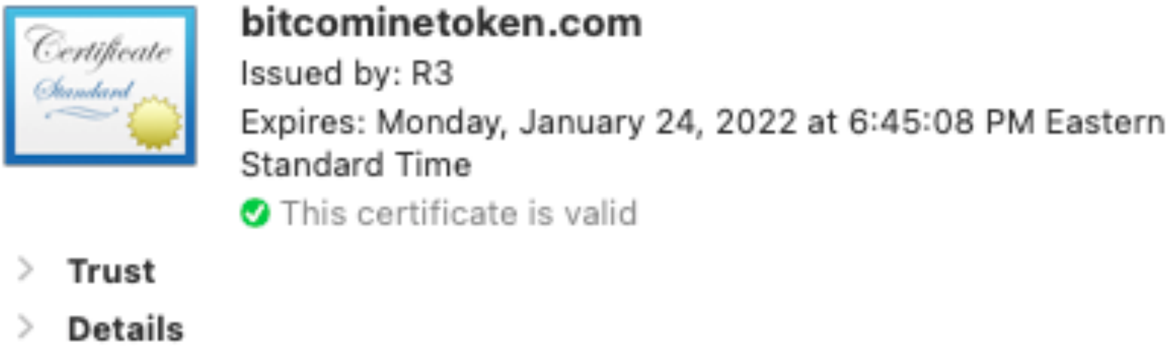
trustworthy crypto environment

BME introduces a new method of rewarding the community by implementing a stable investment program to encourage them to hold the token longest as possible.

BUY CHART

✓JavaScript errors hasn't been found.
✓Malware pop-up windows hasn't been detected.
✓No issues with loading elements, code, or stylesheets.

Project Website SSL Certification



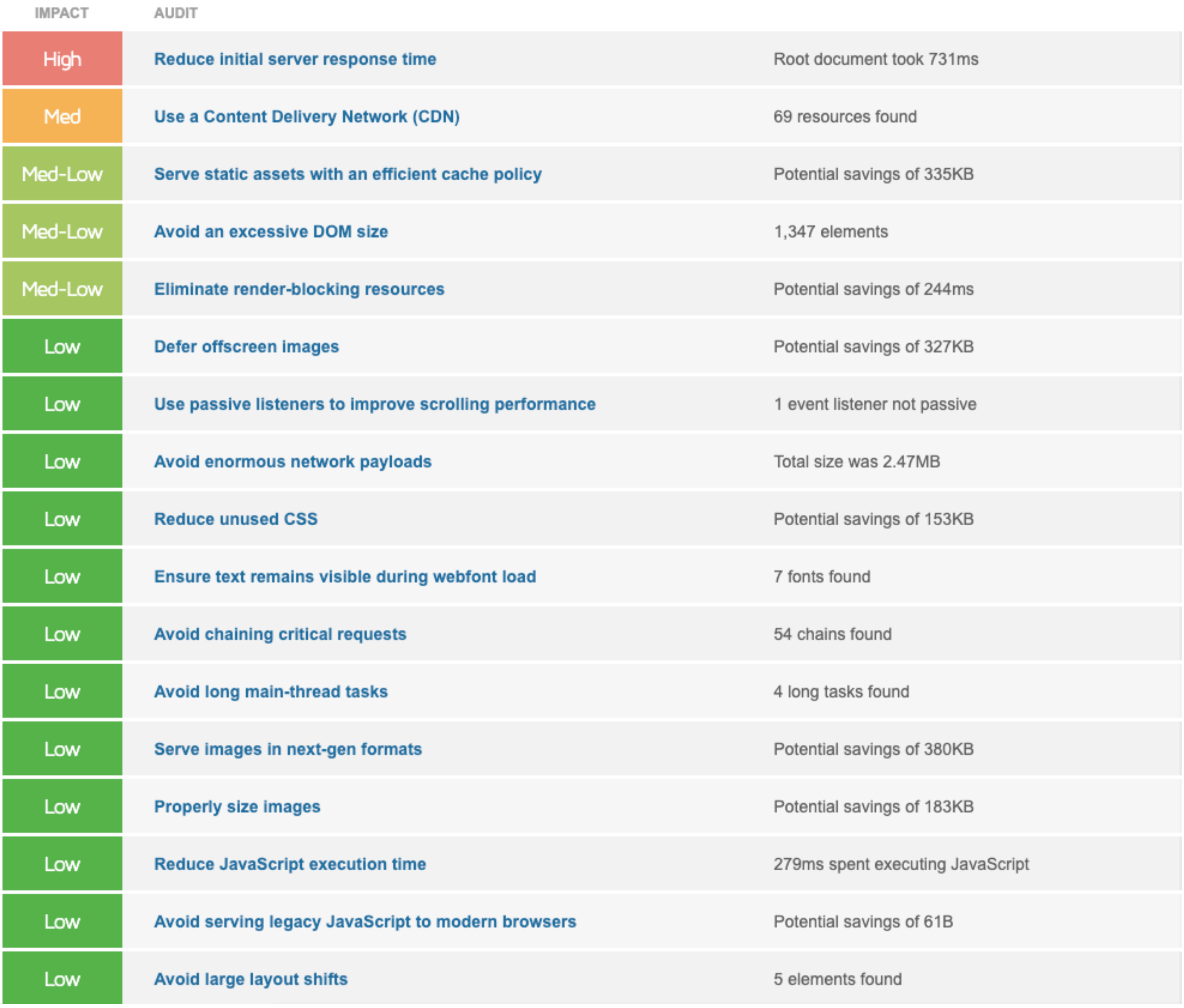
bitcominetoken.com

Issued by: R3

Expires: Monday, January 24, 2022 at 6:45:08 PM Eastern Standard Time

✓ This certificate is valid

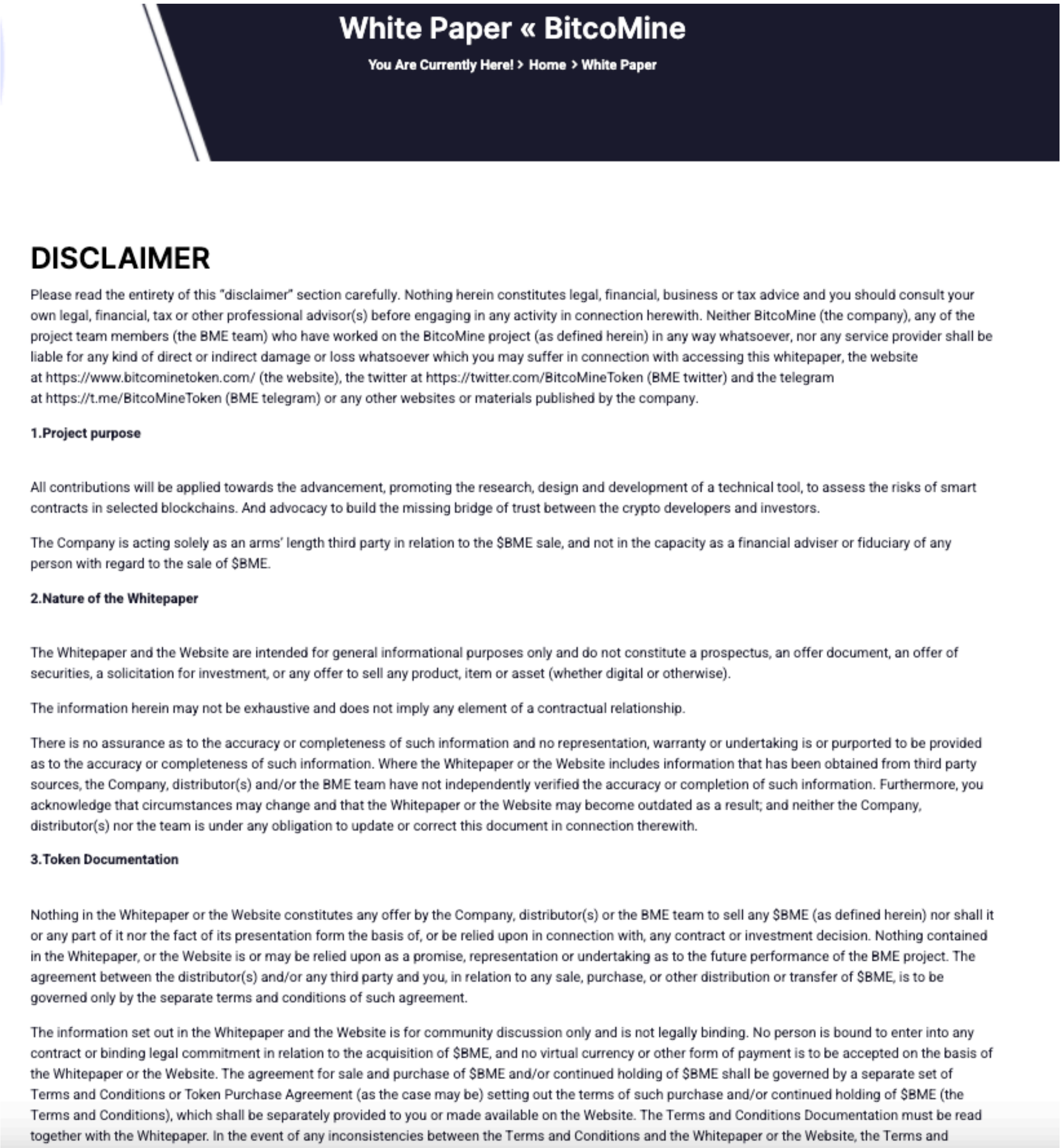
Project Website Performance Audit



IMPACT	AUDIT	
High	Reduce initial server response time	Root document took 731ms
Med	Use a Content Delivery Network (CDN)	69 resources found
Med-Low	Serve static assets with an efficient cache policy	Potential savings of 335KB
Med-Low	Avoid an excessive DOM size	1,347 elements
Med-Low	Eliminate render-blocking resources	Potential savings of 244ms
Low	Defer offscreen images	Potential savings of 327KB
Low	Use passive listeners to improve scrolling performance	1 event listener not passive
Low	Avoid enormous network payloads	Total size was 2.47MB
Low	Reduce unused CSS	Potential savings of 153KB
Low	Ensure text remains visible during webfont load	7 fonts found
Low	Avoid chaining critical requests	54 chains found
Low	Avoid long main-thread tasks	4 long tasks found
Low	Serve images in next-gen formats	Potential savings of 380KB
Low	Properly size images	Potential savings of 183KB
Low	Reduce JavaScript execution time	279ms spent executing JavaScript
Low	Avoid serving legacy JavaScript to modern browsers	Potential savings of 61B
Low	Avoid large layout shifts	5 elements found

Whitepsaper of the project

The whitepaper of Bitcomine project has been verified on behalf of Soken team.



White Paper « BitcoMine

You Are Currently Here! > Home > White Paper

DISCLAIMER

Please read the entirety of this "disclaimer" section carefully. Nothing herein constitutes legal, financial, business or tax advice and you should consult your own legal, financial, tax or other professional advisor(s) before engaging in any activity in connection herewith. Neither BitcoMine (the company), any of the project team members (the BME team) who have worked on the BitcoMine project (as defined herein) in any way whatsoever, nor any service provider shall be liable for any kind of direct or indirect damage or loss whatsoever which you may suffer in connection with accessing this whitepaper, the website at https://www.bitcominetoken.com/ (the website), the twitter at https://twitter.com/BitcoMineToken (BME twitter) and the telegram at https://t.me/BitcoMineToken (BME telegram) or any other websites or materials published by the company.

1.Project purpose

All contributions will be applied towards the advancement, promoting the research, design and development of a technical tool, to assess the risks of smart contracts in selected blockchains. And advocacy to build the missing bridge of trust between the crypto developers and investors.

The Company is acting solely as an arms' length third party in relation to the $BME sale, and not in the capacity as a financial adviser or fiduciary of any person with regard to the sale of $BME.

2.Nature of the Whitepaper

The Whitepaper and the Website are intended for general informational purposes only and do not constitute a prospectus, an offer document, an offer of securities, a solicitation for investment, or any offer to sell any product, item or asset (whether digital or otherwise).

The information herein may not be exhaustive and does not imply any element of a contractual relationship.

There is no assurance as to the accuracy or completeness of such information and no representation, warranty or undertaking is or purported to be provided as to the accuracy or completeness of such information. Where the Whitepaper or the Website includes information that has been obtained from third party sources, the Company, distributor(s) and/or the BME team have not independently verified the accuracy or completion of such information. Furthermore, you acknowledge that circumstances may change and that the Whitepaper or the Website may become outdated as a result; and neither the Company, distributor(s) nor the team is under any obligation to update or correct this document in connection therewith.

3.Token Documentation

Nothing in the Whitepaper or the Website constitutes any offer by the Company, distributor(s) or the BME team to sell any $BME (as defined herein) nor shall it or any part of it nor the fact of its presentation form the basis of, or be relied upon in connection with, any contract or investment decision. Nothing contained in the Whitepaper, or the Website is or may be relied upon as a promise, representation or undertaking as to the future performance of the BME project. The agreement between the distributor(s) and/or any third party and you, in relation to any sale, purchase, or other distribution or transfer of $BME, is to be governed only by the separate terms and conditions of such agreement.

The information set out in the Whitepaper and the Website is for community discussion only and is not legally binding. No person is bound to enter into any contract or binding legal commitment in relation to the acquisition of $BME, and no virtual currency or other form of payment is to be accepted on the basis of the Whitepaper or the Website. The agreement for sale and purchase of $BME and/or continued holding of $BME shall be governed by a separate set of Terms and Conditions or Token Purchase Agreement (as the case may be) setting out the terms of such purchase and/or continued holding of $BME (the Terms and Conditions), which shall be separately provided to you or made available on the Website. The Terms and Conditions Documentation must be read together with the Whitepaper. In the event of any inconsistencies between the Terms and Conditions and the Whitepaper or the Website, the Terms and

Whitepaper link: **https://bitcominetoken.com/white-paper/**

Contract Function Details

+ BME Contract.sol
- [Pub] isExIFFees
- [Prv] _setAMMPairs
- [Pub] updateGFProcess
- [Pub] updateUniswapV2Router
- [Pub] ExIFromF
- [Pub] setAMMPairs
- [Pub] MaxSA
- [Ext] getTotaldd
- [Ext] getTotalddBME
- [Ext] getTISBTC
- [Ext] getTISBME
- [Ext] getTotalNoH
- [Pub] WbIDofBTC
- [Pub] WbIDofBME
- [Ext] getAccountdI
- [Ext] ProcessDT
- [Ext] claim
- [Ext] getlastProcidx
- [Ext] setMinTtoGetR
- [Ext] ExIFromD
- [Int] _transfer
- [Prv] swapAndLiquify
- [Prv] AutoBurn
- [Pub] Burn
- [Prv] SwapTFETH
- [Prv] SwapTFBTC
- [Prv] addLiquidity
- [Prv] SWandSendBTCd
- [Int] _transfer
- [Pub] withdrawDividend
- [Ext] setMinTtoGetR
- [Ext] getAccountDividendsInfo
- [Ext] ExIFromD
- [Ext] getLastProcessedIndex
- [Ext] getNumberOfTokenHolders
- [Pub] getAccount
- [Ext] setBalance
- [Pub] process
- [Pub] processAccount

+ Context
- [Int] _msgSender
- [Int] _msgData

+ DividendPayingToken.sol
- [Pub] distributeDividends
- [Pub] withdrawDividend
- [Pub] _withdrawDividendOfUserBME
- [Pub] dividendOf
- [Pub] withdrawableDividendOf
- [Pub] withdrawnDividendOf
- [Pub] accumulativeDividendOf
- [Pub] setBMEadd
- [Pub] dividendOfBME
- [Pub] withdrawableDividendOfBME
- [Pub] withdrawnDividendOfBME
- [Pub] accumulativeDividendOfBME
- [Int] _mint
- [Int] _burn
- [Int] _mintBME
- [Int] _burnBME
- [Int] _setBalance
- [Int] _setBalanceBME

+ DividendPayingToken.sol
- [Pub] distributeBUSDDividends
- [Pub] withdrawDividend
- [Pub] _withdrawDividendOfUser
- [Pub] dividendOf
- [Pub] withdrawableDividendOf
- [Pub] withdrawnDividendOf
- [Pub] accumulativeDividendOf
- [Int] _transfer
- [Int] _mint
- [Int] _burn
- [Int] _setBalance

+ DividendPayingTokenInterface.sol
- [Ext] dividendOf
- [Ext] withdrawDividend

+ DividendPayingTokenOptionalInterface.sol
- [Ext] withdrawableDividendOf
- [Ext] withdrawnDividendOf
- [Ext] accumulativeDividendOf

+ ERC20 is Context, IERC20
- [Pub] name
- [Pub] symbol
- [Pub] decimals
- [Pub] totalSupply
- [Pub] balanceOf
- [Pub] transfer #
- [Pub] allowance
- [Pub] approve #
- [Pub] transferFrom #
- [Pub] increaseAllowance
- [Pub] decreaseAllowance
- [Int] _transfer
- [Int] _mint
- [Int] _burn
- [Int] _approve
- [Int] _beforeTokenTransfer

- +DividendPayingToken.sol
- [Ext] totalSupply
- [Ext] balanceOf
- [Ext] transfer #
- [Ext] allowance #
- [Ext] approve
- [Ext] transferFrom #

+ [Int] IERC20Metadata is IERC20
- [Ext] name
- [Ext] symbol
- [Ext] decimals

+ [Lib] IterableMapping.sol
- [Pub] get
- [Pub] getIndexOfKey
- [Pub] getKeyAtIndex
- [Pub] size
- [Pub] set
- [Pub] remove

+ [Int] IUniswapV2Factory
- [Ext] feeTo
- [Ext] feeToSetter
- [Ext] getPair
- [Ext] allPairs

- [Ext] allPairsLength
- [Ext] createPair #
- [Ext] setFeeTo #
- [Ext] setFeeToSetter #

+ [Int] IUniswapV2Pair
- [Ext] name
- [Ext] symbol
- [Ext] decimals
- [Ext] totalSupply
- [Ext] balanceOf
- [Ext] allowance
- [Ext] approve #
- [Ext] transfer #
- [Ext] transferFrom #
- [Ext] DOMAIN_SEPARATOR
- [Ext] PERMIT_TYPEHASH
- [Ext] nonces
- [Ext] permit #
- [Ext]_LIQUIDITY
- [Ext] factory
- [Ext] token0
- [Ext] token1
- [Ext] getReserves
- [Ext] price0CumulativeLast
- [Ext] price1CumulativeLast
- [Ext] kLast
- [Ext] mint
- [Ext] burn #
- [Ext] swap #
- [Ext] skim #
- [Ext] sync #
- [Ext] initialize #

+ [Int] IUniswapV2Router01
- [Ext] factory
- [Ext] WETH
- [Ext] addLiquidity #
- [Ext] addLiquidityETH ($)
- [Ext] removeLiquidity #
- [Ext] removeLiquidityETH #
- [Ext] removeLiquidityWithPermit #
- [Ext] removeLiquidityETHWithPermit #
- [Ext] swapExactTokensForTokens #
- [Ext] swapTokensForExactTokens #

- [Ext] swapExactETHForTokens ($)
- [Ext] swapTokensForExactETH #
- [Ext] swapExactTokensForETH #
- [Ext] swapETHForExactTokens ($)
- [Ext] quote
- [Ext] getAmountOut
- [Ext] getAmountIn
- [Ext] getAmountsOut
- [Ext] getAmountsIn

+ [Int] IUniswapV2Router02 (IUniswapV2Router01)
- [Ext] removeLiquidityETHSupportingFeeOnTransferTokens #
- [Ext] removeLiquidityETHWithPermitSupportingFeeOnTransferTokens #
- [Ext] swapExactTokensForTokensSupportingFeeOnTransferTokens #
- [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens ($)
- [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #

+ Ownable.sol (Context)
- [Pub] <Constructor> #
- [Pub] owner
- [Pub] renounceOwnership #
    - modifiers: onlyOwner
- [Pub] transferOwnership #
    - modifiers: onlyOwner

+ [Lib] SafeMath
- [Int] add
- [Int] sub
- [Int] sub
- [Int] mul
- [Int] div
- [Int] div
- [Int] mod
- [Int] mod

+ [Lib] SafeMathInt
- [Int] mul
- [Int] div
- [Int] sub
- [Int] add
- [Int] abs
- [Int] toUint256Safe

+ [Lib] SafeMathUint
- [Int] toUint256Safe

($) = payable function
# = non-constant function

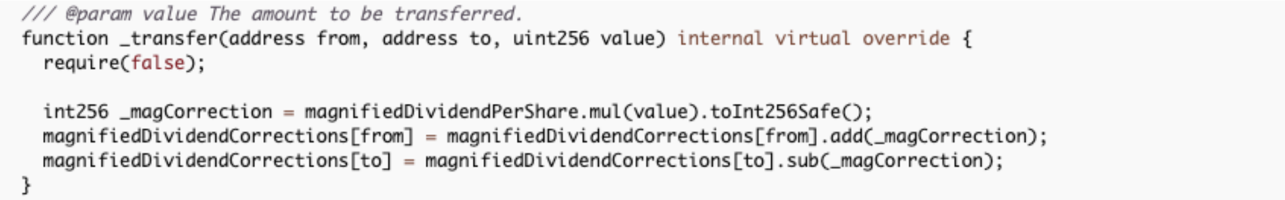
Vulnerabilities checking

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) Unreachable code:

Given the require(false) statement, the code block will never be executed and is unnecessary.



```
/// @param value The amount to be transferred.
function _transfer(address from, address to, uint256 value) internal virtual override {
  require(false);

  int256 _magCorrection = magnifiedDividendPerShare.mul(value).toInt256Safe();
  magnifiedDividendCorrections[from] = magnifiedDividendCorrections[from].add(_magCorrection);
  magnifiedDividendCorrections[to] = magnifiedDividendCorrections[to].sub(_magCorrection);
}
```

Recommendation:

We recommend removing the unreachable / unnecessary code block

2) Missing Emit Events:

The function that affects the status of sensitive variables should be able to emit events as notifications to customers. E.g. _transfer( ) ; setBalance()

Recommendation:

We recommend adding events for sensitive actions, and emit them in the function.

3) Owner privileges:

The function that affects the status of sensitive variables should be able to emit events as notifications to customers. E.g. _transfer( ) ; setBalance()

Recommendation:

We recommend adding events for sensitive actions, and emit them in the function.

4) Volatile Code:

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

Recommendation:

We recommend using variables to receive the return value of the functions mentioned above and handle both success and failure cases if needed by the business logic.

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