2024

Smart Contract
Shares Slon Plus

Audit Certificate

Contract: SharesSlonPlus

Solidity Version: 0.8.20

SlonWeb Studio
18.07.2024

Smart Contract Audit Certificate

Contract: SharesSlonPlus

Solidity Version: 0.8.20

General Information

Parameter	Value
Token Name	Shares SlonPlus
Token Symbol	SLS+
Decimal Places	18
Total Supply	560,000,000 SLS+
Token Price	1 USD in wei (1e18)
Contract Owner	0x... (Owner address)
New Owner	0x... (New owner address, if set)
Contract Status	Active/Paused

Contract Variables and State

Variable	Type	Description
`owner`	address	Address of the current contract owner
`newOwner`	address	Address of the new contract owner being set
`paused`	bool	Flag to pause the contract operations
`balances`	mapping	Mapping of each address's token balance
`allowed`	mapping	Mapping of allowances for token transfers

Owner Management Functions

Function	Description
`transferOwnership`	Assigns a new contract owner (only current owner can call)
`acceptOwnership`	Accepts ownership of the contract (only the new owner can call)

Core TRC20 Functions

Function	Description
`totalSupply`	Returns the total number of tokens in circulation, excluding the zero address
`balanceOf`	Returns the token balance of a specified address
`transfer`	Transfers tokens from sender to a specified address
`approve`	Approves a specified address to spend a certain number of tokens on behalf of the sender

Function	Description
`transferFrom`	Transfers tokens from one address to another with sufficient allowance
`allowance`	Returns the number of tokens a specified address is allowed to spend

Token Purchase and Sale Functions

Function	Description
`buyTokens`	Allows purchasing tokens with ether (contract must be active)
`sellTokens`	Allows selling tokens for ether (contract must be active)

Contract State Management Functions

Function	Description
`pause`	Pauses all contract functions (only owner can call)
`unpause`	Resumes all contract functions (only owner can call)

Security Checks

Check	Status	Description
Null address check in `transfer`	Passed ✓	Ensure `to` is not the zero address
Balance check in `transfer`	Passed ✓	Ensure sender's balance is sufficient for the transfer
Null address check in `transferFrom`	Passed ✓	Ensure `to` is not the zero address
Balance check in `transferFrom`	Passed ✓	Ensure sender's balance is sufficient for the transfer
Allowance check in `transferFrom`	Passed ✓	Ensure allowance is sufficient for the transfer
Contract state check in `buyTokens`	Passed ✓	Ensure contract is not paused
Contract state check in `sellTokens`	Passed ✓	Ensure contract is not paused

Additional Functions

Function	Description
`receive`	Empty function that can be overridden to handle ether sent to the contract

Additional Usage Scenario Testing Results

1. Transfer Function Tests

Test	Expected Result	Result
Successful token transfer	Tokens transferred, `Transfer` event emitted	Passed ✓
Transfer of zero tokens	No tokens transferred, `Transfer` event not emitted	Passed ✓
Transfer to zero address	Transaction reverted	Passed ✓

2. Approve Function Tests

Test	Expected Result	Result
Successful approval of allowance	Allowance set, `Approval` event emitted	Passed ✓
Approval of zero allowance	Allowance set, `Approval` event emitted	Passed ✓

3. TransferFrom Function Tests

Test	Expected Result	Result
Successful token transfer	Tokens transferred, `Transfer` event emitted	Passed ✓
Transfer of zero tokens	No tokens transferred, `Transfer` event not emitted	Passed ✓
Transfer to zero address	Transaction reverted	Passed ✓

4. BuyTokens Function Tests

Test	Expected Result	Result
Successful token purchase	Tokens credited to buyer, `Transfer` event emitted	Passed ✓
Purchase with contract paused	Transaction reverted	Passed ✓

5. SellTokens Function Tests

Test	Expected Result	Result
Successful token sale	Ether transferred to seller, `Transfer` event emitted	Passed ✓
Sale with contract paused	Transaction reverted	Passed ✓

6. Owner Management Functions Tests

Test	Expected Result	Result
Successful ownership transfer	New owner set, old owner loses privileges	Passed ✓
New owner accepts ownership	New owner confirmed, new owner set	Passed ✓

Conclusions

The SharesSlonPlus contract has undergone all additional checks and tests, including various usage scenarios and edge cases. All functionalities are performing as intended and securely. The contract is prepared for deployment in a production environment.

The smart contract audit was conducted by experts at SlonWeb Studio, with the assistance of Artificial Intelligence during the process.

SlonWeb Report Disclaimer

Current Information

The content of this report is accurate as of the publication date and is subject to change without prior notice unless otherwise stated by SlonWeb. SlonWeb does not warrant the accuracy, timeliness, or completeness of any report accessed via the internet or other means and is not obligated to update the information after publication.

Confidentiality Notice

This report, including its content, data, and methodologies, is subject to the confidentiality and feedback provisions in your agreement with SlonWeb. These materials are not to be disclosed, extracted, copied, or distributed except as expressly permitted by SlonWeb.

Links to Other Websites

You may access websites operated by entities other than SlonWeb through hyperlinks or other computer links provided for your convenience. The responsibility for these websites lies with their respective owners. SlonWeb is not liable for the content or operation of these third-party websites and assumes no responsibility for your use of them. A hyperlink from this website to another does not signify that SlonWeb endorses the content or operators of that site. You are responsible for determining the extent to which you may use any content on linked websites. SlonWeb assumes no responsibility for the accuracy or completeness of any outcomes generated by third-party software used on the website.

Disclaimer

This report is based on a limited review of materials and documentation provided at the time of the audit and may not be comprehensive or inclusive of all vulnerabilities. The review and this report are provided "as-is," "where-is," and "as-available." Your access and use, including any associated services, products, protocols, platforms, content, and materials, are at your own risk. Blockchain technology is still developing and may have unknown risks and flaws. The review does not cover the compiler layer or other programming aspects that could pose security risks. This report does not endorse any particular project or team nor guarantee its security. No third party should rely on these reports for making decisions to buy or sell any product, service, or asset. To the fullest extent permitted by law, we disclaim all warranties, express or implied, including but not limited to implied warranties of merchantability, fitness for a particular purpose, and non-infringement, regarding this report, its content, and related services and products. We do not endorse or assume responsibility for any product or service advertised or offered by a third party through the product, any open-source or third-party software, code, libraries, materials, or information linked to, called by, referenced by, or accessible through the report, its content, and related services and products, any hyperlinked websites, or any websites or mobile applications appearing in any advertising. We are not responsible for monitoring any transaction between you and third-party providers of products or services. As with any product or service, use your best judgment and exercise caution.

FOR AVOIDANCE OF DOUBT, THE REPORT, ITS CONTENT, ACCESS, AND/OR USAGE, INCLUDING ANY ASSOCIATED SERVICES OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS FINANCIAL, INVESTMENT, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.