CryptoBlades

合約審計報告

VER 1.0

2022年5月24日

No. 20220524111230

項目總結

1. 項目介紹

CryptoBlades 是币安智能鏈上的一款 NFT 角色扮演遊戲，遊戲的核心圍繞著在擊敗敵人和參與突襲後用 SKILL 代幣獎勵玩家。玩家可以雇傭多個角色以及鍛造獨特的武器，還可以重鑄這些武器以增加他們的整體力量。玩家可以在開放的市場上交易他們的角色和武器。他們還可以質押他們的 SKILL 收入並獲得額外的 SKILL 作為獎勵。

2. 審計詳情

項目名稱	CryptoBlades	平台	N/A
通證名稱	N/A	通證代號	N/A
開始時間	2022年5月9日	語言	Solidity
結束時間	2022年5月23日	官網	N/A
Github	https://github.com/CryptoBlades/cryptoblades	白皮書	N/A

3. 審計範圍

ID	文件	SHA-256 checksum
contracts	BasicPriceOracle.sol	6B74837A0A92134938908A77A258561EB2F203B2CCDE4814D615E10534013FD2
contracts	Blacksmith.sol	60BDF2952875535F9EBE5FCC9BFDE0DB47539320085AA8590F85CCB8531CD9AF
contracts	BurningManager.sol	5C37E4C43FC7460CF32493E3783DB298BD468E4F4D4E2CA7F3E6C24A82CFBAB7
contracts	BytesChunker.sol	8D5BF0A137F0B33E222431FE966EF2666BFD1B33B65AE3255A7537068BFECA50
contracts	CBKLand.sol	368A456F3FF2F6A64901F846582677BCE0B914E3E5DB385398FD1664C5638BBF
contracts	CBKLandSale.sol	95EC00B88273C9FFF3CFCD6B36073D5FADA2D9E398C0D3FA4FF0C1BCBCB5737C

2022年5月24日

ID	文件	SHA-256 checksum
contracts	CBKLandT1StakingRewardsUpgradeable.sol	07473F121738DEFE5A64456CF92DB8917C4E909C25B68EDDAA77756469E67EAE
contracts	CBKLandT2StakingRewardsUpgradeable.sol	C7F1EC81B47505CCEFE9392CB54A7A994B9419D1750945BC816F41E284F667A2
contracts	CBKLandT3StakingRewardsUpgradeable.sol	4EEF42E74422F3CD1DD1C61E44FFE7278479D6E91E6A265676FFC96970736C01
contracts	ChainlinkRandoms.sol	78B906E7432A33000A380D3CC875F067CFFE95E16214E39EADB012D740D04C8C
contracts	CharacterCosmetics.sol	A78686AFF6B1FB5989B1714C7CC1CFEB5364EF7FB9BADF7C5212E4DE8567E416
contracts	CharacterEarthTraitChangeConsumables.sol	D45EDEDF22D854CD760E65A14595A990C4D508B6D3B375607EDB31D4C8703393
contracts	CharacterFireTraitChangeConsumables.sol	68B9D74395A8104EBE0278CE160BA1547D170E8AB76B6E1436B58EBE5AAF9B65
contracts	CharacterLightningTraitChangeConsumables.sol	F2A017F9FC66063B866075CA9CF7CDEBA0DC64D0DDE97928BDF640042023E5F6
contracts	CharacterRenameTagConsumables.sol	51C3E94D86D629D32B3E0708B9E1F7E7773D57B8E3E0EC4231B47EBAA4DE7A5B
contracts	characters.sol	ECF7DBA0F8A02692DAD6D9F018F8C5BE216E59B23C2A30555E43D17D1CB2F3E4
contracts	CharactersBridgeProxyContract.sol	03AA50F5FE9A44063889A5C0623183C8BE84767DE75E491D071D93CF7DD333C7
contracts	CharacterWaterTraitChangeConsumabl.sol	A68F254BA2193FC26C4752557E45A9AF7B86808E33AD4BF3D55643E79470ECC9
contracts	common.sol	D2F0D043AF2CBDC0561D3EAB8A21D70DA79CAE6846462CA077AA80652141BA4F
contracts	Consumables.sol	B92740A8C357DADE01710F9A54B7B85A4B78E8726061DB0B4537C0AE8D5C4C98
contracts	Cosmetics.sol	FAEF0BA44CC6AB1E94486972D7E2D739CF6E71A10A868D0E0C22531D3D22AFAE
contracts	cryptoblades.sol	F15886F286FD1CEA79EFE020CF9539B86A7B0A3C3127DB1792A5D5F80106734A
contracts	DummyRandoms.sol	EF033F5E18BF99437B74CBCAE862B19A558AB7AEE1235F0E50833483117AE7EC
contracts	ExperimentToken.sol	532A49E50087D9C55CD66CFE40FDA312FB736EED92CB05DA49BB07286BE5A7F8
contracts	ExperimentToken2.sol	B41C61C0956D2AE31174583407E7C62519803FA7C99032FC4BAD2DD2C6D2F406
contracts	Garrison.sol	097CE77EA4CF28C2E199C66470F9F5B0A0DE7E9CCA5E4F390D07DB672642DE0FHasMain
contracts	HasMain.sol	ADE76CAF8541F654A42050292A07154DB063432C4AAB6EEE3DB49330020AC810
contracts	JunkBridgeProxyContract.sol	89AC946916DE3139AB8B6B43F8FB958A6629525981E5DA564A38934556971 49D
contracts	KingStakingRewardsUpgradeable.sol	5DD1B5E6153C30B129C95FFB859EE89EBF73384A541EEB7500D6ABE2BB31D1D5

2022年5月24日

ID	文件	SHA-256 checksum
contracts	KingStakingRewardsUpgradeable180.sol	E6939FE6817285305E9CCF403D9B2D4D74D174771B36F08C9607F2DB8DB50D80
contracts	KingStakingRewardsUpgradeable90.sol	1320A57BFB6A271FD9E18115770DB27758180AE00AD1120AB165994F7A7DCE65
contracts	Launchpad.sol	DE17595C5390442B7D226EEE70F6E181C2FDF37A852EA358781C701E9ED034EB
contracts	LP2StakingRewardsUpgradeable.sol	D8E4866F7A318F93CA4FD1E6A74698E996D5E550A33816031F1BEB4759CAA5A2
contracts	LPStakingRewards.sol	497ACCA19732FE07804B2C778726EE60C60A8082EDD73D2DCE7F3AA1081F670B
contracts	LPStakingRewardsUpgradeable.sol	8CB7154BB9E3AC57C787B09C8F8D7AAEA1B97ECA8B8AA02225010179407F08CA
contracts	Merchandise.sol	F3677E74CF17EC78DDE40982A6771A940D1AD780CC154CDB2F6B3BF10B6F1EFC
contracts	Migrations.sol	4FD6092BDFA8B42F19D535C5AC69C4323B0B894717C699E58D5552EEABD04CD4
contracts	multiAccessUpgradeable.sol	51D1DADEFC2EBB7983E6DD5A3FB9C0963CC253D7008F678D1130053E417CFDEF
contracts	NFTMarket.sol	F996D82125DB2FF71CC57C8D5E5E5F70256CB160573685159C59BD2BBC2C01D2
contracts	NFTStorage.sol	FAE74439B6E288CEE75F5EED869AE7ED87017074D0F36CF04919F547B8AC7664
contracts	PartnerVault.sol	37031B9A9C8CF5CC894689019950328F197BD4461EA8C9C0AB4BC054701BBA73
contracts	Promos.sol	D61D62EEDC48FBAA96E8A1C44945934E4CEB072FB83076CFF8E754E495B9DF78
contracts	PvpArena.sol	204B3D545BB16C65F339F8F6AEBF7A7A161F98D633F647A15BFBB4AFE6EC6AA5
contracts	PvpCore.sol	B349A413F7DA0EA42EF994E2410B5F11544F6E444A7A59C2C3992A899741A748
contracts	PvpRankings.sol	E1807313DA6447E3D0CAE004254C9ADD7C6AA558B4D23B6696D4735C5B1CA9D1
contracts	raid.sol	84FA2D6B71B5E72188E3966C407E16C9DD7B2F6815018A0834C9DEEDF95ACF11
contracts	raid1.sol	F8CA8278D4BBB356E6255566259D1D86E8CC88B24A0464676B494079D4DCCBD8
contracts	raidBasic.sol	015450887C1CBB0E6985B6927D59538B447696B64A0BDB2210795740DABE8B73
contracts	SafeRandoms.sol	01245926BA4C2EB278267806D2E1F3FA3C1F0B3DA029B7037563CBE23C8A0BEB
contracts	ShieldBridgeProxyContract.sol	53F1937A507207F65C6F2B3DD928B5F9A71CAFADD660BFA7E14CAB709613F25B
contracts	shields.sol	B0E72D032C9A538B66CDD7C89EFA52F43AB20AB4ABB09E9D58A6FCB27C585371
contracts	SimpleQuests.sol	E91418B6F00115274DCFC5EF6049DE02CAFD719A59DB9EFA771FC88D89E5BE6C

2022年5月24日

ID	文件	SHA-256 checksum
contracts	SkillStakingRewards.sol	070DFA29DCADA388C5F2EFFA1CD638E7E1370D7C7947B452265C21A7029EDD37
contracts	SkillStakingRewardsUpgradeable.sol	FA3D5D22FE37096CE97467FC48A52F548C94B760E9729555A7D616B5A7094369
contracts	SkillStakingRewardsUpgradeable180.sol	FCA6CAF52348E44A8D9A997048D4CB57077514D6AABDA7CF81F70F0EB750F20F
contracts	SkillStakingRewardsUpgradeable90.sol	69D2EC389C9D41566290D56ADCBE002CB07EEE7B586561BAE74B0B3DA2F9A424
contracts	skillToken.sol	570615C27D6CFA7D19B25672B38708ACBE6CD4D3F14E5E83A0CA7666A8C05212
contracts	SpecialWeaponsManager.sol	537AE2E55BC7E78F8B4E49FDC12F9DF92DB9F6EB48FE9DF7782EBCF3244F56D9
contracts	TokensManager.sol	378F980AD3DD50813560E95A144E6A9C839E0DA20C58FBDF58F0E83F5A738C12
contracts	Treasury.sol	4FB90891418BE9C2E1758F781194B72F287CC6CDDD9A06A88DC5A9E39DD74F51
contracts	util.sol	BBBEBFB6A0E22DFDB9564F1739D8CE20E5CA8854D4650AC371E9088DE21AB744
contracts	WaxBridge.sol	3E9FAE3A274357E5CB3CD07B187D05A1FBCDDF4C3686C3BA88E39298C2B00991
contracts	WeaponBridgeProxyContract.sol	D7BF9869E95D70871C40E489A2EBC6F99C183D2B8EAACF36F131E6C5B9B13EA4
contracts	WeaponCosmetics.sol	59C961AF4C252B59B0DC9BC6AF4016CD5CADE7D35E3CAC54B95A6484BB49E47A
contracts	WeaponRenameTagConsumables.sol	7D550EA70E243129F005964E30C1D01D3B725DAA558E014BCDA9714443F61A2D
contracts	weapons.sol	569D377BA889C279EC76CD1E60D9588BCA2631E17C731A309F3AB5195D8DF5BD
contracts/interfaces	IBridgeProxy.sol	2375177B55BA63FBEAAACF50D068A873BF56D5A5260E036F1B50F99496C69A6F
contracts/interfaces	IPriceOracle.sol	C2029D68AE22C64094A67BB6F69839C2DC56A11FA1CBE113142F5E9EB6CA91BD
contracts/interfaces	IRandoms.sol	67CC481B9C1A783F04798FD03D3886C059DC4CD909394D342EC3108878047D57
contracts/interfaces	IStakeFromGame.sol	CBDD0CCAD39DE96FDE4C8F4C534A3E609651A3C0B550D57278E8658D1E972AFF
contracts/interfaces	ITransferCooldownable.sol	5D55CACBBDC387759910EC85B88B32F73C1967FA3F0916C9B600FD2893842A78
contracts/items	Junk.sol	347A8C3CA0768C0689675AD28567A3F52D3392B60B2F19EFB8FC01B84F8C256E
contracts/items	KeyLootbox.sol	C8B6B71E01F7B24D4657DCBC9E9D5B469F9A93FF5D654BAFB003F9D37ABBABF5
contracts/items	RaidTrinket.sol	568B5D7EEF0B3109057D87FF76D88889D84AAA3349C32F544BC4A531A52DD4D9
contracts\partner-giveaways	PartnerGiveaways.sol	A7F5250BC08B0F0A3C7CF734F64E2BCE122BBA7763FC56ACF10A1E847528D878

2022年5月24日

ID	文件	SHA-256 checksum
contracts\staking	Failsafe.sol	03C1AEDF4E1F8A8ED5211F405CDFB68FFD1E13589FC52047277F95AD34ED6348
contracts\staking	FailsafeUpgradeable.sol	4990E928CF0CCC5A66C4A8F752A295A73010DAAFA8F6F661E764FD4C67874692
contracts\staking	NftStakingRewardsUpgradeable.sol	F1A7F293FFC885799654FCDE62DFE9B440DD5FEB446EDB39542BD2B0FF82BF5C
contracts\staking	Owned.sol	1027500BA5A3A511112F3B87ED010608659ED62E8A5476CF6D49268C317BFF32
contracts\staking	RewardsDistributionRecipient.sol	4313F49552C583B9ED751D5C997943B0A06E6CCE1ABBB203AF1FA647509E1B2B
contracts\staking	RewardsDistributionRecipientUpgradeable.sol	7E6F2F4C79B20940B7D5A43F2BBE4F1CF62D9394C4F154A55439466F890F5B8F
contracts\staking	StakingRewards.sol	2FD7D8D5E7AF5D9335F4038C3957FB83B801E2C9BC9A521D0C876F7BF0FDCF05
contracts\staking	StakingRewardsUpgradeable.sol	C30BB33129D1CB2212F1747D9A60A6703D42730ACFDB48D3E0DF0916A104DF06
contracts\staking	SynthetixPausable.sol	B99B71E828E5FB7851E2C35E4937B3800274A5C2D4580FB0B516A7EF82D43D2C
contracts\staking\interfaces	INftStakingRewards.sol	4731DA9F835E3F5A64CFBEDB401A4804DA6678530C9D9E3BED71B554ED0C3D28IStakingRewards.sol
contracts\staking\interfaces	IStakingRewards.sol	DA40E01CEA3358F99DA3E927F9BF10116ADF801A2E4422C5DA17404AC3C762DB

2022年5月24日

4. 代碼結構

| BasicPriceOracle.sol
| Blacksmith.sol
| BurningManager.sol
| BytesChunker.sol
| CBKLand.sol
| CBKLandSale.sol
| CBKLandT1StakingRewardsUpgradeable.sol
| CBKLandT2StakingRewardsUpgradeable.sol
| CBKLandT3StakingRewardsUpgradeable.sol
| ChainlinkRandoms.sol
| CharacterCosmetics.sol
| CharacterEarthTraitChangeConsumables.sol
| CharacterFireTraitChangeConsumables.sol
| CharacterLightningTraitChangeConsumables.sol
| CharacterRenameTagConsumables.sol
| characters.sol
| CharactersBridgeProxyContract.sol
| CharacterWaterTraitChangeConsumables.sol
| common.sol
| Consumables.sol
| Cosmetics.sol
| cryptoblades.sol
| DummyRandoms.sol
| ExperimentToken.sol
| ExperimentToken2.sol
| Garrison.sol
| HasMain.sol
| JunkBridgeProxyContract.sol
| KingStakingRewardsUpgradeable.sol
| KingStakingRewardsUpgradeable180.sol
| KingStakingRewardsUpgradeable90.sol
| Launchpad.sol
| LP2StakingRewardsUpgradeable.sol
| LPStakingRewards.sol
| LPStakingRewardsUpgradeable.sol
| Merchandise.sol
| Migrations.sol
| multiAccessUpgradeable.sol
| NFTMarket.sol
| NFTStorage.sol
| PartnerVault.sol

```
|   Promos.sol
|   PvpArena.sol
|   PvpCore.sol
|   PvpRankings.sol
|   raid.sol
|   raid1.sol
|   raidBasic.sol
|   SafeRandoms.sol
|   ShieldBridgeProxyContract.sol
|   shields.sol
|   SimpleQuests.sol
|   SkillStakingRewards.sol
|   SkillStakingRewardsUpgradeable.sol
|   SkillStakingRewardsUpgradeable180.sol
|   SkillStakingRewardsUpgradeable90.sol
|   skillToken.sol
|   SpecialWeaponsManager.sol
|   TokensManager.sol
|   Treasury.sol
|   util.sol
|   WaxBridge.sol
|   WeaponBridgeProxyContract.sol
|   WeaponCosmetics.sol
|   WeaponRenameTagConsumables.sol
|   weapons.sol
|
├──interfaces
|       IBridgeProxy.sol
|       IPriceOracle.sol
|       IRandoms.sol
|       IStakeFromGame.sol
|       ITransferCooldownable.sol
|
├──items
|       Junk.sol
|       KeyLootbox.sol
|       RaidTrinket.sol
|
├──partner-giveaways
|       PartnerGiveaways.sol
|
```

2022年5月24日

```
└──staking
   |   Failsafe.sol
   |   FailsafeUpgradeable.sol
   |   NftStakingRewardsUpgradeable.sol
   |   Owned.sol
   |   RewardsDistributionRecipient.sol
   |   RewardsDistributionRecipientUpgradeable.sol
   |   StakingRewards.sol
   |   StakingRewardsUpgradeable.sol
   |   SynthetixPausable.sol
   |
   └──interfaces
       INftStakingRewards.sol
       IStakingRewards.sol
```

2022年5月24日

審計報告匯總

1. 審計方式

通過清晰地理解該項目的設計目的、運行原理和實現管道，稽核團隊對合約程式碼進行了深入的研究和分析。 在分清各個合約及其函數的調用關係的基礎上，對合約可能存在的漏洞進行了定位及分析。 最終產生問題描述和給出相應的修改意見。

審計方法	Static analysis, Manual Review

2. 審計流程

步驟	操作	詳細內容
1	背景研究	閱讀項目介紹、白皮書、合約源碼等項目方團隊提供的相關信息，確保正確理解項目功能
2	自動化檢測	主要用自動化工具掃描源碼，找到常見的潛在漏洞
3	人工審閱	工程師逐行閱讀代碼，找到潛在漏洞
4	邏輯校對	工程師將對代碼的理解和項目方提供的信息比較，檢查代碼實現是否符合項目白皮書信息
5	測試用例檢測	包括測試用例設計，測試範圍分析、符號執行等
6	優化審查	根據應用場景、調用方式及最新的研究成果從可維護性、安全性及可操作性等方面審查項目

2022年5月24日

3. 風險分級

風險級別	風險描述
致命	存在致命風險及隱患，需要立即解決
高危	存在高危風險及隱患，將引發相同問題，必須解決
中度	存在中度風險及隱患，可能導致潛在風險，最終仍然需要解決
低危	存在低風險及隱患，指各類處理不當或會引發警告信息的細節，這類問題可暫時擱置
建議	存在可優化的部分，這類問題可以擱置，但建議最終解決

4. 審計結果

編號	審計項目	風險級別	狀態
1	重入	高	已告知
2	注入	無	
3	權限繞過	無	
4	Mempool搶跑	中	已告知
5	回滾	無	
6	條件競爭	無	
7	循環耗盡gas	中	已告知
8	閃電貸高影響	無	
9	經濟模型不合理	高	已告知
10	可預見的隨機數	無	
11	投票權管理混亂	無	

2022年5月24日

編號	審計項目	風險級別	狀態
12	數據隱私洩露	無	
13	鏈上時間使用不當	無	
14	Fallback函數編碼不當	無	
15	鑒權不當	高	已告知
16	Opcode使用不當	無	
17	內聯匯編使用不當	無	
18	構造函數不規範	無	
19	返回值不規範	無	
20	Event不規範	無	
21	關鍵字使用不規範	無	
22	未遵循ERC標準	無	
23	條件判斷不規範	中	已告知
24	流動性枯竭風險	無	
25	中心化風險	無	
26	邏輯變更風險	無	
27	整數溢出	無	
28	函數可見性不當	無	
29	變量初始化不當	高	已告知
30	合約間調用不當	無	
31	變量不規範	無	
32	重放	無	
33	隨機存儲位置寫入	無	
34	蜜罐邏輯	無	
35	哈希碰撞	無	
36	計算精度丟失	低	已告知
37	無意義的合約	低	已告知
38	已棄用的合約	低	已告知

上述表格中，狀態欄內容若為「已告知」，則表示審計團隊已告知項目方項目存在的漏洞，但項目方未對漏洞進行修改，或未告知審計團隊漏洞的修改進度。若狀態欄中填寫「已修改」則表示項目方已進行對漏洞的修改，並通過審計團隊確認。

2022年5月24日

5. 風險項與修改方案

以下部分為審計後得知的風險項相關詳細信息，其中內容包括風險類型、風險級別、問題位置、問題描述、修改建議及項目方反饋。

風險類型	鑒權不當	風險級別	高风险
位置	Line 303, 309	合約文件	cryptobaldes.sol
問題描述	函數中使用tx.origin作為參數，存在釣魚攻擊或繞過鑒權的隱患		
修改建議	採用msg. sender作為傳參代替tx.origin		
項目方反饋			

風險類型	鑒權不當	風險級別	高风险
位置	Line 133, 136	合約文件	BurningManager.sol
問題描述	函數中使用tx.origin作為支付操作的參數，存在釣魚攻擊或繞過鑒權的隱患		
修改建議	採用msg. sender作為傳參代替tx.origin		
項目方反饋			

風險類型	循環耗盡	風險級別	中風險
位置	Line 114	合約文件	BurningManager.sol
問題描述	該方法可被其他寫方法調用，迴圈沒有限制		
修改建議	限制迴圈次數，或限制調用許可權		
項目方反饋			

風險類型	循環耗盡	風險級別	中風險
位置	Line149,161,184,204,327	合約文件	PVPRankings.sol
問題描述	迴圈次數未知		
修改建議	限制迴圈次數，或限制調用許可權		
項目方反饋			

2022年5月24日

風險類型	經濟模型不合理	風險級別	高风险
位置	Line 8, 13	合約文件	KingStakingRewardsUpgradeable.sol
問題描述	因為super. withdraw（amount）； 和super. getReward（）； 兩個函數並沒有收取手續費，所以withdrawWithoutFee函數和getRewardWithoutFee函數會多返還1%的取款金額。		
修改建議	取消返還手續費		
項目方反饋			

風險類型	條件判斷不規範	風險級別	中風險
位置	Line 254	合約文件	weapons.sol
問題描述	當前只支持5星武器，mintSpecialWeapon函數中對星級的限制為require（stars < 8）；， minter可以鑄造高於當前版本星級限制的武器。		
修改建議	判斷語句設定為require（stars < 6）		
項目方反饋			

風險類型	条件判断不规范	風險級別	中風險
位置	Line 178, 192	合約文件	shields.sol
問題描述	當前只支持5星盾牌，mintShieldsWithStars函數中對星級的限制為require（stars < 8，“Stars parameter too high！ （max 7）”）；， minter可以鑄造高於當前版本星級限制的盾牌。		
修改建議	判斷語句設定為require（stars < 6）；		
項目方反饋			

風險類型	条件判断不规范	風險級別	中風險
位置	Line 45, 50	合約文件	CharacterRenameTagConsumables.sol
問題描述	在setMinSize和setMaxSize函數中，沒有檢查修改後的結果是否滿足_ minSize < _ maxSize，可能導致改名功能失效。		
修改建議	添加判斷語句require（newMinSize < _maxSize）； 和require（_minSize < newMaxSize）；		
項目方反饋			

2022年5月24日

風險類型	鑒權不當	風險級別	高风险
位置	Line 30	合約文件	DummyRandoms.sol
問題描述	setRandomNumberForTestingPurposes函數可以被任何人調用，進而修改uint256 private seed的值		
修改建議	添加鑒權檢測		
項目方反饋			

風險類型	計算精度丟失	風險級別	低風險
位置	Line 158, 169, 355 Line 91, 93	合約文件	Launchpad.sol Treasury.sol
問題描述	計算過程中採用先除後乘的順序，有可能遺失精度		
修改建議	調整為先乘後除		
項目方反饋			

風險類型	重入	風險級別	高風險
位置	Line 429	合約文件	Launchpad.sol
問題描述	該函數在safeTransfer處能够被進行重入，使得emit的順序倒轉		
修改建議	將safeTransfer的位置放到函數的最後		
項目方反饋			

風險類型	重入	風險級別	高風險
位置	Line 163	合約文件	Treasury.sol
問題描述	claim在轉帳之後，，仍然有數值計算，如果為惡意erc20合約，可造成重入		
修改建議	添加重入鎖		
項目方反饋			

風險類型	重入	風險級別	高風險
位置	Line 456	合約文件	Launchpad.sol
問題描述	該函數在safeTransferFrom處能够被進行重入，前提是lp. fundingTokenAddress代幣是惡意的，可以繞過require（launchTotalRaised[launchId] + amount <= launchFundsToRaise[launchId]）檢測		
修改建議	添加重入鎖		
項目方反饋			

2022年5月24日

風險類型	條件判斷不規範	風險級別	中风险
位置	Line 586	合約文件	NFTMarket.sol
問題描述	沒有判斷上一個函數調用executePurchaseLogic的返回值，警惕假轉帳風險		
修改建議	添加返回值判斷		
項目方反饋			

風險類型	mempool搶跑	風險級別	中風險
位置	Line 522	合約文件	NFTMarket.sol
問題描述	用戶出價購買時，賣家可以搶跑提高價格		
修改建議	判斷餘額是否够finalprice		
項目方反饋			

風險類型	變數初始化不當	風險級別	低風險
位置	Line 119, 120, 126, 136	合約文件	NFTStorage.sol
問題描述	合約並沒有對transferInsMeta，transferInSeeds，transferInChainId，_transferInsLog四個變數賦值的功能（變數為空），但是他們在函數的執行過程中被訪問。		
修改建議	添加變數賦值的功能		
項目方反饋			

風險類型	無意義的合約	風險級別	低風險
位置		合約文件	CKingStakingRewardsUpgradeable180.sol KingStakingRewardsUpgradeable90.sol LP2StakingRewardsUpgradeable.sol LPStakingRewardsUpgradeable.sol SkillStakingRewardsUpgradeable180.sol SkillStakingRewardsUpgradeable90.sol
問題描述	以上合約沒有實際的程式碼邏輯		
修改建議	從項目中移除		
項目方反饋			

風險類型	已弃用的合約	風險級別	低風險
位置	L16	合約文件	raid.sol raidBasic.sol
問題描述	以上合約已被弃用，且沒有被調用的情況		
修改建議	從項目中移除		
項目方反饋			

2022年5月24日

6. 增強建議

N/A

2022年5月24日

免責聲明

i. 本審計報告僅針對最終出具報告中載明的審計類型進行審計，其他未知安全漏洞不在本次審計責任範圍之內，我方無需為此承擔責任。

ii. 我方僅應根據審計報告發布之前存在或發生的攻擊或漏洞發布審計報告。對於將來存在或發生的新攻擊或漏洞，我方無法確定對其項目安全狀態的可能影響，對此概不負責。

iii. 我方發布的審計報告中的安全審計分析及其他內容應僅基於項目方在發布審計報告之前向我方提供的文件和材料（包括但不限於合約代碼），並且上述文件和資料不應該存在缺乏信息、被篡改、刪除或隱藏的情況，如果項目方提供的文件和資料存在不真實、不準確、缺乏信息、被篡改、刪除或隱藏的情況，或者對上述文件和資料的改動是在發布審計報告之後作出的，我方不承擔因反映情況與實際情況不一致引起的損失和不利影響 。

iv. 項目方知曉我方出具的審計報告系根據項目方提供的文件和資料、依靠我方現掌握的技術而作出的。但由於任何機構均存在技術的局限性，我方作出的審計報告仍存在無法完整檢測出全部風險的可能性。我方審計團隊鼓勵項目的開發團隊以及任何相關利益方對項目進行後續的測試及審計。

v. 項目方保證其委托我方提供審計或測試服務的項目合法、合規，且不違反適用法律。審計報告僅用於項目方參考，審計報告的內容、獲取方式、使用以及任何其所涉及的服務或資源都不能作為任何形式的投資、稅務、法律、監管及建議等的依據，我方不因此承擔相關責任。在未經我方書面同意之前，項目方不得將審計報告的全部或部分內容以任何形式提及、引用、展示或發送給任何第三方，否則由此產生的任何損失和責任由項目方自行承擔。我方對任何人依賴審計報告或將之用於任何目的概不承擔責任 。

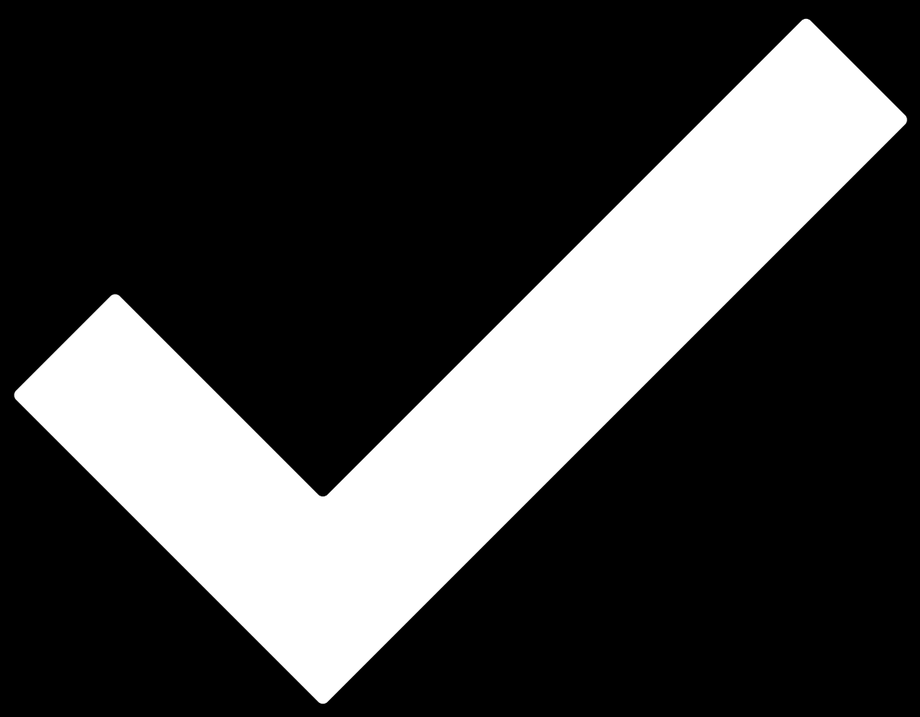
vi. 本審計報告不涉及合約的編譯器及任何超出智能合約編程語言的領域，所審計的智能合約因引用鏈下信息或資源所導致的風險及責任，由項目方自行承擔 。

vii. 不可抗力。不可抗力是指雙方在訂立合同時不能預見、對其發生和後果不能避免且不能克服的事件，包括但不限於戰爭、臺風、水災、火災、地震、潮汐、雷電、天災、罷工、核爆炸、流行病等自然災害和法律、法規和政策變更及政府行為等其它不可預見，對其發生和後果不能防止或避免的事件，且該事件妨礙、影響或延誤任何一方根據合同履行其全部或部分義務。

viii. 如果有一方認為不可抗力發生影響履行本協議義務，應迅速通知另一方，按事件對履約影響的程度，由雙方協商決定是否終止合同或部分免除履約的責任，或者延期履約。

ix. 當不可抗力發生時，任何一方都不能被視作違約或不履行本協議義務。在事件前存在的經濟上的責任，不應受到影響，項目方應對我方已完成工作做出支付。

2022年5月24日



審計通過.

日期 2022年5月24日

審計 歐科雲鏈

本次稽核的目的是為了審閱CryptoBlades項目基於Solidity語言實現的遊戲內容，其中包括角色和裝備的NFT代幣、角色陞級系統、裝備重鑄系統、競技場功能、土地販賣功能、以及獎勵發放等，研究其設計、架構，發現潛在的安全隱患，並試圖找到可能存在的漏洞。