SAFUAUDIT
SMART CONTRACT AUDITING

DAOBAO

SMART CONTRACT AUDIT

February 21, 2022

INTRODUCTION

Client	DAOBAO
Language	Solidity
Contract address	0x21982F0A78e8248f7318Aa7DD6c19dAac9018ECb
Website	https://daobao.tech/
Telegram	https://t.me/DAOBAOFinance
Twitter	https://twitter.com/DAOBAOFinance

Description

DAOBAO is positioned to lead a revolution in DeFi with the $BAO Autostaking and Auto-Compounding Protocol or BAP, a new financial protocol that makes staking easier, and gives $BAO token holders the highest stable returns in crypto.

TABLE OF CONTENTS

Approach

Audit Details

Our comprehensive audit report provides a full overview of the audited system's architecture, smart contract codebase, and details on any vulnerabilities found within the system.

Audit Goals

The audit goal is to ensure that the project is built to protect investors and users, preventing potentially catastrophic vulnerabilities after launch, that lead to scams and rugpulls.

,

Code Quality

Our analysis includes both automatic tests and manual code analysis for the following aspects:

- Exploits
- Back-doors
- Vulnerability
- Accuracy
- Readability

Tools

- Remix IDE
- MythX, Mythril
- SWC Registry
- Open Zeppelin Code Analyzer
- Solidity Code Complier

RISK CLASSIFICATION

CRITICAL

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

MEDIUM

Issues on this level could potentially bring problems and should eventually be fixed.

LOW

Issues on this level are minor details and warnings that can remain unfixed but would be better fixed at some point in the future

INFORMATIONAL

Information level is to offer suggestions for improvement of efficacity or security for features with a risk free factor.

ABSTRACT

Fees	Rebase	Mint function
Buy Fees: 13% Sell Fees: 18%	Yes	No manual mint function found

Owner can set fees	Max Tx amount	Pause
Owner can't set the buy/sell fees	Owner can set max tx amount	Owner can't pause trading

SWC Attacks

SWC ID	Description	
SWC-100	Function Default Visibility	Passed
SWC-101	Integer Overflow and Underflow	Passed
SWC-102	Outdated Compiler Version	Passed
SWC-103	Floating Pragma	Low
SWC-104	Unchecked Call Return Value	Passed
SWC-105	Unprotected Ether Withdrawal	Passed
SWC-106	Unprotected SELF-DESTRUCT Instruction	Passed
SWC-107	Re-entrancy	Passed
SWC-108	State Variable Default Visibility	Low
SWC-109	Uninitialized Storage Pointer	Passed
SWC-110	Assert Violation	Passed
SWC-111	Use of Deprecated Solidity Functions	Passed
SWC-112	Delegate Call to Untrusted Callee	Passed
SWC-113	DoS with Failed Call	Passed
SWC-114	Transaction Order Dependence	Passed
SWC-115	Authorization through tx.origin	Passed

SWC-116	Block values as a proxy for time	**Passed**
SWC-117	Signature Malleability	**Passed**
SWC-118	Incorrect Constructor Name	**Passed**
SWC-119	Shadowing State Variables	**Passed**
SWC-120	Weak Sources of Randomness from Chain Attributes	**Passed**
SWC-121	Missing Protection against Signature Replay Attacks	**Passed**
SWC-122	Lack of Proper Signature Verification	**Passed**
SWC-123	Requirement Violation	**Passed**
SWC-124	Write to Arbitrary Storage Location	**Passed**
SWC-125	Incorrect Inheritance Order	**Passed**
SWC-126	Insufficient Gas Griefing	**Passed**
SWC-127	Arbitrary Jump with Function Type Variable	**Passed**
SWC-128	DoS With Block Gas Limit	**Passed**
SWC-129	Typographical Error	**Passed**
SWC-130	Right-To-Left-Override control character (U+202E)	**Passed**
SWC-131	Presence of unused variables	**Passed**
SWC-132	Unexpected Ether balance	**Passed**
SWC-133	Hash Collisions With Multiple Variable Length Arguments	**Passed**
SWC-134	Message call with the hardcoded gas amount	**Passed**
SWC-135	Code With No Effects (Irrelevant/Dead Code)	**Passed**
SWC-136	Unencrypted Private Data On-Chain	**Passed**

MANUAL ANALYSIS

The contract is verified to check if functions do and work as they should and malicious code is not inserted.

	Tested	Result
Transfer	Yes	**Passed**
Total Supply	Yes	**Passed**
Buy Back	Yes	**NA**
Burn	Yes	**Passed**
Mint	Yes	**NA**
Rebase	Yes	**Passed**
Pause	Yes	**NA**
Blacklist	Yes	**NA**
Lock	Yes	**NA**
Max Transaction	Yes	**Low**
Transfer Ownership	Yes	**Passed**
Renounce Ownership	Yes	**Passed**

MANUAL AUDIT

Important snippets

Owner can set max sell amount

```
function setMaxSellTransaction(uint256 _maxTxn) external onlyOwner {
    maxSellTransactionAmount = _maxTxn;
}
```

The owner can update the reward yield and the reward yield denominator.

```
function setRewardYield(uint256 _rewardYield, uint256 _rewardYieldDenominator)
external onlyOwner {
    rewardYield = _rewardYield;
    rewardYieldDenominator = _rewardYieldDenominator;
}
```

Owner can exclude multiple Addreses from fees

```
function setFeeExempt(address _addr, bool _value) external onlyOwner {
    require(_isFeeExempt[_addr] != _value, "Not changed");
    _isFeeExempt[_addr] = _value;
}
```

Owner can trigger manual rebase

```
function manualRebase() external onlyOwner{
    require(!inSwap, "Try again");
    require(nextRebase <= block.timestamp, "Not in time");

    uint256 circulatingSupply = getCirculatingSupply();
    int256 supplyDelta = int256(circulatingSupply.mul(rewardYield).div(rewardYieldDenominator));

    coreRebase(supplyDelta);
    manualSync();
}
```

WEBSITE

Website	https://daobao.tech/
Domain Registry	http://www.namecheap.com
Domain Valability	Expires on 2023-02-15
Response Code	200
SSL Checker and HTTPS Test	Passed
Deprecated HTML tags	Passed
Robots.txt	Informational
Sitemap Test	Informational
SEO Friendly URL	Passed
Responsive Test	Passed
JS Error Test	Passed
Console Errors Test	Informational
Site Loading Speed Test	Passed 1.69s
HTTP2 Test	Passed
Safe Browsing Test	Passed

DISCLAIMER

SafuAudit.com is not a financial institution and the information provided on this website does not constitute investment advice, financial advice, trading advice or any other sort of advice. You should not treat any of the website's content as such. Investing in crypto assets carries a high level of risk and does not hold guarantees for not sustaining financial loss due to their volatility.

Accuracy of Information

SafuAudit will strive to ensure accuracy of information listed on this website although it will not hold any responsibility for any missing or wrong information. SafuAudit provides all information as is. You understand that you are using any and all information available here at your own risk. Any use or reliance on our content and services is solely at your own risk and discretion.

The purpose of the audit is to analyse the on-chain smart contract source code, and to provide basic overview of the project.

While we have used all the information available to us for this straightforward investigation, you should not rely on this report only — we recommend proceeding with several independent audits Be aware that smart contracts deployed on a blockchain aren't secured enough against external vulnerability, or a hack. Be aware that active smart contract owner privileges constitute an elevated impact to smart contract's safety and security. Therefore, SafuAudit does not guarantee the explicit security of the audited smart contract. The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.

AUDIT RESULTS

CRITICAL

No critical severity issues have been found.

MEDIUM

No medium severity issues have been found.

LOW

1. Owner can set Max Transaction amount to 0

2. Floating Pragma - Locking the pragma helps to ensure that contracts do not accidentally get deployed using, for example, an outdated compiler version that might introduce bugs that affect the contract system negatively

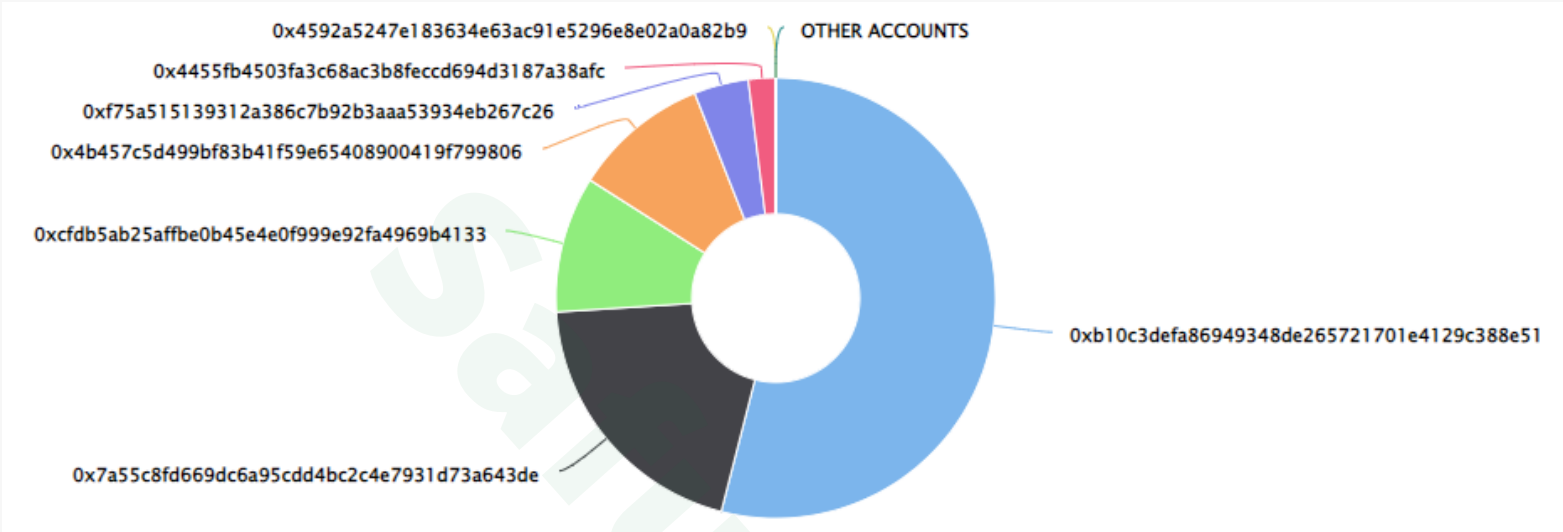
3. State Variable Default Visibility - Labeling the visibility explicitly makes it easier to catch incorrect assumptions about who can access the variable.

INFORMATIONAL

The standard audit model does not offer suggestions and consulting for improvements of the smart contract.

SUMMARY

Top 10 holders



1	0xb10c3defa86949348de265721701e4129c388e51	2,699,999,998.56	54.0000%
2	0x7a55c8fd669dc6a95cdd4bc2c4e7931d73a643de	1,000,000,000	20.0000%
3	0xcfdb5ab25affbe0b45e4e0f999e92fa4969b4133	500,000,000	10.0000%
4	0x4b457c5d499bf83b41f59e65408900419f799806	500,000,000	10.0000%
5	0xf75a515139312a386c7b92b3aaa53934eb267c26	200,000,000	4.0000%
6	0x4455fb4503fa3c68ac3b8feccd694d3187a38afc	100,000,000	2.0000%
7	0x4592a5247e183634e63ac91e5296e8e02a0a82b9	1.44	0.0000%

Conclusion

Project DaoBao does not contain any severe issues! SafuAudit has tested the security based on manual and automated tests. Please note that we don't offer any warranties for business model.