smart state

Web3 security easier than ever

EYWA

CLP

Smart contract audit report

December 22, 2023

Table of contents

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 EYWA CLP smart contracts, smart contracts for processing synth and burn operations, as well as mint and lock tokens. They are also responsible for swap processing and liquidity handling operations.

Disclaimer

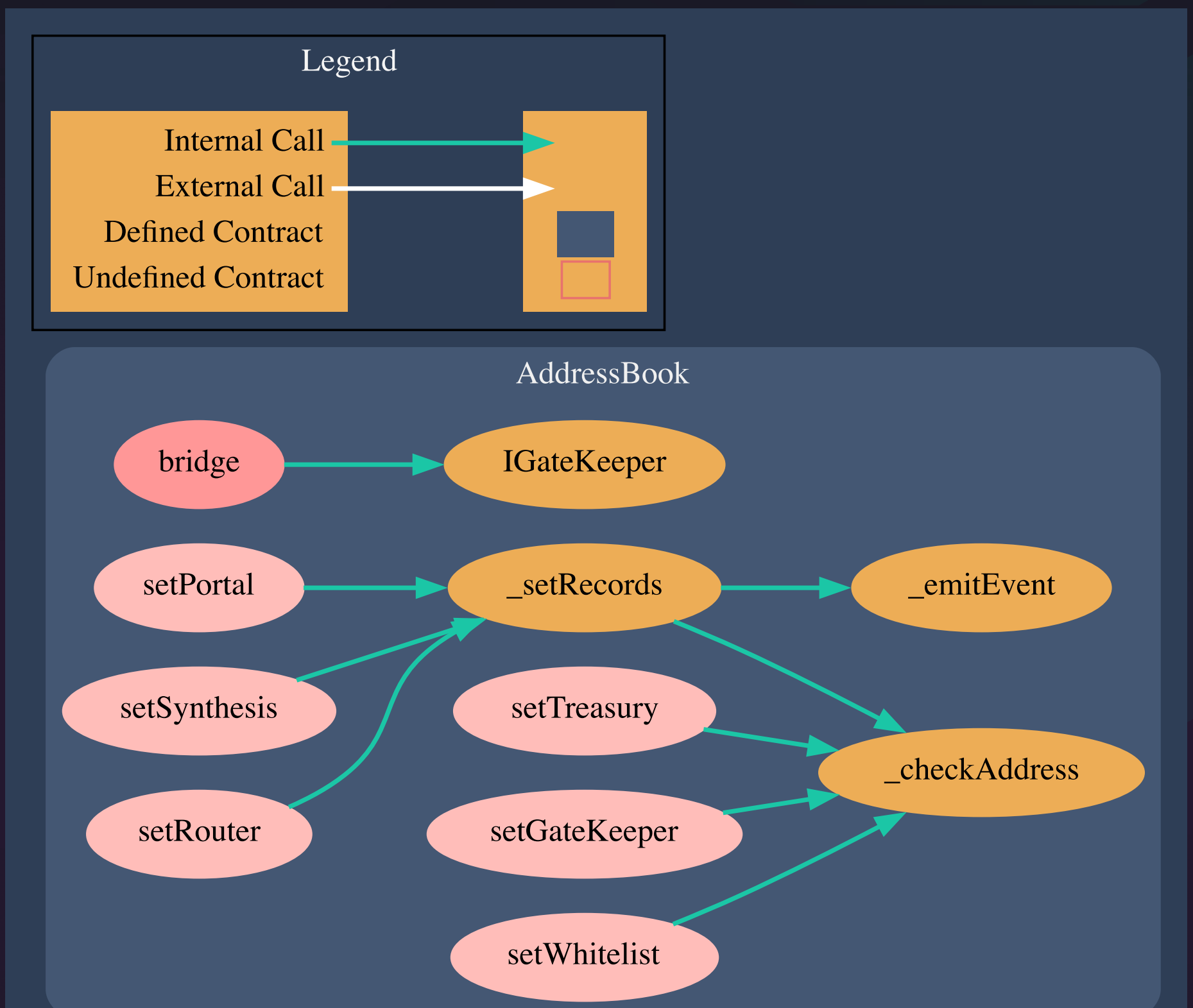
This is a final public security audit report version that doesn’t include vulnerabilities that had been found and fixed during the audit process.
An audit does not provide any warranties regarding the code security. We presume that a single audit cannot be considered totally sufficient and always recommend 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:

AddressBook



pic.1.1 AddressBook

1.2 AddressBook contract methods analysis:

bridge() returns(address)
Vulnerabilities not detected

setPortal(AddressBook.Record[]) returns()
Vulnerabilities not detected

setSynthesis(AddressBook.Record[]) returns()
Vulnerabilities not detected

setRouter(AddressBook.Record[]) returns()
Vulnerabilities not detected

setTreasury(address) returns()
Vulnerabilities not detected

setGateKeeper(address) returns()
Vulnerabilities not detected

setWhitelist(address) returns()
Vulnerabilities not detected

_setRecords(mapping(uint64 => address), AddressBook.Record[],AddressBook.RecordTypes) returns()
Vulnerabilities not detected

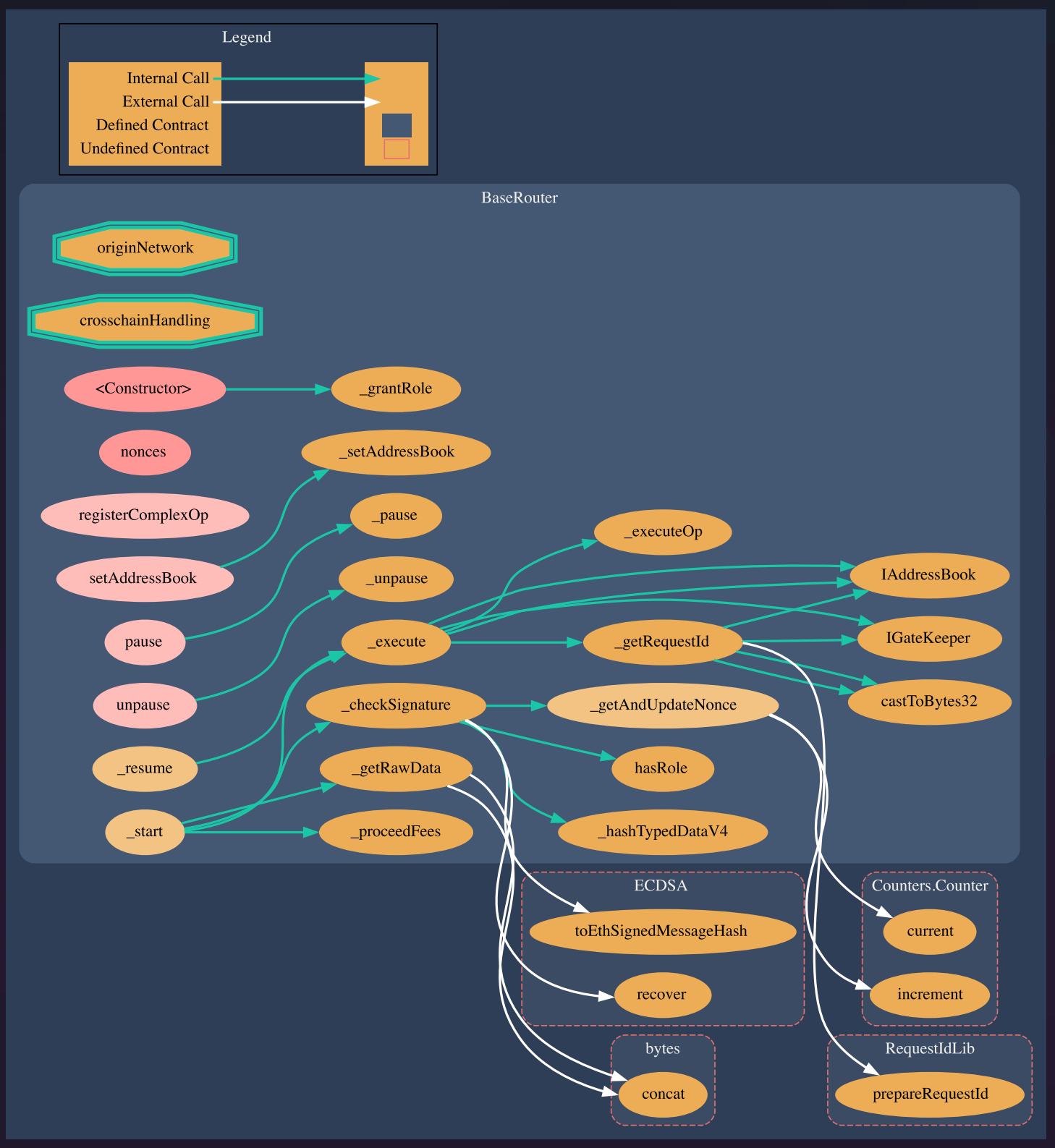
1.2 AddressBook contract methods analysis:

`_emitEvent(address,uint64,AddressBook.RecordTypes) returns()`
Vulnerabilities not detected

`_checkAddress(address) returns()`
Vulnerabilities not detected

2.1 Structure of contract:

BaseRouter



pic.2.1 BaseRouter

2.2 BaseRouter contract methods analysis:

constructor(address) returns()
Vulnerabilities not detected

nonces(address) returns(uint256)
Vulnerabilities not detected

registerComplexOp(BaseRouter.ComplexOp[]) returns()
Vulnerabilities not detected

setAddressBook(address) returns()
Vulnerabilities not detected

pause() returns()
Vulnerabilities not detected

unpause() returns()
Vulnerabilities not detected

_start(string[],bytes[],IRouterParams.Invoice) returns()
Vulnerabilities not detected

_resume(bytes32,uint8,string[],bytes[]) returns()
Vulnerabilities not detected

2.2 BaseRouter contract methods analysis:

_execute(uint256,string[],bytes[]) returns(bytes32,uint64,BaseRouter.ExecutionResult,uint8)
Vulnerabilities not detected

_getAndUpdateNonce(address) returns(uint256)
Vulnerabilities not detected

_checkSignature(address,bytes32,bytes,IRouterParams.Invoice) returns(address)
Vulnerabilities not detected

_getRawData(string[],bytes[]) returns(bytes32,bytes)
Vulnerabilities not detected

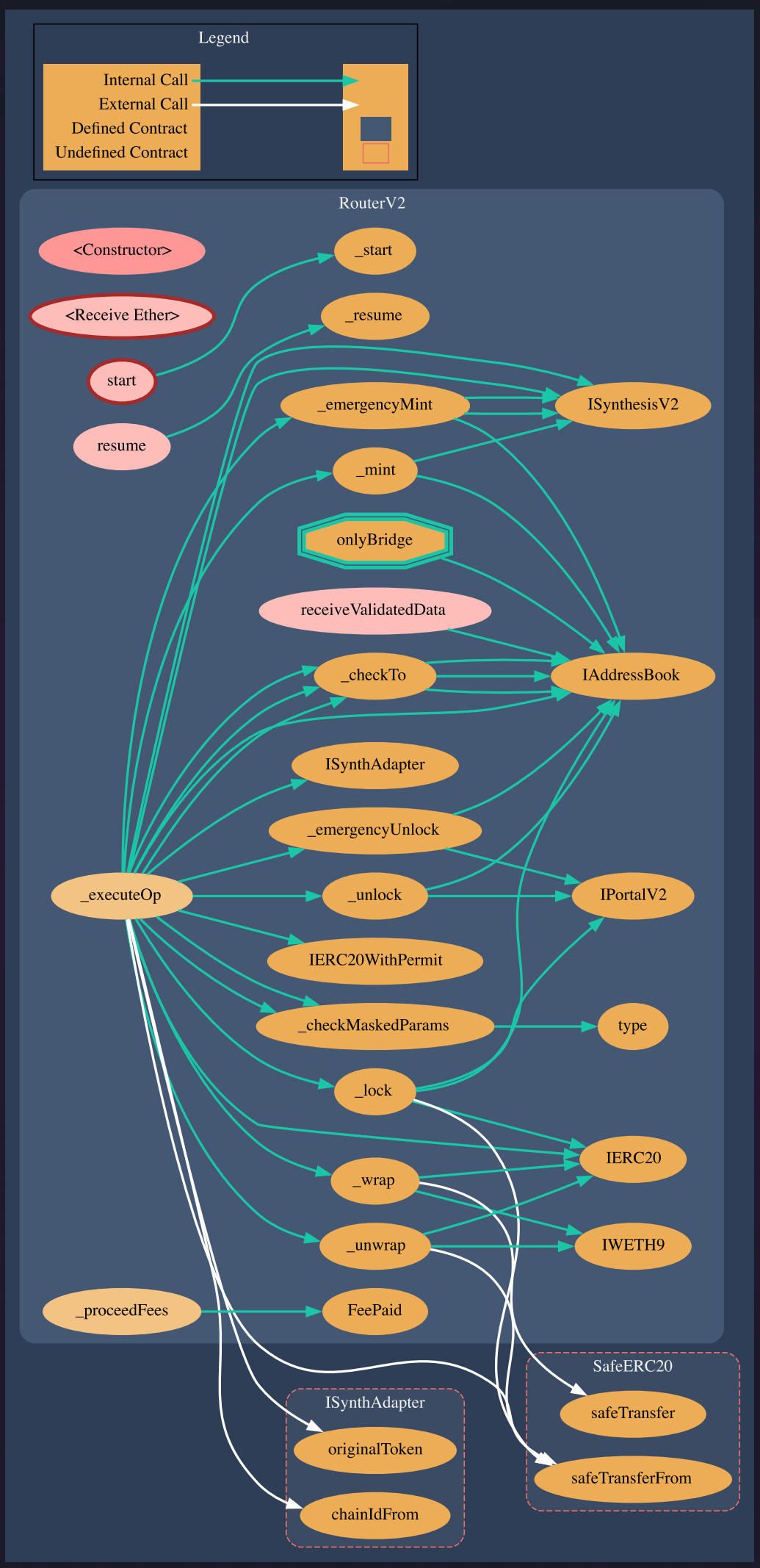
_getRequestId(address,uint64) returns(bytes32)
Vulnerabilities not detected

_proceedFees(uint256,address) returns()
Vulnerabilities not detected

_executeOp(bool,bytes32,bytes32,bytes, BaseRouter.MaskedParams) returns(uint64,bytes,BaseRouter.MaskedParams, BaseRouter.ExecutionResult)
Vulnerabilities not detected

3.1 Structure of contract:

RouterV2



pic.3.1 RouterV2

3.2 RouterV2 contract methods analysis:

constructor(address) returns()
Vulnerabilities not detected

receive() returns()
Vulnerabilities not detected

receiveValidatedData(bytes4,address,uint64) returns(bool)
Vulnerabilities not detected

start(string[],bytes[],IRouterParams.Invoice) returns()	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, public

resume(bytes32,uint8,string[],bytes[]) returns()
Vulnerabilities not detected

_executeOp(bool,bytes32,bytes32,bytes, BaseRouter.MaskedParams) returns(uint64,bytes, BaseRouter.MaskedParams,BaseRouter.ExecutionResult)
Vulnerabilities not detected

_lock(IRouterParams.SynthParams) returns()
Vulnerabilities not detected

_unlock(IRouterParams.SynthParams) returns(uint256)
Vulnerabilities not detected

3.2 RouterV2 contract methods analysis:

`_emergencyUnlock(IRouterParams.SynthParams) returns(uint256)`
Vulnerabilities not detected

`_mint(IRouterParams.SynthParams) returns(uint256)`
Vulnerabilities not detected

`_emergencyMint(IRouterParams.SynthParams) returns(uint256)`
Vulnerabilities not detected

`_wrap(IRouterParams.WrapParams) returns(uint256)`
Vulnerabilities not detected

`_unwrap(IRouterParams.WrapParams) returns(uint256)`
Vulnerabilities not detected

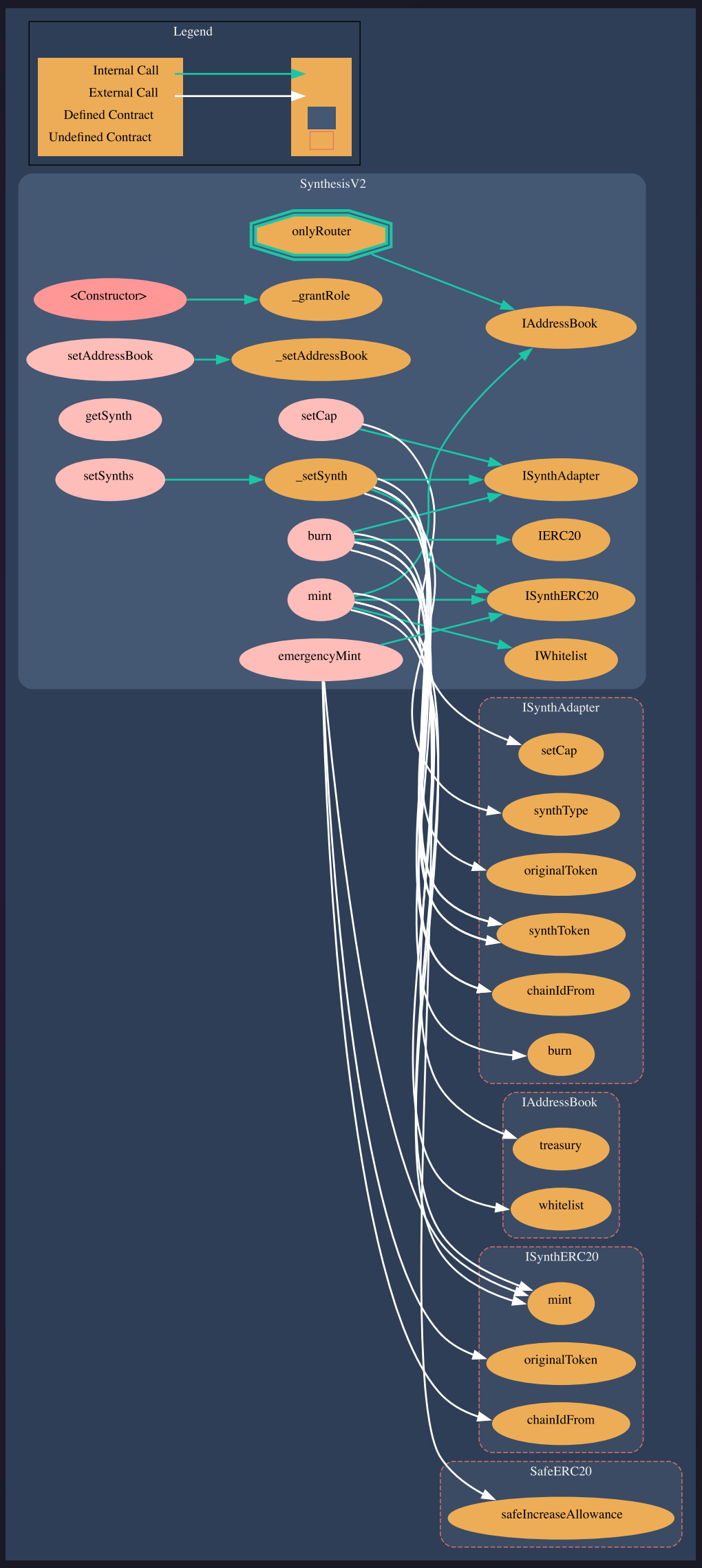
`_proceedFees(uint256,address) returns()`
Vulnerabilities not detected

`_checkMaskedParams(uint256,address,address,BaseRouter.MaskedParams) returns(uint256,address,address)`
Vulnerabilities not detected

`_checkTo(address,address,uint64,bytes32) returns(address)`
Vulnerabilities not detected

4.1 Structure of contract:

SynthesisV2



pic.4.1 SynthesisV2

4.2 SynthesisV2 contract methods analysis:

constructor(address) returns()
Vulnerabilities not detected

setAddressBook(address) returns()
Vulnerabilities not detected

setCap(address,uint256) returns()
Vulnerabilities not detected

getSynth(uint64,address) returns(address)
Vulnerabilities not detected

mint(address,uint256,address,address,uint64) returns(uint256)
Vulnerabilities not detected

emergencyMint(address,uint256,address,address) returns(uint256)
Vulnerabilities not detected

burn(address,uint256,address,address,uint64) returns()
Vulnerabilities not detected

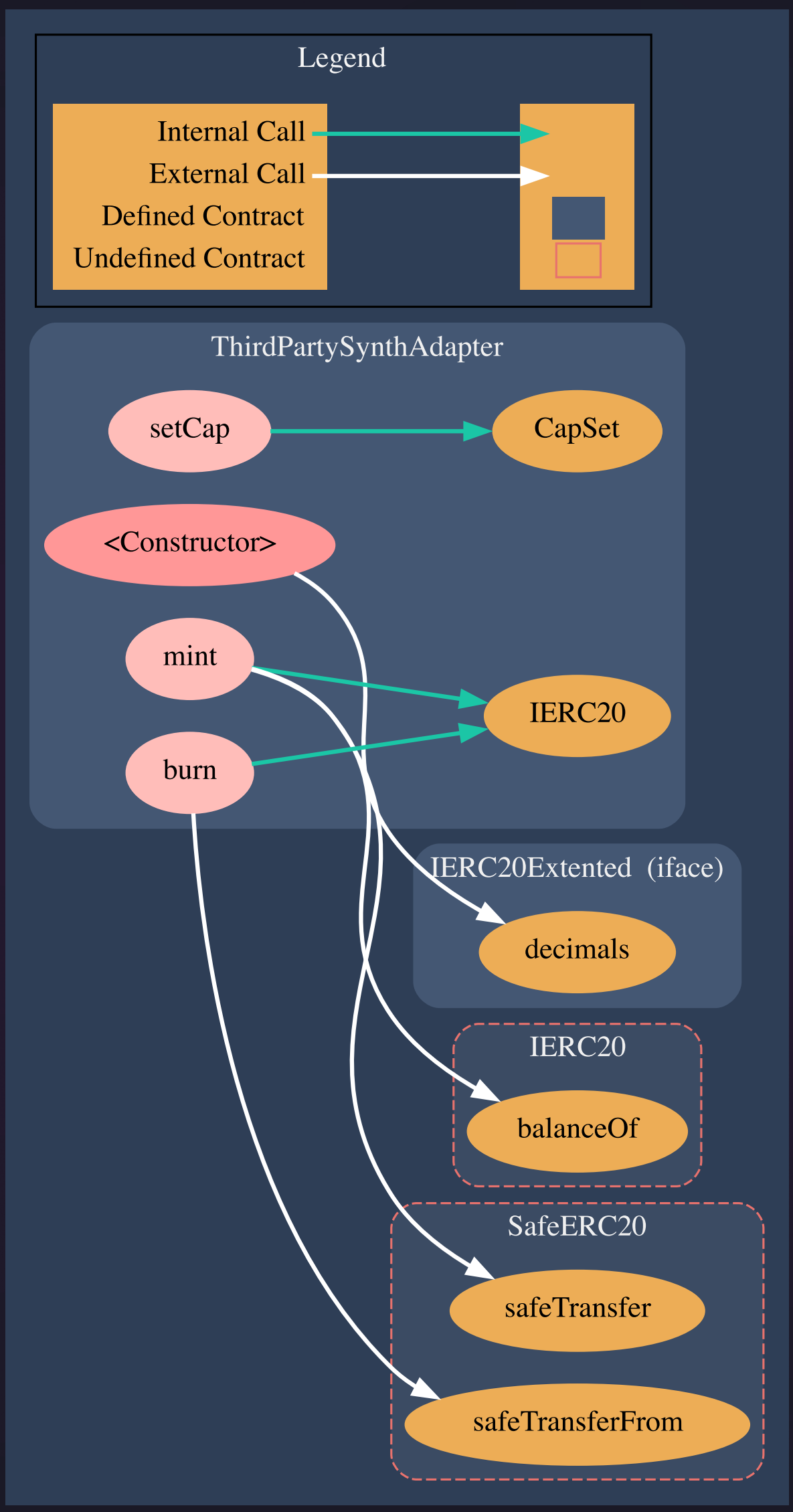
setSynths(address[]) returns()
Vulnerabilities not detected

4.2 SynthesisV2 contract methods analysis:

_setSynth(address) returns()
Vulnerabilities not detected

5.1 Structure of contract:

ThirdPartySynthAdapter



pic.5.1 ThirdPartySynthAdapter

5.2 ThirdPartySynthAdapter contract methods analysis:

constructor(address,address,uint64,string,uint8) returns()
Vulnerabilities not detected

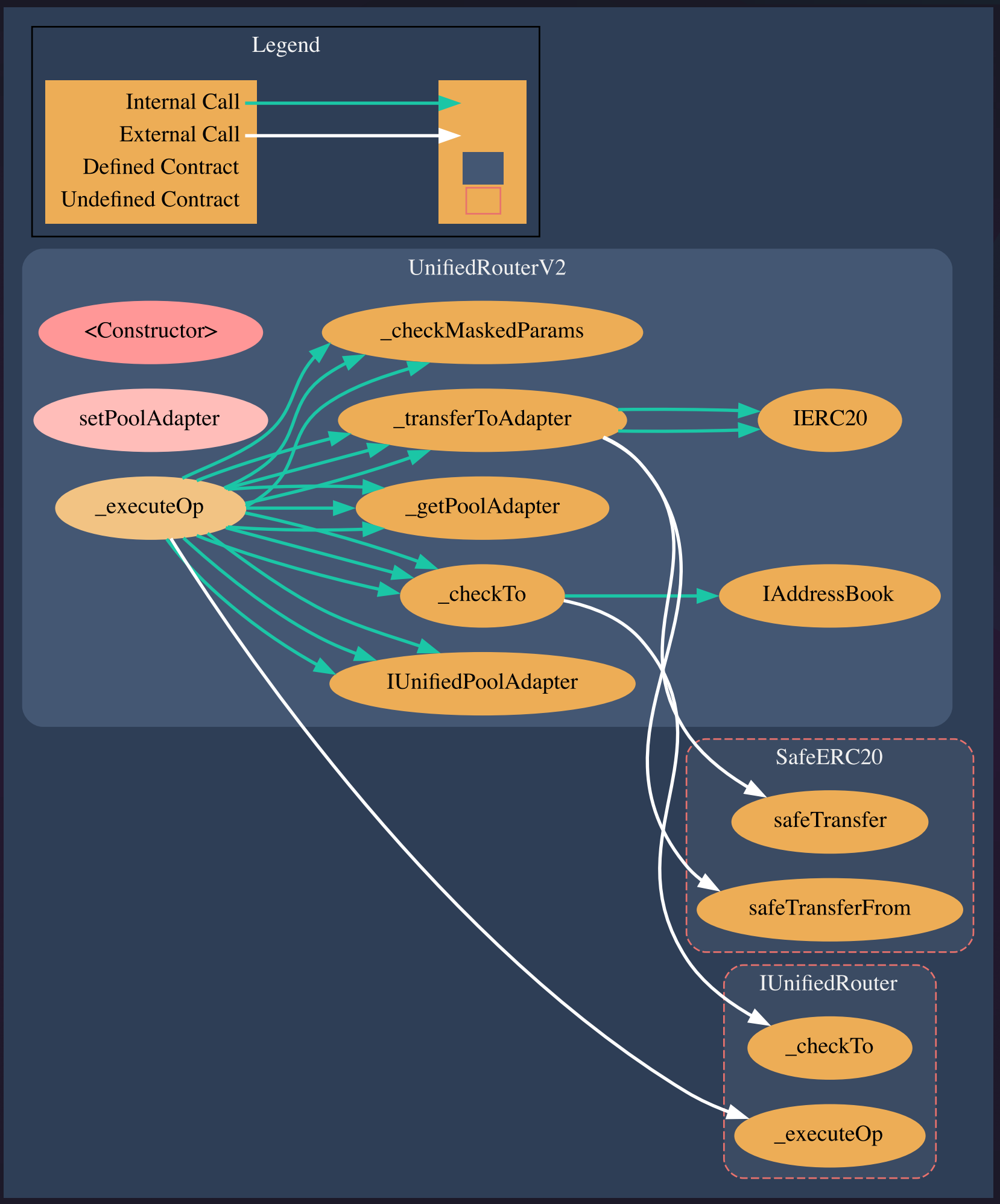
setCap(uint256) returns()
Vulnerabilities not detected

mint(address,uint256) returns()
Vulnerabilities not detected

burn(address,uint256) returns()
Vulnerabilities not detected

6.1 Structure of contract:

UnifiedRouterV2



pic.6.1 UnifiedRouterV2

6.2 UnifiedRouterV2 contract methods analysis:

constructor(address) returns()
Vulnerabilities not detected

setPoolAdapter(address,address) returns()
Vulnerabilities not detected

_executeOp(bool,bytes32,bytes32,bytes, BaseRouter.MaskedParams) returns(uint64,bytes,BaseRouter.MaskedParams, BaseRouter.ExecutionResult)
Vulnerabilities not detected

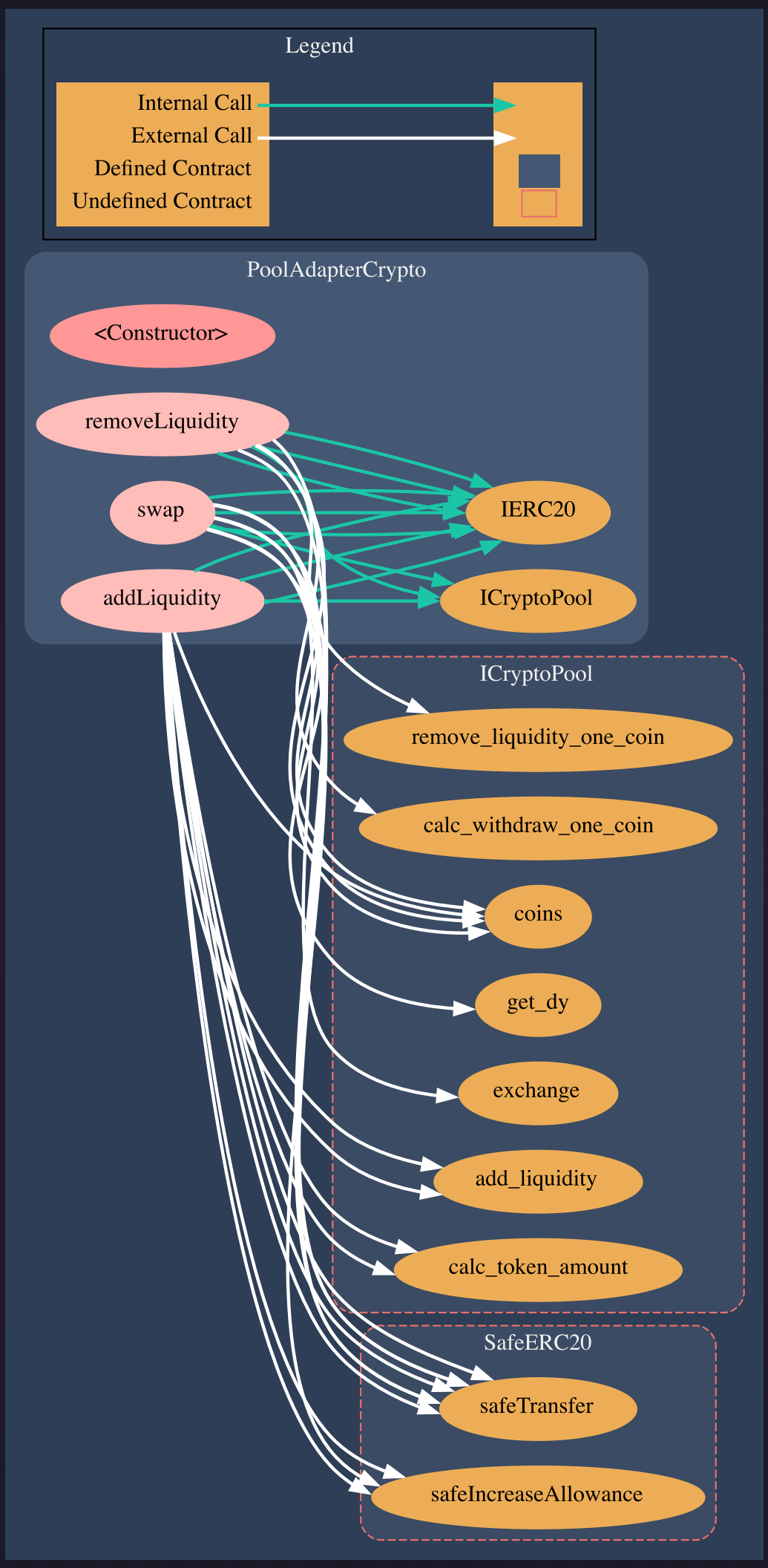
_checkTo(address,address,uint64,bytes32) returns(address)
Vulnerabilities not detected

_getPoolAdapter(address) returns(address)
Vulnerabilities not detected

_transferToAdapter(address,address,address,uint256) returns()
Vulnerabilities not detected

7.1 Structure of contract:

adapters/crypto1/PoolAdapterCrypto



pic.7.1 adapters/crypto1/PoolAdapterCrypto

7.2 adapters/crypto1/PoolAdapterCrypto contract methods analysis:

constructor(address,uint8) returns()
Vulnerabilities not detected

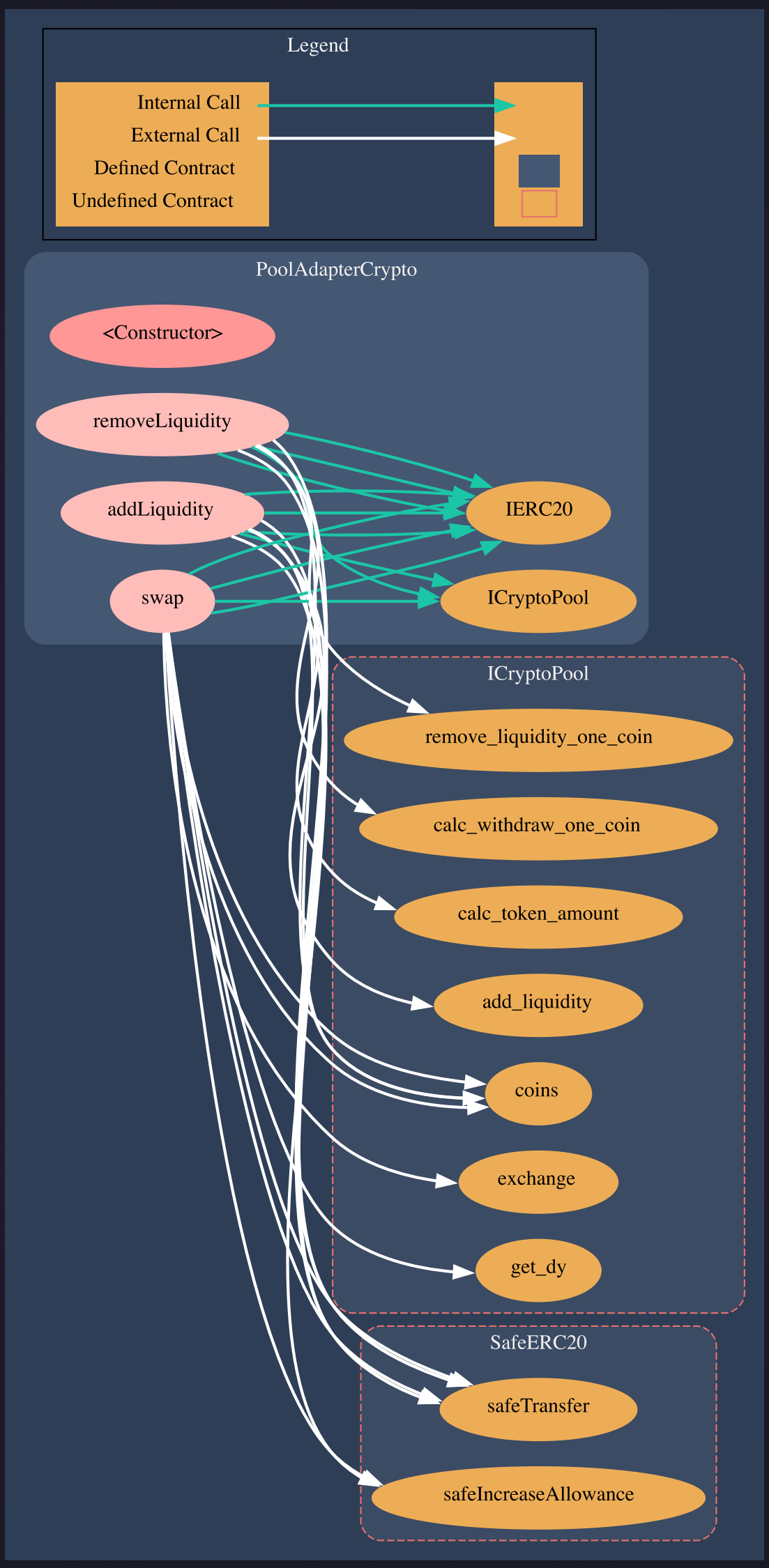
addLiquidity(address,uint256,address,address,uint256,uint8,address) returns(uint256)	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, tokens out, public

swap(address,uint256,address,address,uint256,uint8,uint8,address) returns(uint256)	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, tokens out, public

removeLiquidity(address,uint256,address,address,uint256,uint8,address) returns(uint256)	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, tokens out, public

8.1 Structure of contract:

adapters/crypto2/PoolAdapterCrypto



pic.8.1 adapters/crypto2/PoolAdapterCrypto

8.2 adapters/crypto2/PoolAdapterCrypto contract methods analysis:

constructor(address) returns()
Vulnerabilities not detected

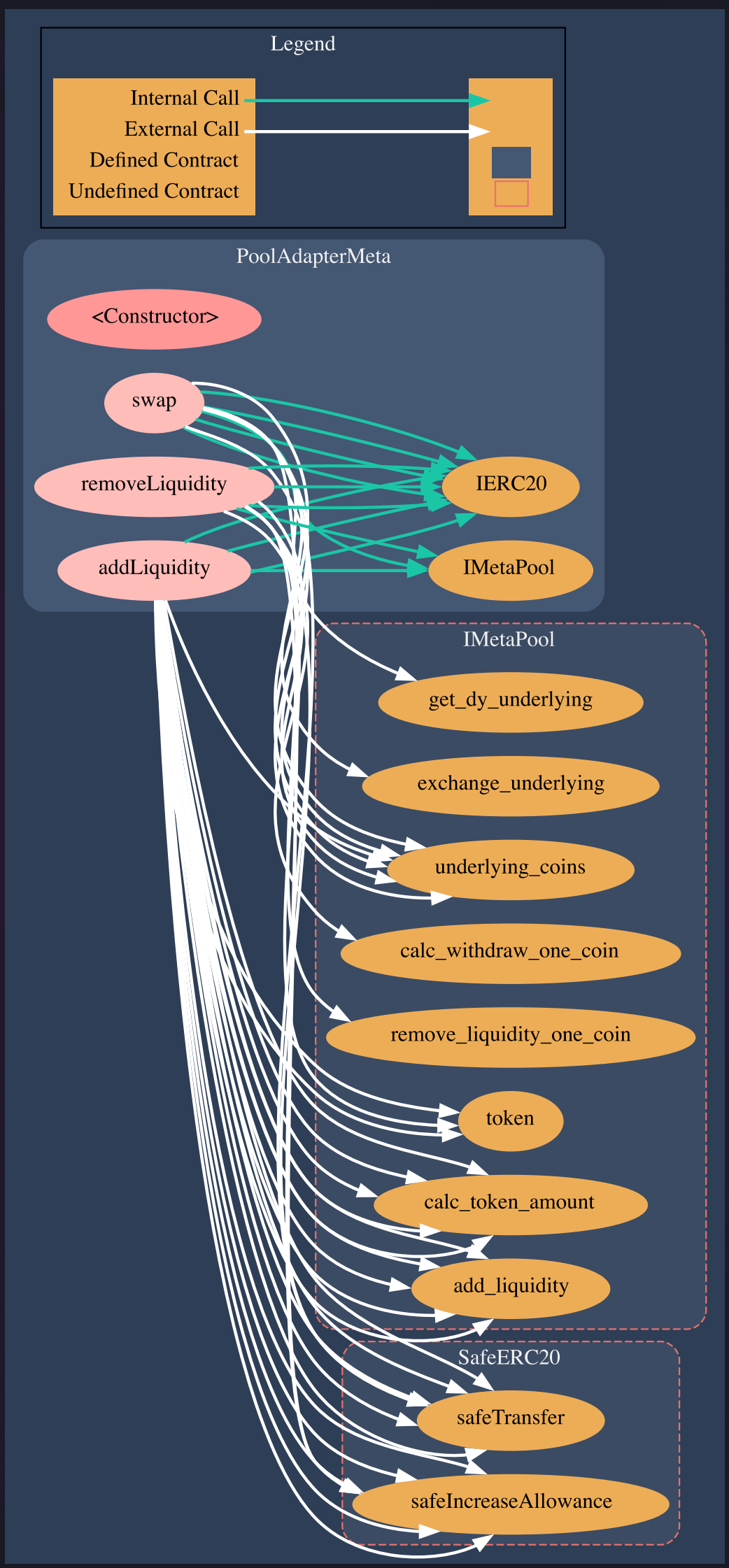
addLiquidity(address,uint256,address,address,uint256,uint8,address) returns(uint256)	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, tokens out, public

swap(address,uint256,address,address,uint256,uint8,uint8,address) returns(uint256)	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, tokens out, public

removeLiquidity(address,uint256,address,address,uint256,uint8,address) returns(uint256)	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, tokens out, public

9.1 Structure of contract:

adapters/meta1/PoolAdapterMeta



pic.9.1 adapters/meta1/PoolAdapterMeta

9.2 adapters/meta1/PoolAdapterMeta contract methods analysis:

constructor(uint8) returns()
Vulnerabilities not detected

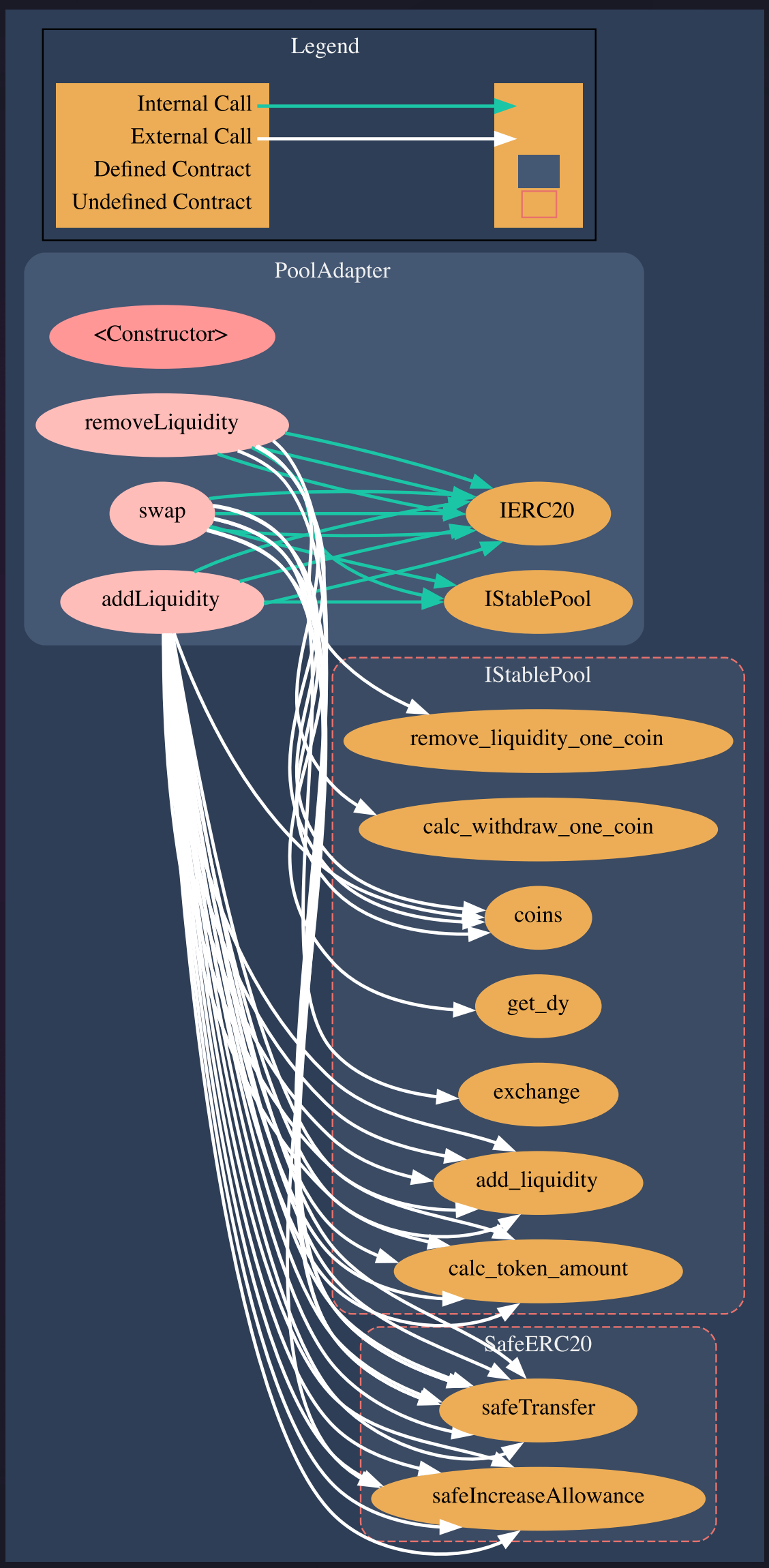
addLiquidity(address,uint256,address,address,uint256,uint8,address) returns(uint256)	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, tokens out, public

swap(address,uint256,address,address,uint256,uint8,uint8,address) returns(uint256)	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, tokens out, public

removeLiquidity(address,uint256,address,address,uint256,uint8,address) returns(uint256)	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, tokens out, public

10.1 Structure of contract:

adapters/stable1/PoolAdapter



pic.10.1 adapters/stable1/PoolAdapter

10.2 adapters/stable1/PoolAdapter contract methods analysis:

constructor(address, uint8) returns()
Vulnerabilities not detected

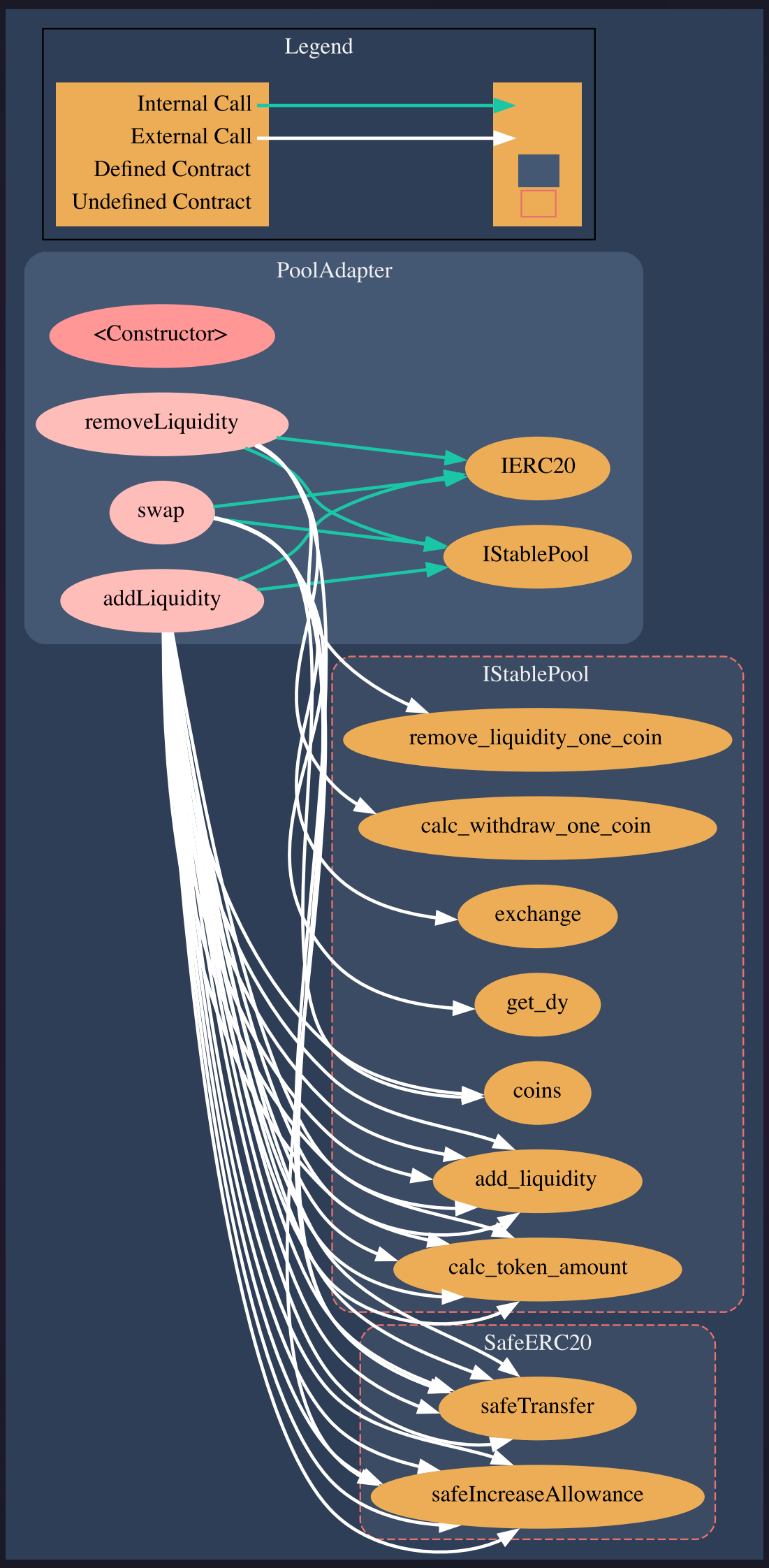
addLiquidity(address,uint256,address,address,uint256,uint8,address) returns(uint256)	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, tokens out, public

swap(address,uint256,address,address,uint256,uint8,uint8,address) returns(uint256)	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, tokens out, public

removeLiquidity(address,uint256,address,address,uint256,uint8,address) returns(uint256)	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, tokens out, public

11.1 Structure of contract:

adapters/stable2/PoolAdapter



pic.11.1 adapters/stable2/PoolAdapter

11.2 adapters/stable2/PoolAdapter contract methods analysis:

constructor(uint8) returns()	
Vulnerabilities not detected	

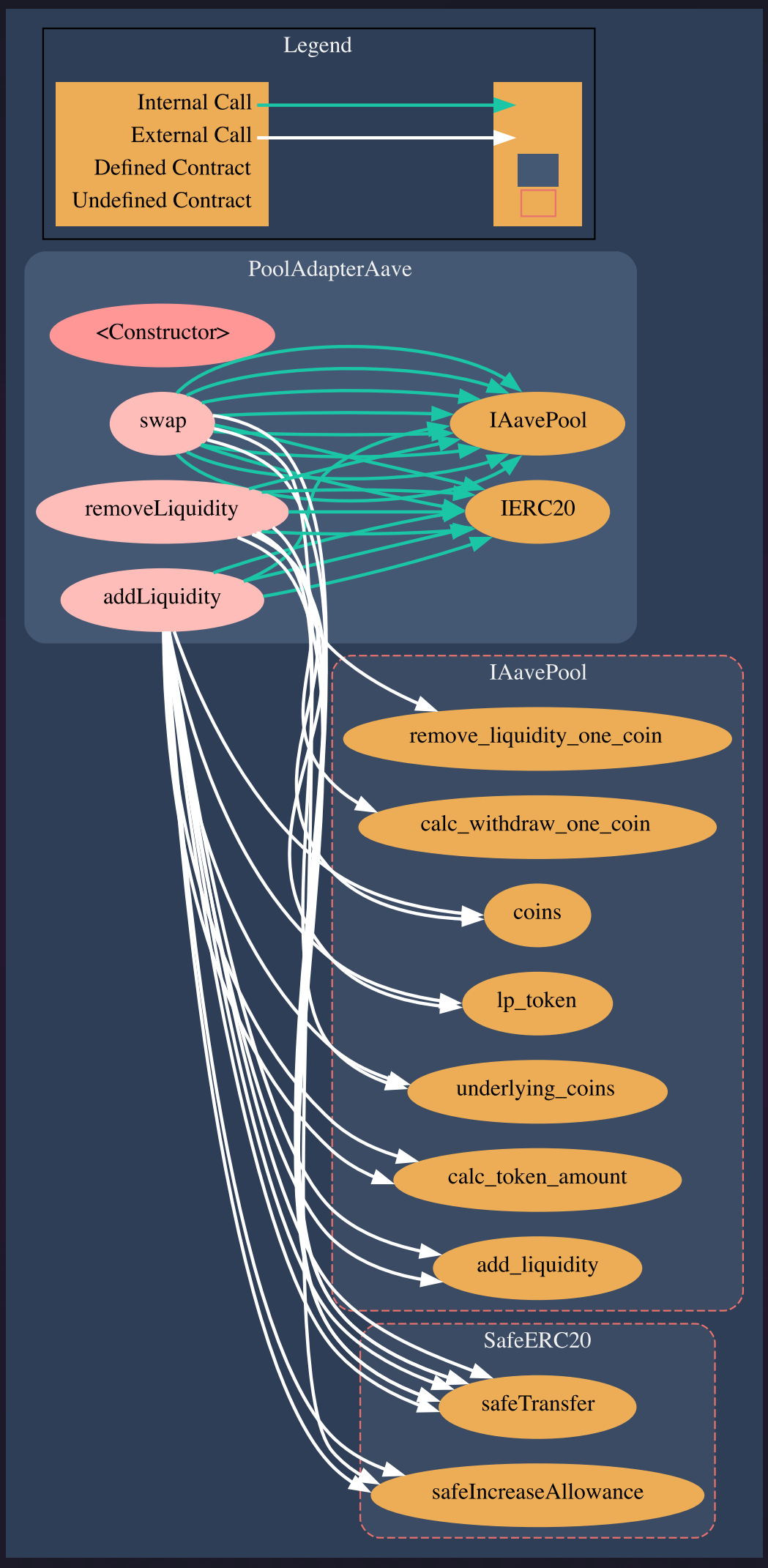
addLiquidity(address,uint256,address,address,uint256,uint8,address) returns(uint256)	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, tokens out, public

swap(address,uint256,address,address,uint256,uint8,uint8,address) returns(uint256)	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, tokens out, public

removeLiquidity(address,uint256,address,address,uint256,uint8,address) returns(uint256)	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, tokens out, public

12.1 Structure of contract:

adapters/stable3/PoolAdapterAave



pic.12.1 adapters/stable3/PoolAdapterAave

12.2 adapters/stable3/PoolAdapterAave contract methods analysis:

constructor(uint8) returns()
Vulnerabilities not detected

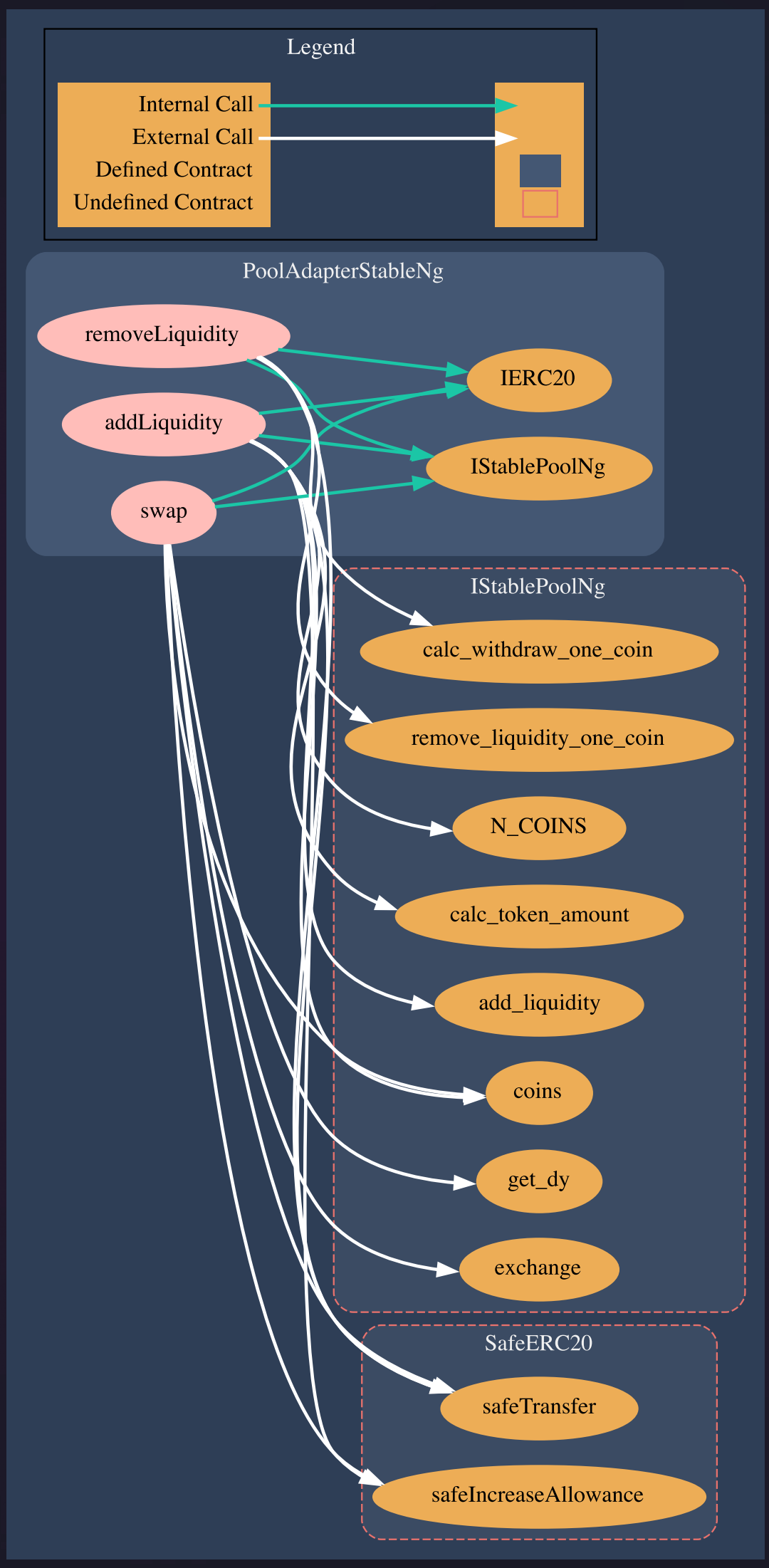
addLiquidity(address,uint256,address,address,uint256,uint8,address) returns(uint256)	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, tokens out, public

swap(address,uint256,address,address,uint256,uint8,uint8,address) returns(uint256)	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, tokens out, public

removeLiquidity(address,uint256,address,address,uint256,uint8,address) returns(uint256)	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, tokens out, public

13.1 Structure of contract:

adapters/stable4/PoolAdapterStableNg



pic.13.1 adapters/stable4/PoolAdapterStableNg

13.2 adapters/stable4/PoolAdapterStableNg contract methods analysis:

addLiquidity(address,uint256,address,address,uint256,uint8,address) returns(uint256)	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, tokens out, public

swap(address,uint256,address,address,uint256,uint8,uint8,address) returns(uint256)	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, tokens out, public

removeLiquidity(address,uint256,address,address,uint256,uint8,address) returns(uint256)	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in, tokens out, public

14.1 Structure of contract:

VirtualPriceReceiver

pic.14.1 VirtualPriceReceiver

14.2 VirtualPriceReceiver contract methods analysis:

constructor(address,uint64[],address[]) returns()
Vulnerabilities not detected

receiveValidatedData(bytes4,address,uint64) returns(bool)
Vulnerabilities not detected

setAddressBook(address) returns()
Vulnerabilities not detected

setVirtualPriceSender(uint64,address) returns()
Vulnerabilities not detected

receiveVirtualPrice(uint256,uint256,uint64) returns()
Vulnerabilities not detected

getVPStableEth() returns(uint256)
Vulnerabilities not detected

getVPStableArb() returns(uint256)
Vulnerabilities not detected

getVPStableBsc() returns(uint256)
Vulnerabilities not detected

14.2 VirtualPriceReceiver contract methods analysis:

getVPStablePol() returns(uint256)
Vulnerabilities not detected

getVPStableAvax() returns(uint256)
Vulnerabilities not detected

getVPStableOpt() returns(uint256)
Vulnerabilities not detected

getVPCryptoEth() returns(uint256)
Vulnerabilities not detected

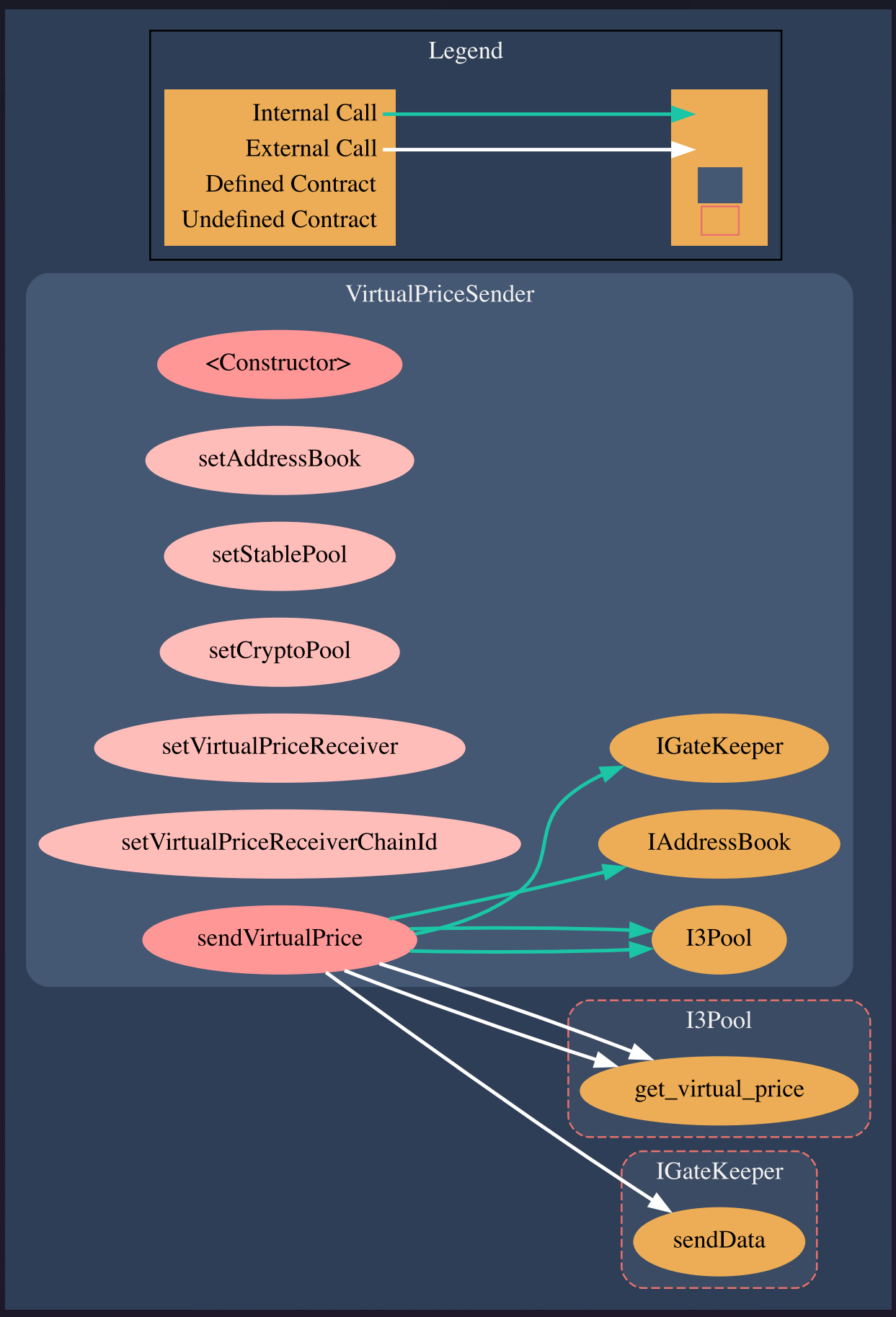
getVPCryptoArb() returns(uint256)
Vulnerabilities not detected

getVPCryptoPol() returns(uint256)
Vulnerabilities not detected

getVPCryptoAvax() returns(uint256)
Vulnerabilities not detected

15.1 Structure of contract:

VirtualPriceSender



pic.15.1 VirtualPriceSender

15.2 VirtualPriceSender contract methods analysis:

constructor(address,address,address,address,uint64) returns()
Vulnerabilities not detected

setAddressBook(address) returns()
Vulnerabilities not detected

setStablePool(address) returns()
Vulnerabilities not detected

setCryptoPool(address) returns()
Vulnerabilities not detected

setVirtualPriceReceiver(address) returns()
Vulnerabilities not detected

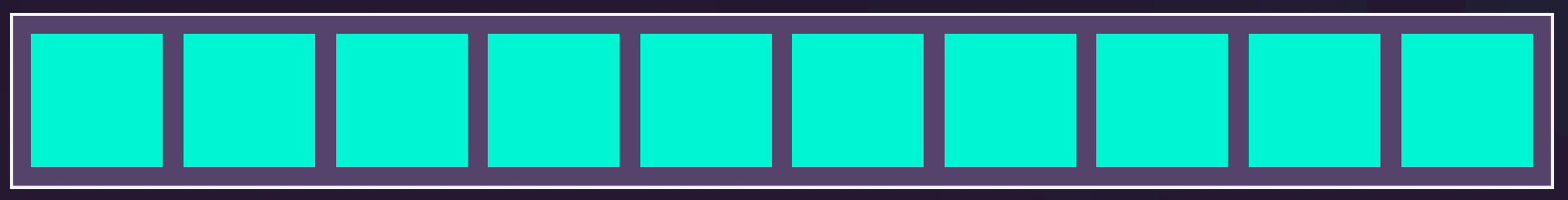
setVirtualPriceReceiverChainId(uint64) returns()
Vulnerabilities not detected

sendVirtualPrice() returns()
Vulnerabilities not detected

Verification checksums

Contract name	Bytecode hash(SHA-256)
AddressBook	a955ee64cd37eae0d3c591f94295f6d7b4196a40c8146587be6f1bf7f12799c4
BaseRouter	664c4db353f84c9a90b542256a7c8db877bb3478cbc770e9873b71f2a6e8c06c
RouterV2	5fd8da0024c3aeddc1296fb874a841b14605ea53b83cd663a7a2c91d9a91c63f
SynthesisV2	6bc455b00f144c85f6a9df9e1f38f7c7649366b058695e7cf34104d797d9357a
ThirdPartySynthAdapter	dd77a214bea69f01b8e8b66ad2e870d0d5a01394cb16275c6ea65bef407192df
UnifiedRouterV2	eb3f55b3387ca443707921256b7df8b5cbfcc36bbb1c23255648d479c486e9d0
adapters/crypto1/PoolAdapterCrypto	df41ba0aabb26afbc69640f2408f56c826582f1035f046c1c4fc3adcbc41ccd1
adapters/crypto2/PoolAdapterCrypto	336bca3de04f2e1ea6d98c9071ddfa9bb5b0b8aedf8eefaeaf093241210f6417
adapters/meta1/PoolAdapterMeta	fc6be076245427f968486e508453c20697f568594d726e588fd2391d4fb7446d
adapters/stable1/PoolAdapter	8403e0ce202bee95488ded4471e82d7125a2209b12e7355b0db2372c108fccae
adapters/stable2/PoolAdapter	71a17f1744c43501f859cc2747e41f98a8cd0d9b4a2df27420eb2852a1f75bc7
adapters/stable3/PoolAdapterAave	6708fe32370527b7d42c937950f8578eb4ff9eca691cfe2dd8ccabe3a508c20e
adapters/stable4/PoolAdapterStableNg	1901b527f0450a5f402d277b0c4e5a07e8282641c644b3f9b16946e59cef902d
VirtualPriceReceiver	192ebce5cd68a8b564339127587d88ac314784f1b3a099c53a35dea7a3a7742f
VirtualPriceSender	836c7fbb0508010477a8ce34cdcc353e81ab80e67b586195b10818a2afb5faa0

Project evaluation



10/10

Get in touch 👋

@smartstatetech

@smartstate

@SmartStateAudit

@smartstatetech

@smartstate.tech

View this report on Smartstate.tech

info@smartstate.tech

smartstate.tech