smart state

Web3 security easier than ever

EYWA

NFT

Smart contract audit report

February 12, 2024

Table of contents

Methodology

- Manual code analysis
- Best code practices
- ERC20/BEP20 compliance (if applicable)
- Locked ether
- Pool Asset Security (backdoors in the underlying ERC-20)
- FA2 compliance (if applicable)
- Logical bugs & code logic issues
- Error handling issues
- General Denial Of Service(DOS)
- Cryptographic errors
- Weak PRNG / Random number generators issues
- Protocol and header parsing errors
- Private data leaks
- Using components with known vulnerabilities
- Unchecked call return method
- Code with no effects
- Unused vars
- Use of deprecated functions
- Authorization issues
- Re-entrancy
- Arithmetic Overflows / Underflows
- Hidden Malicious Code
- External Contract Referencing
- Short Address/Parameter Attack
- Race Conditions / Front Running
- Uninitialized Storage Pointers
- Floating Points and Precision
- Signatures Replay

Summary

EYWA is a system that allows different blockchain ecosystems to interact with each other. Project enable users to move their assets between different networks quickly and cheaply, and enable developers to efficiently implement cross-chain logic for their decentralized applications.

The mission of the project is to bring DeFi together. EYWA intends to make decentralized finance simple, convenient and understandable even for beginners.

This audit encompasses the examination of smart contracts of the EYWA NFT management system designed to organize the functionality of the EYWA NFTs: Container, Merge, veEYWA booster.

Disclaimer

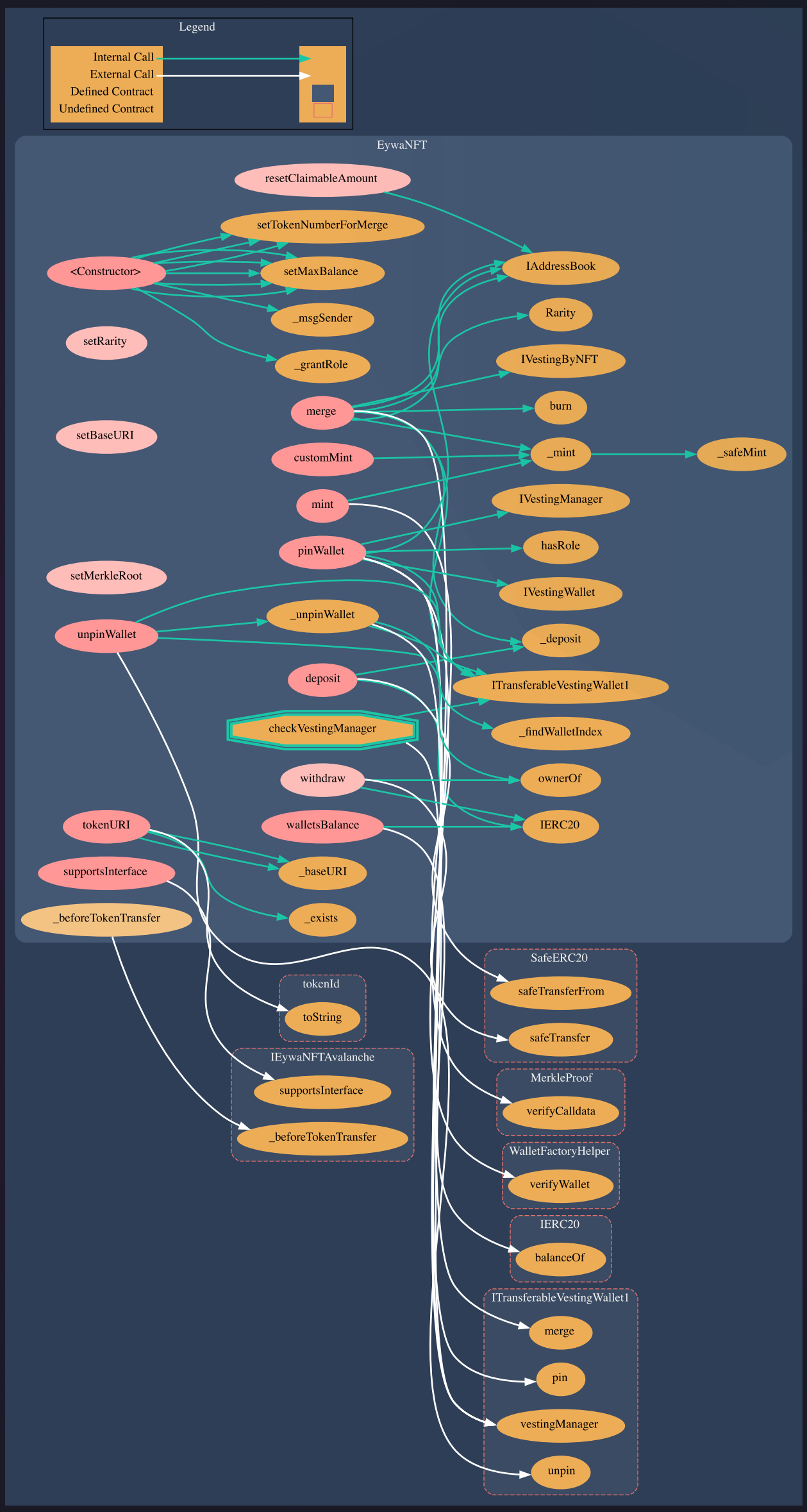
This is a final public security audit report version and does not include vulnerabilities that might have been found and addressed during the audit process.
An audit does not provide any warranties regarding the code security. We presume that a single audit cannot be considered totally sufficient and always recommend several independent audits and a public bug bounty program to ensure code security.
Please do not consider this report as investment and / or financial advice of any kind.

Vulnerabilities found by type

Info	0
Warning	0
Warning	0
Total	0

1.1 Structure of contract:

EywaNFT



pic.1.1 EywaNFT

1.2 EywaNFT contract methods analysis:

constructor(address eywaToken_, address addressBook_)
Vulnerabilities not detected

setRarity(uint256 tokenId, Rarity newRarity)
Vulnerabilities not detected

setBaseURI(string memory newBaseURI)
Vulnerabilities not detected

resetClaimableAmount(uint256 tokenId)
Vulnerabilities not detected

deposit(uint256 tokenId, uint256 amount)	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, public

merge(uint256[] memory tokenIds, uint256 mainTokenId)	
Vulnerabilities not detected	
TOKEN FLOW	Tokens out, public

mint(address to_, uint256 tokenId_, Rarity rarity_, uint256 claimableAmount_)
Vulnerabilities not detected

1.2 EywaNFT contract methods analysis:

setMaxBalance(Rarity rarity_, uint256 newMaxBalance)
Vulnerabilities not detected

setTokenNumberForMerge(Rarity rarity_, uint32 newTokenNumberForMerge)
Vulnerabilities not detected

pinWallet(uint256 tokenId, address wallet)
Vulnerabilities not detected

unpinWallet(uint256 tokenId, address wallet)
Vulnerabilities not detected

withdraw(uint256 tokenId, uint256 amount)	
Vulnerabilities not detected	
TOKEN FLOW	Tokens out, public

walletsBalance(uint256 tokenId)
Vulnerabilities not detected

tokenURI(uint256 tokenId)
Vulnerabilities not detected

supportsInterface(bytes4 interfaceId)
Vulnerabilities not detected

1.2 EywaNFT contract methods analysis:

`_beforeTokenTransfer(`
`address from,`
`address to,`
`uint256 tokenId,`
`uint256 batchSize`
`)`

Vulnerabilities not detected

`_baseURI()`
Vulnerabilities not detected

`_mint(address to_, uint256 tokenId_, Rarity rarity_)`
Vulnerabilities not detected

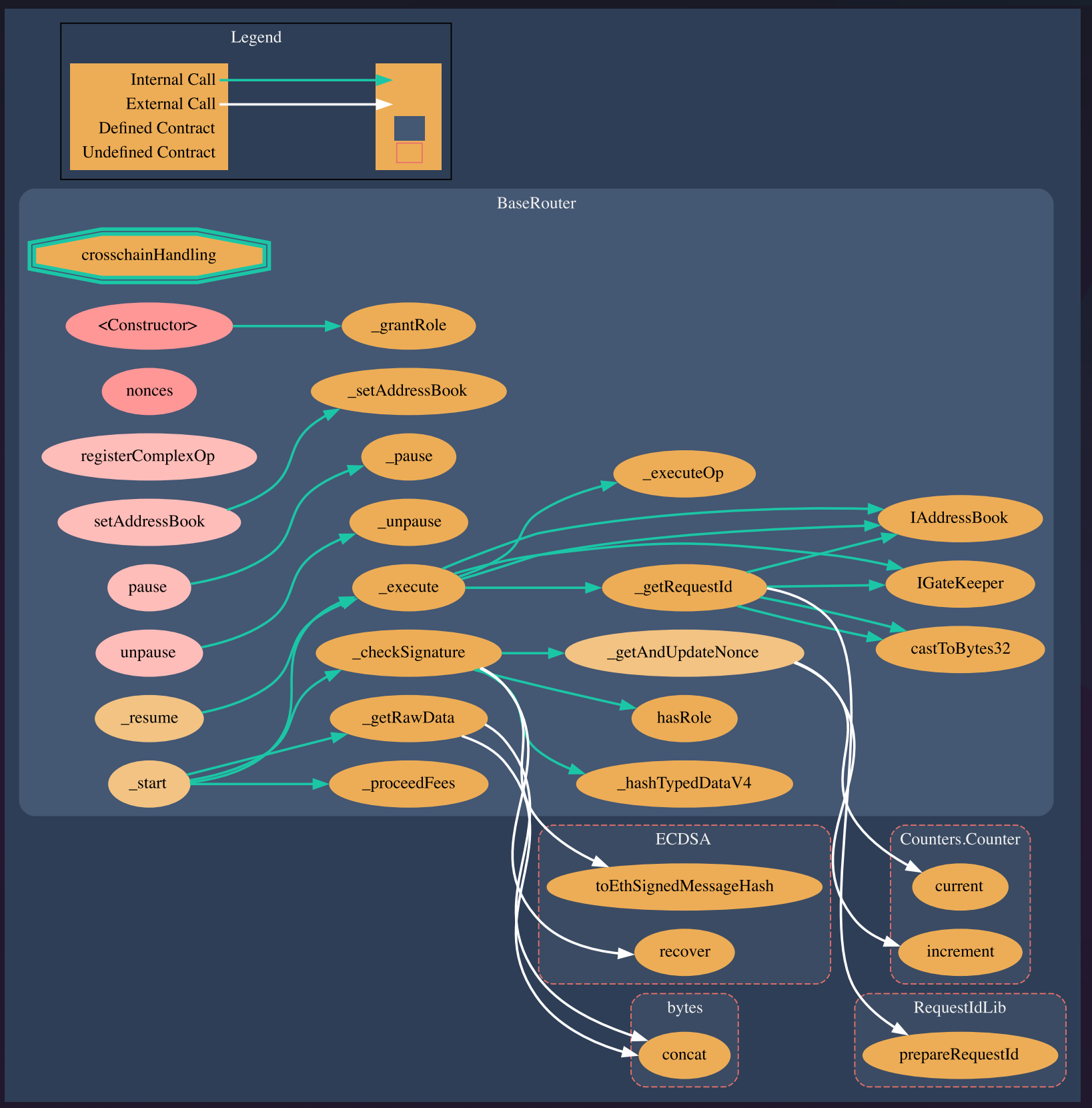
`_deposit(uint256 tokenId, uint256 amount)`
Vulnerabilities not detected

`_unpinWallet(uint256 tokenId, address wallet)`
Vulnerabilities not detected

`_findWalletIndex(uint256 tokenId, address wallet,` `address vestingManager)`
Vulnerabilities not detected

2.1 Structure of contract:

BaseRouter



pic.2.1 BaseRouter

2.2 BaseRouter contract methods analysis:

`constructor(address addressBook_)`
Vulnerabilities not detected

`nonces(address whose)`
Vulnerabilities not detected

`registerComplexOp(ComplexOp[] memory complexOps_)`
Vulnerabilities not detected

`setAddressBook(address addressBook_)`
Vulnerabilities not detected

`pause()`
Vulnerabilities not detected

`unpause()`
Vulnerabilities not detected

`start(`
`  string[] calldata operations,`
`  bytes[] memory params,`
`  IRouterParams.Invoice calldata receipt`
`)`

Vulnerabilities not detected

2.2 BaseRouter contract methods analysis:

```
_resume(
bytes32 requestId,
uint8 cPos,
string[] calldata operations,
bytes[] memory params
)
```

Vulnerabilities not detected

```
_execute(uint256 cPos, string[] calldata operations, bytes[]
memory params) internal virtual whenNotPaused returns (
bytes32 nextRequestId,
uint64 chainIdTo,
ExecutionResult result,
uint8 lastOp
)
```

Vulnerabilities not detected

```
_getAndUpdateNonce(address whose)
```

Vulnerabilities not detected

```
_checkSignature(
address from,
bytes32 operationHash,
bytes memory data,
IRouterParams.Invoice calldata receipt
)
```

Vulnerabilities not detected

2.2 BaseRouter contract methods analysis:

_getRawData(string[] calldata operations, bytes[] memory params)
Vulnerabilities not detected

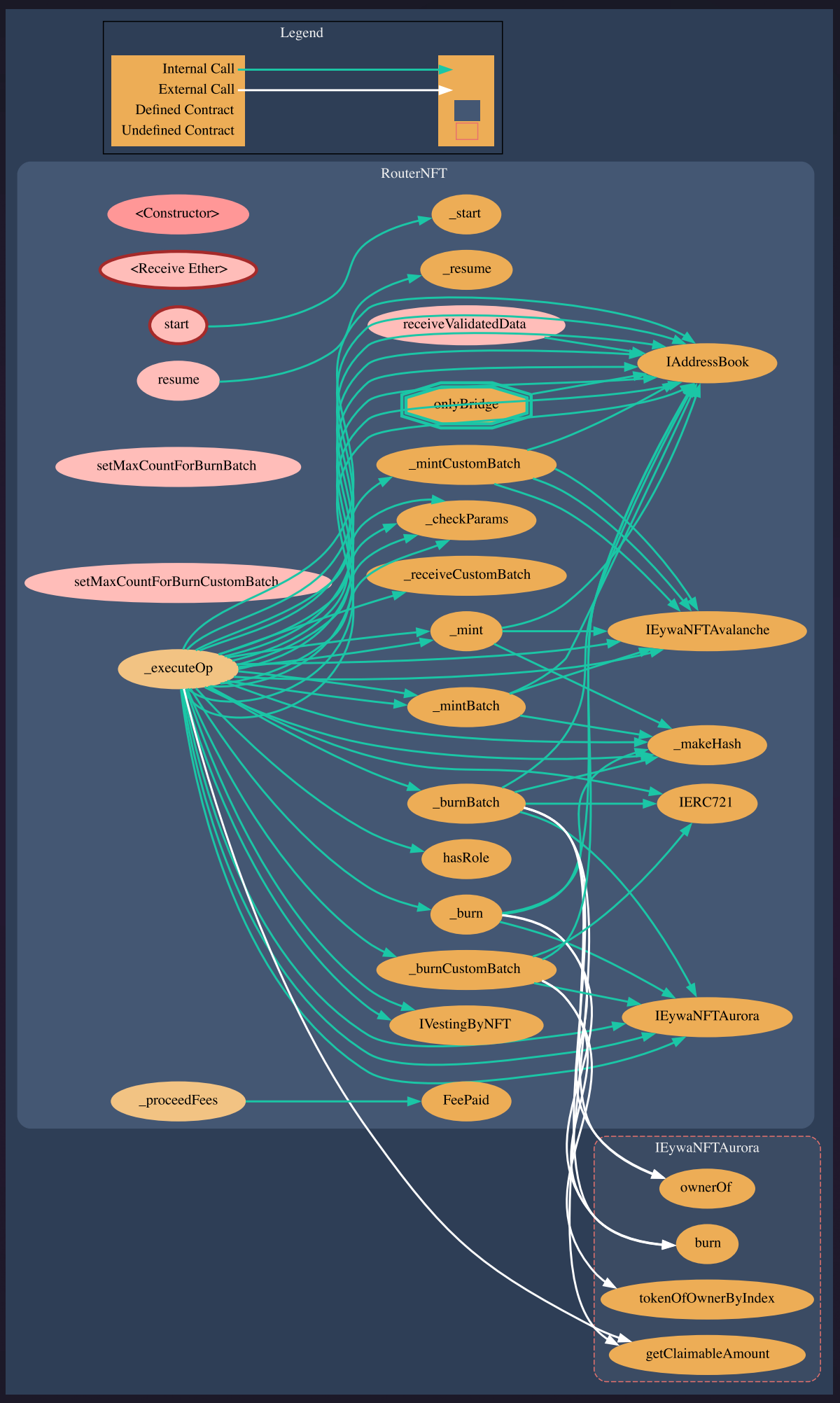
_getRequestId(address receiver, uint64 chainIdTo)
Vulnerabilities not detected

_proceedFees(uint256 executionPrice, address accountant)
Vulnerabilities not detected

_executeOp(bool isOpHalfDone, bytes32 op, bytes32 nextOp, bytes memory params, MaskedParams memory prevMaskedParams)
Vulnerabilities not detected

3.1 Structure of contract:

RouterNFT



pic.3.1 RouterNFT

3.2 RouterNFT contract methods analysis:

constructor(address addressBook_, uint64 chainIdTo_)
Vulnerabilities not detected

receiveValidatedData(bytes4 selector, address from, uint64 chainIdFrom)
Vulnerabilities not detected

start(string[] calldata operations, bytes[] memory params, Invoice calldata receipt)
Vulnerabilities not detected

resume(bytes32 requestId, uint8 cPos, string[] calldata operations, bytes[] memory params)
Vulnerabilities not detected

setMaxCountForBurnBatch(uint32 newMaxCountForBurnBatch)
Vulnerabilities not detected

setMaxCountForBurnCustomBatch(uint32 newMaxCountForBurnCustomBatch)
Vulnerabilities not detected

3.2 RouterNFT contract methods analysis:

`_executeOp(`
`bool isOpHalfDone,`
`bytes32 op,`
`bytes32 nextOp,`
`bytes memory params,`
`MaskedParams memory prevMaskedParams`
`)`

Vulnerabilities not detected

`_burn(NFTParams memory p)`
Vulnerabilities not detected

`_mint(NFTParams memory p)`
Vulnerabilities not detected

`_burnBatch(BatchParams memory p)`
Vulnerabilities not detected

`_mintBatch(BatchParams memory p)`
Vulnerabilities not detected

`_burnCustomBatch()`
Vulnerabilities not detected

`_mintCustomBatch(CustomBatchParams memory p)`
Vulnerabilities not detected

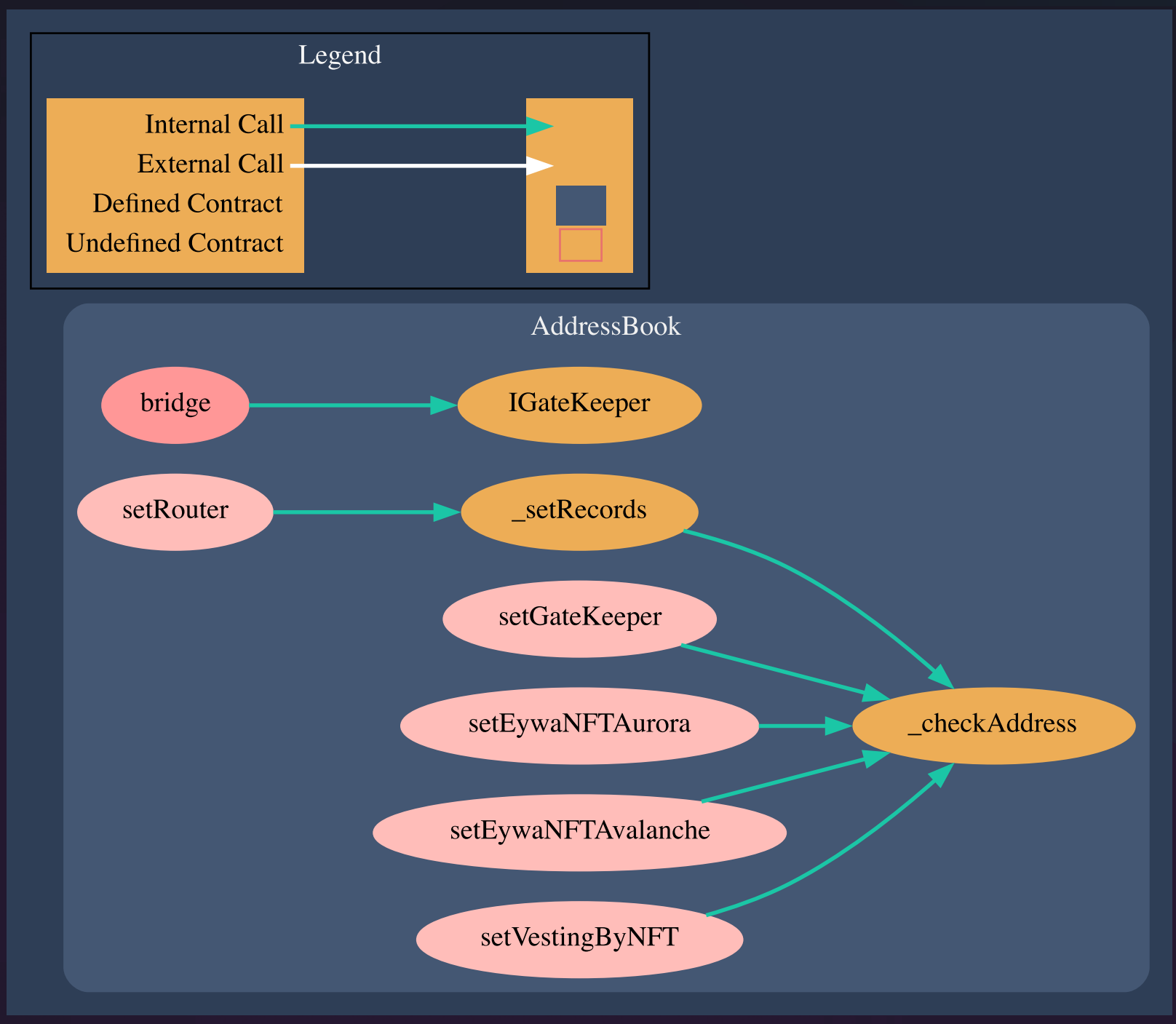
3.2 RouterNFT contract methods analysis:

_proceedFees(uint256 executionPrice, address accountant)
Vulnerabilities not detected

_checkParams(address from, address to, address emergencyTo)
Vulnerabilities not detected

4.1 Structure of contract:

AddressBook



pic.4.1 AddressBook

4.2 AddressBook contract methods analysis:

bridge()
Vulnerabilities not detected

setRouter(Record[] memory records)
Vulnerabilities not detected

setGateKeeper(address gateKeeper_)
Vulnerabilities not detected

setEywaNFTAurora(address eywaNFTAurora_)
Vulnerabilities not detected

setEywaNFTAvalanche(address eywaNFTAvalanche_)
Vulnerabilities not detected

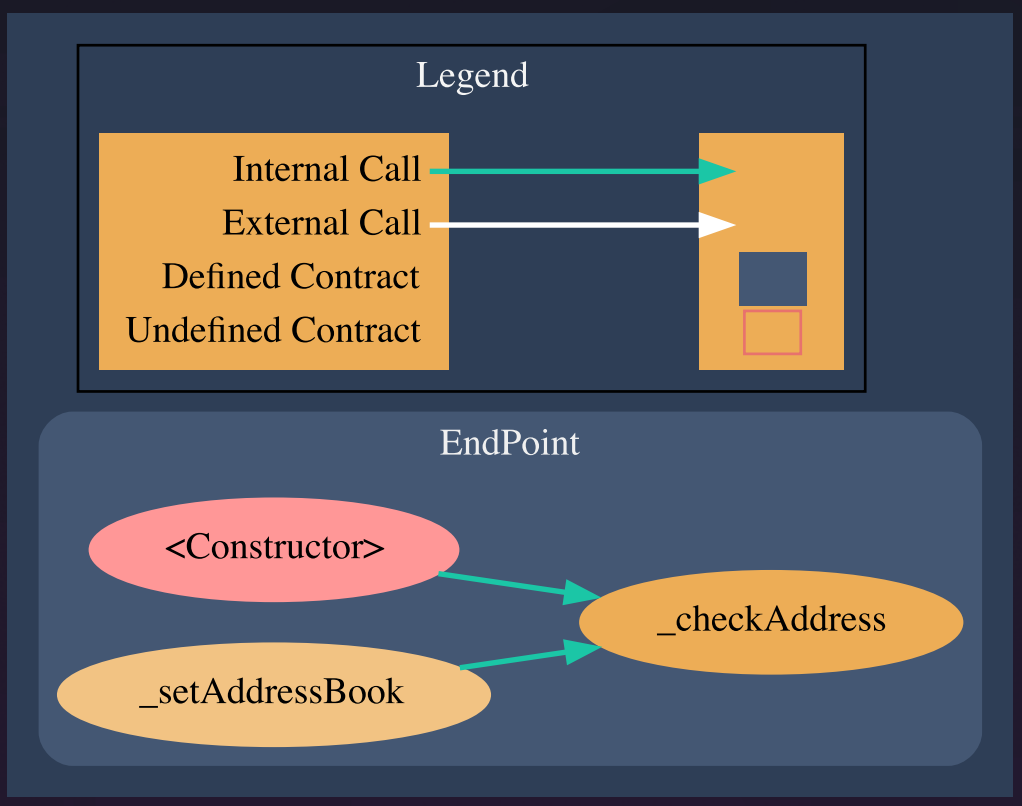
setVestingByNFT(address vestingManager_)
Vulnerabilities not detected

setRecords(mapping(uint64 => address) storage map, Record[] memory records)
Vulnerabilities not detected

_checkAddress(address checkingAddress)
Vulnerabilities not detected

5.1 Structure of contract:

EndPoint



pic.5.1 EndPoint

5.2 EndPoint contract methods analysis:

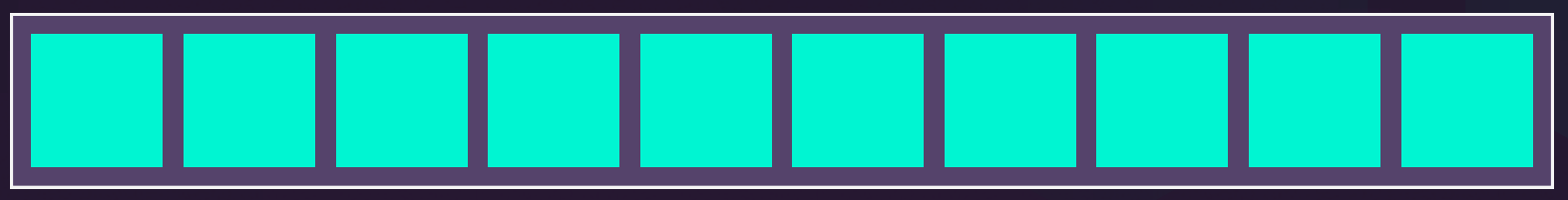
setAddressBook(address addressBook)
Vulnerabilities not detected

_checkAddress(address checkingAddress)
Vulnerabilities not detected

Verification checksums

Contract name	Bytecode hash(SHA-256)
EywaNFT	6046018975d39ac4c1b32113667853dad715509581b2947affed86a563deab07
BaseRouter	819ef80e5896bb174164adbebe8b5797d023c6f31c6a1338bcc83b66c9772bcc
RouterNFT	900489787c291330ef4797d15793ca5df33d4e9fafafe8c5859ffc830950f8ea
AddressBook	ea6d58a1aff60495be2c72354e024453253ddb6a62256245018c88bcc74f43bd
EndPoint	83164404b5037bed479b3175a71725665b5fb1c821308bb3a9ca432e5d536c9e

Project evaluation



10/10

Get in touch 👋

@smartstatetech

@smartstate

@SmartStateAudit

@smartstatetech

@smartstate.tech

View this report on Smartstate.tech

info@smartstate.tech

smartstate.tech