



Cyberscope

Audit Report

PCAI

May 2023

Network BSC

Address 0xac9D9Ca333C629Af5B2612c35f93B654a4FF08C8

Audited by © cyberscope

Table of Contents

Table of Contents	1
Review	2
Audit Updates	2
Source Files	3
Findings Breakdown	4
Analysis	5
MT - Mints Tokens	6
Description	6
Recommendation	6
Diagnostics	7
L15 - Local Scope Variable Shadowing	8
Description	8
Recommendation	8
L04 - Conformance to Solidity Naming Conventions	9
Description	9
Recommendation	9
Functions Analysis	10
Inheritance Graph	11
Flow Graph	12
Summary	13
Disclaimer	14
About Cyberscope	15

Review

Contract Name	PCAI
Compiler Version	v0.8.17+commit.8df45f5f
Optimization	200 runs
Explorer	https://bscscan.com/address/0xac9d9ca333c629af5b2612c35f93b654a4ff08c8
Address	0xac9d9ca333c629af5b2612c35f93b654a4ff08c8
Network	BSC
Symbol	PCAI
Decimals	18
Total Supply	420,690,000,000,000

Audit Updates

Initial Audit	07 May 2023
---------------	-------------

Source Files

Filename	SHA256
@openzeppelin/contracts/access/Ownable.sol	9353af89436556f7ba8abb3f37a6677249a a4df6024fbfaa94f79ab2f44f3231
@openzeppelin/contracts/token/ERC20/ERC20.sol	bce14c3fd3b1a668529e375f6b70ffdf9cef 8c4e410ae99608be5964d98fa701
@openzeppelin/contracts/token/ERC20/extensions /ERC20Burnable.sol	0344809a1044e11ece2401b4f7288f414ea 41fa9d1dad24143c84b737c9fc02e
@openzeppelin/contracts/token/ERC20/extensions /IERC20Metadata.sol	af5c8a77965cc82c33b7ff844deb9826166 689e55dc037a7f2f790d057811990
@openzeppelin/contracts/token/ERC20/IERC20.sol	94f23e4af51a18c2269b355b8c7cf4db800 3d075c9c541019eb8dcf4122864d5
@openzeppelin/contracts/utils/Context.sol	1458c260d010a08e4c20a4a517882259a2 3a4baa0b5bd9add9fb6d6a1549814a
@openzeppelin/contracts/utils/math/SafeMath.sol	0dc33698a1661b22981abad8e5c6f5ebca 0dfe5ec14916369a2935d888ff257a
contracts/PepechainAI.sol	1137f579390c78e1c7b10301f2b1a96443f 59cd30fae735021057673f575457e

Findings Breakdown



● Critical	0
● Medium	0
● Minor / Informative	3

Severity	Unresolved	Acknowledged	Resolved	Other
● Critical	0	0	0	0
● Medium	0	0	0	0
● Minor / Informative	3	0	0	0

Analysis

● Critical ● Medium ● Minor / Informative ● Pass

Severity	Code	Description	Status
●	ST	Stops Transactions	Passed
●	OCTD	Transfers Contract's Tokens	Passed
●	OTUT	Transfers User's Tokens	Passed
●	ELFM	Exceeds Fees Limit	Passed
●	ULTW	Transfers Liquidity to Team Wallet	Passed
●	MT	Mints Tokens	Unresolved
●	BT	Burns Tokens	Passed
●	BC	Blacklists Addresses	Passed

MT - Mints Tokens

Criticality	Minor / Informative
Location	contracts/PepechainAI.sol#L28
Status	Unresolved

Description

The contract owner has the authority to mint tokens. The owner may take advantage of it by calling the `mint` function. At the moment, the max supply is capped, but since the contract implements the ERC20Burnable contract from the `openzeppelin` library, the users are able to burn their own tokens or another users' tokens if they have the required allowance. As a result, the owner will be able to call the `mint` function up to the equivalent burn amount and the contract tokens will be highly inflated.

```
function mint(address _user, uint256 _amount) external onlyOwner {
    uint256 _totalSupply = totalSupply();
    require(_totalSupply.add(_amount) <= MAX_SUPPLY, "PCAI: No more
    minting allowed!");

    _mint(_user, _amount);
}
```

Recommendation

The team should carefully manage the private keys of the owner's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions. Some suggestions are:

- Introduce a time-locker mechanism with a reasonable delay.
- Introduce a multi-sign wallet so that many addresses will confirm the action.
- Introduce a governance model where users will vote about the actions.
- Renouncing the ownership will eliminate the threats but it is non-reversible.

Diagnostics

● Critical ● Medium ● Minor / Informative

Severity	Code	Description	Status
●	L15	Local Scope Variable Shadowing	Unresolved
●	L04	Conformance to Solidity Naming Conventions	Unresolved

L15 - Local Scope Variable Shadowing

Criticality	Minor / Informative
Location	contracts/PepechainAI.sol#L29
Status	Unresolved

Description

Local scope variable shadowing occurs when a local variable with the same name as a variable in an outer scope is declared within a function or code block. When this happens, the local variable "shadows" the outer variable, meaning that it takes precedence over the outer variable within the scope in which it is declared.

```
uint256 _totalSupply = totalSupply()
```

Recommendation

It's important to be aware of shadowing when working with local variables, as it can lead to confusion and unintended consequences if not used correctly. It's generally a good idea to choose unique names for local variables to avoid shadowing outer variables and causing confusion.

L04 - Conformance to Solidity Naming Conventions

Criticality	Minor / Informative
Location	contracts/PepechainAI.sol#L14,28
Status	Unresolved

Description

The Solidity style guide is a set of guidelines for writing clean and consistent Solidity code. Adhering to a style guide can help improve the readability and maintainability of the Solidity code, making it easier for others to understand and work with.

The followings are a few key points from the Solidity style guide:

1. Use camelCase for function and variable names, with the first letter in lowercase (e.g., myVariable, updateCounter).
2. Use PascalCase for contract, struct, and enum names, with the first letter in uppercase (e.g., MyContract, UserStruct, ErrorEnum).
3. Use uppercase for constant variables and enums (e.g., MAX_VALUE, ERROR_CODE).
4. Use indentation to improve readability and structure.
5. Use spaces between operators and after commas.
6. Use comments to explain the purpose and behavior of the code.
7. Keep lines short (around 120 characters) to improve readability.

```
uint256 public immutable MAX_SUPPLY
uint256 _amount
address _user
```

Recommendation

By following the Solidity naming convention guidelines, the codebase increased the readability, and maintainability, and makes it easier to work with.

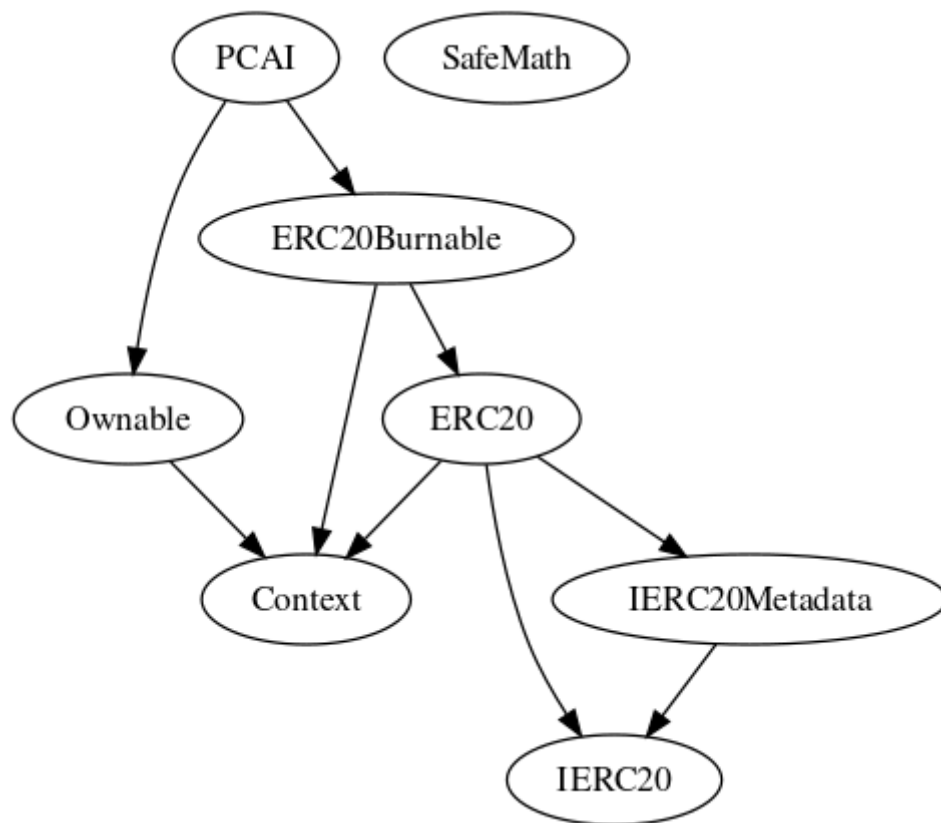
Find more information on the Solidity documentation

<https://docs.soliditylang.org/en/v0.8.17/style-guide.html#naming-convention>.

Functions Analysis

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
PCAI	Implementation	ERC20Burnable, Ownable		
		Public	✓	ERC20
	_burn	Internal	✓	
	mint	External	✓	onlyOwner

Inheritance Graph



Legend

- Internal Call (Green Arrow)
- External Call (Orange Arrow)
- Defined Contract (Grey Box)
- Undefined Contract (White Box)

SafeMath (lib)

- tryAdd
- trySub
- tryMul
- tryDiv
- tryMod
- add
- sub
- mul
- div
- mod

Context

- _msgSender
- _msgData

IERC20 (iface)

- totalSupply
- balanceOf
- transfer
- allowance
- approve
- transferFrom

IERC20Metadata (iface)

- name
- symbol
- decimals

ERC20Burnable

- burn
- burnFrom

PCAI

- <Constructor>
- _burn
- mint
- totalSupply

Ownable

- onlyOwner
- renounceOwnership
- transferOwnership
- _burn
- _checkOwner
- owner
- _transferOwnership
- _msgSender

ERC20

- <Constructor>
- name
- symbol
- decimals
- totalSupply
- balanceOf
- transfer
- transferFrom
- _mint
- _transfer
- _beforeTokenTransfer
- _afterTokenTransfer
- approve
- increaseAllowance
- decreaseAllowance
- _spendAllowance
- type

totalBurned

- add

_totalSupply

- add

Summary

PCAI contract implements a token mechanism. This audit investigates security issues, business logic concerns, and potential improvements. PCAI is an interesting project that has a friendly and growing community. The Smart Contract analysis reported no compiler errors or critical issues. The contract Owner can access some admin functions that can not be used in a malicious way to disturb the users' transactions. The contract owner can mint tokens, only after users have burned tokens.

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 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.



The Cyberscope team

<https://www.cyberscope.io>