SOLIDProof TrustNet

Login | Request a Quote →

- Discovery
- Trending
- Launches
- KYC Verified
- Watchlist
- Risk Alerts
- Token Minter
- AI Threat Detection
- Token Burner
- Blog & News
- Docs
- Visit SolidProof.io

⚠ **Disclaimer** Not a financial advice. Always DYOR.

Sock Coin Info

sockcoin.io

Sock Coin is a collective adventure where everyone gets a lot of Socks. Imagine this: 70% of the total supply is distributed to the community!

Share

Onboarded date 23/01/2024

Team and KYC Verification

The team has securely submitted their personal information to SolidProof.io for verification.

In the event of any fraudulent activities, this information will be promptly reported to the relevant authorities to ensure accountability and compliance.

KYC Tier Gold | KYC Pinksale COMPLIANT | KYC+ GemPad COMPLIANT

TrustNet Score

The TrustNet Score evaluates crypto projects based on audit results, security, KYC verification, and social media presence. This score offers a quick, transparent view of a project's credibility, helping users make informed decisions in the Web3 space.

100.00

Poor — Excellent

Real-Time Threat Detection

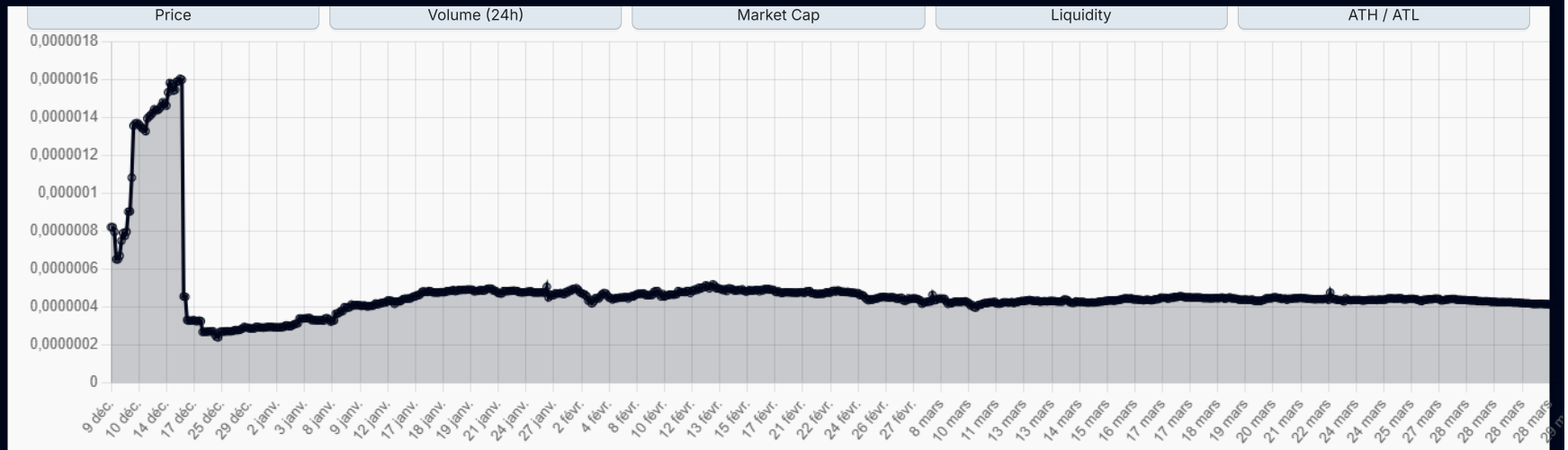
Real-time threat detection, powered by Cyvers.io, is currently not activated for this project.

This advanced feature provides continuous monitoring and instant alerts to safeguard your assets from potential security threats. Real-time detection enhances your project's security by proactively identifying and mitigating risks. For more information, click here.

TrustNet DataPulse

0x3E097678aB790AACd8b42721099b3983f40aA827

Chart & Essentials | CEX / DEX | Locking & Vesting | Fundraising



Data provided by mobula.io. Need data? Get your API.

Security Assessments

Audit No. 1034

Static Analysis | Dynamic Analysis | Symbolic Execution | SWC Check | Manual Review

CONTRACT ADDRESS 0x3E09...A827	NETWORK BNB Smart Chain - Mainnet	LICENSE N/A	COMPILER N/A
TYPE N/A	LANGUAGE Solidity	ONBOARD DATE 2024/04/05	REVISION DATE In progress

Summary and **Final Words**

No crucial issues found

The contract does not contain issues of high or medium criticality. This means that no known vulnerabilities were found in the source code.

Contract owner cannot mint

Final Words

observations, offering valuable context and clarity.

Contract owner cannot blacklist addresses.

It is not possible to lock user funds by blacklisting addresses.

Contract owner cannot set high fees

The fees, if applicable, can be a maximum of 25% or lower. The contract can therefore not be locked. Please take a look in the comment section for more details.

Contract cannot be locked

Owner cannot lock any user funds.

Token cannot be burned

There is no burning within the contract without any allowances

Ownership is not renounced

Contract can be manipulated by owner functions.

Scope of Work

This audit encompasses the evaluation of the files listed below, each verified with a SHA-1 Hash. The team referenced above has provided the necessary files for assessment.

The auditing process consists of the following systematic steps:

1. **Specification Review:** Analyze the provided specifications, source code, and instructions to fully understand the smart contract's size, scope, and functionality.
2. **Manual Code Examination:** Conduct a thorough line-by-line review of the source code to identify potential vulnerabilities and areas for improvement.
3. **Specification Alignment:** Ensure that the code accurately implements the provided specifications and intended functionalities.

Ownership Privileges

- The owner can lock/unlock the ownership.
- The owner can exclude/include wallets in rewards.
- The owner can exclude/include wallets in fees.
- The owner can update the tax, liquidity, burn, wallet, and buyback fees of not more than 10%.
- The owner can update any arbitrary amount in the buy-back upper limit including zero.
- The owner can update the max transaction and max wallet amount percent to not less than 1%.
- The owner can enable/disable swapping.
- The owner can update the fee wallet address.
- The owner can claim the stuck tokens from the contract.

Note - This Audit report consists of a security analysis of the **Siri** smart contract. This analysis did not include functional testing (or unit testing) of the contract's logic. Moreover, we only audited one token contract for the **Siri** team. Other contracts associated with the project were not audited by our team. We recommend investors do their own research before investing.

Files and details

Token.sol

dfa57c1d9ad93ff99ad4b5a3d46cdd1ceb5cb360

execution paths, identifying potential edge cases and vulnerabilities.

6. **Best Practices Evaluation:** Assess the smart contracts against established industry and academic best practices to enhance efficiency, maintainability, and security.
7. **Actionable Recommendations:** Provide detailed, specific, and actionable steps to secure and optimize the smart contracts.

A file with a different Hash has been intentionally or otherwise modified after the security review. A different Hash may indicate a changed condition or potential vulnerability that was not within the scope of this review.

Findings and Audit result

Critical	High	Medium	Low	Optimization	Informational
✓	✓	✓	4	2	2

Low Issues | 4 Findings

#1 LOW ISSUE ⓘ
Local variables shadowing (shadowing-local)

Pending

TOKEN.SOL
L842 L1072

DESCRIPTION
Rename the local variables that shadow another component.

#2 LOW ISSUE ⓘ
Missing Events Arithmetic (events-maths)

Pending

TOKEN.SOL
L932-943 L949-951 L953-958 L960-965

DESCRIPTION

#3 LOW ISSUE ⓘ
Missing Zero Address Validation (missing-zero-check)

Pending

TOKEN.SOL
L779

DESCRIPTION
Check that the address is not zero.

#4 LOW ISSUE ⓘ
Remove safemath library

Pending

TOKEN.SOL
L90-231

DESCRIPTION
The compiler version above 0.8.0 has the ability to control arithmetic overflow/underflow. It is recommended to remove the unwanted code in order to avoid high gas fees.

Optimization Issues | 2 Findings

#1 OPTIMIZATION ISSUE ⓘ
State variables that could be declared constant (constable-states)

Pending

TOKEN.SOL
L703 L707 L709 L705 L706 L708 L710 L711 L730 L722

DESCRIPTION
Add the `constant` attributes to state variables that never change.

#2 OPTIMIZATION ISSUE ⓘ
Public function that could be declared external (external-function)

Pending

TOKEN.SOL
L500-503 L509-513 L515-517 L520-525 L528-533 L816-818 L820-822 L824-826 L828-830 L837-840 L842-844 L846-849 L851-855 L857-860 L862-865 L867-869 L871-873 L875-882 L884-893 L901-908 L924-926 L928-930 L945-947 L967-970 L1068-1070 L1325-1329

DESCRIPTION
Use the `external` attribute for functions never called from the contract.

Informational Issues | 2 Findings

#1 INFORMATIONAL ISSUE ⓘ
Costly operations in a loop (costly-loop)

Pending

TOKEN.SOL

L910-921

DESCRIPTION

Use a local variable to hold the loop computation result.

#2 INFORMATIONAL ISSUE ⓘ
Functions that are not used (dead-code)

Pending

TOKEN.SOL

L359-380 | L319-321 | L329-331 | L344-346 | L354-357 | L266-275 | L293-299 | L238-241 | L437-447 | L410-419 | L426-429 | L421-424 | L395-397 | L399-401 | L211-213 | L227-230

DESCRIPTION

Remove unused functions.