



SOLIDProof
Bring trust into your projects

Blockchain Security | Smart Contract Audits | KYC

MADE IN GERMANY

DPAD Finance

Audit

Security Assessment
05. May, 2022

For



Disclaimer	3
Description	5
Project Engagement	5
Logo	5
Contract Link	5
Methodology	7
Used Code from other Frameworks/Smart Contracts (direct imports)	8
Tested Contract Files	9
Source Lines	11
Risk Level	11
Capabilities	12
Inheritance Graph	14
CallGraph	15
Scope of Work/Verify Claims	16
Modifiers and public functions	18
Source Units in Scope	23
Critical issues	25
High issues	25
Medium issues	25
Low issues	25
Informational issues	26
Commented Code exist	27
Audit Comments	28
SWC Attacks	29

Disclaimer

SolidProof.io reports are not, nor should be considered, an “endorsement” or “disapproval” of any particular project or team. These reports are not, nor should be considered, an indication of the economics or value of any “product” or “asset” created by any team. SolidProof.io do not cover testing or auditing the integration with external contract or services (such as Uniswap, Uniswap, PancakeSwap etc’...)

SolidProof.io Audits do not provide any warranty or guarantee regarding the absolute bug- free nature of the technology analyzed, nor do they provide any indication of the technology proprietors. SolidProof Audits should not be used in any way to make decisions around investment or involvement with any particular project. These reports in no way provide investment advice, nor should be leveraged as investment advice of any sort.

SolidProof.io Reports represent an extensive auditing 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. SolidProof’s position is that each company and individual are responsible for their own due diligence and continuous security. SolidProof in no way claims any guarantee of security or functionality of the technology we agree to analyze.

Version	Date	Description
1.0	05. May 2022	<ul style="list-style-type: none">• Layout project• Automated- /Manual-Security Testing• Summary

Network

Binance Smart Chain (BEP20)

Website

<https://dpad.finance/>

Telegram

<https://t.me/dpadfinance>

<https://t.me/dpadAnn>

Twitter

<https://twitter.com/DpadFinance>

Instagram

<https://instagram.com/dpadfinance>

Github

<https://github.com/dpad-finance>

Medium

<https://dpadofficial.medium.com/>

Youtube

https://www.youtube.com/channel/UC05XTz4x_KNisSHHwlgaSBA

Description

Dpad protocol is the world's first social venture builder.

Build the next generation Launchpad for founders focused on decentralized Web3 platforms.

Project Engagement

During the 3rd of May 2022, **DPAD Finance Team** engaged Solidproof.io to audit smart contracts that they created. The engagement was technical in nature and focused on identifying security flaws in the design and implementation of the contracts. They provided Solidproof.io with access to their code repository and whitepaper.

Logo



Contract Link

v1.0

- Github
 - <https://gitlab.com/bsc-launchpad/launchpad-contracts/-/tree/master/contracts>
 - Commit: 185018925bbd5931d237d07e609a0122baf3c2f2

Vulnerability & Risk Level

Risk represents the probability that a certain source-threat will exploit vulnerability, and the impact of that event on the organization or system. Risk Level is computed based on CVSS version 3.0.

Level	Value	Vulnerability	Risk (Required Action)
Critical	9 - 10	A vulnerability that can disrupt the contract functioning in a number of scenarios, or creates a risk that the contract may be broken.	Immediate action to reduce risk level.
High	7 – 8.9	A vulnerability that affects the desired outcome when using a contract, or provides the opportunity to use a contract in an unintended way.	Implementation of corrective actions as soon as possible.
Medium	4 – 6.9	A vulnerability that could affect the desired outcome of executing the contract in a specific scenario.	Implementation of corrective actions in a certain period.
Low	2 – 3.9	A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective.	Implementation of certain corrective actions or accepting the risk.
Informational	0 – 1.9	A vulnerability that have informational character but is not effecting any of the code.	An observation that does not determine a level of risk

Auditing Strategy and Techniques Applied

Throughout the review process, care was taken to evaluate the repository for security-related issues, code quality, and adherence to specification and best practices. To do so, reviewed line-by-line by our team of expert pentesters and smart contract developers, documenting any issues as there were discovered.

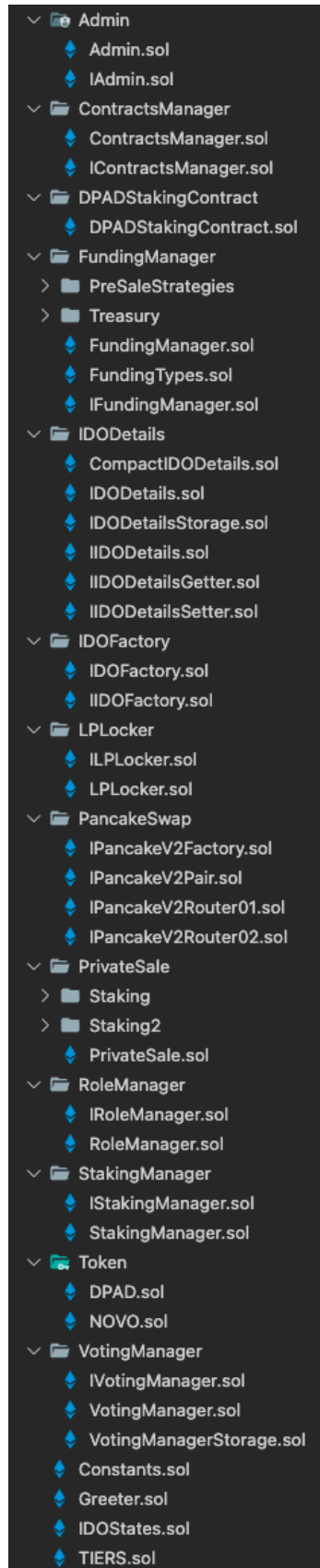
Methodology

The auditing process follows a routine series of steps:

1. Code review that includes the following:
 - i) Review of the specifications, sources, and instructions provided to SolidProof to make sure we understand the size, scope, and functionality of the smart contract.
 - ii) Manual review of code, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
 - iii) Comparison to specification, which is the process of checking whether the code does what the specifications, sources, and instructions provided to SolidProof describe.
2. Testing and automated analysis that includes the following:
 - i) Test coverage analysis, which is the process of determining whether the test cases are actually covering the code and how much code is exercised when we run those test cases.
 - ii) Symbolic execution, which is analysing a program to determine what inputs causes each part of a program to execute.
3. Best practices review, which is a review of the smart contracts to improve efficiency, effectiveness, clarify, maintainability, security, and control based on the established industry and academic practices, recommendations, and research.
4. Specific, itemized, actionable recommendations to help you take steps to secure your smart contracts.

Used Code from other Frameworks/Smart Contracts (direct imports)

Imported packages:



▼ Admin
Admin.sol
IAdmin.sol
▼ ContractsManager
ContractsManager.sol
IContractsManager.sol
▼ DPADStakingContract
DPADStakingContract.sol
▼ FundingManager
> PreSaleStrategies
> Treasury
FundingManager.sol
FundingTypes.sol
IFundingManager.sol
▼ IDODetails
CompactIDODetails.sol
IDODetails.sol
IDODetailsStorage.sol
IIDODetails.sol
IIDODetailsGetter.sol
IIDODetailsSetter.sol
▼ IDOFactory
IDOFactory.sol
IIDOFactory.sol
▼ LPLocker
ILPLocker.sol
LPLocker.sol
▼ PancakeSwap
IPancakeV2Factory.sol
IPancakeV2Pair.sol
IPancakeV2Router01.sol
IPancakeV2Router02.sol
▼ PrivateSale
> Staking
> Staking2
PrivateSale.sol
▼ RoleManager
IRoleManager.sol
RoleManager.sol
▼ StakingManager
IStakingManager.sol
StakingManager.sol
▼ Token
DPAD.sol
NOVO.sol
▼ VotingManager
IVotingManager.sol
VotingManager.sol
VotingManagerStorage.sol
Constants.sol
Greeter.sol
IDOSates.sol
TIERS.sol

Dependency / Import Path	Count
@openzeppelin/contracts-upgradeable/access/OwnableUpgradeable.sol	2
@openzeppelin/contracts-upgradeable/proxy/utils/Initializable.sol	7
@openzeppelin/contracts/access/AccessControlEnumerable.sol	1
@openzeppelin/contracts/token/ERC20/ERC20.sol	2
@openzeppelin/contracts/token/ERC20/IERC20.sol	7
@openzeppelin/contracts/token/ERC20/extensions/ERC20Burnable.sol	2
@openzeppelin/contracts/token/ERC20/extensions/IERC20Metadata.sol	2
@openzeppelin/contracts/utils/Address.sol	1
@openzeppelin/contracts/utils/Counters.sol	2
@openzeppelin/contracts/utils/math/SafeMath.sol	7
hardhat/console.sol	1

Tested Contract Files

This audit covered the following files listed below with a SHA-1 Hash.

A file with a different Hash has been modified, intentionally or otherwise, after the security review. A different Hash could be (but not necessarily) an indication of a changed condition or potential vulnerability that was not within the scope of this review.

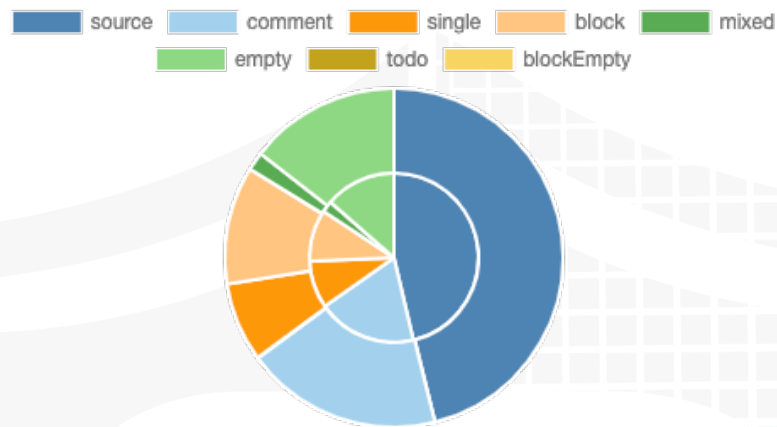
v1.0

File Name	SHA-1 Hash
contracts/VotingManager/IVotingManager.sol	be68e7b1cb5d72bdaeb9fc117a0aabe10c5c3aa7
contracts/VotingManager/VotingManager.sol	2bd3ef516441dcd0aba83ed56859d4d0710c0be9
contracts/VotingManager/VotingManagerStorage.sol	8166f196178eb78d93c9c7157ad971deda1ad949
contracts/PrivateSale/Staking/Staking.sol	f74a5fb020ed741b05e1bf6ea862d3889301b466
contracts/PrivateSale/Staking/math/SafeMath.sol	43ae5905ed6ab95525ffe157f231efbc8df83b1e
contracts/PrivateSale/Staking/utills/Address.sol	b7073b366ca2d639ddae2cbd8a02f15c841bf60c
contracts/PrivateSale/Staking/GSN/Context.sol	62650c73f54a5f6cca403089e478a03f2d80bf78
contracts/PrivateSale/Staking/access/Manageable.sol	24fdda8a04ff933ea2f0bab8ce7a79264064f577
contracts/PrivateSale/Staking/access/Ownable.sol	73e7b65f5a789e690056fadc230326752d4a290e
contracts/PrivateSale/Staking/token/BEP20/IBEP20.sol	64032a14e1013dca01d9fd6f1a9959f9bdbb93df
contracts/PrivateSale/Staking/token/BEP20/SafeBEP20.sol	1144ea26c68a76051e02adf11356dbd8f9cea009
contracts/PrivateSale/Staking2/ISStaking.sol	5ef3af72e3f0eed1efd794c6acd0d8afb7257b36
contracts/PrivateSale/Staking2/math/SafeMath.sol	5586d1f49859d8c247ecb5cc4558c4eb42515783
contracts/PrivateSale/Staking2/utills/Address.sol	e9d9e02869e40353495b0a8f62244a2d0df4a19b
contracts/PrivateSale/Staking2/StakingUpgradable.sol	1894865f19a06bea6391917e44abccbed5ad3e30
contracts/PrivateSale/Staking2/GSN/Context.sol	62650c73f54a5f6cca403089e478a03f2d80bf78
contracts/PrivateSale/Staking2/token/BEP20/IBEP20.sol	6c3f82008282600ee33760b0422e888c4e418d22
contracts/PrivateSale/Staking2/token/BEP20/SafeBEP20.sol	e95a0d9d2aeef151327f4cd1914ff76367583157
contracts/PrivateSale/PrivateSale.sol	f96dd044961037b133ad866b3f7e75d315031cb5
contracts/DPADStakingContract/DPADStakingContract.sol	e02bed669bbe54d1d844b8c3c9b516ea63da732e
contracts/IDODetails/IIODDetailsSetter.sol	78bb180100959ccb7110f9c88efd02bd26f3b81f
contracts/IDODetails/IDODetailsStorage.sol	54c3d5acc80e5e212f4b0b36c3bdc221717d5ea8
contracts/IDODetails/IIODDetailsGetter.sol	309d484c14c3452d1c755a52c90651680dcb846
contracts/IDODetails/IDODetails.sol	98c18752e0b3307dcc229a5036afb83db9752761
contracts/IDODetails/CompactIIODDetails.sol	349970e52c7beb7cf82956d8f964f072fb9f4f1
contracts/IDODetails/IIODDetails.sol	36733d9d46055ad22629892436fca6bade88c6e
contracts/TIERS.sol	80fb4ff1f5ed46077a1b07db6f2391e6ed907685
contracts/Constants.sol	b32ee89659bd207ccca9ee6fe3d91d82271a781c
contracts/LPLocker/LPLocker.sol	ca01ed2ab1def1037e5037ad1dd677e96dc8db57
contracts/LPLocker/ILPLocker.sol	343f6961c9f664fb064188c92c13e852ace05ad2
contracts/PancakeSwap/IPancakeV2Pair.sol	1fe43d098743167d12ccb1e54845cb2e47b2421a
contracts/PancakeSwap/IPancakeV2Factory.sol	589820a96b51a70683943d292125c9619409afc4
contracts/PancakeSwap/IPancakeV2Router01.sol	3eb644512acb10a3edb2403ec479a77f2daee2e1
contracts/PancakeSwap/IPancakeV2Router02.sol	f79ee71632815371a4264e3101fe7ecb9dc0628d
contracts/RoleManager/RoleManager.sol	ceea7af0104a748e81ee0058b0b1e8f4fe2943fb
contracts/RoleManager/IRoleManager.sol	2f573409d34a18b5a14821b5478ad549c7ed761a
contracts/IDOSStates.sol	b602bcd0bef595306711dea3bd84887d7d6ed15b
contracts/Greeter.sol	d4fcbae5c961f23cb34bb998d73e05d8dd9c5504

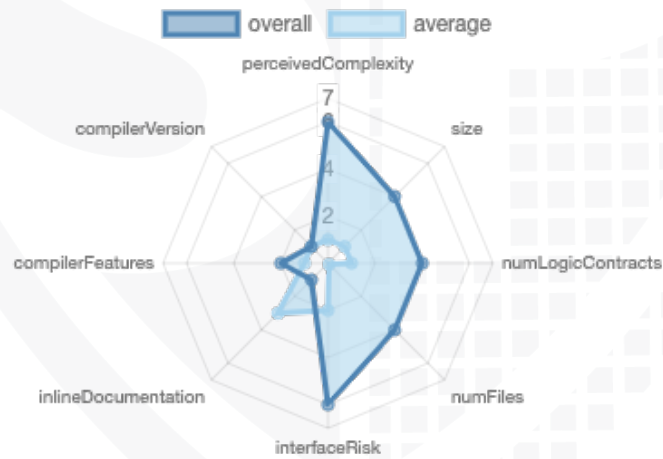
contracts/Admin/Admin.sol	7f69975cedbaa8c0aa2ed58559ead7bdd49ce6da
contracts/Admin/IAdmin.sol	386926fcd5ecbc98b74233676fe5a13b99c53260
contracts/StakingManager/StakingManager.sol	d3dd61a5773483d5f40dce85758c7451ac110df4
contracts/StakingManager/IStakingManager.sol	7803de0273603298aeb16415c9e5530f19e48185
contracts/IDOFactory/IDOFactory.sol	bfbad297f169827098acd4f7b78b019bb25a2956
contracts/IDOFactory/IIDOFactory.sol	9526b9529b135cfaea9a4781905f58ef813d4ff5
contracts/FundingManager/FundingTypes.sol	d11d886be16d9524a8dca4e424f61c997716437b
contracts/FundingManager/Treasury/Treasury.sol	c3bab426f0b5b09b65fe2d9de92f008a1a174433
contracts/FundingManager/Treasury/ITreasury.sol	942787a90288e77ff2edfd4c7edcfd36bcfece22
contracts/FundingManager/PreSaleStrategies/AuctionPreSale/AuctionPreSaleStrategy.sol	9c2b79dd8fcc028e4997e398ebb96e896343a01
contracts/FundingManager/PreSaleStrategies/AuctionPreSale/SortedDescendingList.sol	7d5dcf36118ee440c51575be86abced97fceb03e
contracts/FundingManager/PreSaleStrategies/AuctionPreSale/SortedAscendingList.sol	addbb1b7f93415d4d9547a529f9965a7a9ec39ae
contracts/FundingManager/PreSaleStrategies/IPreSaleStrategy.sol	70ea15690c943270dcee45293dd69ad42f64635b
contracts/FundingManager/PreSaleStrategies/FCFSPreSale/FCFSPreSaleStrategy.sol	e40fda1d5d63ce70669dfe3a7882cba8f493dc7b
contracts/FundingManager/PreSaleStrategies/BasePreSaleStrategy.sol	8937ec8d74b5e1574a7ca997ce2ed7f2364921f4
contracts/FundingManager/IFundingManager.sol	3e8421228c0702d21d1f99f37b5c0226b521a782
contracts/FundingManager/FundingManager.sol	9d7100c5234814b7da84c79a639f617cfc287629
contracts/ContractsManager/ContractsManager.sol	fa2597ee14babc9198e3d8c75f037b47107c9324
contracts/ContractsManager/IContractsManager.sol	7c8cc990f97c20c681c486e1e79b8eae06d6d80f
contracts/Token/DPAD.sol	c652a1e600dddf58be56d57fc0aedf906d26cb4
contracts/Token/NOVO.sol	f609ce1f1cba31e20f7fd45dd9da46f2e062b731

Metrics

Source Lines v1.0



Risk Level v1.0



Capabilities

Components

Version	Contracts	Libraries	Interfaces	Abstract
1.0	25	14	20	0

Exposed Functions

This section lists functions that are explicitly declared public or payable. Please note that getter methods for public stateVars are not included.

Version	Public	Payable
1.0	348	9

Version	External	Internal	Private	Pure	View
1.0	245	373	4	32	134

State Variables

Version	Total	Public
1.0	95	66

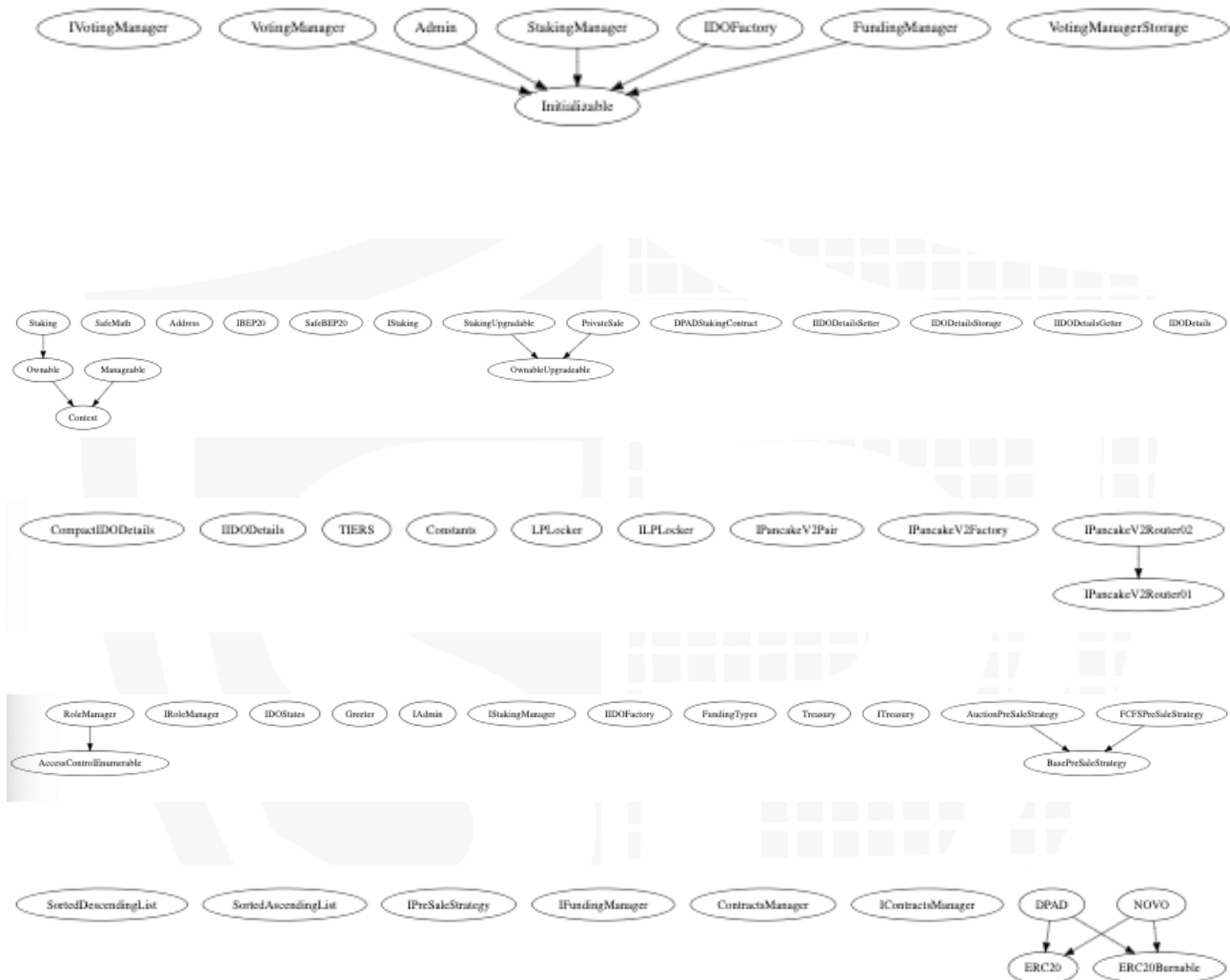
Capabilities

Version	Solidity Versions observed	Experimental Features	Can Receive Funds	Uses Assembly	Has Destroyable Contracts
1.0	<code>^0.8.0</code> <code>0.6.12</code> <code>>=0.4.0</code>		<code>yes</code>	<code>yes</code> (4 asm blocks)	

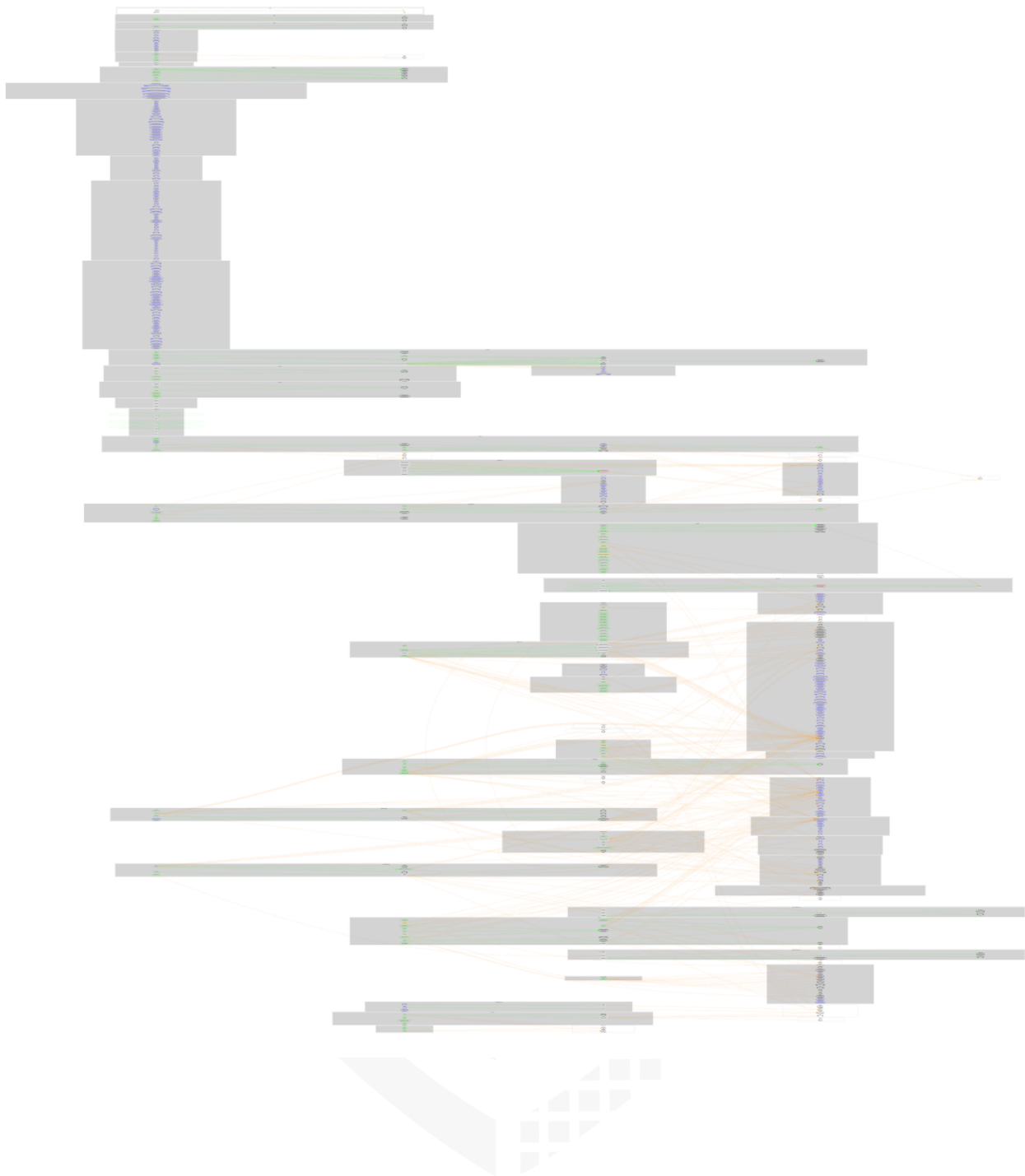
Version	Transfers ETH	Low-Level Calls	DelegateCall	Uses Hash Functions	EC Recover	New/Create/Create2
1.0	yes			yes		yes → NewContract: IDODetails → NewContract: Treasury → NewContract: FCFSPreSaleStrategy

Inheritance Graph

v1.0



CallGraph v1.0



Scope of Work/Verify Claims

The above token Team provided us with the files that needs to be tested (Github, Bscscan, Etherscan, files, etc.). The scope of the audit is the main contract (usual the same name as team appended with .sol).

We will verify the following claims:

1. Overall checkup (Smart Contract Security)



Overall checkup (Smart Contract Security)

Tested	Verified
✓	✓

Legend

Attribute	Symbol
Verified / Checked	✓
Partly Verified	⚠
Unverified / Not checked	✗
Not available	—

Modifiers and public functions

v1.0

Admin

- initialize
 - initializer
- updateTierMaxPurchaseLimit
 - onlyAdmin
- updateDevRewards
 - onlyAdmin
- updateStakingRewards
 - onlyAdmin

DPADStakingContract

- stake
- unstake

AuctionPreSaleStrategy

- finalize
- contribute

ContractsManager

- updateIDOFactory
 - onlyAdmin
- updateRoleManager
 - onlyAdmin
- updateVotingManager
 - onlyAdmin
- updateFundingManager
 - onlyAdmin
- updateStakingManager
 - onlyAdmin
- updateTokenAddress
 - onlyAdmin
- updateDeveloperAddress
 - onlyAdmin
- updatePCSRouter
 - onlyAdmin
- updateLpLocker
 - onlyAdmin
- updateAdminContract
 - onlyAdmin
- updateBUSDAddress
 - onlyAdmin

FCFSPreSaleStrategy

- finalize
- refund
- contribute

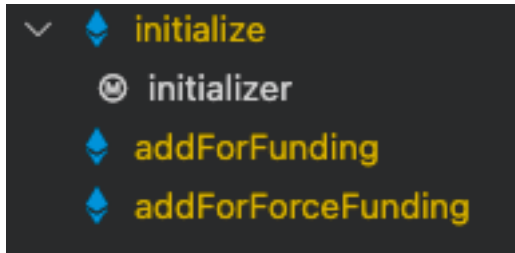
BasePreSaleStrategy

- claim

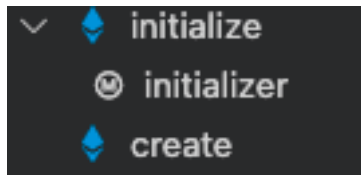
Treasury

- contribute
 - onlyPresale
- claim
 - onlyPresale
- refund
 - onlyPresale
- addToLP
 - onlyPresale
- transferDevRewards
 - onlyPresale
- transferStakingRewards
 - onlyPresale
- adminTransferToken
 - onlyAdmin
- adminTransferBNB
 - onlyAdmin

FundingManager



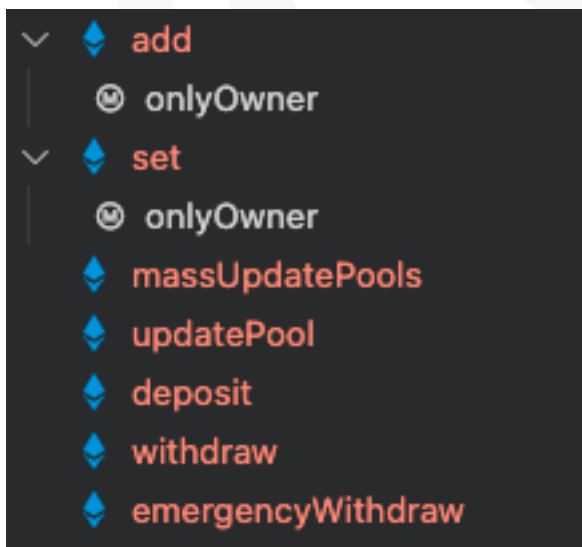
IDOFactory



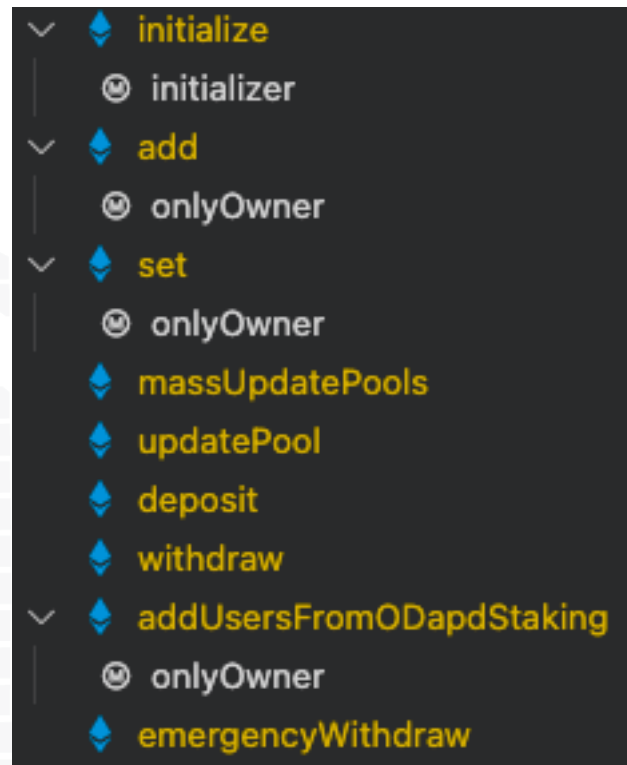
LPLocker



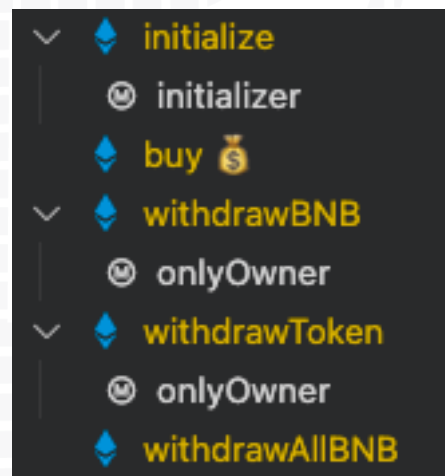
Staking



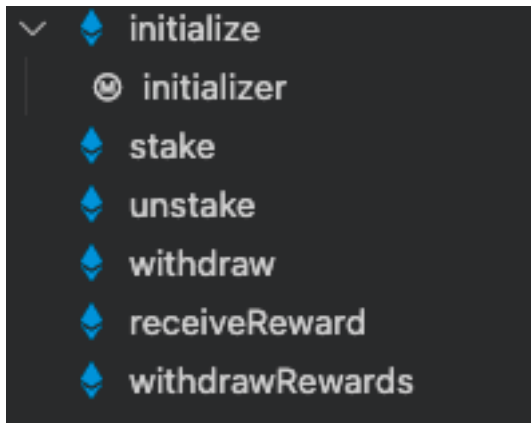
StakingUpgradeable



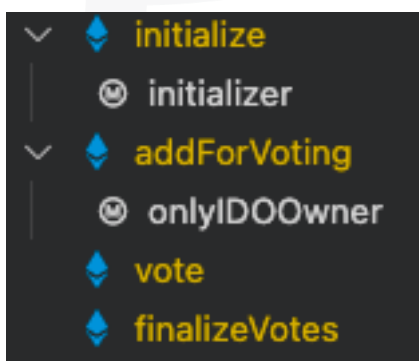
PrivateSale



StakingManager



VotingManager



Comments

- Deployer can set following state variables without any limitations
 - Admin
 - stakingRewards
 - devRewards
 - tierWiseldoMaxPurchasePerWalletOverrides[_idold][_tier]
 - ContractsManager
 - IDODetails
 - multiplier
 - Max $2^{16} - 1$
 - lpLockerId
 - inHeadStartTill
 - pcsListingDetails.listingRate
 - pcsListingDetails.lpLockDuration
 - pcsListingDetails.allocationToLPInBP
 - votingDetails.voteStartTime
 - votingDetails.voteEndTime
 - basicIdoDetails.tokenPrice
 - basicIdoDetails.softCap
 - basicIdoDetails.hardCap
 - basicIdoDetails.minPurchasePerWallet

- basicIdoDetails.maxPurchasePerWallet
- basicIdoDetails.saleStartTime
 - Max $2^{64} - 1$
- basicIdoDetails.saleEndTime
 - Max $2^{64} - 1$
- basicIdoDetails.headStart
 - Max $2^{32} - 1$
- Deployer can enable/disable following state variables
 - Admin
 - ContractsManager
 - IDODetails
- Deployer can set following addresses/enums
 - Admin
 - ContractsManager
 - busd
 - adminContract
 - lpLocker
 - pcsRouter
 - developerAddress
 - tokenAddress
 - stakingManager
 - fundingManager
 - votingManager
 - roleManager
 - idoFactory
 - IDODetails
 - treasury
 - preSale
 - state
 - projectInformation.saleDescription
 - projectInformation.website
 - projectInformation.telegram
 - projectInformation.github
 - projectInformation.twitter
 - projectInformation.logo
 - projectInformation.whitePaper
 - projectInformation.kyc
 - projectInformation.video
 - projectInformation.audit
 - ownerAddress
 - tokenAddress
 - Staking
 - Add/set new poolinfo

- There is no checking if the staking token exists or not while adding
- Existing Modifiers
 - Admin
 - onlyAdmin
 - ContractsManager
 - onlyAdmin
 - Treasury
 - onlyPresale
 - onlyAdmin
 - IDODetails
 - onlyProjectOwnerOrIDOModerator
 - onlyIDOManager
 - onlyInModeration
 - VotingManager
 - onlyIDOOwner
 - onlyIDOOwner
- Variables/functions with no functionality
 - IDODetails
 - lpLockerId L203
 - updateLpLockerId L202
 - IIDOFactory
 - idIdTracker L9
- There are several authorities which are authorized to call some functions, that means, if the owner is renounced, another address is still authorized to call functions
 - Be aware of this
- ContractsManager
 - Make sure to change the busd contract address from test net address to mainnet address in L24
- PrivateSale
 - Only owner can withdraw bnb and specific token from contract

Please check if an OnlyOwner or similar restrictive modifier has been forgotten.

Source Units in Scope

v1.0

Type	File	Logic Contracts	Interfaces	Lines	nLines	nSLOC	Comment Lines	Complex. Score	Capabilities
	contracts/VotingManager/VotingManager.sol	————	1	14	7	4	1	9	————
	contracts/VotingManager/VotingManagerStorage.sol	1	————	90	90	62	3	56	————
	contracts/VotingManager/VotingManagerStorage.sol	1	————	14	14	10	2	1	————
	contracts/PrivateSale/Staking/Staking.sol	1	————	223	223	151	48	111	
	contracts/PrivateSale/Staking/math/SafeMath.sol	1	————	189	177	54	107	14	————
	contracts/PrivateSale/Staking/utlis/Address.sol	1	————	161	128	57	87	37	
	contracts/PrivateSale/Staking/GSN/Context.sol	1	————	28	28	11	14	1	
	contracts/PrivateSale/Staking/access/Manageable.sol	1	————	76	76	30	36	24	————
	contracts/PrivateSale/Staking/access/Ownable.sol	1	————	76	76	30	36	24	————
	contracts/PrivateSale/Staking/token/BEP20/IBEP20.sol	————	1	98	23	17	66	21	————
	contracts/PrivateSale/Staking/token/BEP20/SafeBEP20.sol	1	————	101	79	37	32	25	————
	contracts/PrivateSale/Staking2/IStaking.sol	————	1	50	26	16	17	19	————
	contracts/PrivateSale/Staking2/math/SafeMath.sol	1	————	189	177	54	107	14	————
	contracts/PrivateSale/Staking2/utlis/Address.sol	1	————	161	128	57	87	37	
	contracts/PrivateSale/Staking2/StakingUpgradable.sol	1	————	253	250	164	55	124	
	contracts/PrivateSale/Staking2/GSN/Context.sol	1	————	28	28	11	14	1	
	contracts/PrivateSale/Staking2/token/BEP20/IBEP20.sol	————	1	98	23	17	66	21	————
	contracts/PrivateSale/Staking2/token/BEP20/SafeBEP20.sol	1	————	101	79	37	32	25	————
	contracts/PrivateSale/PrivateSale.sol	1	————	95	95	68	12	83	
	contracts/DPADStakingContract/DPADStakingContract.sol	1	————	44	44	33	1	24	
	contracts/IDODetails/IDODetailsSetter.sol	————	1	67	8	5	1	61	————
	contracts/IDODetails/IDODetailsStorage.sol	1	————	42	42	36	16	1	————
	contracts/IDODetails/IDODetailsGetter.sol	————	1	34	9	6	1	27	————
	contracts/IDODetails/IDODetails.sol	1	————	213	213	142	39	89	————
	contracts/IDODetails/CompactIDODetails.sol	1	————	38	28	21	2	13	————
	contracts/IDODetails/IDODetails.sol	————	1	97	9	6	1	89	————
	contracts/TIERS.sol	1	————	6	6	4	1	1	————
	contracts/Constants.sol	1	————	8	8	6	1	4	————
	contracts/LPLocker/LPLocker.sol	1	————	83	83	58	4	33	
	contracts/LPLocker/LPLocker.sol	————	1	10	5	3	1	7	————
	contracts/PancakeSwap/IPancakeV2Pair.sol	————	1	53	8	5	1	55	————
	contracts/PancakeSwap/IPancakeV2Factory.sol	————	1	18	7	4	1	17	————

	contracts/PancakeSwap/IPancakeV2Router01.sol		1	96	5	3	1	48	
	contracts/PancakeSwap/IPancakeV2Router02.sol		1	45	7	4	1	16	
	contracts/RoleManager/RoleManager.sol	1		38	38	28	4	31	
	contracts/RoleManager/IRoleManager.sol		1	19	6	3	1	15	
	contracts/IDOSStates.sol	1		46	46	34	5	14	
	contracts/Greeter.sol	1		23	23	16	1	8	
	contracts/Admin/Admin.sol	1		42	42	30	4	24	
	contracts/Admin/IAdmin.sol		1	12	7	4	1	7	
	contracts/StakingManager/StakingManager.sol	1		167	167	105	22	93	
	contracts/StakingManager/IStakingManager.sol		1	11	5	3	1	13	
	contracts/IDOFactory/IDOFactory.sol	1		68	62	35	15	29	
	contracts/IDOFactory/IIDOFactory.sol		1	26	9	5	1	13	
	contracts/FundingManager/FundingTypes.sol	1		6	6	4	1	1	
	contracts/FundingManager/Treasury/Treasury.sol	1		125	125	92	13	106	
	contracts/FundingManager/Treasury/ITreasury.sol		1	24	5	3	1	24	
	contracts/FundingManager/PreSaleStrategies/AuctionPreSale/AuctionPreSaleStrategy.sol	1		106	106	81	2	63	
	contracts/FundingManager/PreSaleStrategies/AuctionPreSale/SortedDescendingList.sol	1		82	82	65	1	20	
	contracts/FundingManager/PreSaleStrategies/AuctionPreSale/SortedAscendingList.sol	1		82	82	65	1	20	
	contracts/FundingManager/PreSaleStrategies/IPreSaleStrategy.sol		1	18	5	3	1	15	
	contracts/FundingManager/PreSaleStrategies/FCFSPreSale/FCFSPreSaleStrategy.sol	1		86	86	63	7	69	
	contracts/FundingManager/PreSaleStrategies/BasePreSaleStrategy.sol	1		99	99	56	31	64	
	contracts/FundingManager/IFundingManager.sol		1	7	5	3	1	5	
	contracts/FundingManager/FundingManager.sol	1		134	134	84	24	91	
	contracts/ContractsManager/ContractsManager.sol	1		103	103	76	1	48	
	contracts/ContractsManager/IContractsManager.sol		1	30	5	3	1	27	
	contracts/Token/DPAD.sol	1		12	12	9	2	9	
	contracts/Token/NOVO.sol	1		12	12	9	2	9	
	Totals	39	20	4277	3481	2102	1038	1950	

Legend

Attribute	Description
Lines	total lines of the source unit
nLines	normalized lines of the source unit (e.g. normalizes functions spanning multiple lines)
nSLOC	normalized source lines of code (only source-code lines; no comments, no blank lines)
Comment Lines	lines containing single or block comments
Complexity Score	a custom complexity score derived from code statements that are known to introduce code complexity (branches, loops, calls, external interfaces, ...)

Audit Results

AUDIT PASSED

Critical issues

No critical issues

High issues

No high issues

Medium issues

No medium issues

Low issues

Issue	File	Type	Line	Description
#1	Main	Contract doesn't import npm packages from source (like OpenZeppelin etc.)	-	We recommend to import all packages from npm directly without flatten the contract. Functions could be modified or can be susceptible to vulnerabilities
#2	All	A floating pragma is set	At the top of source code	The current pragma Solidity directive is „^0.“.
#3	ContractsManager	Missing Zero Address Validation (missing-zero-check)	27-36, 96, 100, 84, 72, 60, 92, 88, 64, 76, 80, 68	Check that the address is not zero
#4	IDODetails	Missing Zero Address Validation (missing-zero-check)	44, 45, 113, 190, 109, 194	Check that the address is not zero

#5	PrivateSale	Missing Zero Address Validation (missing-zero-check)	21, 78	Check that the address is not zero
#6	Treasury	State variable visibility is not set	22, 24	It is best practice to set the visibility of state variables explicitly
#7	Staking Manager	State variable visibility is not set	18, 19	It is best practice to set the visibility of state variables explicitly
#8	Voting Manager	State variable visibility is not set	22, 25	It is best practice to set the visibility of state variables explicitly
#9	IDODetails	Missing Events Arithmetic	114	Emit an event for critical parameter changes
#10	Staking	Missing Events Arithmetic	90, 109	Emit an event for critical parameter changes
#11	Staking Upgradeable	Missing Events Arithmetic	97, 116	Emit an event for critical parameter changes
#12	DPADStakingContract	Uninitialized state variables	15	Initialize all the variables. If a variable is meant to be initialized to zero, explicitly set it to zero to improve code readability
#13	FundingManager	Reverted function	62	If preSale is not set (is address 0), the function will be reverted because of the preSale.treasury() function
#14	Auction PreSale Strategy	Contracts lock ether	See description	You cannot withdraw contract balance
#15	FCFSPreSaleStrategy	Contracts lock ether	See description	You cannot withdraw contract balance

Informational issues

Issue	File	Type	Line	Description
#1	SortedAscendingList	Functions that are not used	53, 25	Remove unused functions

#2	SortedDescendingList	Functions that are not used	53, 25	Remove unused functions
#3	FundingManager	Functions that are not used	70, 77	Remove unused functions
#4	StakingManager	Unused state variables	19	Remove unused state variables
#5	SortedAscendingList	Error message is missing	20, 27, 28	Provide an error message for require statement
#6	SortedDescendingList	Error message is missing	20, 27, 28	Provide an error message for require statement
#7	Treasury	Incorrect comment + too high value	95	Mathematical operation doesn't calculate 2% of dividends, because stakingRewards can be set over 2%. The stakingRewards can be set without any limitations in admin contract.
#8	PrivateSale	currentPsHour cannot be negative	37	Comment say that the variable can be go in negative area but this is impossible because the variable type is an uint. It can overflow/underflow but not go into the negative.

Commented Code exist

There are some instances of code being commented out in the following files that should be removed:

There are a lot of commented lines in the source codes.

E.g.

FundingManager L35-51, L131

Recommendation

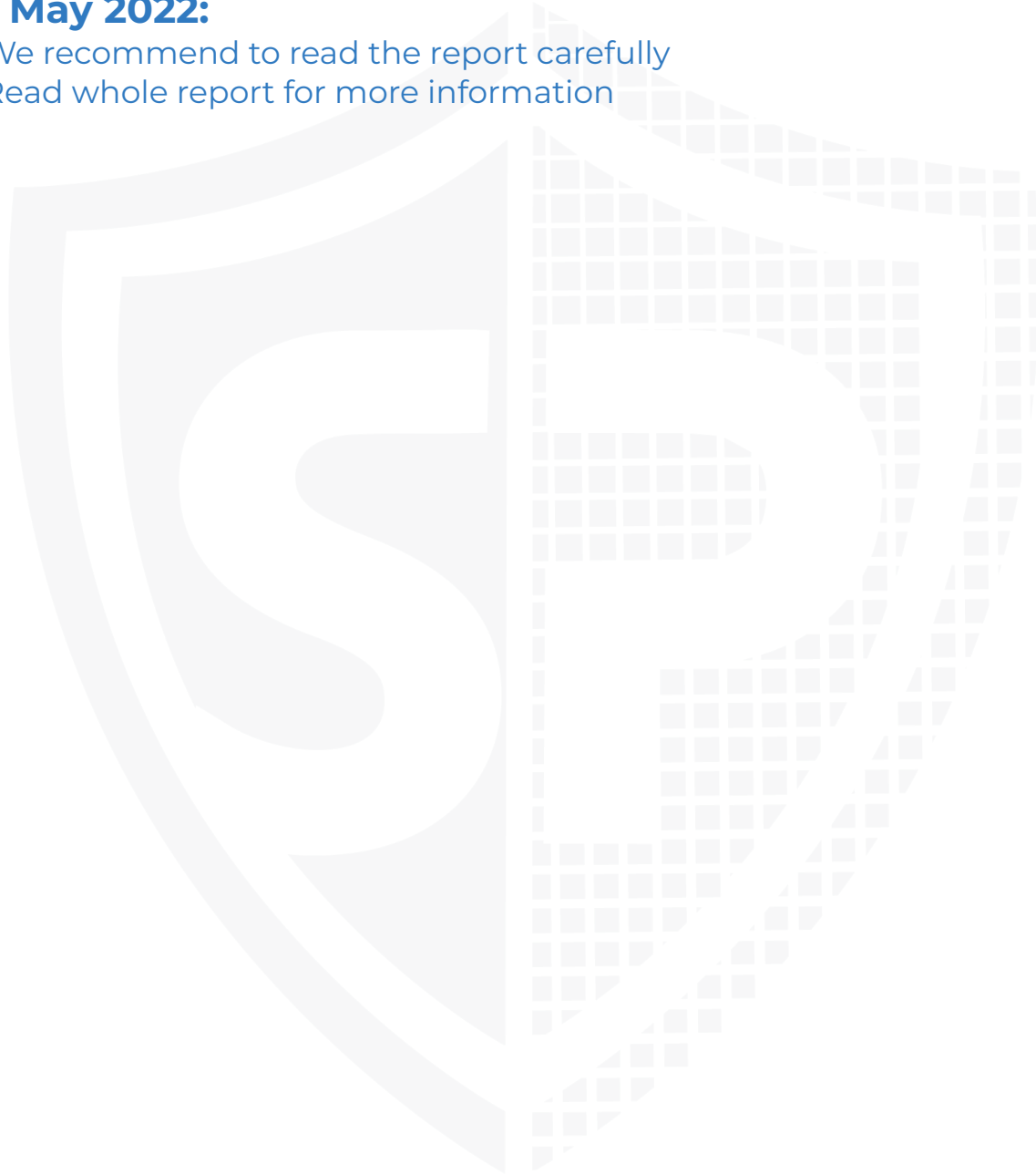
Remove the commented code, or address them properly.

Audit Comments

We recommend you to use the special form of comments (NatSpec Format, Follow link for more information <https://docs.soliditylang.org/en/v0.5.10/natspec-format.html>) for your contracts to provide rich documentation for functions, return variables and more. This helps investors to make clear what that variables, functions etc. do.

05. May 2022:

- We recommend to read the report carefully
- Read whole report for more information



SWC Attacks

ID	Title	Relationships	Status
SW C-1 36	Unencrypted Private Data On-Chain	CWE-767: Access to Critical Private Variable via Public Method	PASSED
SW C-1 35	Code With No Effects	CWE-1164: Irrelevant Code	PASSED
SW C-1 34	Message call with hardcoded gas amount	CWE-655: Improper Initialization	PASSED
SW C-1 33	Hash Collisions With Multiple Variable Length Arguments	CWE-294: Authentication Bypass by Capture-replay	PASSED
SW C-1 32	Unexpected Ether balance	CWE-667: Improper Locking	PASSED
SW C-1 31	Presence of unused variables	CWE-1164: Irrelevant Code	NOT PASSED
SW C-1 30	Right-To-Left-Override control character (U+202E)	CWE-451: User Interface (UI) Misrepresentation of Critical Information	PASSED
SW C-1 29	Typographical Error	CWE-480: Use of Incorrect Operator	PASSED
SW C-1 28	DoS With Block Gas Limit	CWE-400: Uncontrolled Resource Consumption	PASSED

SW C-1 27	Arbitrary Jump with Function Type Variable	CWE-695: Use of Low-Level Functionality	PASSED
SW C-1 25	Incorrect Inheritance Order	CWE-696: Incorrect Behavior Order	PASSED
SW C-1 24	Write to Arbitrary Storage Location	CWE-123: Write-what-where Condition	PASSED
SW C-1 23	Requirement Violation	CWE-573: Improper Following of Specification by Caller	PASSED
SW C-1 22	Lack of Proper Signature Verification	CWE-345: Insufficient Verification of Data Authenticity	PASSED
SW C-1 21	Missing Protection against Signature Replay Attacks	CWE-347: Improper Verification of Cryptographic Signature	PASSED
SW C-1 20	Weak Sources of Randomness from Chain Attributes	CWE-330: Use of Insufficiently Random Values	PASSED
SW C-11 9	Shadowing State Variables	CWE-710: Improper Adherence to Coding Standards	PASSED
SW C-11 8	Incorrect Constructor Name	CWE-665: Improper Initialization	PASSED
SW C-11 7	Signature Malleability	CWE-347: Improper Verification of Cryptographic Signature	PASSED

SW C-11 6	Timestamp Dependence	CWE-829: Inclusion of Functionality from Untrusted Control Sphere	PASSED
SW C-11 5	Authorization through tx.origin	CWE-477: Use of Obsolete Function	PASSED
SW C-11 4	Transaction Order Dependence	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	PASSED
SW C-11 3	DoS with Failed Call	CWE-703: Improper Check or Handling of Exceptional Conditions	PASSED
SW C-11 2	Delegatecall to Untrusted Callee	CWE-829: Inclusion of Functionality from Untrusted Control Sphere	PASSED
SW C-11 1	Use of Deprecated Solidity Functions	CWE-477: Use of Obsolete Function	PASSED
SW C-11 0	Assert Violation	CWE-670: Always-Incorrect Control Flow Implementation	PASSED
SW C-1 09	Uninitialized Storage Pointer	CWE-824: Access of Uninitialized Pointer	PASSED
SW C-1 08	State Variable Default Visibility	CWE-710: Improper Adherence to Coding Standards	NOT PASSED
SW C-1 07	Reentrancy	CWE-841: Improper Enforcement of Behavioral Workflow	PASSED
SW C-1 06	Unprotected SELFDESTRUCT Instruction	CWE-284: Improper Access Control	PASSED

SW C-1 05	Unprotected Ether Withdrawal	CWE-284: Improper Access Control	PASSED
SW C-1 04	Unchecked Call Return Value	CWE-252: Unchecked Return Value	PASSED
SW C-1 03	Floating Pragma	CWE-664: Improper Control of a Resource Through its Lifetime	NOT PASSED
SW C-1 02	Outdated Compiler Version	CWE-937: Using Components with Known Vulnerabilities	PASSED
SW C-1 01	Integer Overflow and Underflow	CWE-682: Incorrect Calculation	PASSED
SW C-1 00	Function Default Visibility	CWE-710: Improper Adherence to Coding Standards	PASSED

The logo features the word "SolidProof" in a white, elegant script font. The "P" is particularly large and stylized, with a long horizontal stroke that extends to the left. The background is a solid blue color with a faint, large shield emblem. The shield has a grid-like pattern on its right side and a solid blue area on its left side.

SolidProof

Blockchain Security | Smart Contract Audits | KYC

A small horizontal bar representing the German flag, with black, red, and gold stripes.

MADE IN GERMANY