Cyberscope

A TAC Security Company

Audit Report

Data Backed Stable Coin

November 2025

Network	BSC
Address	0xdd30cb833fAe1761B4E9E5ad76025ff3Ae450Ef1
Audited by	© cyberscope

Analysis

Critical Medium Minor / Informative Pass

Severity	Code	Description	Status
●	ST	Stops Transactions	Passed
●	OTUT	Transfers User's Tokens	Passed
●	ELFM	Exceeds Fees Limit	Passed
●	MT	Mints Tokens	Acknowledged
●	BT	Burns Tokens	Passed
●	BC	Blacklists Addresses	Passed

Diagnostics

Critical Medium Minor / Informative

Severity	Code	Description	Status
●	CCR	Contract Centralization Risk	Acknowledged

Table of Contents

Risk Classification

The criticality of findings in Cyberscope's smart contract audits is determined by evaluating multiple variables. The two primary variables are:

1. **Likelihood of Exploitation**: This considers how easily an attack can be executed, including the economic feasibility for an attacker.
2. **Impact of Exploitation**: This assesses the potential consequences of an attack, particularly in terms of the loss of funds or disruption to the contract's functionality.

Based on these variables, findings are categorized into the following severity levels:

1. **Critical**: Indicates a vulnerability that is both highly likely to be exploited and can result in significant fund loss or severe disruption. Immediate action is required to address these issues.
2. **Medium**: Refers to vulnerabilities that are either less likely to be exploited or would have a moderate impact if exploited. These issues should be addressed in due course to ensure overall contract security.
3. **Minor**: Involves vulnerabilities that are unlikely to be exploited and would have a minor impact. These findings should still be considered for resolution to maintain best practices in security.
4. **Informative**: Points out potential improvements or informational notes that do not pose an immediate risk. Addressing these can enhance the overall quality and robustness of the contract.

Severity	Likelihood / Impact of Exploitation
Critical	Highly Likely / High Impact
Medium	Less Likely / High Impact or Highly Likely/ Lower Impact
Minor / Informative	Unlikely / Low to no Impact

Review

Contract Name	DataBackedStableCoin
Compiler Version	v0.8.27+commit.40a35a09
Optimization	200 runs
Explorer	https://bscscan.com/address/0xdd30cb833fae1761b4e9e5ad76025ff3ae450ef1
Address	0xdd30cb833fae1761b4e9e5ad76025ff3ae450ef1
Network	BSC
Symbol	DBSC
Decimals	18

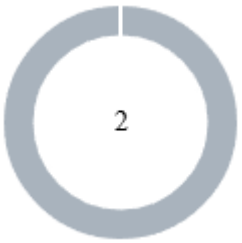
Audit Updates

Initial Audit	10 Nov 2025 https://github.com/cyberscope-io/audits/tree/main/dbsc/v1/audit.pdf
Corrected Phase 2	26 Nov 2025

Source Files

Filename	SHA256
contracts/DataBackedStableCoin.sol	6312a7a7862f26c15111e2d7cf7e1c46d37a976da3c912606d68cdde95b6eecf

Findings Breakdown



Critical	0
Medium	0
Minor / Informative	2

Severity	Unresolved	Acknowledged	Resolved	Other
Critical	0	0	0	0
Medium	0	0	0	0
Minor / Informative	0	2	0	0

MT - Mints Tokens

Criticality	Critical
Location	DBSC_Final.sol#L209
Status	Acknowledged

Description

Any address granted the `MINTER_ROLE` is authorized to mint new tokens. The `DEFAULT_ADMIN_ROLE` holder has control over assigning the `MINTER_ROLE` for any address. Since the admin can grant themselves (or another address) minting permissions, they can mint additional tokens. As a result, the contract tokens will be highly inflated.

```shell
function mint(address to, uint256 amount) public
onlyRole(MINTER_ROLE){
_mint(to, amount);
emit TokensMinted(to, amount);}
```

Recommendation

The team should carefully manage the private keys of the `DEFAULT_ADMIN_ROLE` and `MINTER_ROLE` accounts. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions.

Temporary Solutions:

These measurements do not decrease the severity of the finding

- Introduce a time-locker mechanism with a reasonable delay.
- Introduce a multi-signature wallet so that many addresses will confirm the action.
- Introduce a governance model where users will vote about the actions.

Permanent Solution:

- Renouncing all roles, which will eliminate the threats but it is non-reversible.

CCR - Contract Centralization Risk

Criticality	Minor / Informative
Location	DBSC_Final.sol#L82,209
Status	Acknowledged

Description

The contract's functionality and behavior are heavily dependent on external parameters or configurations. While external configuration can offer flexibility, it also poses several centralization risks that warrant attention. Centralization risks arising from the dependence on external configuration include Single Point of Control, Vulnerability to Attacks, Operational Delays, Trust Dependencies, and Decentralization Erosion.

Shell

```
function scheduleRoleChange(bytes32 role, address account,
bool grant)
external
onlyRole(DEFAULT_ADMIN_ROLE)
returns (uint256 changeId)
{
require(account != address(0), "zero account");
uint64 eta = uint64(block.timestamp + roleChangeDelay);

changeId = ++_nextChangeId;
scheduledChanges[changeId] = ScheduledChange({
account: account,
role: role,
grant: grant,
executeAfter: eta,
exists: true
});

emit RoleChangeScheduled(changeId, role, account, grant, eta);

}
```

```shell
function mint(address to, uint256 amount)
public
onlyRole(MINTER_ROLE)
{
_mint(to, amount);
emit TokensMinted(to, amount);

}
```

Recommendation

To address this finding and mitigate centralization risks, it is recommended to evaluate the feasibility of migrating critical configurations and functionality into the contract's codebase itself. This approach would reduce external dependencies and enhance the contract's self-sufficiency. It is essential to carefully weigh the trade-offs between external configuration flexibility and the risks associated with centralization.

Functions Analysis

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
DataBackedStableCoin	Implementation	ERC20, ERC20Permit, AccessControl		
		Public	✓	ERC20 ERC20Permit
	scheduleRoleChange	External	✓	onlyRole
	cancelRoleChange	External	✓	onlyRole
	executeRoleChange	External	✓	-
	grantRole	Public	✓	onlyRole
	revokeRole	Public	✓	onlyRole
	mint	Public	✓	onlyRole
	burn	Public	✓	onlyRole
	burnFrom	Public	✓	onlyRole
	supportsInterface	Public		-

Summary

Data Backed Stable Coin contract implements a token mechanism. This audit investigates security issues, business logic concerns and potential improvements. There are some functions that can be abused by the administrator like mint tokens. If the contract administrator abuses the mint functionality, then the contract will be highly inflated. A multi-wallet signing pattern will provide security against potential hacks. Temporarily locking the contract or renouncing the role will eliminate all the contract threats.

Disclaimer

The information provided in this report does not constitute investment, financial or trading advice and you should not treat any of the document's content as such. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes nor may copies be delivered to any other person other than the Company without Cyberscope's prior written consent. This report is not nor should be considered an "endorsement" or "disapproval" of any particular project or team. This report is not nor should be regarded as an indication of the economics or value of any "product" or "asset" created by any team or project that contracts Cyberscope to perform a security assessment. This document does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors' business, business model or legal compliance. This report should not be used in any way to make decisions around investment or involvement with any particular project. This report represents an extensive assessment process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk Cyberscope's position is that each company and individual are responsible for their own due diligence and continuous security Cyberscope's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies and in no way claims any guarantee of security or functionality of the technology we agree to analyze. The assessment services provided by Cyberscope are subject to dependencies and are under continuing development. You agree that your access and/or use including but not limited to any services reports and materials will be at your sole risk on an as-is where-is and as-available basis Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives false negatives and other unpredictable results. The services may access and depend upon multiple layers of third parties.

About Cyberscope

Cyberscope is a TAC blockchain cybersecurity company that was founded with the vision to make web3.0 a safer place for investors and developers. Since its launch, it has worked with thousands of projects and is estimated to have secured tens of millions of investors' funds.

Cyberscope is one of the leading smart contract audit firms in the crypto space and has built a high-profile network of clients and partners.

A **TAC Security** Company

The Cyberscope team

cyberscope.io