SOLIDProof

Bring trust into your projects

Blockchain Security | Smart Contract Audits | KYC

MADE IN GERMANY

The world state

Audit

Security Assessment

16. May, 2022

For

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 Unicrypt, 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	12. May 2022	• Layout project • Automated- /Manual-Security Testing • Summary
	13. - 15- May 2022	• Manual overview of files • Project structure check • Issues check
	16. May 2022	• Finalize report

Network
Polygon Matic

Website
https://www.theworldstate.io/

Telegram

Twitter

Facebook

Instagram

Github

Reddit

Medium

Discord

Youtube

TikTok

LinkedIn

Description
TBA

Project Engagement
During the 11th of May 2022, **The world state 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://github.com/EddRudd/Project_T01
  - Commit: bcd417c73a4c197d639e20eae343bcd7c25721fd

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 aspossible.
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:

Dependency / Import Path	Count
@openzeppelin/contracts-upgradeable/access/IAccessControlEnumerableUpgradeable.sol	1
@openzeppelin/contracts-upgradeable/access/IAccessControlUpgradeable.sol	1
@openzeppelin/contracts-upgradeable/access/OwnableUpgradeable.sol	2
@openzeppelin/contracts-upgradeable/proxy/utils/Initializable.sol	9
@openzeppelin/contracts-upgradeable/token/ERC20/ERC20Upgradeable.sol	1
@openzeppelin/contracts-upgradeable/token/ERC20/extensions/ERC20BurnableUpgradeable.sol	1
@openzeppelin/contracts-upgradeable/token/ERC721/ERC721Upgradeable.sol	20
@openzeppelin/contracts-upgradeable/token/ERC721/IERC721ReceiverUpgradeable.sol	2
@openzeppelin/contracts-upgradeable/token/ERC721/IERC721Upgradeable.sol	5
@openzeppelin/contracts-upgradeable/token/ERC721/extensions/ERC721BurnableUpgradeable.sol	17
@openzeppelin/contracts-upgradeable/token/ERC721/extensions/ERC721EnumerableUpgradeable.sol	17
@openzeppelin/contracts-upgradeable/token/ERC721/extensions/ERC721URIStorageUpgradeable.sol	17
@openzeppelin/contracts-upgradeable/token/ERC721/extensions/IERC721EnumerableUpgradeable.sol	2
@openzeppelin/contracts-upgradeable/token/ERC721/extensions/IERC721MetadataUpgradeable.sol	2
@openzeppelin/contracts-upgradeable/utils/AddressUpgradeable.sol	2
@openzeppelin/contracts-upgradeable/utils/ContextUpgradeable.sol	21
@openzeppelin/contracts-upgradeable/utils/StringsUpgradeable.sol	6
@openzeppelin/contracts-upgradeable/utils/cryptography/SignatureCheckerUpgradeable.sol	20
@openzeppelin/contracts-upgradeable/utils/cryptography/draft-EIP712Upgradeable.sol	20
@openzeppelin/contracts-upgradeable/utils/introspection/ERC165Upgradeable.sol	3
@openzeppelin/contracts-upgradeable/utils/structs/EnumerableSetUpgradeable.sol	1
@openzeppelin/contracts/proxy/ERC1967/ERC1967Proxy.sol	1
@openzeppelin/contracts/token/ERC20/IERC20.sol	48
@openzeppelin/contracts/token/ERC20/utils/SafeERC20.sol	46
@openzeppelin/contracts/token/ERC721/IERC721.sol	1
@openzeppelin/contracts/token/ERC721/utils/ERC721Holder.sol	1
@openzeppelin/contracts/utils/Strings.sol	3
@openzeppelin/contracts/utils/structs/EnumerableSet.sol	1
@uniswap/v2-core/contracts/interfaces/IUniswapV2Pair.sol	1
@uniswap/v2-periphery/contracts/interfaces/IUniswapV2Router02.sol	1

Tested Contract Files

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

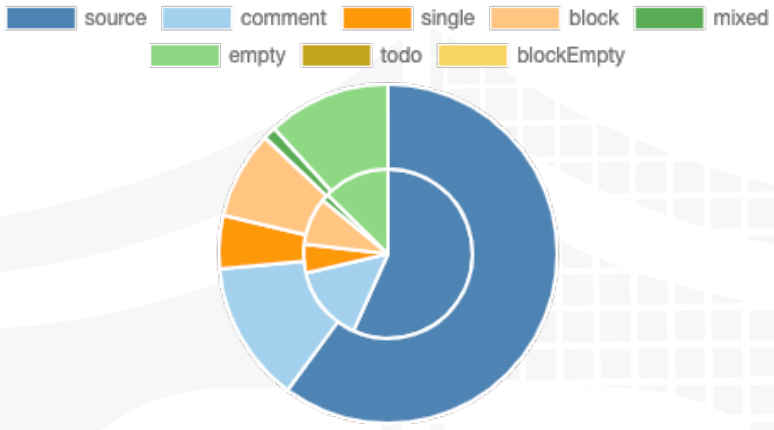
A file with a different Hash has been modified, intentionally or otherwise, after the security review. A different Hash could be (but not necessarily) an indication of a changed condition or potential vulnerability that was not within the scope of this review.

v1.0

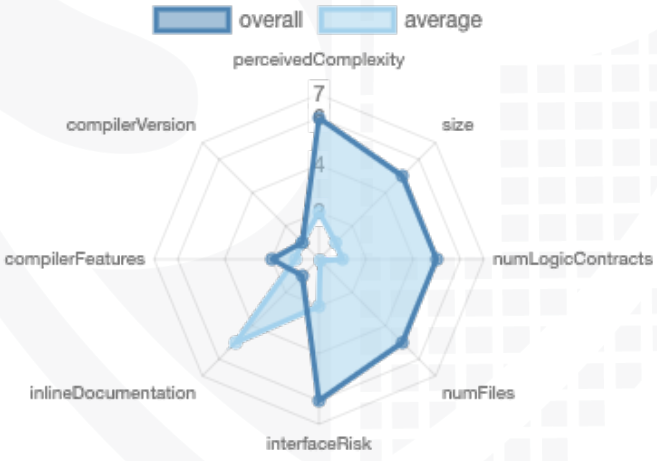
File Name	SHA-1 Hash
contracts/interfaces/INFTParty.sol	c911cd9f8eaf1fb286ac2f0a0f30f760c027d5de
contracts/VotingWindow.sol	d1403c7ad3613275dbdc48f9db0ef11738c2081b
contracts/NFTPartyMembership.sol	604422d7cacd891efaf893a421ee31cd3ad598b
contracts/NFTPartyLeader.sol	532e7b73c94dd09b243ba0b42fe80920cc0995cb
contracts/NFTNomineeForCandidate.sol	191117d0966084d0bf059194ad2b56ef5987a2c2
contracts/Coin.sol	35d3bf303ad04e3a1e09ad19da73b4f5eab1ded1
contracts/NFTNomineeForPartyLeader.sol	045557bc211f7fd467dd5d8dbfafd6572560dfcf
contracts/NFTNomineeForPresident.sol	ab3cb50727889e3122f76c336171043dd35628a5
contracts/NFTBill.sol	c882653a8bd97b23fce3fae0a20d019a01bdfcc6
contracts/NFTPresident.sol	7067423ce4e74c302d6e81fad2bbdbcf306254ba
contracts/NFTParty.sol	811225136ea155bae1abbfdaf8f555520916b78d
contracts/NFTPassport.sol	eb3ab87fbfef57cdc6621731161fb391e335a2eee
contracts/NFTLegislativeInitiative.sol	fdf64bba8a7d9cdbb21c9c0150ff494128b82c01
contracts/utils/MintPriceStorage.sol	ffb5c40c63eefe7219c389cba69019c8c1ee0c73
contracts/utils/MaxInProgressStorage.sol	6c22fa96b7caaecff81a94637fd01fbd90b7a8ab
contracts/utils/MaxPresidentPeriodsStorage.sol	d8a6b61160008e864ca8fe7863326f48319b83fd
contracts/utils/Utils.sol	9fb2e7bb4f5f3b49b8283b0fc4bc37a6b84486e4
contracts/utils/WaitingDelayBetweenMintsSecondsForPartyLeaderStorage.sol	fd4da56faa86bc62b730f09df99330bda6b297e8
contracts/utils/NFTWalletOwnershipWithOffchainMarketplacePauserMintPriceTransferTaxBase.sol	c69e7b5dcac53ece478b7e39111bd144659eb2ee
contracts/utils/VotingPeriodSecondsStorage.sol	305a7100185b5a086b2b0ff52c462dc4c4b8a651
contracts/utils/OffchainERC721MarketplacePassportOwnershop.sol	7bb5676d4c24eacedecff0820806aaa8367db085
contracts/utils/OffchainERC721Marketplace.sol	642f64e939add8b8e53b4eb5aa4b3ae32ff7f4eb
contracts/utils/NFTPartyMembershipOwnershipERC721BaseEnumerablePausableUpgradeable.sol	4f601fd4a8eb1792f45ca565fcd74d721d075b5
contracts/utils/fabric/NFTPartyDraftRulesFabric.sol	495b4601c7ec883ac4b9de9b661d902a5661fe7d
contracts/utils/fabric/NFTPartyRulesFabric.sol	fd2262600b470a1bfdb0fcaa056292509e981334
contracts/utils/fabric/NFTPartyMembershipFabric.sol	98b2fd7b3c0e86404622d980e8fbbc23d1acb01d
contracts/utils/fabric/PartyVotingWindowFabric.sol	dd3576f884e1a9668720448852f9948cd08a5df0
contracts/utils/fabric/NFTPartyLeaderFabric.sol	b1b03269d8501f77d5dc23467f53c0019e59f843
contracts/utils/fabric/NFTNomineeForPartyLeaderFabric.sol	975f8c06340431894e4a6d269c589715e02463a9
contracts/utils/QuorumNumeratorStorage.sol	6fc4413040da0908e1c677db3446967ca7fb3f75
contracts/utils/MinVotesStorage.sol	4490796d2038340465f3106b516f98444c87b8
contracts/utils/CoinStorage.sol	ae93eb41f45e973893786ca9a6b375d4c21dee5b
contracts/utils/NFTPassportOwnershipWithOffchainMarketplacePauserMintPriceTransferTaxBase.sol	c9fb3eb61a5f0714e44de1abc11089bab2cb8bfa
contracts/utils/PartyVotingWindowStorage.sol	accb2d8b5f1f388704b364e6972290170226fc15e
contracts/utils/BurnAllowedStorage.sol	e555a004c621cfdf80b8d6ea3d164fb2eae03e5b
contracts/utils/LevelAcceptedNumeratorStorage.sol	6fa7e260c52c0cf862d277b1aedb5195031d669f
contracts/utils/ImplementationStorage.sol	ff59124d5f6b98f7d1c45611a5874b1ee6eee843
contracts/utils/Base.sol	766f18e27d98f9b5d292858ebe93a9b5233706b0
contracts/utils/MaxPartyLeaderPeriodsStorage.sol	291714578b642f7986a04cdf03c45324ed58cd
contracts/utils/WaitingDelayBetweenMintsSecondsForPresidentStorage.sol	ada3b9bccfa2fa2ffcc9410a64bbd216c88386d9
contracts/utils/AcceptedExpirationSecondsStorage.sol	b8e82c629d8a4df3e9eb5858b70293b0502c01f7
contracts/utils/NFTPassportStorage.sol	5e9200b094a80734942e2bd15a310ea3a1741684
contracts/utils/Initializable2.sol	9a4857e35b57db576ef9cec714e47eb76cd48f21
contracts/utils/NFTPartyMembershipStorage.sol	a7bec0a1afde8721e699ce455ad80f6d1a4c4562
contracts/utils/AccessControlEnumerableUpgradeable.sol	877610d59e4b77e6b330b9e248f822b0da97e636
contracts/utils/TreasuryStorage.sol	70ea450cef86f773c89ab552df36cf4263a91fdd
contracts/utils/TransferTaxStorage.sol	3accf255bb74d7cba29830341bcba0dd1cdace3e
contracts/utils/TransparentUpgradeableProxy.sol	55fa11b1f8995432a33fd0c89fa296668077bb42
contracts/utils/NFTPartyMembershipOwnershipWithOffchainMarketplacePauserMintPriceTransferTaxBase.sol	a652354fb0f2d14db8c3aa54c4b0fb8512cd8e6d
contracts/utils/OffchainERC721MarketplacePartyMembershipOwnership.sol	5bf6148865ed2b5564ab706001f59d7f64b08a55
contracts/utils/Access.sol	113258f2265bb23535ef37e67c9a62892b6443cc
contracts/utils/NFTPassportOwnershipERC721BaseEnumerablePausableUpgradeable.sol	48dc4a1ffc770a0c59e041824bafe50e2fb1602a
contracts/utils/ERC20PresetMinterUpgradeable.sol	808569b886772ac2bd7539aa4e1d995656c49a82
contracts/utils/VotePowerPoints.sol	3f174c56baa793dd87cba0baef1dfd5d6f79c6f7
contracts/utils/VotingWindowStorage.sol	095543e91f4db3371631da65cb867fdb049701cd
contracts/utils/MinPowerPointsStorage.sol	47bc163dbf3de216edb48c442555bb747a9e510d7
contracts/utils/NFTPartyStorage.sol	c99d612c17112a672544dd830470db68f568eca9
contracts/utils/WaitingDelayBetweenMintsSecondsStorage.sol	f0f4474f20a3ee2ea82627ffc25f03607f057d62
contracts/utils/MintPowerPointsStorage.sol	f2f99ab64220186725cb5531f881761a804858b5
contracts/utils/LevelElectedNumeratorStorage.sol	a036c944ac85a159bf2a754ab9c65f028683e23b
contracts/utils/AvatarsMixin.sol	71bbbfd02279191bdbfd92a2a5d3ebc140ef04b8
contracts/utils/SaleTaxNumeratorStorage.sol	3c6508a9b8732490834112745fe93dc625ce3c8c9
contracts/utils/NFTPresidentStorage.sol	27e230c7f1f6951b8f529d4bd26c19f1f74cbe73
contracts/PartyVotingWindow.sol	d68b849b49db1997bc577103bb3ebb7ac2a47b0d
contracts/NFTPartyRules.sol	4a4dc4410260a01662f25359f8ea8e71fdc84f45
contracts/NFTPartyDraftRules.sol	6097afeca45ac8a4534172ea4fcf19b264270f75
contracts/Errors.sol	7d254a3804049332fed5e7eab4d3488248d48c1b
contracts/NFTAct.sol	fc699d63b3878dfd6486066271fc47f5a113e84

Metrics

Source Lines
v1.0



Risk Level
v1.0



Capabilities

Components

Version	Contracts	Libraries	Interfaces	Abstract
1.0	26	2	3	40

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	324	2

Version	External	Internal	Private	Pure	View
1.0	152	503	13	2	125

State Variables

Version	Total	Public
1.0	176	119

Capabilities

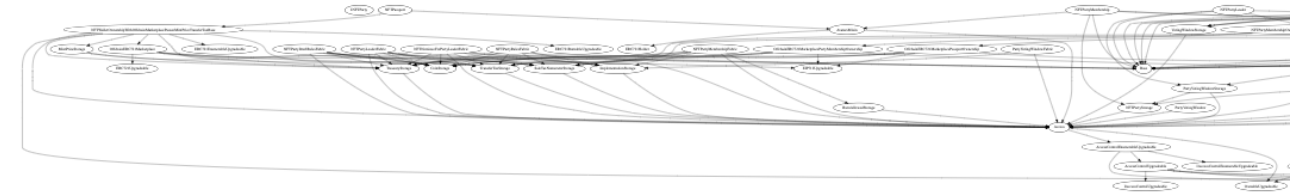
Version	Solidity Versions observed	Experimental Features	Can Receive Funds	Uses Assembly	Has Destroyable Contracts
1.0	`0.8.6`	`ABIEncoderV2`	`yes`	`yes` (2 asm blocks)	

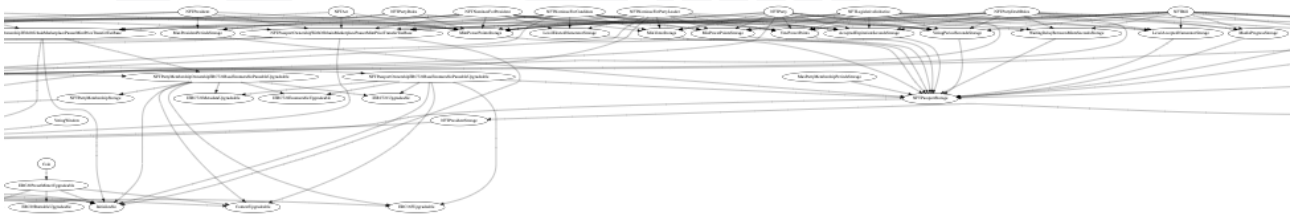
Version	Transfers ETH	Low-Level Calls	DelegateCall	Uses Hash Functions	EC Recover	New/Create/Create2

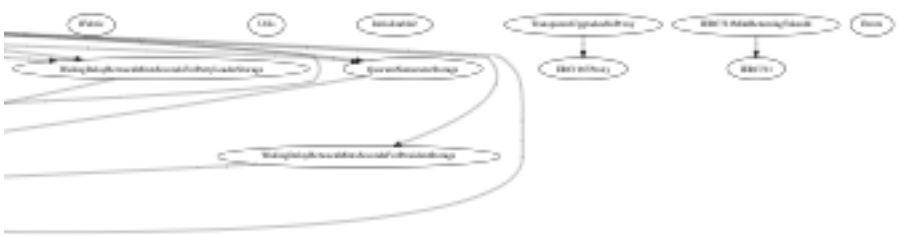
1.0				`yes`		`yes → NewContract:TransparentUpgradeableProxy`

Inheritance Graph

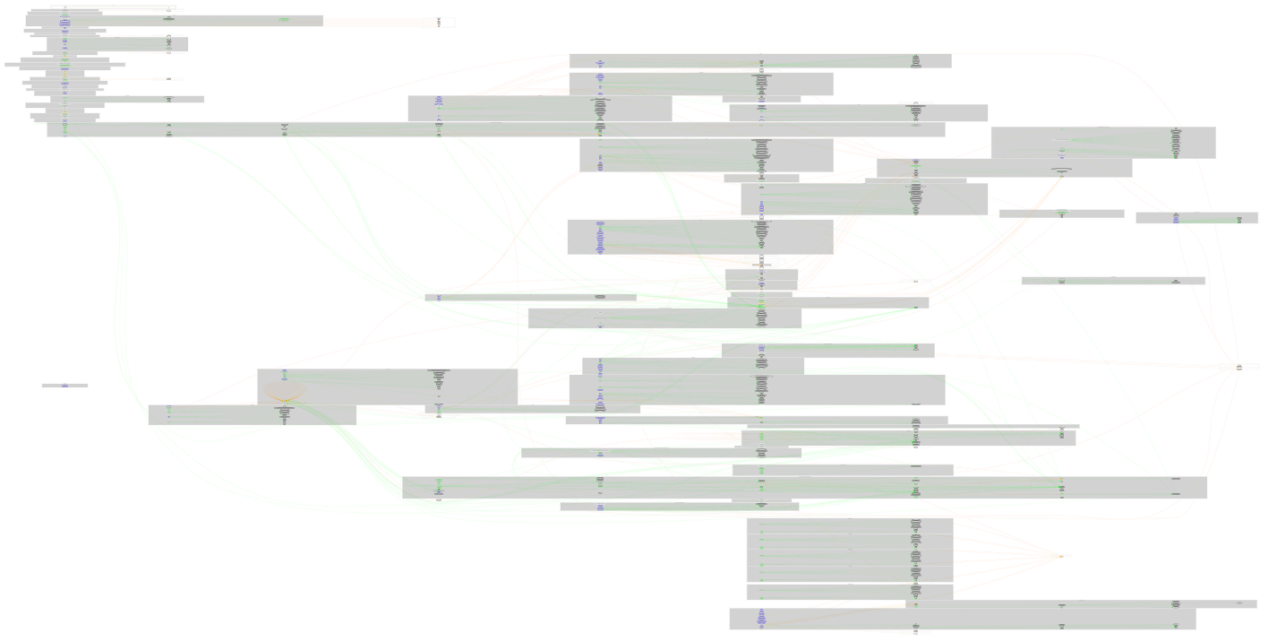
v1.0







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)

Write functions of contract v1.0

Note: Functions are only listed from contract itself without any libraries. For more information look in the *"modifiers and public functions"* section below.

```
' -- Coin --
+addPool()
+removePool()
+addTaxWhitelist()
+removeTaxWhitelist()
+setTreasury()
+setTransferTaxNumerator()
+setPurchaseDEXTaxNumerator()
+setSaleDEXTaxNumerator()
+setPurchaseDEXTaxForLPNumerator()
+setSaleDEXTaxForLPNumerator()
+initialize()
+processDexTax()
```

```
' -- NFTAct --
+initialize()
+initialize2()
+mint()
```

```
' -- NFTBill --
+initialize()
+initialize2()
+initialize3()
+initAct()
+mint()
+vote()
+finalize()
+executeAccepted()
+setStatusExpired()
```

```
' -- NFTPresident --
+initialize()
+initialize2()
+mint()
```

```
' -- NFTLegislativeInitiative --
+initialize()
+initialize2()
+initBill()
+mint()
+vote()
+finalize()
+executeAccepted()
+setStatusExpired()
```

```
' -- NFTNomineeForCandidate --
+initialize()
+initialize2()
+initNomineeForPresident()
+mint()
+vote()
+finalizeAllWindowTokens()
+finalizeNWindowTokensFromIndex()
+finalizeToken()
+executeElected()
```

```
' -- VotingWindow --
+initialize()
+create()
+update()
```

```
' -- PartyVotingWindow --
+initialize()
+checkIsLastFinishedPartyVotingWindow()
+create()
+update()
```

```
' -- NFTPassport --
+initialize()
+setPowerPointsBurnRateNumeratorOnTransfer()
+mint()
+addPowerPoints()
+increasePresidentCounter()
```

```
' -- NFTPartyRules --
+initialize()
+initialize2()
+initialize3()
+mint()
```

```
' -- NFTPartyMembership --
+setBurnAllowed()
+initialize()
+initialize2()
+mint()
+burn()
```

```
' -- NFTPartyLeader --
+initialize()
+initialize2()
+initialize3()
+mint()
+burn()
```

```
' -- NFTParty --
+setUpgradeAdmin()
+setNFTPartyMembershipFabric()
+setNFTPartyDraftRulesFabric()
+setNFTPartyRulesFabric()
+setPartyWindowFabric()
+setNFTNomineeForPartyLeaderFabric()
+setNFTPartyLeaderFabric()
+initialize()
+initialize2()
+mint()
+vote()
+finalize()
+executeAccepted()
+setStatusExpired()
```

```
' -- NFTPartyDraftRules --
+initialize()
+initialize2()
+initialize3()
+initNFTPartyRules()
+mint()
+vote()
+finalize()
+executeAccepted()
+setStatusExpired()
```

```
' -- NFTNomineeForPresident --
+initialize()
+initialize2()
+initNFTPresident()
+mint()
+vote()
+finalizeAllWindowTokens()
+finalizeNWindowTokensFromIndex()
+finalizeToken()
+executeElected()
+executeExpired()
```

```
' -- NFTNomineeForPartyLeader --
+initialize()
+initialize2()
+initialize3()
+initNFTPartyLeader()
+mint()
+vote()
+finalizeAllWindowTokens()
+finalizeNWindowTokensFromIndex()
+finalizeToken()
+executeElected()
+executeExpired()
```

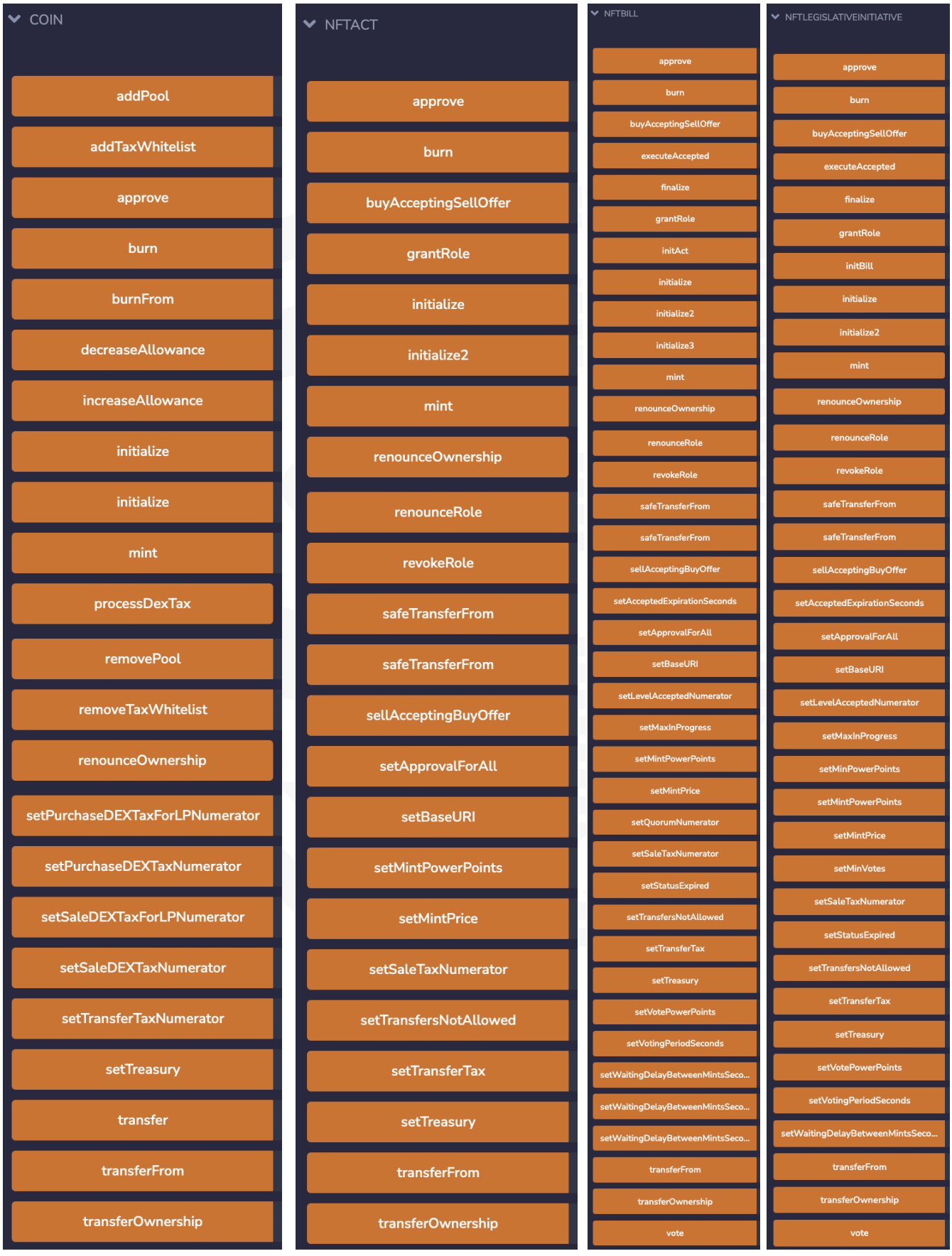
Overall checkup (Smart Contract Security)

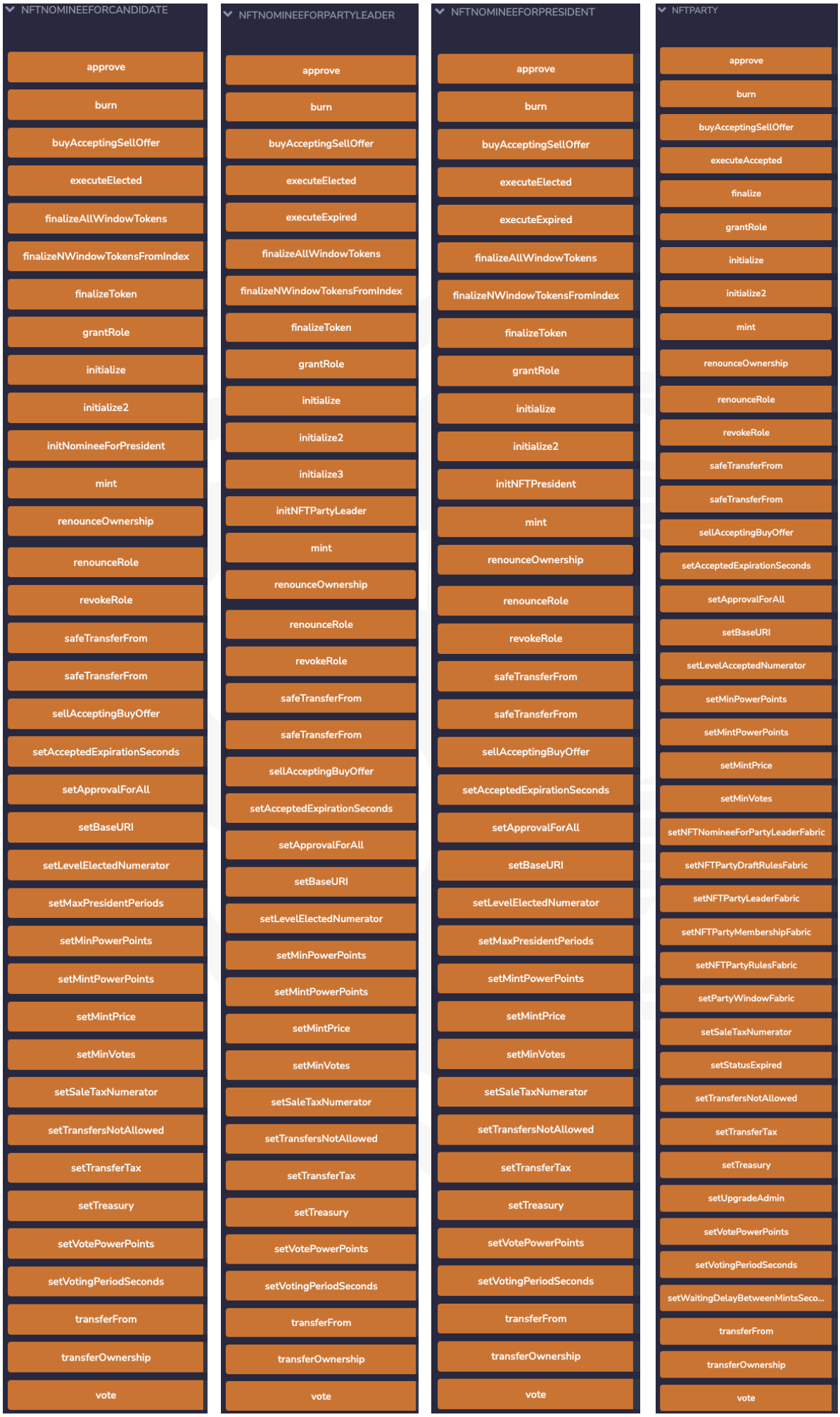
Tested	Verified
✓	✓

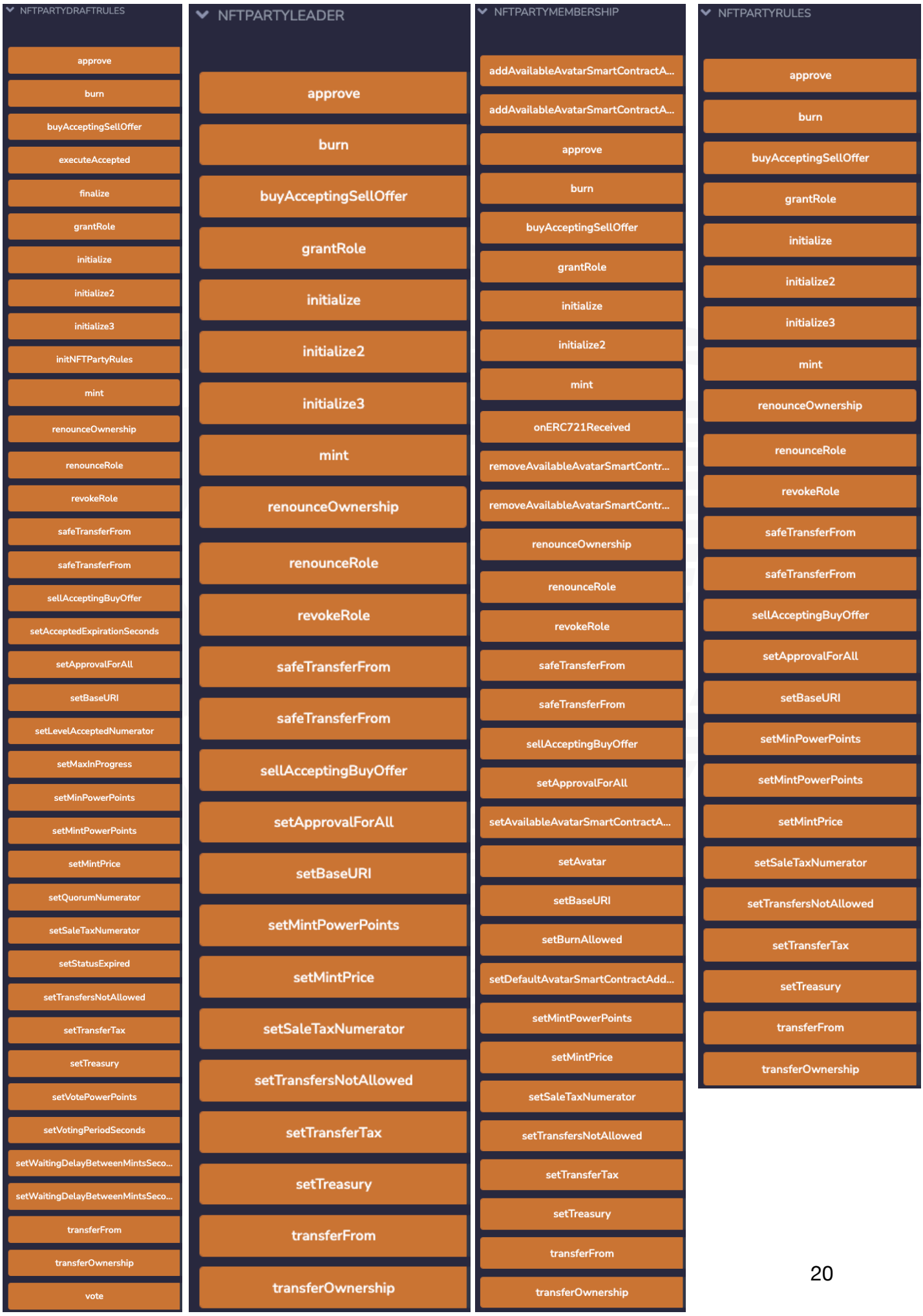
Legend

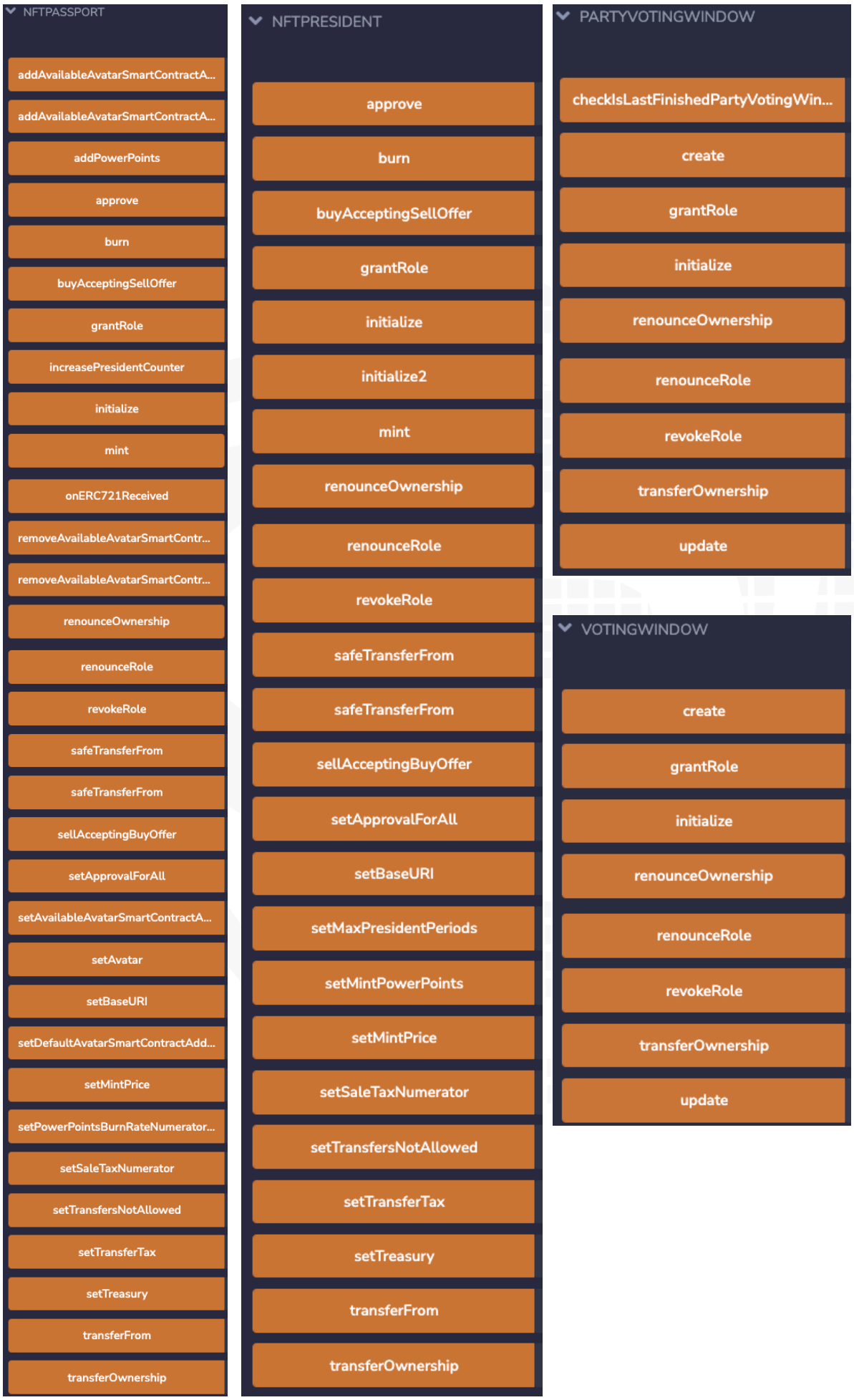
Attribute	Symbol
Verfified / Checked	✓
Partly Verified	⚑
Unverified / Not checked	✗
Not available	-

Modifiers and public functions
v1.0




NFTNOMINEEFORCANDIDATE
approve
burn
buyAcceptingSellOffer
executeElected
finalizeAllWindowTokens
finalizeNWindowTokensFromIndex
finalizeToken
grantRole
initialize
initialize2
initNomineeForPresident
mint
renounceOwnership
renounceRole
revokeRole
safeTransferFrom
safeTransferFrom
sellAcceptingBuyOffer
setAcceptedExpirationSeconds
setApprovalForAll
setBaseURI
setLevelElectedNumerator
setMaxPresidentPeriods
setMinPowerPoints
setMintPowerPoints
setMintPrice
setMinVotes
setSaleTaxNumerator
setTransfersNotAllowed
setTransferTax
setTreasury
setVotePowerPoints
setVotingPeriodSeconds
transferFrom
transferOwnership
vote
NFTNOMINEEFORPARTYLEADER
approve
burn
buyAcceptingSellOffer
executeElected
executeExpired
finalizeAllWindowTokens
finalizeNWindowTokensFromIndex
finalizeToken
grantRole
initialize
initialize2
initialize3
initNFTPartyLeader
mint
renounceOwnership
renounceRole
revokeRole
safeTransferFrom
safeTransferFrom
sellAcceptingBuyOffer
setAcceptedExpirationSeconds
setApprovalForAll
setBaseURI
setLevelElectedNumerator
setMinPowerPoints
setMintPowerPoints
setMintPrice
setMinVotes
setSaleTaxNumerator
setTransfersNotAllowed
setTransferTax
setTreasury
setVotePowerPoints
setVotingPeriodSeconds
transferFrom
transferOwnership
vote
NFTNOMINEEFORPRESIDENT
approve
burn
buyAcceptingSellOffer
executeElected
executeExpired
finalizeAllWindowTokens
finalizeNWindowTokensFromIndex
finalizeToken
grantRole
initialize
initialize2
initNFTPresident
mint
renounceOwnership
renounceRole
revokeRole
safeTransferFrom
safeTransferFrom
sellAcceptingBuyOffer
setAcceptedExpirationSeconds
setApprovalForAll
setBaseURI
setLevelElectedNumerator
setMaxPresidentPeriods
setMintPowerPoints
setMintPrice
setMinVotes
setSaleTaxNumerator
setTransfersNotAllowed
setTransferTax
setTreasury
setVotePowerPoints
setVotingPeriodSeconds
transferFrom
transferOwnership
vote
NFTPARTY
approve
burn
buyAcceptingSellOffer
executeAccepted
finalize
grantRole
initialize
initialize2
mint
renounceOwnership
renounceRole
revokeRole
safeTransferFrom
safeTransferFrom
sellAcceptingBuyOffer
setAcceptedExpirationSeconds
setApprovalForAll
setBaseURI
setLevelAcceptedNumerator
setMinPowerPoints
setMintPowerPoints
setMintPrice
setMinVotes
setNFTNomineeForPartyLeaderFabric
setNFTPartyDraftRulesFabric
setNFTPartyLeaderFabric
setNFTPartyMembershipFabric
setNFTPartyRulesFabric
setPartyWindowFabric
setSaleTaxNumerator
setStatusExpired
setTransfersNotAllowed
setTransferTax
setTreasury
setUpgradeAdmin
setVotePowerPoints
setVotingPeriodSeconds
setWaitingDelayBetweenMintsSeco...
transferFrom
transferOwnership
vote


NFTPARTYDRAFTRULES
approve
burn
buyAcceptingSellOffer
executeAccepted
finalize
grantRole
initialize
initialize2
initialize3
initNFTPartyRules
mint
renounceOwnership
renounceRole
revokeRole
safeTransferFrom
safeTransferFrom
sellAcceptingBuyOffer
setAcceptedExpirationSeconds
setApprovalForAll
setBaseURI
setLevelAcceptedNumerator
setMaxInProgress
setMinPowerPoints
setMintPowerPoints
setMintPrice
setQuorumNumerator
setSaleTaxNumerator
setStatusExpired
setTransfersNotAllowed
setTransferTax
setTreasury
setVotePowerPoints
setVotingPeriodSeconds
setWaitingDelayBetweenMintsSeco...
setWaitingDelayBetweenMintsSeco...
transferFrom
transferOwnership
vote
NFTPARTYLEADER
approve
burn
buyAcceptingSellOffer
grantRole
initialize
initialize2
initialize3
mint
renounceOwnership
renounceRole
revokeRole
safeTransferFrom
safeTransferFrom
sellAcceptingBuyOffer
setApprovalForAll
setBaseURI
setMintPowerPoints
setMintPrice
setSaleTaxNumerator
setTransfersNotAllowed
setTransferTax
setTreasury
transferFrom
transferOwnership
NFTPARTYMEMBERSHIP
addAvailableAvatarSmartContractA...
addAvailableAvatarSmartContractA...
approve
burn
buyAcceptingSellOffer
grantRole
initialize
initialize2
mint
onERC721Received
removeAvailableAvatarSmartContr...
removeAvailableAvatarSmartContr...
renounceOwnership
renounceRole
revokeRole
safeTransferFrom
safeTransferFrom
sellAcceptingBuyOffer
setApprovalForAll
setAvailableAvatarSmartContractA...
setAvatar
setBaseURI
setBurnAllowed
setDefaultAvatarSmartContractAdd...
setMintPowerPoints
setMintPrice
setSaleTaxNumerator
setTransfersNotAllowed
setTransferTax
setTreasury
transferFrom
transferOwnership
NFTPARTYRULES
approve
burn
buyAcceptingSellOffer
grantRole
initialize
initialize2
initialize3
mint
renounceOwnership
renounceRole
revokeRole
safeTransferFrom
safeTransferFrom
sellAcceptingBuyOffer
setApprovalForAll
setBaseURI
setMinPowerPoints
setMintPowerPoints
setMintPrice
setSaleTaxNumerator
setTransfersNotAllowed
setTransferTax
setTreasury
transferFrom
transferOwnership


NFTPASSPORT
addAvailableAvatarSmartContractA...
addAvailableAvatarSmartContractA...
addPowerPoints
approve
burn
buyAcceptingSellOffer
grantRole
increasePresidentCounter
initialize
mint
onERC721Received
removeAvailableAvatarSmartContr...
removeAvailableAvatarSmartContr...
renounceOwnership
renounceRole
revokeRole
safeTransferFrom
safeTransferFrom
sellAcceptingBuyOffer
setApprovalForAll
setAvailableAvatarSmartContractA...
setAvatar
setBaseURI
setDefaultAvatarSmartContractAdd...
setMintPrice
setPowerPointsBurnRateNumerator...
setSaleTaxNumerator
setTransfersNotAllowed
setTransferTax
setTreasury
transferFrom
transferOwnership
NFTPRESIDENT
approve
burn
buyAcceptingSellOffer
grantRole
initialize
initialize2
mint
renounceOwnership
renounceRole
revokeRole
safeTransferFrom
safeTransferFrom
sellAcceptingBuyOffer
setApprovalForAll
setBaseURI
setMaxPresidentPeriods
setMintPowerPoints
setMintPrice
setSaleTaxNumerator
setTransfersNotAllowed
setTransferTax
setTreasury
transferFrom
transferOwnership
PARTYVOTINGWINDOW
checkIsLastFinishedPartyVotingWin...
create
grantRole
initialize
renounceOwnership
renounceRole
revokeRole
transferOwnership
update
VOTINGWINDOW
create
grantRole
initialize
renounceOwnership
renounceRole
revokeRole
transferOwnership
update

Comments

- *Deployer can set following state variables without any limitations*
  - NFTAct
    - mintPowerPoints
    - transferTax
    - mintPrice
    - mintPowerPoints
  - NFTBill
    - acceptedExpirationSeconds
    - waitingDelayBetweenMintsSecondsForPartyLeader
    - waitingDelayBetweenMintsSecondsForPresident
    - waitingDelayBetweenMintsSeconds
    - votingPeriodSeconds
    - maxInProgress
    - mintPowerPoints
    - votePowerPoints
  - NFTLegislativeInitiative
    - waitingDelayBetweenMintsSeconds
    - maxInProgress
    - minVotes
    - votingPeriodSeconds
    - acceptedExpirationSeconds
    - minPowerPoints
    - mintPowerPoints
    - votePowerPoints
  - NFTNomineeForCandidate
    - maxPresidentPeriods
    - minVotes
    - levelElectedNumerator
    - votingPeriodSeconds
    - acceptedExpirationSeconds
    - minPowerPoints
    - mintPowerPoints
    - votePowerPoints
  - NFTNomineeForPartyLeader
    - minVotes
    - levelElectedNumerator
    - votingPeriodSeconds
    - acceptedExpirationSeconds
    - minPowerPoints
    - mintPowerPoints

    - votePowerPoints
    - mintPrice
    - transferTax

- NFTNomineeForPresident
    - maxPresidentPeriods
    - minVotes
    - levelElectedNumerator
    - votingPeriodSeconds
    - acceptedExpirationSeconds
    - mintPowerPoints
    - votePowerPoints
    - mintPrice
    - saleTaxNumerator
    - transferTax

- NFTParty
    - waitingDelayBetweenMintsSeconds
    - minVotes
    - votingPeriodSeconds
    - acceptedExpirationSeconds
    - minPowerPoints
    - mintPowerPoints
    - votePowerPoints
    - mintPrice
    - saleTaxNumerator
    - transferTax

- NFTPartyDraftRules
    - waitingDelayBetweenMintsSecondsForPartyLeader
    - waitingDelayBetweenMintsSeconds
    - votingPeriodSeconds
    - acceptedExpirationSeconds
    - maxInProgress
    - minPowerPoints
    - mintPowerPoints
    - votePowerPoints
    - transferTax

- NFTPartyLeader
    - mintPowerPoints
    - mintPrice

- NFTPartyMembership
    - mintPrice
    - saleTaxNumerator

        - transferTax
        - mintPowerPoints

    - NFTPartyRules
        - minPowerPoints
        - mintPowerPoints
        - mintPrice
        - saleTaxNumerator

    - NFTPassport
        - mintPrice
        - transferTax

    - NFTPresident
        - maxPresidentPeriods
        - mintPowerPoints
        - mintPrice
        - transferTax

- *Deployer can enable/disable following state variables*
    - Coin
        - isTaxWhitelisted
        - isPool

    - NFTAct
        - transfersNotAllowed

    - NFTBill
        - transfersNotAllowed

    - NFTLegislativeInitiative
        - transfersNotAllowed

    - NFTNomineeForCandidate
        - transfersNotAllowed

    - NFTNomineeForPartyLeader
        - transfersNotAllowed

    - NFTNomineeForPresident
        - transfersNotAllowed

    - NFTParty
        - transfersNotAllowed

- NFTPartyDraftRules
  - transfersNotAllowed
- NFTPartyLeader
  - transfersNotAllowed
- NFTPartyMembership
  - transfersNotAllowed
- NFTPartyRules
  - transfersNotAllowed
- NFTPassport
  - transfersNotAllowed

- *Deployer can set following addresses*
  - Coin
    - treasury
    - _owner
  - NFTAct
    - treasury
    - baseURI
  - NFTBill
    - nftAct
      - Can be set once
    - baseURI
    - treasury
  - NFTLegislativeInitiative
    - nftBill
      - Can be set once
    - baseURI
    - treasury
  - NFTNomineeForCandidate
    - treasury
    - baseURI
  - NFTNomineeForPartyLeader
    - treasury
    - baseURI
  - NFTNomineeForPresident

        - baseURI
        - treasury

    - NFTParty
        - nftPartyLeaderFabric
        - nftNomineeForPartyLeaderFabric
        - partyVotingWindowFabric
        - nftPartyRulesFabric
        - nftPartyDraftRulesFabric
        - nftPartyMembershipFabric
        - upgradeAdmin
        - baseURI
        - treasury

    - NFTPartyDraftRules
        - treasury
        - baseURI
        - _availableAvatarSmartContractAddresses

    - NFTPartyLeader
        - treasury
        - baseURI

    - NFTPartyMembership
        - baseURI
        - treasury
        - _availableAvatarSmartContractAddresses

    - NFTPartyRules
        - treasury
        - baseURI

    - NFTPassport
        - baseURI
        - treasury
        - _availableAvatarSmartContractAddresses
        - defaultAvatartSmartContractAddress

    - NFTPresident
        - baseURI
        - treasury

- *Existing Modifiers*
    - Coin
        - lockTheSwap

- NFTAct
  - initializer2
  - initializer3
  - initializer4
  - onlyNotZeroAddress
  - onlyValidPassportHolder
  - onlyValidPassportHolderOrZeroAddress

- NFTBill
  - initializer2
  - initializer3
  - initializer4
  - onlyNotZeroAddress
  - onlyValidPassportHolder
  - onlyValidPassportHolderOrZeroAddress

- NFTLegislativeInitiative
  - initializer2
  - initializer3
  - initializer4
  - onlyNotZeroAddress
  - onlyValidPassportHolder
  - onlyValidPassportHolderOrZeroAddress

- NFTNomineeForCandidate
  - initializer2
  - initializer3
  - initializer4
  - onlyNotZeroAddress
  - onlyValidPassportHolder
  - onlyValidPassportHolderOrZeroAddress

- NFTNomineeForPartyLeader
  - initializer2
  - initializer3
  - initializer4
  - onlyNotZeroAddress

- NFTNomineeForPresident
  - initializer2
  - initializer3
  - initializer4
  - onlyNotZeroAddress
  - onlyValidPassportHolder
  - onlyValidPassportHolderOrZeroAddress

- NFTParty
  - initializer2
  - initializer3
  - initializer4
  - onlyNotZeroAddress
  - onlyValidPassportHolder
  - onlyValidPassportHolderOrZeroAddress

- NFTPartyDraftRules
  - initializer2
  - initializer3
  - initializer4
  - onlyNotZeroAddress

- NFTPartyLeader
  - initializer2
  - initializer3
  - initializer4
  - onlyNotZeroAddress

- NFTPartyMembership
  - initializer2
  - initializer3
  - initializer4
  - onlyNotZeroAddress
  - onlyValidPassportHolder
  - onlyValidPassportHolderOrZeroAddress

- NFTPartyRules
  - initializer2
  - initializer3
  - initializer4
  - onlyNotZeroAddress

- NFTPassport
-
- NFTPresident
  - initializer2
  - initializer3
  - initializer4
  - onlyNotZeroAddress
  - onlyValidPassportHolder
  - onlyValidPassportHolderOrZeroAddress

- 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

- Coin
  - Everybody is able to burn

- NFTAct
  - Owner is able to
    - burn tokens
    - Grant/revoke roles

- NFTBill
  - Owner is able to
    - burn tokens
    - Grant/revoke roles
  - Owner can lock minting by setting maxInProgress to 0

- NFTLegislativeInitiative
  - Owner is able to
    - burn tokens
    - Grant/revoke roles

- NFTNomineeForCandidate
  - Owner is able to
    - burn tokens
    - Grant/revoke roles

- NFTNomineeForPartyLeader
  - Owner is able to
    - burn tokens
    - Grant/revoke roles

- NFTParty
  - Owner is able to
    - burn tokens
    - Grant/revoke roles

- NFTPassport
  - Address with increase_president_counter_role can increase presidentCounter by one
  - Address with add_power_points_role role can increase powerPoints by one
  - Anyone can call mint

- Keep it in mind that if you are deleting a struct, the mappings in it will not deleted
- Contracts can be updated

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/interfaces/INFTParty.sol		1	4	2	2		5	
📝	contracts/VotingWindow.sol	1		262	237	205	16	93	
📝	contracts/NFTPartyMembership.sol	1		139	114	79	17	52	
📝	contracts/NFTPartyLeader.sol	1		203	172	118	26	74	
📝	contracts/NFTNomineeForCandidate.sol	1		297	263	189	36	121	
📝	contracts/Coin.sol	1		257	245	183	38	133	
📝	contracts/NFTNomineeForPartyLeader.sol	1		332	295	217	42	141	
📝	contracts/NFTNomineeForPresident.sol	1		358	322	231	53	141	
📝	contracts/NFTBill.sol	1		352	309	239	33	139	
📝	contracts/NFTPresident.sol	1		198	168	118	20	69	
📝🔍	contracts/NFTParty.sol	1	1	396	335	263	24	172	
📝	contracts/NFTPassport.sol	1		157	131	76	33	48	🧱
📝	contracts/NFTLegislativeInitiative.sol	1		299	262	196	33	116	
💊	contracts/utils/MintPriceStorage.sol	1		28	28	20	1	10	
💊	contracts/utils/MaxInProgressStorage.sol	1		25	25	18	1	9	
💊	contracts/utils/MaxPresidentPeriodsStorage.sol	1		21	21	15	1	8	
📚	contracts/utils/Utils.sol	1		19	19	14	1	6	
💊	contracts/utils/WaitingDelayBetweenMintsSecondsForPartyLeaderStorage.sol	1		21	21	15	1	8	
📝	contracts/utils/NFTWalletOwnershipWithOffchainMarketplacePauserMintPriceTransferTaxBase.sol	1		173	146	100	19	83	
💊	contracts/utils/VotingPeriodSecondsStorage.sol	1		25	25	18	1	8	
💊	contracts/utils/OffchainERC721MarketplacePassportOwnershop.sol	1		190	164	138	9	75	🧱
💊	contracts/utils/OffchainERC721Marketplace.sol	1		171	145	126	7	70	🧱
💊	contracts/utils/NFTPartyMembershipOwnershipERC721BaseEnumerablePausableUpgradeable.sol	1		650	611	300	228	220	🖥♻
📝	contracts/utils/fabric/NFTPartyDraftRulesFabric.sol	1		142	127	103	12	69	🌀
📝	contracts/utils/fabric/NFTPartyRulesFabric.sol	1		142	127	102	12	67	🌀
📝	contracts/utils/fabric/NFTPartyMembershipFabric.sol	1		120	105	90	3	70	🌀
📝	contracts/utils/fabric/PartyVotingWindowFabric.sol	1		73	64	55	1	38	🌀
📝	contracts/utils/fabric/NFTPartyLeaderFabric.sol	1		143	128	104	11	69	🌀
📝	contracts/utils/fabric/NFTNomineeForPartyLeaderFabric.sol	1		143	128	104	11	69	🌀

	contracts/utils/QuorumNumeratorStorage.sol	1		23	23	17	1	10	
	contracts/utils/MinVotesStorage.sol	1		25	25	18	1	8	
	contracts/utils/CoinStorage.sol	1		17	17	11	1	3	
	contracts/utils/NFTPassportOwnershipWithOffchainMarketplacePauserMintPriceTransferTaxBase.sol	1		123	109	76	14	54	
	contracts/utils/PartyVotingWindowStorage.sol	1		18	18	13	1	9	
	contracts/utils/BurnAllowedStorage.sol	1		23	23	17	1	8	
	contracts/utils/LevelAcceptedNumeratorStorage.sol	1		23	23	17	1	10	
	contracts/utils/ImplementationStorage.sol	1		24	24	18	1	10	
	contracts/utils/Base.sol	1		30	30	23	2	7	
	contracts/utils/MaxPartyLeaderPeriodsStorage.sol	1		19	19	13	1	8	
	contracts/utils/WaitingDelayBetweenMintsSecondsForPresidentStorage.sol	1		21	21	15	1	8	
	contracts/utils/AcceptedExpirationSecondsStorage.sol	1		25	25	18	1	8	
	contracts/utils/NFTPassportStorage.sol	1		55	55	42	1	36	
	contracts/utils/Initializable2.sol	1		67	67	17	41	6	
	contracts/utils/NFTPartyMembershipStorage.sol	1		39	39	29	1	20	
	contracts/utils/AccessControlEnumerableUpgradeable.sol	2		308	308	120	158	97	
	contracts/utils/TreasuryStorage.sol	1		26	26	20	1	10	
	contracts/utils/TransferTaxStorage.sol	1		22	22	16	1	8	
	contracts/utils/TransparentUpgradeableProxy.sol	1		124	124	38	75	43	
	contracts/utils/NFTPartyMembershipOwnershipWithOffchainMarketplacePauserMintPriceTransferTaxBase.sol	1		180	153	97	25	75	
	contracts/utils/OffchainERC721MarketplacePartyMembershipOwnership.sol	1		169	143	124	7	68	
	contracts/utils/Access.sol	1		31	31	22	2	21	
	contracts/utils/NFTPassportOwnershipERC721BaseEnumerablePausableUpgradeable.sol	1		650	611	298	232	222	
	contracts/utils/ERC20PresetMinterUpgradeable.sol	1		61	61	25	29	26	
	contracts/utils/VotePowerPoints.sol	1		25	25	18	1	9	
	contracts/utils/VotingWindowStorage.sol	1		18	18	13	1	6	
	contracts/utils/MinPowerPointsStorage.sol	1		26	26	19	1	10	
	contracts/utils/NFTPartyStorage.sol	1		18	18	13	1	7	
	contracts/utils/WaitingDelayBetweenMintsSecondsStorage.sol	1		21	21	15	1	8	
	contracts/utils/MintPowerPointsStorage.sol	1		30	30	22	1	11	
	contracts/utils/LevelElectedNumeratorStorage.sol	1		21	21	15	1	8	
	contracts/utils/AvatarsMixin.sol	1	1	109	105	86	2	88	
	contracts/utils/SaleTaxNumeratorStorage.sol	1		25	25	18	2	12	
	contracts/utils/NFTPresidentStorage.sol	1		18	18	13	1	6	
	contracts/PartyVotingWindow.sol	1		204	187	159	12	69	
	contracts/NFTPartyRules.sol	1		170	140	104	14	55	
	contracts/NFTPartyDraftRules.sol	1		345	303	220	42	125	
	contracts/Errors.sol	1		9	9	7	1	5	
	contracts/NFTAct.sol	1		157	130	96	13	45	
	Totals	**68**	**3**	**8639**	**7812**	**5360**	**1383**	**3422**	

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	Shortcut Description
#1	C_C	State variable visibility is not set	34	It is best practice to set the visibility of state variables explicitly
#2	U_A2		11, 20	
#3	U_E1		25, 26, 35, 38, 40, 43, 44	
#4	C_C		109, 110, 112-116	
#5	U_E1		25, 35, 43	
#6	C_N1		56, 57, 64,	
#7	C_N2		112, 113, 120	
#8	C_N3		97, 98, 105	
#9	C_N4		95, 96, 103	
#10	C_N5		103, 104, 111	

#11	U_F_N1	Local variables shadowing	61	Local_shadowing
#12	U_F_N2		60	
#13	U_F_N3		61	
#14	U_F_N4		36	
#15	U_F_N5		60	
#16	U_F_P1		40	
#17	C_N6		105, 106, 113	
#18	C_N7		192, 193, 200	
#19	C_N8		102, 103, 110	
#20	C_N9		76, 77, 84	
#21	C_N10		50, 51, 58	
#22	C_N11		59, 60, 67	
#23	C_N12		42, 43, 51	
#24	C_N13		74, 75, 82	
#25	C_P1		44	
#26	C_V1		49	
#27	U_N1		436, 376, 305, 448, 183, 117, 214, 142, 539, 175	
#28	U_N2		53	
#29	U_N5		444, 379, 308, 455, 183, 120, 217, 142, 538, 175	
#30	U_N6		50	
#31	U_N9		54	

Informational issues

Issue	File Shortcut	Type	Line	Description Shortcut
#1	U_A3		232, 55, 205	
#2	U_M2		11	
#3	U_M7		22	

#4	U_M5	Functions that are not used	27	Remove unused functions
#5	U_N1		91, 319, 327	
#6	U_N5		94, 322, 330	
#7	U_T2		113	
#8	U_U1		11	
#9	U_A4	Misspelling	See description	Change following words: - defaultAvatartSmartContractAddress L17, L38, L43, ... Make sure to change it everywhere else as well.
#10	C_N2		See description	Change following words: - saletax L304 Make sure to change it everywhere else as well.
#11	C_N3		See description	Change following words: - WatingDays L162, L163, L166 Make sure to change it everywhere else as well.
#12	C_N7		See description	Change following words: - WatingDays L247, L248 Make sure to change it everywhere else as well.
#13	All	NatSpec documentation missing	-	If you started to comment your code, also comment all other functions, variables etc.

#14	All	Wrong import name		Import for upgradeable contracts from open zeppelin should be: Import “@openzeppelin/contracts-upgradeable/...” Instead of import “@openzeppelin-upgradeable/contracts/...” _____ Import “@uniswap/v2-core/...” Instead of import “@uniswao-v2-core/...” ”
#15	C_I_N1	SPDX License is missing	Top of source file	SPDX_License_missing
#16	U_A1		17, 22	
#17	U_A4		70, 76, 82, 92	
#18	U_B2		19	
#19	U_E1		56	
#20	U_F_N1		139	
#21	U_F_N2		138	
#22	U_F_N3		139	
#23	U_F_N4		116	
#24	U_F_N5		138	
#25	U_I1		20	
#26	U_L1		18	
#27	U_L2		17	
#28	U_M1		17	
#29	U_M2		15	
#30	U_M3		17	
#31	U_M4		17	

#32	U_M5		17	
#33	U_M6		24	
#34	U_M7		17	
#35	U_N2		81, 164, 175	
#36	U_N3		36	
#37	U_N6		119	
#38	U_N7		46, 52	
#39	U_N9		80, 139, 147, 156,	
#40	U_O1		48	
#41	U_O2	Wrong visibility order	49	Visibility_order
#42	U_O3		51, 186	
#43	U_Q1		18	
#44	U_S1		20	
#45	U_T1		18	
#46	U_T3		22	
#47	U_U1		6, 11	
#48	U_V1		17	
#49	U_V2		17	
#50	U_W1		17	
#51	U_W2		17	
#52	U_W3		17	
#53	C_C		52, 57, 62, 68, 73, 78, 84, 90, 96, 102	
#54	C_N2		174, 308	
#55	C_N3		131, 254	
#56	C_N4		70	
#57	C_N5		71	
#58	C_N6		72	
#59	C_N7		302	
#60	C_N8		300	

#61	C_N9	58	
#62	C_N12	68, 117	
#63	C_N13	59, 103	
#64	C_P1	44, 58	
#65	C_V1	49, 63, 112-119	
#66	U_L1	14, 19	
#67	U_A3	175	
#68	U_A4	37, 45, 61, 71, 72, 88	
#69	U_B1	9, 15, 21, 27	
#70	U_I1	53	
#71	U_L1	14, 19	
#72	U_M1	23	
#73	U_M4	24	
#74	U_N1	118, 141, 151, 175, 184, 188, 227, 252, 281, 304, 335, 352, 353, 406, 407, 452, 481, 540, 555	
#75	U_N2	122, 134	
#76	U_N4	14	
#77	U_N5	121, 141, 151, 173, 184, 188, 198, 230, 255, 284, 307, 338, 355, 356, 410, 409, 459, 488, 539, 554	
#78	U_N6	90	
#79	U_N7	18, 23, 27, 32, 36, 42, 48	
#80	U_N9	96, 121, 133,	

#81	U_O1	Error is not from Errors file	54, 114, 112, 142, 151, 153	Import_error_message_from _errors_file
#82	U_O2		111, 113, 149, 151	
#83	U_O3		57, 106, 115, 117, 145, 154, 156	
#84	U_Q1		14, 19	
#85	U_T2		121	
#86	U_U1		7, 12, 16	
#87	C_N1		93, 104	
#88	C_N2		175, 185, 196, 214, 233-238, 262, 263, 299, 318, 319, 334, 335	
#89	C_N3		160, 164, 181-186, 206, 207, 242, 264, 265, 280, 281	
#90	C_N4		141, 155, 158, 161, 179, 185, 189, 223, 232, 241, 264, 278, 279	
#91	C_N5		156, 169, 172, 190, 196, 200, 247, 256, 265, 281, 305, 306, 314, 315	
#92	C_N6		152, 160, 169, 176, 187, 190, 208, 214, 218, 268, 277, 286, 323, 324, 335, 340	
#93	C_N7		249, 263-268, 284, 285, 312, 378, 379	

#94	C_N8		196, 200, 216, 217, 223, 247, 248, 274, 288, 310, 311, 326, 327	
#95	C_N9		129, 140, 162, 178	
#96	C_N10		101, 103, 116, 117	
#97	C_N11		103, 144	
#98	C_N13		116, 124, 137, 176	
#99	C_P1		126, 127, 166-182	
#100	C_V1		204-232	
#101	U_F_P1	Unused function parameter	63-65	Unused_function_parameter
#102	U_M5		26	
#103	U_O2		98, 136	
#104	C_N3		128	
#105	C_N4		124	
#106	C_N5		143	
#107	C_N7		222	
#108	C_N9		112	
#109	C_N1	Unused local variables	96, 98-102	Remove unused local variables
#110	C_N6		172, 173	
#111	C_N9		134-136	
#112	C_N11		106, 108-111	
#113	C_N13		130-133	
#114	U_N7		47	
#115	U_V2	Function can be restricted	22	Function_can_be_view
#116	C_C	Redundant logic	138-152	Logic can be encapsulated in its own function and can be reused for L153-167

Legend:

Files

Contracts	
Shortcut	File
C_C	Coin
C_E	Errors
C_I_N1	interfaces/INFTParty
C_N1	NFTAct
C_N2	NFTBill
C_N3	NFTLegislativeInitiative
C_N4	NFTNomineeForCandidate
C_N5	NFTNomineeForPartyLeader
C_N6	NFTNomineeForPresident
C_N7	NFTParty
C_N8	NFTPartyDraftRules
C_N9	NFTPartyLeader
C_N10	NFTPartyMembership
C_N11	NFTPartyRules
C_N12	NFTPassport
C_N13	NFTPresident
C_P1	PartyVotingWindow
C_V1	VotingWindow

Utils	
Shortcut	File
U_A1	AcceptedExpirationSecondsStorage
U_A2	Access
U_A3	AccessControlEnumerableUpgradeable
U_A4	AvatarsMixin
U_B1	Base
U_B2	BurnAllowedStorage
U_C1	CoinStorage

U_E1	ERC20PresetMinterUpgradeable
U_F_N1	fabric/NFTNomineeForPartyLeaderFabric
U_F_N2	fabric/NFTPartyDraftRulesFabric
U_F_N3	fabric/NFTPartyLeaderFabric
U_F_N4	fabric/NFTPartyMembershipFabric
U_F_N5	fabric/NFTPartyRulesFabric
U_F_P1	fabric/PartyVotingWindowFabric
U_I1	ImplementationStorage
U_I2	Initializable2
U_L1	LevelAcceptedNumeratorStorage
U_L2	LevelElectedNumeratorStorage
U_M1	MaxInProgressStorage
U_M2	MaxPartyLeaderPeriodsStorage
U_M3	MaxPresidentPeriodsStorage
U_M4	MinPowerPointsStorage
U_M5	MintPowerPointsStorage
U_M6	MintPriceStorage
U_M7	MinVotesStorage
U_N1	NFTPartyMembershipOwnershipERC721BaseEnumerablePausableUpgradeable
U_N2	NFTPartyMembershipOwnershipWithOffchainMarketplacePauserMintPriceTransferTaxBase
U_N3	NFTPartyMembershipStorage
U_N4	NFTPartyStorage
U_N5	NFTPassportOwnershipERC721BaseEnumerablePausableUpgradeable
U_N6	NFTPassportOwnershipWithOffchainMarketplacePauserMintPriceTransferTaxBase
U_N7	NFTPassportStorage
U_N8	NFTPresidentStorage
U_N9	NFTWalletOwnershipWithOffchainMarketplacePauserMintPriceTransferTaxBase
U_O1	OffchainERC721Marketplace
U_O2	OffchainERC721MarketplacePartyMembershipOwnership

U_O3	OffchainERC721MarketplacePassportOwnershop
U_P1	PartyVotingWindowStorage
U_Q1	QuorumNumeratorStorage
U_S1	SaleTaxNumeratorStorage
U_T1	TransferTaxStorage
U_T2	TransparentUpgradeableProxy
U_T3	TreasuryStorage
U_U1	Utils
U_V1	VotePowerPoints
U_V2	VotingPeriodSecondsStorage
U_V3	VotingWindowStorage
U_W1	WaitingDelayBetweenMintsSecondsForPartyLeaderStorage
U_W2	WaitingDelayBetweenMintsSecondsForPresidentStorage
U_W3	WaitingDelayBetweenMintsSecondsStorage

Description

Shortcut	Error message
Import_error_message_from_errors_file	If you are started to write the errors into the library then go ahead with it and write the others into it also. Replace strings with Error file variables. We recommend you to adjust the error messages to clarify from which file the error is coming from
Local_shadowing	Rename the local variables that shadow another component
SPDX_License_missing	SPDX license identifier not provided in source file. Consider adding a comment containing “SPDX-License-Identifier: <SPDX-License>”
Visibility_order	Visibility specifier (external, public, internal etc.) should come before other modifiers (pure, view, payable, onlyOwner, etc.)

Unused_function_parameter	If the function has the override key, we recommend you to leave the type and remove the variable name if you are not going to use the function parameter: e.g. you are not going to use “from” parameter: function _transfer(address from, address recipient, uint256 amount) .... to function _transfer(address, address recipient, uint256 amount) .... Look at the red marked text above. Or if you are not using the parameter remove it.
Function_can_be_view	Function state mutability can be restricted to view

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.

. May 2022:

- Read whole report for more information

SWC Attacks

ID	Title	Relationships	Status
SWC-136	Unencrypted Private Data On-Chain	CWE-767: Access to Critical Private Variable via Public Method	PASSED
SWC-135	Code With No Effects	CWE-1164: Irrelevant Code	PASSED
SWC-134	Message call with hardcoded gas amount	CWE-655: Improper Initialization	PASSED
SWC-133	Hash Collisions With Multiple Variable Length Arguments	CWE-294: Authentication Bypass by Capture-replay	PASSED
SWC-132	Unexpected Ether balance	CWE-667: Improper Locking	PASSED
SWC-131	Presence of unused variables	CWE-1164: Irrelevant Code	NOT PASSED
SWC-130	Right-To-Left-Override control character (U+202E)	CWE-451: User Interface (UI) Misrepresentation of Critical Information	PASSED
SWC-129	Typographical Error	CWE-480: Use of Incorrect Operator	PASSED
SWC-128	DoS With Block Gas Limit	CWE-400: Uncontrolled Resource Consumption	PASSED

SWC-127	Arbitrary Jump with Function Type Variable	CWE-695: Use of Low-Level Functionality	PASSED
SWC-125	Incorrect Inheritance Order	CWE-696: Incorrect Behavior Order	PASSED
SWC-124	Write to Arbitrary Storage Location	CWE-123: Write-what-where Condition	PASSED
SWC-123	Requirement Violation	CWE-573: Improper Following of Specification by Caller	PASSED
SWC-122	Lack of Proper Signature Verification	CWE-345: Insufficient Verification of Data Authenticity	PASSED
SWC-121	Missing Protection against Signature Replay Attacks	CWE-347: Improper Verification of Cryptographic Signature	PASSED
SWC-120	Weak Sources of Randomness from Chain Attributes	CWE-330: Use of Insufficiently Random Values	PASSED
SWC-119	Shadowing State Variables	CWE-710: Improper Adherence to Coding Standards	NOT PASSED
SWC-118	Incorrect Constructor Name	CWE-665: Improper Initialization	PASSED
SWC-117	Signature Malleability	CWE-347: Improper Verification of Cryptographic Signature	PASSED

SWC-116	Timestamp Dependence	CWE-829: Inclusion of Functionality from Untrusted Control Sphere	PASSED
SWC-115	Authorization through tx.origin	CWE-477: Use of Obsolete Function	PASSED
SWC-114	Transaction Order Dependence	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	PASSED
SWC-113	DoS with Failed Call	CWE-703: Improper Check or Handling of Exceptional Conditions	PASSED
SWC-112	Delegatecall to Untrusted Callee	CWE-829: Inclusion of Functionality from Untrusted Control Sphere	PASSED
SWC-111	Use of Deprecated Solidity Functions	CWE-477: Use of Obsolete Function	PASSED
SWC-110	Assert Violation	CWE-670: Always-Incorrect Control Flow Implementation	PASSED
SWC-109	Uninitialized Storage Pointer	CWE-824: Access of Uninitialized Pointer	PASSED
SWC-108	State Variable Default Visibility	CWE-710: Improper Adherence to Coding Standards	NOT PASSED
SWC-107	Reentrancy	CWE-841: Improper Enforcement of Behavioral Workflow	PASSED
SWC-106	Unprotected SELFDESTRUCT Instruction	CWE-284: Improper Access Control	PASSED

SWC-105	Unprotected Ether Withdrawal	CWE-284: Improper Access Control	PASSED
SWC-104	Unchecked Call Return Value	CWE-252: Unchecked Return Value	PASSED
SWC-103	Floating Pragma	CWE-664: Improper Control of a Resource Through its Lifetime	PASSED
SWC-102	Outdated Compiler Version	CWE-937: Using Components with Known Vulnerabilities	PASSED
SWC-101	Integer Overflow and Underflow	CWE-682: Incorrect Calculation	PASSED
SWC-100	Function Default Visibility	CWE-710: Improper Adherence to Coding Standards	PASSED

Blockchain Security | Smart Contract Audits | KYC

MADE IN GERMANY