Cyberscope

Audit Report

CryptoWeb3

November 2023

Network	MATIC
Address	0xa3c0dEf5462F124C393b203919b9fA0bDD8ee869
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	Passed
●	BT	Burns Tokens	Passed
●	BC	Blacklists Addresses	Passed

Table of Contents

Review

Contract Name	CryptoWeb3
Compiler Version	v0.8.20+commit.a1b79de6
Optimization	1000 runs
Explorer	https://polygonscan.com/address/0xa3c0def5462f124c393b203919b9fa0bdd8ee869
Address	0xa3c0def5462f124c393b203919b9fa0bdd8ee869
Network	MATIC
Symbol	CW3
Decimals	18
Total Supply	55,555,026

Audit Updates

Initial Audit	05 Nov 2023

Source Files

Filename	SHA256
contracts/CryptoWeb3.sol	c438dc0c8b001c6e25021b8669e6dcebea8389e06ed6d821b0365dff3b0c75f8
@openzeppelin/contracts/utils/Strings.sol	0519199dbc635f98ce2e4537986604ee618bca665c65e9a1738702dfacf72010

@openzeppelin/contracts/utils/StorageSlot.sol	b4a5fb7ab93bfeda06509eafbd5f71fde0e0de84b6d9129553bd535a42166c15
@openzeppelin/contracts/utils/ShortStrings.sol	ddd52921d2996abf2e3d9c1c4f6d00194a3e3b278a164948f995862371444a55
@openzeppelin/contracts/utils/Nonces.sol	9b4cbb85d1f5053c744e83302538eb643a713ffd14bc37665b224f1c66529339
@openzeppelin/contracts/utils/Context.sol	9c1cc43aa4a2bde5c7dea0d4830cd42c54813ff883e55c8d8f12e6189bf7f10a
@openzeppelin/contracts/utils/types/Time.sol	338550afac6c340197c1f97df3c113a22c0b6730991df1167407d576dbd1fcb0
@openzeppelin/contracts/utils/structs/Checkpoints.sol	bcb82ddf3742b104336967e44fbacf59e609da5b590315eb13a17de36e32739d
@openzeppelin/contracts/utils/math/SignedMath.sol	768c28e3a33c3312e57ae8a1caaec2893bc89ac6e386621de018f85e9a2d6e99
@openzeppelin/contracts/utils/math/SafeCast.sol	089488198de38548e4e8ee7940d307f18396e5b295de5bca7ff7567fd4142cc3
@openzeppelin/contracts/utils/math/Math.sol	a6ee779fc42e6bf01b5e6a963065706e882b016affbedfd8be19a71ea48e6e15
@openzeppelin/contracts/utils/cryptography/MessageHashUtils.sol	2fd5c641cf452efd15f784827cb2835664970d7fbc166bf80824ed27011cc374
@openzeppelin/contracts/utils/cryptography/EIP712.sol	27dac0732a0154f432c0a7a1d1f067ab51116105e157d0e5d68d040fd83954d5
@openzeppelin/contracts/utils/cryptography/ECDSA.sol	37828cb50b47bcc51c7b770bde15d5885d871ef1e67028057a0b788c3568726e
@openzeppelin/contracts/token/ERC20/IERC20.sol	6f2faae462e286e24e091d7718575179644dc60e79936ef0c92e2d1ab3ca3cee
@openzeppelin/contracts/token/ERC20/ERC20.sol	2d874da1c1478ed22a2d30dcf1a6ec0d09a13f897ca680d55fb49fbcc0e0c5b1

@openzeppelin/contracts/token/ERC20/extensions/IERC20Permit.sol	912509e0e9bf74e0f8a8c92d031b5b26d2d35c6d4abf3f56251be1ea9ca946bf
@openzeppelin/contracts/token/ERC20/extensions/IERC20Metadata.sol	1d079c20a192a135308e99fa5515c27acfbb071e6cdb0913b13634e630865939
@openzeppelin/contracts/token/ERC20/extensions/ERC20Votes.sol	697a396ebd26913f4dcc80430f457da291189ba333a75e1f5383a4d8e156e5ea
@openzeppelin/contracts/token/ERC20/extensions/ERC20Permit.sol	677cb995a34f0cc937f3d77d4626c46fbf47cdef4c9cc0314c27672c0459cf80
@openzeppelin/contracts/token/ERC20/extensions/ERC20Burnable.sol	2e6108a11184dd0caab3f3ef31bd15fed1bc7e4c781a55bc867ccedd8474565c
@openzeppelin/contracts/interfaces/draft-IERC6093.sol	4aea87243e6de38804bf8737bf86f750443d3b5e63dd0fd0b7ad92f77cdbd3e3
@openzeppelin/contracts/interfaces/IERC6372.sol	2294c70df203a6a38985d064adca030293bec4b7aaa1237b62c7b1a34154f130
@openzeppelin/contracts/interfaces/IERC5805.sol	6ecc2370599496e6d862c2b4893975ec240f0ef8475daef1d20b5dd1efa90102
@openzeppelin/contracts/interfaces/IERC5267.sol	efd1ebd1e04b6ef9c3b8781a097588f83da954323f438d54a71dc06508e6c7b8
@openzeppelin/contracts/governance/utils/Votes.sol	a51b07bbb6cb017cff537731d0a6355e46d1640330e3df4a20adf6d9353962d0
@openzeppelin/contracts/governance/utils/IVotes.sol	f033b73ce92762d9ed9496b8a0f5f72bd0479e42388da584c2ff276cbb5cb9b1

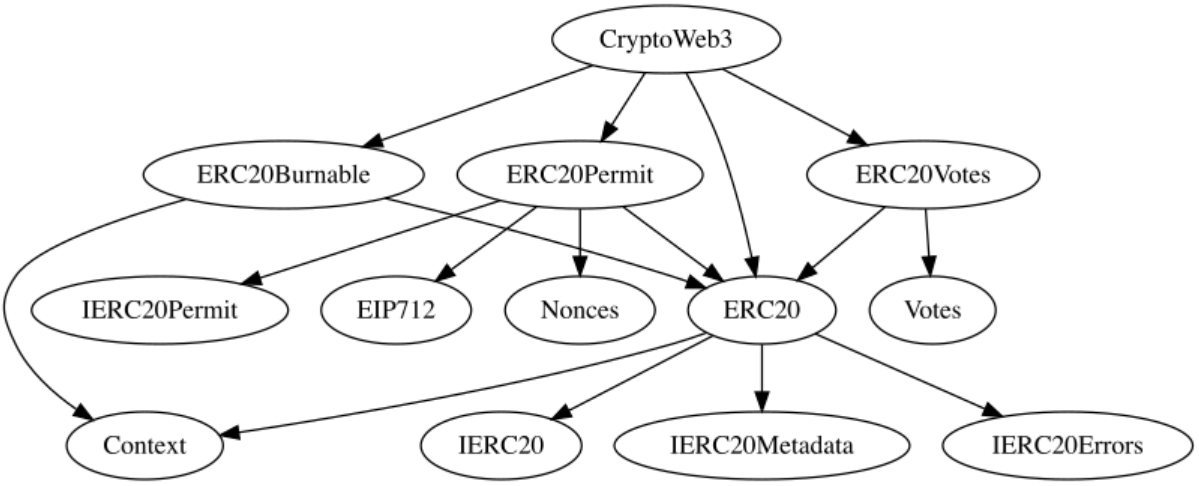
Findings Breakdown

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

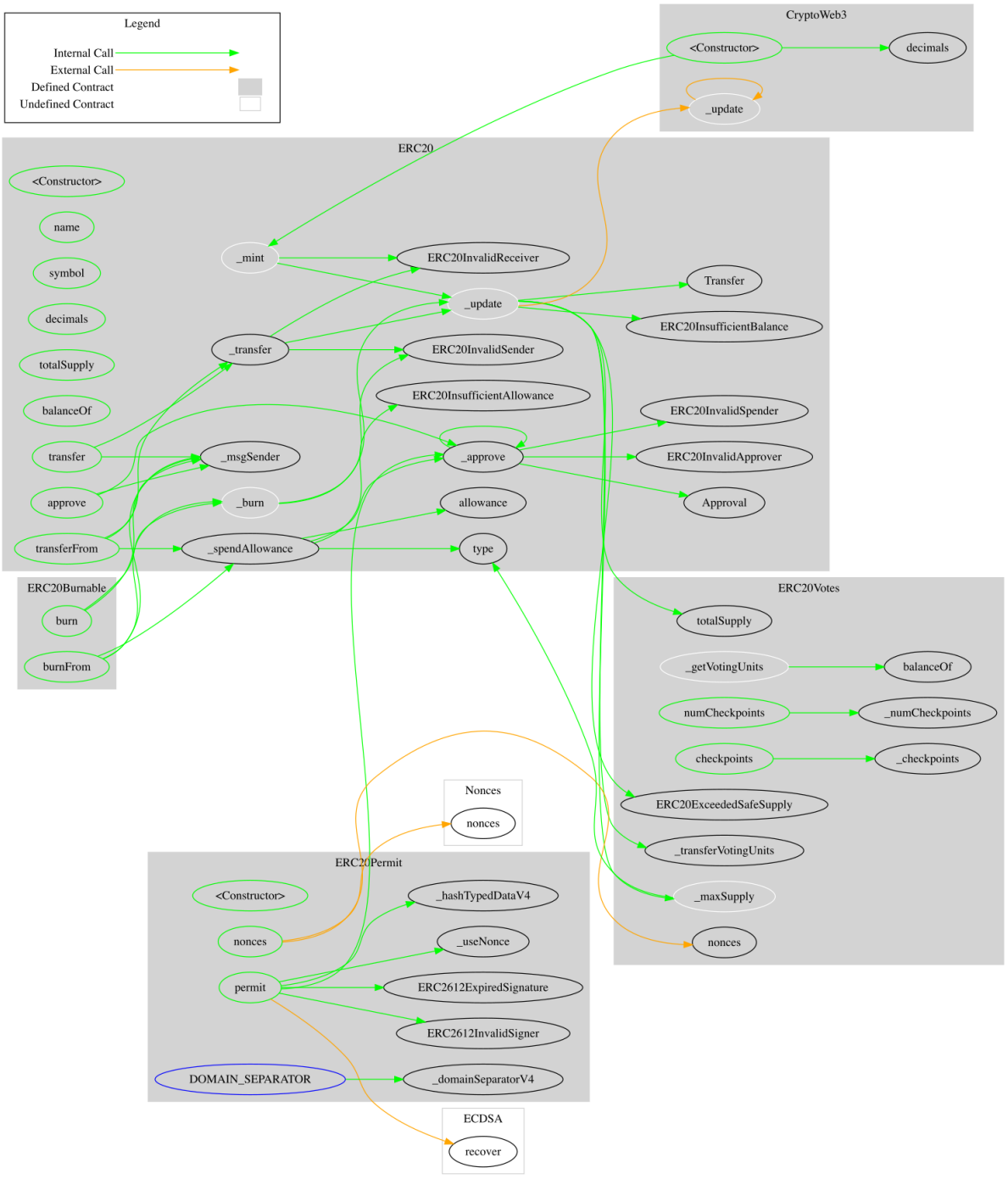
Functions Analysis

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
CryptoWeb3	Implementation	ERC20, ERC20Burnable, ERC20Permit, ERC20Votes		
		Public	✓	ERC20 ERC20Permit
	_update	Internal	✓	
	nonces	Public		-

Inheritance Graph



Flow Graph


Legend
Internal Call
External Call
Defined Contract
Undefined Contract
CryptoWeb3
<Constructor>
decimals
_update
ERC20
<Constructor>
name
symbol
decimals
totalSupply
balanceOf
transfer
approve
transferFrom
_mint
_transfer
_msgSender
_burn
_spendAllowance
ERC20InvalidReceiver
_update
ERC20InvalidSender
ERC20InsufficientAllowance
_approve
allowance
type
Transfer
ERC20InsufficientBalance
ERC20InvalidSpender
ERC20InvalidApprover
Approval
ERC20Burnable
burn
burnFrom
ERC20Votes
totalSupply
_getVotingUnits
balanceOf
numCheckpoints
_numCheckpoints
checkpoints
_checkpoints
ERC20ExceededSafeSupply
_transferVotingUnits
_maxSupply
nonces
Nonces
nonces
ERC20Permit
<Constructor>
nonces
permit
DOMAIN_SEPARATOR
_hashTypedDataV4
_useNonce
ERC2612ExpiredSignature
ERC2612InvalidSigner
_domainSeparatorV4
ECDSA
recover

Summary

CryptoWeb3 contract implements a token mechanism. This audit investigates security issues, business logic concerns, and potential improvements. CryptoWeb3 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.

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