AUDIT+

Integrity | Transparency | Assurance

Audit requested by Dawks MEMES

0xF4818B6755599E268BB932a3bB829495590E3e1f

14th June 2023

Table of Contents

1. Audit Summary

Token Name	Dawks MEMES
Token Symbol	DAWK
Contract Address	0xF4818B6755599E268BB932a3bB829495590E3e1f
Block Explorer	https://bscscan.com/token/0xF4818B6755599E268BB932a3bB829495590E3e1f
Blockchain	BNB Chain
Audit Date	14th June 2023

All reports prepared by Audit+ are based on the findings of a manual static code review and the results of test transactions on an appropriate EVM based testnet.

An audit is only performed on deployed smart contracts that are verified on the respective block explorer. This is to ensure no code is changed from the time of audit to the time of deployment. Smart contracts that are not owned by the project team are not audited.

Additionally, a contract is deemed Audit+ verified when a smart contract shows **zero** potential for a runtime issue to occur which prevents the trading of the token for one or more individuals.

Audit Overview

GoPlus Labs

Attention Items	1
Risky Items	0

SWC Test Cases

Ignored	1
Fail	0
Pass	36

Testnet Examination

Token Transfer	Success
Token Buy via DEX	Success
Token Sell via DEX	Success

Manual Review

Low Risk	0
Moderate Risk	0
High Risk	0

Audit+ Verified

Status	Passed

Audit+ checks all functions within a contract to see whether there is any way for an owner or bad actor to prevent trading.

Dawks MEMES is Audit+ verified as it has **passed** all the necessary checks and the token is deemed unruggable through code.

2. Disclaimer

This audit has been prepared by the Audit+ team at the request of the client.

This report is intended for **informational purposes only** so a reader can understand the potential risks of the smart contract at runtime. A development team may use this information to iterate and improve their code or to merely have assurance that their smart contract performs as intended.

Audit+ is not responsible if the audited project performs an exit scam to deceive investors and is not responsible for any financial losses. This audit is not for determining the safety of an investment but to validate whether the smart contract functions as intended and to identify if any possible runtime issues can occur. Audit+ never endorses, recommends, or suggests investing in a project.

Please, always consider your risks before you make any investment and **always do your own research**.

3. GoPlus Labs

The GoPlus Labs token security API utilises the latest technologies to detect over 30 common security issues with token contracts. We run these checks on a preliminary basis to give a short, comprehensive overview to a reader.

Risk Classification

Ignored	Test was not relevant to the smart contract
Attention	Low-medium risk. This should be investigated further.
Risky	High risk. Investigate further and understand the necessity of such functions

Findings

Ignored Items

There were **two security items** classified under "Ignored".

Item	Reason
Buy Tax	Buy tax has been verified to be no higher than 2%.
Sell Tax	Sell tax has been verified to be no higher than 10%.

Attention Items

There was **one security item** classified under "Attention".

Item	Description
Tax can be modified	Tax can be modified from the starting values and in cases where it can be modified without limits, this can prevent buying and selling. Audit+ has confirmed that the tax cannot be modified higher than the initial 2% buy tax and 10% sell tax.

Risky Items

There were **zero security items** classified under "Risky".

4. SWC Registry

The Smart Contract Weakness Classification Registry (SWC Registry) is an implementation of the weakness classification scheme proposed in EIP-1470. The goals of this project are as follows:

- Provide a straightforward way to classify security issues in smart contract systems.
- Define a common language for describing security issues in smart contract systems' architecture, design, or code.
- Serve as a way to train and increase performance for smart contract security analysis tools.

Although Audit+ runs test cases for all in the registry, some tests may not be considered and are classified as ignored.

Findings

There were **36 passing** test cases and a **1 ignored** test case.

SWC-108

Description	State Variable Default Visibility
Severity	Ignored
Recommendation	Labeling as public explicitly may reduce confusion but in the current usage the variable is intended to be public.

```
466    bool inSwap;
```

5. Testnet Examination

Each smart contract that is audited by the Audit+ team is deployed to a testnet of choice to test that the core functions work as intended.

Testnet	BSC Testnet
Block Explorer URL	https://testnet.bscscan.com/address/0x0E2B66eC4C4C0Edaeb5Cee14031877B2CAc8eC1d

Findings

Transfer
https://testnet.bscscan.com/tx/0x204d1f64414830bbadd753669a1e71cfd62cfb9cb197fcac030e67aaa657cfb4

No issues were detected on a peer-to-peer transfer.

Buy
https://testnet.bscscan.com/tx/0x0a8c4a2373dfe35aa1873ed1e5b020921902dee213e6ddc335bcc32c0e65be22

No issues were detected buying tokens via a DEX.

Sell
https://testnet.bscscan.com/tx/0x79a7c09b3d76f82e926fc7663a196c69b2e33ba246ccd15e9169597b3fc5c0b3

No issues were detected selling tokens via a DEX.

6. Manual Review

Audit+ conducts a line-by-line manual review of the code to identify issues that may not have been detected by automated testing. The audit also includes suggestions for readability and performance improvements.

Each finding is classified to help display to the reader both the impact and likelihood of this causing an issue to an end-user. The higher the risk classification, the more important that a fix is implemented to ensure the smooth running. Projects are always notified of the risks before the final report in case they wish to make any amendments.

Informational	Suggestions to improve readability
Low Risk	Will not cause issues for an end user but could be amended to improve performance and/or readability
Moderate Risk	Moderate possibility of causing issues for end users, should be amended to remove all doubt
High Risk	High possibility of causing an issue that would have a large impact on end users, immediate fix recommended.

Findings

Informational

There were **four** findings classified as informational identified during the manual review.

Item	Description
Tax can be modified	Both buy and sell tax can be modified but can only be set at a value lower than when the contract was deployed. Buy - maximum 2% Sell - maximum 10%
Users can be whitelisted from fees	It is not deemed as a risk as it does not impact the running of a project but some users may have an advantage with buying and selling if they are whitelisted from the taxes.
Uniswap Router is hard coded	The UniswapV2Router is hardcoded to the PancakeSwapV2 router address. A migration to V3 would require a token contract migration as the contract currently sells the tokens into the V2 pool.
Contract ownership	A single EOA controls the contract currently. If a bad actor were to get access to the owner account, the damage they could occur would be severely limited with access to user funds or minting of new tokens not being possible.

Low Risk

There were no findings classified as low risk during the manual review.

Moderate Risk

There were no findings classified as moderate risk during the manual review.

High Risk

There were no findings classified as high risk during the manual review.

7. Additional Notes

There are no further notes from the Audit+ team or the audited team.

End of Report