Cyberscope

Audit Report

Space Xmitter

November 2022

Github	https://github.com/goldcode0/Space-Xmitter
Commit	7a9c6cd73c315981c12be00f61e6862356bf9bc2
Audited by	© cyberscope

Table of Contents

Contract Review

Contract Name	FiboGame
Compiler Version	v0.8.15+commit.e14f2714
Github	https://github.com/goldcode0/Space-Xmitter
Commit	7a9c6cd73c315981c12be00f61e6862356bf9bc2
Test Deploy	https://testnet.bscscan.com/token/0xb53f8fB16A9cB6Be2F05D4A8237FA5AfcC1ac2F6
Domain	spacex.date

Audit Updates

Initial Audit	22nd November 2022
Corrected	

Source Files

Filename	SHA256
@openzeppelin/contracts/access/AccessControl.sol	5af1771388b4fe634e0a566716e32c6d00a5372875099127b274d4cf8a94e9d2
@openzeppelin/contracts/access/IAccessControl.sol	d03c1257f2094da6c86efa7aa09c1c07ebd33dd31046480c5097bc2542140e45
@openzeppelin/contracts/security/Pausable.sol	2072248d2f79e661c149fd6a6593a8a3f038466557c9b75e50e0b001bcb5cf97
@openzeppelin/contracts/token/ERC20/extensions/draft-IERC20Permit.sol	3e7aa0e0f69eec8f097ad664d525e7b3f0a3fda8dcdd97de5433ddb131db86ef
@openzeppelin/contracts/token/ERC20/extensions/IERC20Metadata.sol	af5c8a77965cc82c33b7ff844deb9826166689e55dc037a7f2f790d057811990
@openzeppelin/contracts/token/ERC20/IERC20.sol	94f23e4af51a18c2269b355b8c7cf4db8003d075c9c541019eb8dcf4122864d5
@openzeppelin/contracts/token/ERC20/utils/SafeERC20.sol	fa36a21bd954262006d806b988e4495562e7b50420775e2aa0deecb596fd1902
@openzeppelin/contracts/utils/Address.sol	1e0922f6c0bf6b1b8b4d480dcabb691b1359195a297bde6dc5172e79f3a1f826
@openzeppelin/contracts/utils/Context.sol	1458c260d010a08e4c20a4a517882259a23a4baa0b5bd9add9fb6d6a1549814a
@openzeppelin/contracts/utils/cryptography/ECDSA.sol	4e45d53327d561848fbcf381262ec5c0ac91b2f1f06432210bf76db55279d945

@openzeppelin/contracts/utils/introspection/ERC165.sol	8806a632d7b656cadb8133ff8f2acae4405b3a64d8709d93b0fa6a216a8a6154
@openzeppelin/contracts/utils/introspection/IERC165.sol	701e025d13ec6be09ae892eb029cd83b3064325801d73654847a5fb11c58b1e5
@openzeppelin/contracts/utils/Strings.sol	34127ad0054df5963b0fd694c1b313d17e9114a2f426b85526d6d976210298ab
contracts/FiboGame.sol	ba9d2f5bafa342a6592d2132fc3a6b169e20ca7db9cc1ddee287a450c769b6bd

Introduction

The Space Xmitter contracts act as one of the company's development funds. One of those contracts is FiboGame.

FiboGame

The project allows players to earn money in a fully open and transparent system. Handling fees will be contributed to Space Xmitter's development fund. Users can exchange **spx** points for various token rewards on the official website even if they do not receive token rewards.

The contract owner is responsible for choosing the winners and the additional earning. The information is signed offchain by the owner. Hence, its the owner's responsibility to inject the proper information to the contract.

- Challenge participation costs 100 tokens (ERC-20), and is refreshed daily at 24:00 US Western Time.
- One round lasts for 7 days and the earnings will be automatically increased. The first two rounds have 10 tokens base earnings per round, which can be increased depending on the number of friends that the player has invited will participate on each round. The maximum number of friends that can participate is 5 and each one will increase the base earnings of the round by 40%.
- The game earnings are determined solely by the first two rounds, so even if the player invites friends on the third round onwards the earnings won't increase.
- At the end of each round, the player can decide to either continue the challenge and advance to the next round for higher earnings, or end the challenge and get the sum of his previous earnings.
- Starting the challenge once more requires the player to invite friends and pay for participation again.

Roles

The FiboGame has an admin and a pauser role.

Admin

The admin has the authority to

- Update the signing address.
- Update the dev's address.

Pauser

The pauser has the authority to

- To pause the challenge temporarily.
- To unpause the challenge.

Contract Diagnostics

● Critical ● Medium ● Minor / Informative

Severity	Code	Description	Status
●	L04	Conformance to Solidity Naming Conventions	Unresolved
●	L08	Tautology or Contradiction	Unresolved
●	L13	Divide before Multiply Operation	Unresolved

L04 - Conformance to Solidity Naming Conventions

Criticality	minor / informative
Location	contracts/FiboGame.sol#L61,23,21,57,213,20,22
Status	Unresolved

Description

Solidity defines a naming convention that should be followed. Rule exceptions:

- Allow constant variable name/symbol/decimals to be lowercase.
- Allow _ at the beginning of the mixed_case match for private variables and unused parameters.

```
_signer
DEV
TICKET_PRICE
_dev
_user
BASIC_REWARDS
SIGNER
```

Recommendation

Follow the Solidity naming convention.
https://docs.soliditylang.org/en/v0.8.17/style-guide.html#naming-conventions.

L08 - Tautology or Contradiction

Criticality	minor / informative
Location	contracts/FiboGame.sol#L97,162
Status	Unresolved

Description

Detects expressions that are tautologies or contradictions. For instance, an uint variable will always be greater than or equal to zero.

```
require(bool,string)(round2Invitations >= 0,round2Invitations must be greater than or equal to 0)
require(bool,string)(round1Invitations >= 0,round1Invitations must be greater than or equal to 0)
```

Recommendation

Fix the incorrect comparison by changing the value type or the comparison.

L13 - Divide before Multiply Operation

Criticality	minor / informative
Location	contracts/FiboGame.sol#L162
Status	Unresolved

Description

Performing divisions before multiplications may cause lose of prediction.

```
amounts[index] = BASIC_REWARDS + ((BASIC_REWARDS * 4) / 10) * (round2Invitations)
amounts[index] = BASIC_REWARDS + ((BASIC_REWARDS * 4) / 10) * (round1Invitations)
```

Recommendation

The multiplications should be prior to the divisions.

Contract Functions

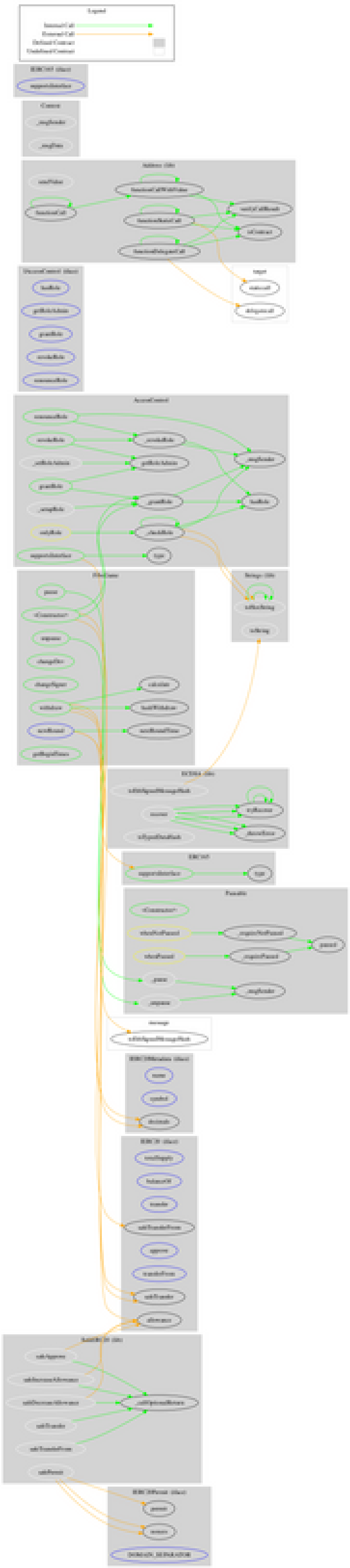
Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
AccessControl	Implementation	Context, IAccessControl, ERC165		
	supportsInterface	Public		-
	hasRole	Public		-
	_checkRole	Internal		
	_checkRole	Internal		
	getRoleAdmin	Public		-
	grantRole	Public	✓	onlyRole
	revokeRole	Public	✓	onlyRole
	renounceRole	Public	✓	-
	_setupRole	Internal	✓	
	_setRoleAdmin	Internal	✓	
	_grantRole	Internal	✓	
	_revokeRole	Internal	✓	
IAccessControl	Interface			
	hasRole	External		-
	getRoleAdmin	External		-
	grantRole	External	✓	-
	revokeRole	External	✓	-
	renounceRole	External	✓	-
Pausable	Implementation	Context		
	<Constructor>	Public	✓	-
	paused	Public		-
	_requireNotPaused	Internal		
	_requirePaused	Internal		

	_pause	Internal	✓	whenNotPaused
	_unpause	Internal	✓	whenPaused
IERC20Permit	Interface			
	permit	External	✓	-
	nonces	External		-
	DOMAIN_SEPARATOR	External		-
IERC20Metadata	Interface	IERC20		
	name	External		-
	symbol	External		-
	decimals	External		-
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
SafeERC20	Library			
	safeTransfer	Internal	✓	
	safeTransferFrom	Internal	✓	
	safeApprove	Internal	✓	
	safeIncreaseAllowance	Internal	✓	
	safeDecreaseAllowance	Internal	✓	
	safePermit	Internal	✓	
	_callOptionalReturn	Private	✓	
Address	Library			
	isContract	Internal		
	sendValue	Internal	✓	
	functionCall	Internal	✓	

	functionCall	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionStaticCall	Internal		
	functionStaticCall	Internal		
	functionDelegateCall	Internal	✓	
	functionDelegateCall	Internal	✓	
	verifyCallResult	Internal		
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
ECDSA	Library			
	_throwError	Private		
	tryRecover	Internal		
	recover	Internal		
	tryRecover	Internal		
	recover	Internal		
	tryRecover	Internal		
	recover	Internal		
	toEthSignedMessageHash	Internal		
	toEthSignedMessageHash	Internal		
	toTypedDataHash	Internal		
ERC165	Implementation	IERC165		
	supportsInterface	Public		-
IERC165	Interface			
	supportsInterface	External		-
Strings	Library			
	toString	Internal		
	toHexString	Internal		
	toHexString	Internal		

	toHexString	Internal		
FiboGame	Implementation	Pausable, AccessControl		
	<Constructor>	Public	✓	-
	pause	Public	✓	onlyRole
	unpause	Public	✓	onlyRole
	changeDev	Public	✓	onlyRole
	changeSigner	Public	✓	onlyRole
	newRound	External	✓	whenNotPaused
	withdraw	Public	Payable	whenNotPaused
	calculate	Public		-
	nextRoundTime	Public		-
	getBeginTimes	Public		-
	hashWithdraw	Public		-

Contract Flow



Domain Info

Domain Name	spacex.date
Registry Domain ID	DA0A29D2B845148FDA0F1223A4667FB1F-GDREG
Creation Date	2022-10-31T05:14:14Z
Updated Date	2022-11-05T05:14:14Z
Registry Expiry Date	2023-10-31T05:14:14Z
Registrar WHOIS Server	whois.aliyun.com
Registrar URL	www.alibabacloud.com
Registrar	ALIBABA.COM SINGAPORE E-COMMERCE PRIVATE LIMITED
Registrar IANA ID	3775

The domain was created 22 days before the creation of the audit. It will expire in 11 months.

There is no public billing information, the creator is protected by the privacy settings.

Summary

Space Xmitter implements a gaming mechanism based on rounds. 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