CryptoBlades

Contract Audit Report

VER 1.0

24 May 2022

No. 2022052421171

Project Summary

1. Project Introduction

CryptoBlades is an NFT role-playing game on BNB SmartChain. The core of the game is to reward players with SKILL tokens after defeating enemies and participating in raids. Players can hire multiple characters and forge distinctive weapons. They can also recast these weapons to increase their all-round strength. Players can trade their characters and weapons in an open market. They can also mortgage their SKILL and get extra SKILL as a reward.

2. Audit Summary

Project Name	CryptoBlades	Platform	N/A
Token	N/A	Token symbol	N/A
Start date	2022年5月9日	Language	Solidity
End date	2022年5月23日	Website	N/A
Github	https://github.com/CryptoBlades/cryptoblades	Whitepaper	N/A

3. Audit Scope

ID	File	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

ID	File	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	89AC946916DE3139AB8B6B43F8FB958A6629525981E5DA564A3893455697149D
contracts	KingStakingRewardsUpgradeable.sol	5DD1B5E6153C30B129C95FFB859EE89EBF73384A541EEB7500D6ABE2BB31D1D5

ID	File	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

ID	File	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

ID	File	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

4. Code Structure

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

Audit Report Summary

1. Audit Methods

The audit was conducted to gain a clear understanding of how the project was implemented and how it works. The audit team conducted in-depth research, analysis, and testing of the project code and collected detailed data. In this report, the audit team will list in detail each issue identified, where it is located, the root cause of the issue, and a description of the issue, and will recommend changes to the issue accordingly.

Audit methods	Static analysis, Manual Review

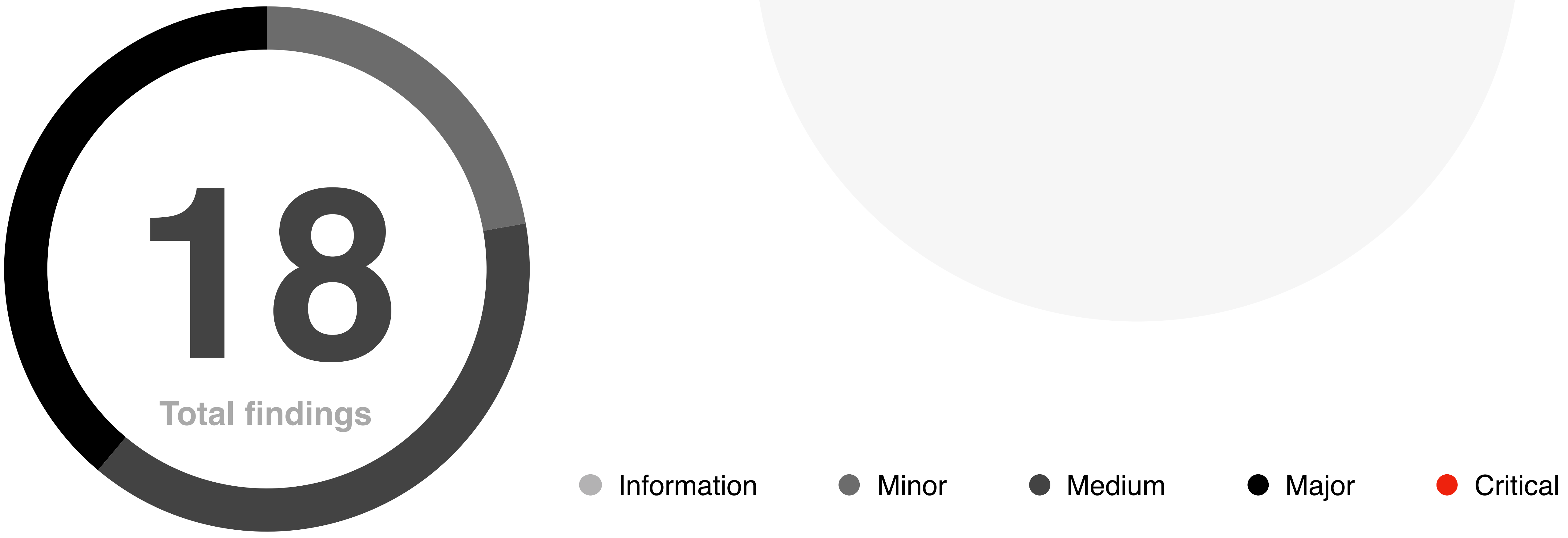
2. Audit Process

Steps	Operation	Description
1	Background	Read project descriptions, white papers, contract source code, and other relevant information the project team provides to ensure a proper understanding of project functions.
2	Automated testing	Scanning source code mainly with automated tools to find common potential vulnerabilities.
3	Manual reveiw	Engineers read the code line by line to find potential vulnerabilities.
4	Logical proofread	The engineer will compare the understanding of the code with the information provided by the project and check whether the code implementation is in line with the project white paper information.
5	Test case	Including test case design, test scope analysis, symbolic execution, etc.
6	Optimization items	Review of projects in terms of maintainability, safety, and operability based on application scenarios, deployment methods, and latest research results.

3. Risk Levels

Risk level	Issue description
Critical	Fatal risks and hazards that need to fixed immediately.
Major	Some high risks and hazards that will lead to related problems that must be solved
Medium	Some moderate risks and pitfalls may lead to potential risks that will eventually need to be addressed
Minor	There are low risks and hazards, mainly details of various types of mishandling or warning messages, which can be set aside for the time being
Information	Some parts can be optimized, such problems can be shelved, but it is recommended that the final solution

4. Audit Results



ID	Audit project	Risk level	Status
1	Reentrancy	Major	Acknowledged
2	Injection	None	
3	Authentication bypass	None	
4	MEV Possibility	Medium	Acknowledged
5	Revert	None	
6	Race condition	None	
7	Insufficient Gas Griefing	Medium	Acknowledged
8	The major impact of flash loans	None	
9	Unreasonable economic model	Major	Acknowledged
10	Predictable random numbers	None	
11	Voting rights management confusion	None	

ID	Audit project	Risk level	Status
12	Privacy leak	None	
13	Improper use of time on chain	None	
14	Improper codes in fallback function	None	
15	Improper identification	Major	Acknowledged
16	Inappropriate opcode	None	
17	Inappropriate assembly	None	
18	Constructor irregularities	None	
19	Return value irregularity	None	
20	Event irregularity	None	
21	Keywords irregularity	None	
22	Not following ERC standards	None	
23	Irregularity of condition judgment	Medium	Acknowledged
24	Risk of liquidity drain	None	
25	Centralization Risk	None	
26	Logic change risk	None	
27	Integer overflow	None	
28	Improper function visiblity	None	
29	Improper initialization of variables	Major	Acknowledged
30	Improper contract calls	None	
31	Variable irregularities	None	
32	Replay	None	
33	Write to Arbitrary Storage Location	None	
34	Honeypot logic	None	
35	Hash collision	None	
36	Loss of calculation accuracy	Minor	Acknowledged
37	Meaningless contracts	Minor	Acknowledged
38	Abandoned contracts	Minor	Acknowledged

*In the above table, if the status column is “**Acknowledged**”, the audit team has informed the project owner of the vulnerability. Still, the project owner has not made any changes to the vulnerability or has not announced to the audit team the progress of the changes to the vulnerability. If the status column is “**Resolved**”, the project owner has changed the exposure, and the audit team has confirmed the changes.

5. Risk and Modification Program

The following section provides detailed information about the risk items learned after the audit, including the type of risk, risk level, location of the issue, description of the problem, recommendations for changes, and feedback from the project owner.

Risk type	**Improper identification**	**Risk level**	**Major**
Location	Line 303, 309	**Contract file**	cryptobaldes.sol
Description	Tx.origin is used as a parameter in the function, which has the hidden danger of phishing attack or bypassing authentication		
Recommedation	Use msg.sender replaces tx.origin as a parameter		
Update			

Risk type	**Improper identification**	**Risk level**	**Major**
Location	Line 133, 136	**Contract file**	BurningManager.sol
Description	Tx.origin is used as the parameter of payment operation in the function, which has the hidden danger of phishing attack or bypassing authentication		
Recommedation	Use msg.sender replaces tx.origin as a parameter		
Update			

Risk type	**Insufficient Gas Griefing**	**Risk level**	**Medium**
Location	Line 114	**Contract file**	BurningManager.sol
Description	This method can be called by other write methods, and there is no limit on loopback		
Recommedation	Limit the number of loops, or limit the call permission		
Update			

Risk type	**Insufficient Gas Griefing**	**Risk level**	**Medium**
Location	Line149,161,184,204,327	**Contract file**	PVPRankings.sol
Description	Unknown number of loops		
Recommedation	Limit the number of loops, or limit the call permission		
Update			

Risk type	**Unreasonable economic model**	**Risk level**	**Major**
Location	Line 8, 13	**Contract file**	KingStakingRewardsUpgradeable.sol
Description	No commition is charged with two functions (super. Withraw (amount); And super getReward （）；),so the withdrawwithoutfee function and getrewardwithoutfee function will return extra 1% of the withdrawal amount.		
Recommedation	Cancel the design of returning commition		
Update			

Risk type	**Irregularity of condition judgment**	**Risk level**	**Medium**
Location	Line 254	**Contract file**	weapons.sol
Description	At present, only 5-star weapons are supported, and the star is limited in mintspecialweapon function is required (stars < 8);, Minter can mint weapons higher than the limited star of the current version.		
Recommedation	The judgment statement is set to require (stars < 6)		
Update			

Risk type	**Irregularity of condition judgment**	**Risk level**	**Medium**
Location	Line 178, 192	**Contract file**	shields.sol
Description	At present, only 5-star shields are supported. The limit of stars in mintshildswithstars function is required (stars < 8, "stars parameter too high! (max 7)");, Minter can mint shields higher than the limited star of the current version.		
Recommedation	The judgment statement is set to require (stars < 6)		
Update			

Risk type	**Irregularity of condition judgment**	**Risk level**	**Medium**
Location	Line 45, 50	**Contract file**	CharacterRenameTagConsumables.sol
Description	There is no consideration in setminsize and setmaxsize functions whether the results after checked meet the requirements_ minSize < _ Maxsize, which may cause the renaming function to fail.		
Recommedation	Add the judgment statement require (newminsize < _maxsize); And require (_minsize < newmaxsize);		
Update			

Risk type	**Improper identification**	**Risk level**	**Major**
Location	Line 30	**Contract file**	DummyRandoms.sol
Description	The < setrandomnumberfortestingpurposes > function can be called by anyone to modify the value of uint256 private seed		
Recommedation	Add identification detection		
Update			

Risk type	**Loss of calculation accuracy**	**Risk level**	**Minor**
Location	Line 158, 169, 355 Line 91, 93	**Contract file**	Launchpad.sol Treasury.sol
Description	If the order of division before multiplication is adopted in the calculation process, the accuracy may be lost		
Recommedation	Adjust to multiply before divide		
Update			

Risk type	**Reentrancy**	**Risk level**	**Major**
Location	Line 429	**Contract file**	Launchpad.sol
Description	This function can be reentrant at < safetransfer > to reverse the order of emit		
Recommedation	Put the position of < safetransfer > at the end of the function		
Update			

Risk type	**Reentrancy**	**Risk level**	**Major**
Location	Line 163	**Contract file**	Treasury.sol
Description	Claim still has numerical calculation after the transfer. If it is a malicious erc20 contract, it can cause a reentry attack		
Recommedation	Add reentry lock		
Update			

Risk type	**Reentrancy**	**Risk level**	**Major**
Location	Line 456	**Contract file**	Launchpad.sol
Description	This function can be reentrant at < safetransferfrom >, and the premise of this attack is < LP Fundingtokenaddress > tokens are malicious and can bypass the require (launchtotalraised [launchid] + amount < = launchfunds toraise [launchid]) detection		
Recommedation	Add reentry lock		
Update			

Risk type	**Irregularity of condition judgment**	**Risk level**	**Medium**
Location	Line 586	**Contract file**	NFTMarket.sol
Description	Failed to judge the return value of the previous function call < executepurchaselogic >, and was alert to the risk of false transfer		
Recommedation	Add return value judgment		
Update			

Risk type	**MEV Possibility**	**Risk level**	**Medium**
Location	Line 522	**Contract file**	NFTMarket.sol
Description	When users bid to buy, the seller can raise the price in advance		
Recommedation	Determine whether the balance is sufficient for finalprice		
Update			

Risk type	**Improper initialization of variables**	**Risk level**	**Minor**
Location	Line 119, 120, 126, 136	**Contract file**	NFTStorage.sol
Description	The contract does not have the function of assigning values to these four variables (transferinsmeta, transferinseeds, transferinchainid, transferinslog) (the variables are empty), but they are accessed during the execution of the function.		
Recommedation	Add variable assignment function		
Update			

Risk type	**Meaningless contracts**	**Risk level**	**Minor**
Location		**Contract file**	CKingStakingRewardsUpgradeable180.sol KingStakingRewardsUpgradeable90.sol LP2StakingRewardsUpgradeable.sol LPStakingRewardsUpgradeable.sol SkillStakingRewardsUpgradeable180.sol SkillStakingRewardsUpgradeable90.sol
Description	The above contract has no actual code logic		
Recommedation	Remove from project		
Update			

Risk type	**Abandoned contracts**	**Risk level**	**Minor**
Location	L16	**Contract file**	raid.sol raidBasic.sol
Description	The above contract has been abandoned and has not been invoked		
Recommedation	Remove from project		
Update			

6. Recommendation

N/A

Disclaimer

i. This audit report focuses only on the types of audits identified in the final report issued. Other unknown security vulnerabilities are not part of this audit, and we do not accept responsibility for them.

ii. We shall only issue an audit report based on an attack or vulnerability that existed or occurred before the issuance of the audit report. We cannot determine the likely impact on the security posture of our projects for new attacks or vulnerabilities that may exist or occur in the future, and we are not responsible for them.

iii. The security audit analysis and other elements of our published audit report shall be based solely on documents and materials (including, but not limited to, contract codes) provided to us by the Project Party before the release of the audit report. Such documents and materials shall not be untrue, inaccurate, uninformative, altered, deleted, or concealed, and if the documents and materials provided by the Project Party are false, inaccurate, uninformative, changed, deleted or hidden, or if the documents and materials provided by the Project Party are untrue, inaccurate, uninformative, altered, deleted or concealed, or if the documents and materials provided by the Project Party are uninformative, uninformative, altered, deleted or hidden. If the records and information provided by the Project Party are untrue, inaccurate, uninformative, altered, deleted, or concealed, or if changes to such documents and information are made after the issuance of the audit report, we shall not be liable for any loss or adverse effect arising from any inconsistency between the reflected and actual conditions.

iv. The Project Parties are aware that our audit report is based on documents and information provided by the Project Parties and relies on the technology currently available. However, due to the technical limitations of any organization, there is a possibility that our audit report may not fully detect all risks. Our audit team encourages the project development team and any interested parties to conduct subsequent testing and audits of the project.

v. The project owner warrants that the project for which we are engaged to provide audit or testing services is legal, compliant, and does not violate applicable laws. The audit report is for the project owner's reference only, and the contents, manner of obtaining, use of, and any services or resources involved in the audit report shall not be relied upon for investment, tax, legal, regulatory, or advisory purposes of any kind, and we shall not be liable therefor. The Project Party shall not refer to, quote, display, or send the Audit Report in whole or in part to any third party without our prior written consent. The Project Party shall bear any loss or liability arising from that place. We assume no responsibility for any reliance on or use of the audit report for any purpose.

vi. This audit report does not cover the compiler of the contract or any areas beyond the programming language of the Smart Contract. The risk and liability of the audited Smart Contract arising from references to off-chain information or resources is the sole responsibility of the project party.

Passed.

Date	24 May 2022
Audit Team	歐科雲鏈

The purpose of this audit is to review the game content of CryptoBlades based on solidity, including NFT token of characters and equipment, character upgrade system, equipment recasting system, arena function, land selling function, reward distribution, etc. The design and architecture will be studied to find potential security risks and try to find possible vulnerabilities.