Cyberscope

Audit Report

BlockATM

June 2023

Audited by © cyberscope

Table of Contents

Review

Audit Updates

Initial Audit	24 May 2023 https://github.com/cyberscope-io/audits/blob/main/batm/v1/audit.pdf
Corrected Phase 2	08 Jun 2023 https://github.com/cyberscope-io/audits/blob/main/batm/v2/audit.pdf
Corrected Phase 3	10 Jun 2023

Source Files

Filename	SHA256
BlockATM.sol	61d00765dbb6aaa3274922b6a0b295ec92960aeca01e25173501e5e9966ceed8
BlockATMCustomer.sol	5556fb4311d14a61cb1ff01afe57a0e9f3e53b477d9fa54d59c6cf155a57489a
BlockCommon.sol	1624414ff7e14158c7524ca790c541ef80de79dc2a664ac6d8d610640a45c670
BlockOrder.sol	1c9dc2413ec1214bf047a52866a1b1fc2a12f6149a17b9d32500128a4f072280
BlockPlatform.sol	be11d5b13ffbd41331df3160f11a30e82527bb2b7f9c5cb13447ddd7b2401680
BlockPlatformStandard.sol	1f374e28659da11ea2090fc3f2e3b81567e09c485a58f702962ca05bfe3b88c6

BlockRecharge.sol	b3f7e9f11d00bb48dc15af221608e5d9e7bbf3e416d6e5276bd6fc1c0c0c83b2

Introduction

The BlockATM ecosystem consists of four distinct contracts: BlockATM, BlockATMCustomer, BlockOrder, and BlockRecharge. The BlockATM contract serves as an automated teller machine for cryptocurrencies, enabling users to transfer ERC20 tokens and Ether (ETH) to a designated withdrawal address. The BlockATMCustomer contract is designed for customers of the BlockATM system, allowing them to transfer ERC20 tokens and subsequently withdraw them to specified addresses. BlockOrder facilitates the transfer of ERC20 tokens associated with orders or specific transactions to a designated withdrawal address. Lastly, BlockRecharge offers the same functionality as the BlockOrder contract. These contracts provide various features and functionality related to token transfers and withdrawals, with the contract owners having control over withdrawal addresses, supported tokens, and other related settings.

Roles

BlockATM

Owner

The owner has authority over the following functions:

- `function modifyWithdrawAddress(address payable newAddress)`
- `function addCoinList(address _address)`
- `function closeCoinList(address newAddress)`

User

The user can interact with the following functions:

- `function transferToken(address token,uint256 amount,string memory orderId)`
- `function transferETH(string memory orderId)`
- `function getWithdrawAddress()`
- `function getCoinList(address _address)`

BlockATMCustomer

Owner

The owner has authority over the following functions:

- `function withdrawToken(uint256 amount,address withdrawAddress)`
- `function setActiveFlag()`

User

The user can interact with the following functions:

- `function transferToken(uint256 amount,string memory orderId)`
- `function getTokenAddress()`
- `function getActiveFlag()`
- `function getWithdrawAddressList()`
- `function checkWithdrawAddress(address withdrawAddress)`
- `function getWithdrawAddressFlag(address withdrawAddress)`
- `function getOnwerAddressFlag(address ownerAddress))`
- `function getOwnerAddressList()`

BlockOrder

Owner

The owner has authority over the following functions:

- `function modifyWithdrawAddress(address payable _address)`
- `function addCoinList(address _address)`
- `function closeCoinList(address _address)`

User

The user can interact with the following functions:

- `function transferToken(address token,uint256 amount,string memory orderId)`
- `function getWithdrawAddress()`
- `function getCoinList(address _address)`

BlockRecharge

Owner

The owner has authority over the following functions:

- `function modifyWithdrawAddress(address payable _address)`
- `function addCoinList(address _address)`
- `function closeCoinList(address _address)`

User

The user can interact with the following functions:

- `function transferToken(address token,uint256 amount,string memory orderId)`
- `function getWithdrawAddress()`
- `function getCoinList(address _address)`

Test Deployments

Contract	Explorer
BlockATM	https://testnet.bscscan.com/address/0x2a3950f22070C0a67a7750Da92dd0700062d5DE0
BlockATMCustomer	https://testnet.bscscan.com/address/0x88299418278D560A16D24d6b9cE89811D3AE2950
BlockOrder	https://testnet.bscscan.com/address/0xd57Dfe308CF62E9D160A812B09C818A7efc320f2
BlockRecharge	https://testnet.bscscan.com/address/0x6d72Df79dF9c3aAC4ac6D77EFCc5A3E5401B3477

Findings Breakdown

Critical	0
Medium	0
Minor / Informative	0

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

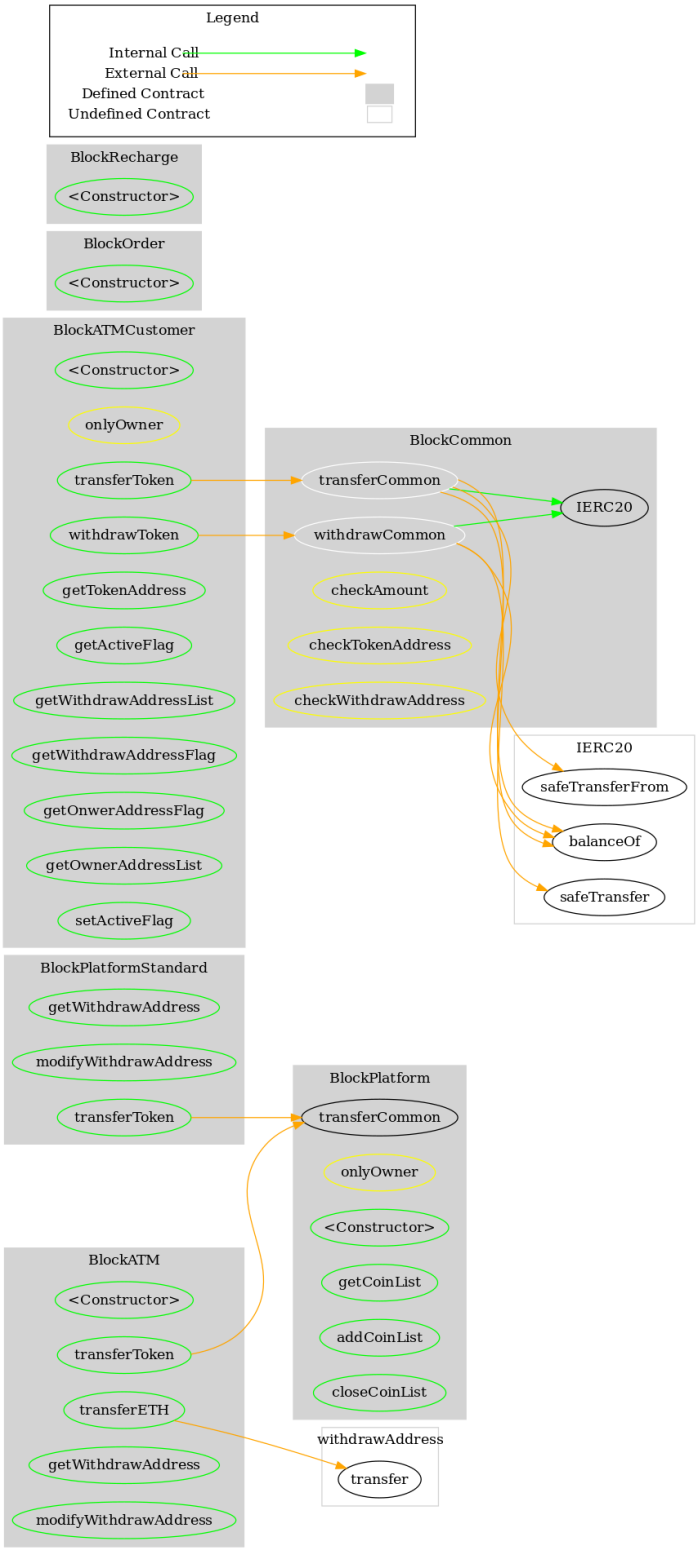
Function Analysis

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
BlockATM	Implementation	BlockPlatform		
		Public	✓	checkWithdrawAddress
	transferToken	Public	✓	-
	transferETH	Public	Payable	checkAmount
	getWithdrawAddress	Public		-
	modifyWithdrawAddress	Public	✓	onlyOwner checkWithdrawAddress
BlockATMCustomer	Implementation	BlockCommon		
		Public	✓	checkTokenAddress
	transferToken	Public	✓	-
	withdrawToken	Public	✓	onlyOwner
	getTokenAddress	Public		-
	getActiveFlag	Public		-
	getWithdrawAddressList	Public		-
	getWithdrawAddressFlag	Public		-
	getOnwerAddressFlag	Public		-
	getOwnerAddressList	Public		-

	setActiveFlag	Public	✓	onlyOwner
BlockCommon	Implementation			
	transferCommon	Internal	✓	checkTokenAddress checkAmount
	withdrawCommon	Internal	✓	checkAmount checkTokenAddress checkWithdrawAddress
BlockOrder	Implementation	BlockPlatformStandard		
		Public	✓	checkWithdrawAddress
BlockPlatform	Implementation	BlockCommon		
		Public	✓	-
	getCoinList	Public		-
	addCoinList	Public	✓	onlyOwner checkTokenAddress
	closeCoinList	Public	✓	onlyOwner checkTokenAddress
BlockPlatformStandard	Implementation	BlockPlatform		
	getWithdrawAddress	Public		-
	modifyWithdrawAddress	Public	✓	onlyOwner checkWithdrawAddress
	transferToken	Public	✓	-

BlockRecharge	Implementation	BlockPlatformStandard		
		Public	✓	checkWithdrawAddress

Flow Graph


Legend
Internal Call
External Call
Defined Contract
Undefined Contract
BlockRecharge
<Constructor>
BlockOrder
<Constructor>
BlockATMCustomer
<Constructor>
onlyOwner
transferToken
withdrawToken
getTokenAddress
getActiveFlag
getWithdrawAddressList
getWithdrawAddressFlag
getOnwerAddressFlag
getOwnerAddressList
setActiveFlag
BlockCommon
transferCommon
withdrawCommon
checkAmount
checkTokenAddress
checkWithdrawAddress
IERC20
IERC20
safeTransferFrom
balanceOf
safeTransfer
BlockPlatformStandard
getWithdrawAddress
modifyWithdrawAddress
transferToken
BlockPlatform
transferCommon
onlyOwner
<Constructor>
getCoinList
addCoinList
closeCoinList
BlockATM
<Constructor>
transferToken
transferETH
getWithdrawAddress
modifyWithdrawAddress
withdrawAddress
transfer

Summary

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

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