



CAIRO SECURITY  
CLAN

# ATOMIQ EXCHANGE - EVM

SECURITY ASSESMENT REPORT

JULY 2025

Prepared for  
ATOMIQ LABS



## Contents

<b>1</b>	<b>About Cairo Security Clan</b>	<b>2</b>
<b>2</b>	<b>Disclaimer</b>	<b>2</b>
<b>3</b>	<b>Executive Summary</b>	<b>3</b>
<b>4</b>	<b>Summary of Audit</b>	<b>4</b>
4.1	Scoped Files	4
4.2	Issues	4
<b>5</b>	<b>Risk Classification</b>	<b>5</b>
<b>6</b>	<b>Issues by Severity Levels</b>	<b>6</b>
6.1	High	6
6.1.1	Front-running issue in <code>ExecutionContract.create()</code> allows blocking of legitimate <code>SpvSwapVault</code> transactions	6
6.2	Medium	7
6.2.1	Success action execution failures do not revert the claim transaction	7
6.2.2	Attacker can intentionally limit gas to sabotage the success action execution	9
6.3	Informational	10
6.3.1	Claimer cannot initialize escrow with native ETH	10
6.4	Best Practices	11
6.4.1	Misleading parameter name <code>src</code> in <code>_payOut()</code> function	11
6.4.2	Deposit function should use safe arithmetic operations like <code>withdraw</code> function	11
<b>7</b>	<b>Test Compilation Evaluation</b>	<b>12</b>
7.1	Compilation Output	12
7.2	Tests Output	13



# 1 About Cairo Security Clan

Cairo Security Clan is a leading force in the realm of blockchain security, dedicated to fortifying the foundations of the digital age. As pioneers in the field, we specialize in conducting meticulous smart contract security audits, ensuring the integrity and reliability of decentralized applications built on blockchain technology.

At Cairo Security Clan, we boast a multidisciplinary team of seasoned professionals proficient in blockchain security, cryptography, and software engineering. With a firm commitment to excellence, our experts delve into every aspect of the Web3 ecosystem, from foundational layer protocols to application-layer development. Our comprehensive suite of services encompasses smart contract audits, formal verification, and real-time monitoring, offering unparalleled protection against potential vulnerabilities.

Our team comprises industry veterans and scholars with extensive academic backgrounds and practical experience. Armed with advanced methodologies and cutting-edge tools, we scrutinize and analyze complex smart contracts with precision and rigor. Our track record speaks volumes, with a plethora of published research papers and citations, demonstrating our unwavering dedication to advancing the field of blockchain security.

At Cairo Security Clan, we prioritize collaboration and transparency, fostering meaningful partnerships with our clients. We believe in a customer-oriented approach, engaging stakeholders at every stage of the auditing process. By maintaining open lines of communication and soliciting client feedback, we ensure that our solutions are tailored to meet the unique needs and objectives of each project.

Beyond our core services, Cairo Security Clan is committed to driving innovation and shaping the future of blockchain technology. As active contributors to the ecosystem, we participate in the development of emerging technologies such as Starknet, leveraging our expertise to build robust infrastructure and tools. Through strategic guidance and support, we empower our partners to navigate the complexities of the blockchain landscape with confidence and clarity.

In summary, Cairo Security Clan stands at the forefront of blockchain security, blending technical prowess with a client-centric ethos to deliver unparalleled protection and peace of mind in an ever-evolving digital landscape. Join us in safeguarding the future of decentralized finance and digital assets with confidence and conviction.

# 2 Disclaimer

Disclaimer Limitations of this Audit:

This report is based solely on the materials and documentation provided by you to Cairo Security Clan for the specific purpose of conducting the security review outlined in the [Summary of Audit](#) and [Scoped Files](#). The findings presented here may not be exhaustive and may not identify all potential vulnerabilities. Cairo Security Clan provides this review and report on an "as-is" and "as-available" basis. You acknowledge that your use of this report, including any associated services, products, protocols, platforms, content, and materials, occurs entirely at your own risk.

Inherent Risks of Blockchain Technology:

Blockchain technology remains in its developmental stage and is inherently susceptible to unknown risks and vulnerabilities. This review is specifically focused on the smart contract code and does not extend to the compiler layer, programming language elements beyond the reviewed code, or other potential security risks outside the code itself.

Report Purpose and Reliance:

This report should not be construed as an endorsement of any specific project or team, nor does it guarantee the absolute security of the audited smart contracts. No third party should rely on this report for any purpose, including making investment or purchasing decisions.

Liability Disclaimer:

To the fullest extent permitted by law, Cairo Security Clan disclaims all liability associated with this report, its contents, and any related services and products arising from your use. This includes, but is not limited to, implied warranties of merchantability, fitness for a particular purpose, and non-infringement.

Third-Party Products and Services:

Cairo Security Clan does not warrant, endorse, guarantee, or assume responsibility for any products or services advertised by third parties within this report, nor for any open-source or third-party software, code, libraries, materials, or information linked to, referenced by, or accessible through this report, its content, and related services and products. This includes any hyperlinked websites, websites or applications appearing on advertisements, and Cairo Security Clan will not be responsible for monitoring any transactions between you and third-party providers. It is recommended that you exercise due diligence and caution when considering any third-party products or services, just as you would with any purchase or service through any medium.

Disclaimer of Advice:

FOR THE AVOIDANCE OF DOUBT, THIS REPORT, ITS CONTENT, ACCESS, AND/OR USE, INCLUDING ANY ASSOCIATED SERVICES OR MATERIALS, SHOULD NOT BE CONSIDERED OR RELIED UPON AS FINANCIAL, INVESTMENT, TAX, LEGAL, REGULATORY, OR OTHER PROFESSIONAL ADVICE.



### 3 Executive Summary

This document presents the security review performed by [Cairo Security Clan](#) on the [Atomiq Exchange](#).

atomiq.exchange is a fully trustless cross-chain decentralized exchange (DEX) allowing you to swap between smart chains and Bitcoin, without having to trust any intermediary in the process.

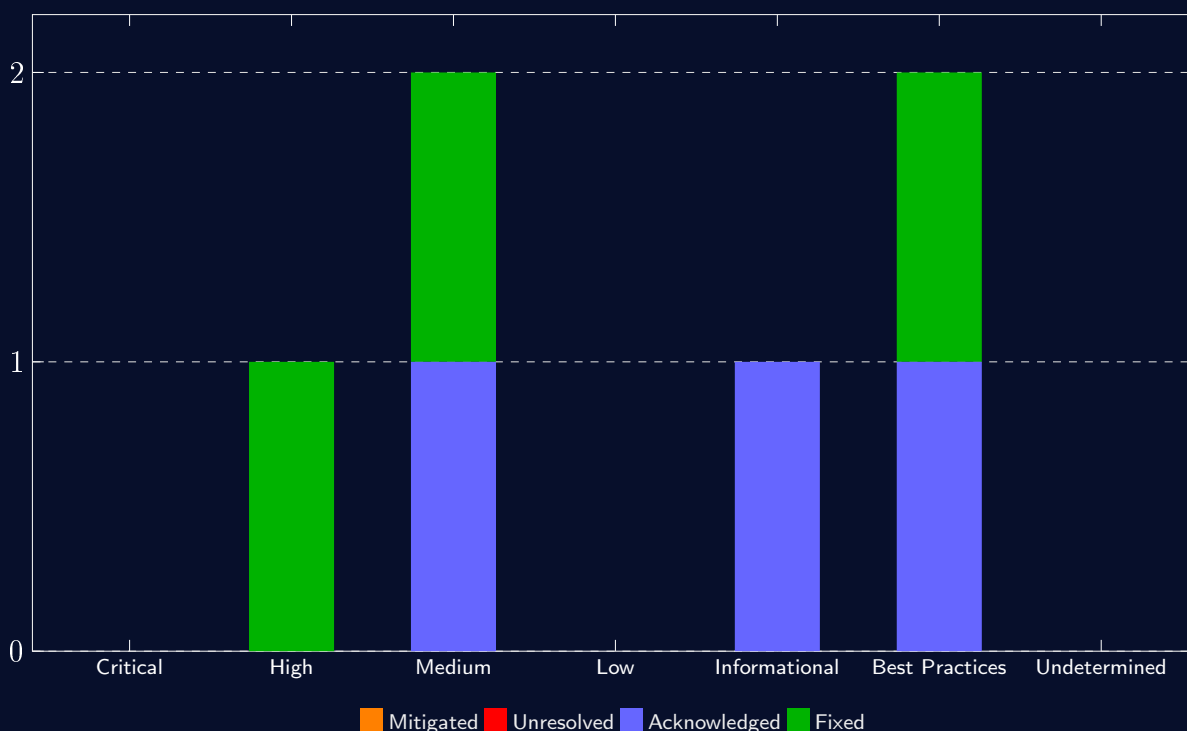
All transactions are processed atomically with strong security guarantees based on bitcoin light client (leveraging bitcoin's proof-of-work security) & submarine swaps (leveraging HTLCs - hash-time locked contracts over bitcoin's lightning network). With this approach atomiq.exchange is able to offer security guarantees far exceeding those of existing bridging or cross-chain swapping solutions. Learn more from [docs](#) and [FAQ](#).

#### The audit was performed using

- manual analysis of the codebase,
- automated analysis tools,
- simulation of the smart contract,
- analysis of edge test cases

There are 6 points of attention, where 0 are classified as Critical, 1 as High, 2 as Medium, 0 as Low, 1 as Informational, 2 as Best Practices, and 0 as Undetermined. The issues are summarized in Fig. 1.

**This document is organized as follows.** Section 1 About Cairo Security Clan. Section 2 Disclaimer. Section 3 Executive Summary. Section 4 Summary of Audit. Section 5 Risk Classification. Section 6 Issues by Severity Levels. Section 7 Test Evaluation.



**Fig 1: Distribution of issues:** Critical (0), High (1), Medium (2), Low (0), Informational (1), Best Practices (2), Undetermined (0).  
**Distribution of status:** Fixed (3), Acknowledged (3), Mitigated (0), Unresolved (0).



## 4 Summary of Audit

<b>Audit Type</b>	Security Review
<b>Solidity Version</b>	0.8.28
<b>Final Report</b>	25/07/2025
<b>Repository</b>	atomiqlabs/atomiq-contracts-evm
<b>Initial Commit Hash</b>	d4e5f456d84a6eb1817df4a313c3c5264224e2f0
<b>Final Commit Hash</b>	e416d55e713c9e9da2daafe77e99df83b7c08f36
<b>Documentation</b>	Website documentation
<b>Test Suite Assessment</b>	High

### 4.1 Scoped Files

	Contracts
1	contracts/btc_nonced_output_claim_handler/BitcoinNoncedOutputClaimHandler.sol
2	contracts/btc_output_claim_handler/BitcoinOutputClaimHandler.sol
3	contracts/btc_relay/state/BtcRelayState.sol
4	contracts/btc_relay/structs/CompactBlockHeader.sol
5	contracts/btc_relay/structs/StoredBlockHeader.sol
6	contracts/btc_relay/structs/Difficulty.sol
7	contracts/btc_relay/structs/Nbits.sol
8	contracts/btc_relay/BtcRelay.sol
9	contracts/btc_relay/Constants.sol
10	contracts/btc_relay/Events.sol
11	contracts/btc_txid_claim_handler/BitcoinTxIdClaimHandler.sol
12	contracts/btc_utils/BitcoinMerkleTree.sol
13	contracts/btc_utils/BitcoinTx.sol
14	contracts/btc_utils/Endianness.sol
15	contracts/common/IClaimHandler.sol
16	contracts/common/IRefundHandler.sol
17	contracts/escrow_manager/components/EIP712Sighash.sol
18	contracts/escrow_manager/components/EscrowStorage.sol
19	contracts/escrow_manager/components/LpVault.sol
20	contracts/escrow_manager/components/ReputationTracker.sol
21	contracts/escrow_manager/state/EscrowState.sol
22	contracts/escrow_manager/state/ReputationState.sol
23	contracts/escrow_manager/structs/Escrow.sol
24	contracts/escrow_manager/EscrowManager.sol
25	contracts/escrow_manager/Events.sol
26	contracts/execution_contract/structs/Execution.sol
27	contracts/execution_contract/Events.sol
28	contracts/execution_contract/ExecutionContract.sol
29	contracts/execution_proxy/structs/ContractCall.sol
30	contracts/execution_proxy/structs/ExecutionAction.sol
31	contracts/execution_proxy/ExecutionProxy.sol
32	contracts/execution_proxy/Executor.sol
33	contracts/hashlock_claim_handler/HashlockClaimHandler.sol
34	contracts/spv_swap_vault/state/SpvVaultState.sol
35	contracts/spv_swap_vault/structs/BitcoinVaultTransactionData.sol
36	contracts/spv_swap_vault/structs/SpvVaultParameters.sol
37	contracts/spv_swap_vault/Events.sol
38	contracts/spv_swap_vault/SpvVaultManager.sol
39	contracts/spv_swap_vault/Utils.sol
40	contracts/timelock_refund_handler/TimelockRefundHandler.sol
41	contracts/transfer_utils/TransferUtils.sol
42	contracts/structs/MathUtils.sol

### 4.2 Issues

	Findings	Severity	Update
1	Front-running issue in ExecutionContract.create() allows blocking of legitimate SpvSwapVault transactions	High	Fixed
2	Success action execution failures do not revert the claim transaction	Medium	Acknowledged
3	Attacker can intentionally limit gas to sabotage the success action execution	Medium	Fixed
4	Claimer cannot initialize escrow with native ETH	Informational	Acknowledged
5	Misleading parameter name src in _payOut() function	Best Practices	Fixed
6	Deposit function should use safe arithmetic operations like withdraw function	Best Practices	Acknowledged



## 5 Risk Classification

The risk rating methodology used by **Cairo Security Clan** follows the principles established by the **CVSS risk rating methodology**. The severity of each finding is determined by two factors: **Likelihood** and **Impact**.

**Likelihood** measures how likely an attacker will uncover and exploit the finding. This factor will be one of the following values:

- a) **High**: The issue is trivial to exploit and has no specific conditions that need to be met;
- b) **Medium**: The issue is moderately complex and may have some conditions that need to be met;
- c) **Low**: The issue is very complex and requires very specific conditions to be met.

When defining the likelihood of a finding, other factors are also considered. These can include but are not limited to Motive, opportunity, exploit accessibility, ease of discovery, and ease of exploit.

**Impact** is a measure of the damage that may be caused if an attacker exploits the finding. This factor will be one of the following values:

- a) **High**: The issue can cause significant damage such as loss of funds or the protocol entering an unrecoverable state;
- b) **Medium**: The issue can cause moderate damage such as impacts that only affect a small group of users or only a particular part of the protocol;
- c) **Low**: The issue can cause little to no damage such as bugs that are easily recoverable or cause unexpected interactions that cause minor inconveniences.

When defining the impact of a finding other factors are also considered. These can include but are not limited to Data/state integrity, loss of availability, financial loss, and reputation damage. After defining the likelihood and impact of an issue, the severity can be determined according to the table below.

		Likelihood		
		High	Medium	Low
Impact	High	Critical	High	Medium
	Medium	High	Medium	Low
	Low	Medium	Low	Info/Best Practices

To address issues that do not fit a High/Medium/Low severity, **Cairo Security Clan** also uses three more finding severities: **Informational**, **Best Practices** and **Gas**

- a) **Informational** findings do not pose any risk to the application, but they carry some information that the audit team intends to formally pass to the client;
- b) **Best Practice** findings are used when some piece of code does not conform with smart contract development best practices;
- c) **Gas** findings are used when some piece of code uses more gas than it should be or have some functions that can be removed to save gas.



## 6 Issues by Severity Levels

### 6.1 High

#### 6.1.1 Front-running issue in `ExecutionContract.create()` allows blocking of legitimate `SpvSwapVault` transactions

**File(s):** `contracts/execution_contract/ExecutionContract.sol`

**Description:** The `ExecutionContract.create()` function is permissionless and allows anyone to create an execution commitment for any owner with any salt. When users claim or front in `SpvVaultManager` with execution actions, the contract calls `ExecutionContract.create()` using `data.recipient` as the owner and `btcTxHash` as the salt. Attackers can frontrun these transactions by calling `create()` with the same parameters, causing legitimate transactions to revert with "create: Already initiated" error. This completely blocks users from accessing their funds through the intended execution mechanism.

```
1 function create(address owner, bytes32 salt, Execution calldata execution) external payable {
2     //Make sure execution not yet initialized
3     require(_executionCommitments[owner][salt] == bytes32(0x0), "create: Already initiated");
4
5     //Commit execution
6     bytes32 executionHash = execution.hash();
7     _executionCommitments[owner][salt] = executionHash;
8
9     //Transfer token amount to the contract
10    uint256 totalAmount = execution.amount + execution.executionFee;
11    TransferUtils.transferIn(execution.token, msg.sender, totalAmount);
12
13    //Emit event
14    emit Events.ExecutionCreated(owner, salt, executionHash);
15 }
```

**Recommendation(s):** Consider modifying the salt generation in `ExecutionContract` to include additional information like `msg.sender`. For example, using the hash value of salt and `msg.value`.

**Status:** Fixed

**Update from the client:** Fixed in [e416d55](#), using the recommended method of hashing the user-provided salt with the `msg.sender`, this making the actual salt unique on a per-sender basis. Also fixed in the Cairo contracts in [31e0deb](#) using the same method.



## 6.2 Medium

### 6.2.1 Success action execution failures do not revert the claim transaction

File(s): `contracts/escrow_manager/EscrowManager.sol`

**Description:** When claiming an escrow with a success action, the `claimWithSuccessAction()` function executes the success action immediately via an external call to the ExecutionProxy contract. If the success action execution fails, the transaction does not revert. Instead, it only emits an `ExecutionError` event:

```
1 function claimWithSuccessAction(EscrowData calldata escrow, bytes calldata witness, ExecutionAction calldata
    successAction) external {
2     require(escrow.successActionCommitment==successAction.hash(), "claim:_invalid_success_action");
3     bytes32 escrowHash = _claimWithoutPayout(escrow, witness);
4
5     //Execute through execution proxy instead of paying out
6     (bool success, bytes memory errorResult) = _execute(escrow.token, escrow.amount, successAction, escrow.
        claimer);
7     if(!success) emit Events.ExecutionError(escrowHash, errorResult);
8 }
```

This means that even if the success action fails (due to insufficient gas, contract errors, or other execution issues), the escrow claim is still processed and the funds are transferred to the execution proxy. The success action is effectively lost with no mechanism to retry or recover it.

Comparing with Cairo version of this protocol, the claim action will queue the success action for execution in the ExecutionContract instead of executing it immediately during claiming.

```
1 if escrow.success_action.is_some() {
2     //Transfer funds to execution contract in case success action was defined
3     self._to_execution_contract(escrow.claimer, escrow.token, escrow.amount, escrow.is_pay_out(), escrow.
        success_action.unwrap(), escrow_hash);
4 } else {
5     //Pay out directly to the claimer
6     self._pay_out(escrow.claimer, escrow.token, escrow.amount, escrow.is_pay_out());
7 }
8
9 // [...]
10 fn _to_execution_contract(ref self: ContractState, dst: ContractAddress, token: ContractAddress, amount: u256,
    pay_out: bool, escrow_execution: EscrowExecution, escrow_hash: felt252) {
11     if amount < escrow_execution.fee {
12         //Fee is larger than the full amount, just pay out as a fallback
13         self._pay_out(dst, token, amount, pay_out);
14         return;
15     }
16
17     let execution_contract = IExecutionContractDispatcher{contract_address: self.execution_contract.read()};
18
19     erc20_utils::approve(token, execution_contract.contract_address, amount);
20     execution_contract.create(dst, escrow_hash, token, amount - escrow_execution.fee, escrow_execution.fee,
        escrow_execution.hash, escrow_execution.expiry);
21 }
```

**Recommendation(s):** Consider implementing a queuing mechanism similar to the Cairo version, where success actions are queued for later execution in the Execution Contract.

**Status:** Acknowledged

**Update from the client:** Better clarified in the code at commit [31a6152](#).

This is the expected behavior, when the success action execution fails the funds are just transfered to the user directly. Transferring to execution contract (like done in Cairo contracts) would have the same effect, there it would also just transfer funds directly to the user in case the call fails.

The reason that execution contract is not used in EVM but is used in Cairo, is that outside call error handling in Cairo is limited and you cannot:

- limit gas, making it possible for the calls to always run out of gas
- rely on the call to not revert the whole transaction, if the destination contract doesn't exist the call to it will revert the whole transaction instead of just throwing an error

In both of these cases the claiming of the escrow is blocked and claimer might loose funds by being unable to claim before timeout.





## Cairo Security Clan

---

Compared to EVM where you can limit gas, and catch every possible error case in the code (contract revert, contract panic, contract doesn't exist, out of gas) - making sure that a failing call doesn't revert the whole claim transaction and doesn't block the claim of the escrow.



### 6.2.2 Attacker can intentionally limit gas to sabotage the success action execution

File(s): `contracts/execution_proxy/Executor.sol`

**Description:** When initializing an escrow, a success action can be specified to execute automatically upon a successful claim. This is performed via an external call to an ExecutionProxy contract. If no custom gas limit is set (`executionAction.gasLimit == 0`), the contract defaults to using the full remaining gas (`gasleft()`):

```
1 //Try to execute calls
2 (success, callError) = address(executionProxy).call{gas: executionAction.gasLimit==0 ? gasleft() :
   executionAction.gasLimit}{
3     abi.encodeWithSelector(ExecutionProxy.execute.selector, executionAction.calls)
4 };
```

However, this call can be triggered by any external actor via `claimWithSuccessAction()`, including a malicious one. An attacker could deliberately invoke the function with insufficient gas, causing the success action to fail during execution.

Additionally, failure of the success action does not revert the transaction. Instead, it emits an `ExecutionError` event:

```
1 function claimWithSuccessAction(EscrowData calldata escrow, bytes calldata witness, ExecutionAction calldata
   successAction) external {
2     require(escrow.successActionCommitment==successAction.hash(), "claim:_invalid_success_action");
3     bytes32 escrowHash = _claimWithoutPayout(escrow, witness);
4
5     //Execute through execution proxy instead of paying out
6     (bool success, bytes memory errorResult) = _execute(escrow.token, escrow.amount, successAction, escrow.
   claimer);
7     if(!success) emit Events.ExecutionError(escrowHash, errorResult);
8 }
```

Because the failure is non-reverting and there's no retry mechanism, the success action is effectively lost once a low-gas claim is executed.

**Recommendation(s):** Restrict who can call `claimWithSuccessAction()` to only the `escrow.claimer` if there is no gas limit specified.

**Status:** Fixed

**Update from the client:** Fixed in [4d3f6d3](#) by disabling the feature to forward `gasleft()` when `gasLimit` is 0 and instead immediately failing when `gasLimit` equals 0



## 6.3 Informational

### 6.3.1 Claimer cannot initialize escrow with native ETH

File(s): `contracts/escrow_manager/EscrowManager.sol`

**Description:** The escrow manager contract prevents a claimer from initializing an escrow using native ETH due to a sender verification requirement in the `transferIn()` function.

Specifically, when transferring native ETH (`token == address(0)`), the following check is enforced:

```
1 function transferIn(address token, address src, uint256 amount) internal {
2     if(token==address(0x0)) {
3         //Native token transfer
4         require(src==msg.sender, "transferIn:_sender_not_src");
5         require(msg.value >= amount, "transferIn:_value_too_low");
6     } else {
7         // [...]
8     }
9 }
```

This check fails if the claimer (i.e. not the offerer) tries to initialize the escrow, because the `src` address passed into `transferIn()` is set to `escrow.offerer`, while `msg.sender` would be the claimer.

Here's the relevant snippet from `initialize()`:

```
1 if(escrow.depositToken==escrow.token && escrow.isPayIn() && msg.sender==escrow.offerer) {
2     //Transfer funds in one go
3     _payIn(escrow.offerer, escrow.token, escrow.amount + depositAmount, true);
4 } else {
5     //Transfer funds separately
6     if(depositAmount > 0) TransferUtils.transferIn(escrow.depositToken, msg.sender, depositAmount);
7     _payIn(escrow.offerer, escrow.token, escrow.amount, escrow.isPayIn());
8 }
```

In the else branch, `_payIn()` is called with `src = escrow.offerer`. If native ETH is used, and the caller is not `escrow.offerer`, the `transferIn()` call will revert.

**Recommendation(s):** Consider reviewing the logic to support the claimer to initialize escrow with native ETH. Otherwise, document this behavior clearly in the codebase.

**Status:** Acknowledged

**Update from the client:** Better clarification is provided in the commit [67fa15a](#), clearly stating that initializing an escrow by the claimer when `payIn = true` and using native token (ETH) will always fail.



## 6.4 Best Practices

### 6.4.1 Misleading parameter name src in \_payOut() function

File(s): [contracts/escrow\\_manager/EscrowManager.sol](#)

**Description:** The `_payOut()` function uses the parameter name `src` to represent the recipient of funds, which is misleading and inconsistent with typical naming conventions. In payout operations, the address receiving the funds is usually referred to as `dst` (destination), while `src` (source) implies a sender.

```
1 function _payOut(address src, address token, uint256 amount, bool payOut) internal {
2     if (payOut) {
3         TransferUtils.transferOut(token, src, amount);
4     } else {
5         _LpVault_transferOut(token, src, amount);
6     }
7 }
```

This naming may confuse developers reviewing or maintaining the code, especially since other functions (like `transferOut()`) correctly use `dst` to refer to the recipient.

**Recommendation(s):** Rename the `src` parameter to `dst` (or recipient) to better reflect its role as the payout destination.

**Status:** Fixed

**Update from the client:** Fixed in [1fa48ab](#)

### 6.4.2 Deposit function should use safe arithmetic operations like withdraw function

File(s): [contracts/spv\\_swap\\_vault/state/SpvVaultState.sol](#)

**Description:** The `deposit()` function in `SpvVaultState` does not implement the same safety checks as the `withdraw()` function. While `withdraw()` uses safe arithmetic operations to prevent overflow, `deposit()` relies on unchecked operations:

Withdraw function (lines 80-85) - Uses safe operations:

```
1 //Make sure subtraction doesn't overflow
2 (bool token0AmountSuccess, uint64 token0Amount) = _token0Amount.checkedSubUint64(rawAmount0);
3 if(!token0AmountSuccess) return (false, _withdrawCount, "withdraw:_amount_0");
4 (bool token1AmountSuccess, uint64 token1Amount) = _token1Amount.checkedSubUint64(rawAmount1);
5 if(!token1AmountSuccess) return (false, _withdrawCount, "withdraw:_amount_1");
6 withdrawCount = _withdrawCount.saturatingAddOneUint32();
```

Deposit function (lines 123-125) - Uses unsafe operations:

```
1 _token0Amount += rawAmount0;
2 _token1Amount += rawAmount1;
3 depositCount = ++_depositCount;
```

The deposit function uses unchecked addition (`+=`) which can overflow when `_token0Amount + rawAmount0` or `_token1Amount + rawAmount1` exceeds `type(uint64).max`. Similarly, `++_depositCount` can overflow when it reaches `type(uint32).max`.

**Recommendation(s):** Consider using safe arithmetic functions with proper error handling, similar to the `withdraw()` function, to avoid unexpected overflows.

**Status:** Acknowledged

**Update from the client:** Better clarified that this is the expected behavior at commit [7de2226](#)

It is critical that we don't panic in the withdraw function (since that could lead to funds being locked up), but panicing in deposit is fine because that couldn't lead to loss of funds.



## 7 Test Compilation Evaluation

### 7.1 Compilation Output

```
1 npx hardhat compile
2 Generating typings for: 103 artifacts in dir: typechain-types for target: ethers-v6
3 Successfully generated 300 typings!
4 Compiled 94 Solidity files successfully (evm target: cancun).
```



## 7.2 Tests Output

```
1 BtcRelay
2 [PASS] Valid constructor (514ms)
3 [PASS] Invalid block PoW (blockhash not lower than target) (675ms)
4 [PASS] Invalid block nbits (not same as last block)
5 [PASS] Invalid block nbits at difficulty adjustment (invalidly computed)
6 [PASS] Invalid block previous blockhash (321ms)
7 [PASS] Invalid block median timestamps (56ms)
8 [PASS] Invalid block future timestamp
9 [submitMainAndAssert] Gas usage, num headers: 20 gas used: 572328 gas per header: 28616
10 [PASS] Valid main chain (383ms)
11 [PASS] Invalid main chain, stored blockheader not committed (78ms)
12 [submitMainAndAssert] Gas usage, num headers: 4 gas used: 139280 gas per header: 34820
13 [PASS] Invalid main chain, stored header is not the tip (97ms)
14 [submitMainAndAssert] Gas usage, num headers: 20 gas used: 572268 gas per header: 28613
15 [PASS] Invalid short fork, stored header not in main chain (415ms)
16 [submitMainAndAssert] Gas usage, num headers: 20 gas used: 572292 gas per header: 28615
17 [PASS] Invalid long fork, stored header not in main chain (424ms)
18 [submitMainAndAssert] Gas usage, num headers: 20 gas used: 572304 gas per header: 28615
19 [submitLongForkAndAssert] Gas usage, num headers: 4 gas used: 183198 gas per header: 45800
20 [PASS] Invalid long fork, stored header not in fork state (416ms)
21 [submitMainAndAssert] Gas usage, num headers: 20 gas used: 572292 gas per header: 28615
22 [submitLongForkAndAssert] Gas usage, num headers: 4 gas used: 183210 gas per header: 45803
23 [PASS] Invalid long fork, stored header not fork state tip (436ms)
24 [submitMainAndAssert] Gas usage, num headers: 135 gas used: 3685107 gas per header: 27297
25 [submitShortForkAndAssert] Gas usage, num headers: 134 gas used: 1371293 gas per header: 10234
26 [PASS] Invalid main chain, re-org & try to build on top of now future blockheight (16080ms)
27 [submitMainAndAssert] Gas usage, num headers: 135 gas used: 3684975 gas per header: 27296
28 [submitShortForkAndAssert] Gas usage, num headers: 134 gas used: 1371317 gas per header: 10234
29 [PASS] Invalid short fork, re-org & try to fork again from now future blockheight (16469ms)
30 [submitMainAndAssert] Gas usage, num headers: 135 gas used: 3684927 gas per header: 27296
31 [submitShortForkAndAssert] Gas usage, num headers: 134 gas used: 1371341 gas per header: 10234
32 [PASS] Invalid long fork, re-org & try to fork again from now future blockheight (15775ms)
33 [submitMainAndAssert] Gas usage, num headers: 20 gas used: 572328 gas per header: 28616
34 [submitShortForkAndAssert] Gas usage, num headers: 20 gas used: 302068 gas per header: 15103
35 [PASS] Valid short fork (696ms)
36 [submitMainAndAssert] Gas usage, num headers: 20 gas used: 572280 gas per header: 28614
37 [submitLongForkAndAssert] Gas usage, num headers: 20 gas used: 644808 gas per header: 32240
38 [PASS] Valid long fork (683ms)
39 [submitMainAndAssert] Gas usage, num headers: 20 gas used: 572352 gas per header: 28618
40 [submitLongForkAndAssert] Gas usage, num headers: 4 gas used: 183198 gas per header: 45800
41 [submitLongForkAndAssert] Gas usage, num headers: 16 gas used: 544608 gas per header: 34038
42 [PASS] Valid long fork in 2 txns (697ms)
43 [submitMainAndAssert] Gas usage, num headers: 135 gas used: 3684963 gas per header: 27296
44 [submitShortForkAndAssert] Gas usage, num headers: 134 gas used: 1371245 gas per header: 10233
45 [PASS] Valid short fork, higher chainwork but shorter chain (15643ms)
46 [submitMainAndAssert] Gas usage, num headers: 20 gas used: 572268 gas per header: 28613
47 [PASS] Invalid short fork, not enough length (345ms)
48 [submitMainAndAssert] Gas usage, num headers: 20 gas used: 572352 gas per header: 28618
49 [submitLongForkAndAssert] Gas usage, num headers: 5 gas used: 210816 gas per header: 42163
50 [PASS] Invalid long fork, not enough length (384ms)
51 [submitMainAndAssert] Gas usage, num headers: 123 gas used: 3360399 gas per header: 27320
52 [PASS] Invalid short fork, not enough chainwork, but long enough (7362ms)
53 [submitMainAndAssert] Gas usage, num headers: 123 gas used: 3360483 gas per header: 27321
54 [submitLongForkAndAssert] Gas usage, num headers: 124 gas used: 3477112 gas per header: 28041
55 [PASS] Invalid long fork, not enough chainwork, but long enough (13718ms)
56
57 EscrowManager
58 Claim
59 [PASS] Valid claim (payOut=false,reputation=false,securityDeposit=false,claimerBounty=false,usesNativeToken
=false,usesNativeTokenForDeposit=false,successActionSuccess=false,successActionError=false) (82ms)
60 [PASS] Valid claim (payOut=true,reputation=false,securityDeposit=false,claimerBounty=false,usesNativeToken=
=false,usesNativeTokenForDeposit=false,successActionSuccess=false,successActionError=false)
61 [PASS] Valid claim (payOut=false,reputation=true,securityDeposit=false,claimerBounty=false,usesNativeToken=
=false,usesNativeTokenForDeposit=false,successActionSuccess=false,successActionError=false)
62 [PASS] Valid claim (payOut=true,reputation=true,securityDeposit=false,claimerBounty=false,usesNativeToken=
=false,usesNativeTokenForDeposit=false,successActionSuccess=false,successActionError=false)
63 [PASS] Valid claim (payOut=false,reputation=false,securityDeposit=true,claimerBounty=false,usesNativeToken=
=false,usesNativeTokenForDeposit=false,successActionSuccess=false,successActionError=false)
```





99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130  
131  
132  
133





## Refund cooperative

[illegible]







21





```

388 [PASS] Valid initialize (senderClaimer=false,payIn=true,reputation=false,securityDeposit=true,claimerBounty
    =false,usesNativeToken=true,usesNativeTokenForDeposit=true)
389 [PASS] Valid initialize (senderClaimer=false,payIn=false,reputation=true,securityDeposit=true,claimerBounty
    =false,usesNativeToken=true,usesNativeTokenForDeposit=true)
390 [PASS] Valid initialize (senderClaimer=false,payIn=true,reputation=true,securityDeposit=true,claimerBounty=
    false,usesNativeToken=true,usesNativeTokenForDeposit=true)
391 [PASS] Valid initialize (senderClaimer=false,payIn=false,reputation=false,securityDeposit=false,
    claimerBounty=true,usesNativeToken=true,usesNativeTokenForDeposit=true)
392 [PASS] Valid initialize (senderClaimer=false,payIn=true,reputation=false,securityDeposit=false,
    claimerBounty=true,usesNativeToken=true,usesNativeTokenForDeposit=true)
393 [PASS] Valid initialize (senderClaimer=false,payIn=false,reputation=true,securityDeposit=false,
    claimerBounty=true,usesNativeToken=true,usesNativeTokenForDeposit=true)
394 [PASS] Valid initialize (senderClaimer=false,payIn=true,reputation=true,securityDeposit=false,claimerBounty
    =true,usesNativeToken=true,usesNativeTokenForDeposit=true)
395 [PASS] Valid initialize (senderClaimer=false,payIn=false,reputation=false,securityDeposit=true,
    claimerBounty=true,usesNativeToken=true,usesNativeTokenForDeposit=true)
396 [PASS] Valid initialize (senderClaimer=false,payIn=true,reputation=false,securityDeposit=true,claimerBounty
    =true,usesNativeToken=true,usesNativeTokenForDeposit=true)
397 [PASS] Valid initialize (senderClaimer=false,payIn=false,reputation=true,securityDeposit=true,claimerBounty
    =true,usesNativeToken=true,usesNativeTokenForDeposit=true)
398 [PASS] Valid initialize (senderClaimer=false,payIn=true,reputation=true,securityDeposit=true,claimerBounty=
    true,usesNativeToken=true,usesNativeTokenForDeposit=true)
399 [PASS] Valid initialize (claimer is an erc1271 account)
400 [PASS] Invalid initialize not enough balance (payIn)
401 [PASS] Invalid initialize not enough balance (not payIn)
402 [PASS] Invalid initialize not enough native token sent to the contract
403 [PASS] Invalid initialize (check correct handling of msg.value)
404 [PASS] Invalid initialize not enough allowance (payIn erc-20)
405 [PASS] Invalid initialize not enough deposit token balance (erc-20)
406 [PASS] Invalid initialize not enough deposit token allowance (erc-20)
407 [PASS] Invalid initialize wrong signer
408 [PASS] Invalid initialize bad sign message
409 [PASS] Invalid initialize bad sign message (extra data)
410 [PASS] Invalid initialize 3rd party caller
411 [PASS] Invalid initialize expired
412 [PASS] Invalid initialize sign different timeout
413 [PASS] Invalid initialize commit twice
414
415 ExecutionContract
416 [PASS] Valid create (erc-20)
417 [PASS] Invalid create (erc-20 not enough balance)
418 [PASS] Invalid create (erc-20 not enough allowance)
419 [PASS] Valid create (native token)
420 [PASS] Invalid create (native token invalid msg.value)
421 [PASS] Invalid create twice the same execution
422 [PASS] Valid refund expired
423 [PASS] Invalid refund expired, not initiated
424 [PASS] Invalid refund expired, not expired
425 [PASS] Invalid refund expired, already processed
426 [PASS] Valid refund by owner
427 [PASS] Valid refund by owner (even though not expired yet)
428 [PASS] Invalid refund by owner, caller not owner
429 [PASS] Invalid refund by owner, not initiated
430 [PASS] Invalid refund by owner, try to refund twice
431 [PASS] Valid execute, empty calls
432 [PASS] Valid execute, erc20 transfer calls
433 [PASS] Valid execute, native transfer calls
434 [PASS] Valid execute, dummy emit event
435 [PASS] Valid execute, call reverted
436 [PASS] Valid execute, out of gas
437 [PASS] Valid execute, dummy emit event (drain tokens)
438 [PASS] Valid execute, call reverted (drain tokens)
439 [PASS] Invalid execute, wrong success action provided
440 [PASS] Invalid execute, not scheduled
441 [PASS] Invalid execute, try execute twice
442
443 SpvVaultManager
444 Open
445 [PASS] Valid open vault (51ms)
446 [PASS] Invalid open vault (already opened)

```





## Deposit

```

447 [PASS] Valid deposit (token0Native=false,token1Native=false,token0Type=false,token1Type=false,
448 thirdPartyDeposit=false,noToken0=false,noToken1=false)
449 [PASS] Valid deposit (token0Native=true,token1Native=false,token0Type=false,token1Type=false,
450 thirdPartyDeposit=false,noToken0=false,noToken1=false)
451 [PASS] Valid deposit (token0Native=false,token1Native=true,token0Type=false,token1Type=false,
452 thirdPartyDeposit=false,noToken0=false,noToken1=false)
453 [PASS] Valid deposit (token0Native=true,token1Native=true,token0Type=false,token1Type=false,
454 thirdPartyDeposit=false,noToken0=false,noToken1=false)
455 [PASS] Valid deposit (token0Native=false,token1Native=false,token0Type=true,token1Type=false,
456 thirdPartyDeposit=false,noToken0=false,noToken1=false)
457 [PASS] Valid deposit (token0Native=false,token1Native=true,token0Type=true,token1Type=false,
458 thirdPartyDeposit=false,noToken0=false,noToken1=false)
459 [PASS] Valid deposit (token0Native=false,token1Native=false,token0Type=false,token1Type=true,
460 thirdPartyDeposit=false,noToken0=false,noToken1=false)
461 [PASS] Valid deposit (token0Native=true,token1Native=false,token0Type=false,token1Type=true,
462 thirdPartyDeposit=false,noToken0=false,noToken1=false)
463 [PASS] Valid deposit (token0Native=false,token1Native=false,token0Type=true,token1Type=true,
464 thirdPartyDeposit=false,noToken0=false,noToken1=false)
465 [PASS] Valid deposit (token0Native=false,token1Native=false,token0Type=false,token1Type=false,
466 thirdPartyDeposit=true,noToken0=false,noToken1=false)
467 [PASS] Valid deposit (token0Native=true,token1Native=false,token0Type=false,token1Type=false,
468 thirdPartyDeposit=true,noToken0=false,noToken1=false)
469 [PASS] Valid deposit (token0Native=true,token1Native=true,token0Type=false,token1Type=false,
470 thirdPartyDeposit=true,noToken0=false,noToken1=false)
471 [PASS] Valid deposit (token0Native=false,token1Native=false,token0Type=true,token1Type=false,
472 thirdPartyDeposit=true,noToken0=false,noToken1=false)
473 [PASS] Valid deposit (token0Native=true,token1Native=false,token0Type=true,token1Type=false,
474 thirdPartyDeposit=true,noToken0=false,noToken1=false)
475 [PASS] Valid deposit (token0Native=false,token1Native=false,token0Type=true,token1Type=true,
476 thirdPartyDeposit=true,noToken0=false,noToken1=false)
477 [PASS] Valid deposit (token0Native=false,token1Native=false,token0Type=false,token1Type=true,
478 thirdPartyDeposit=true,noToken0=false,noToken1=true)
479 [PASS] Valid deposit (token0Native=false,token1Native=true,token0Type=false,token1Type=true,
480 thirdPartyDeposit=true,noToken0=false,noToken1=true)
481 [PASS] Valid deposit (token0Native=true,token1Native=false,token0Type=false,token1Type=true,
482 thirdPartyDeposit=true,noToken0=false,noToken1=true)

```

Front

26

27





```

589 [PASS] Invalid front - not enough allowance erc-20 (token0Native=false,token1Native=false,token0Type=false,
token1Type=false,token0NotEnoughAllowance=true,token1NotEnoughAllowance=true)
590 [PASS] Invalid front - not enough allowance erc-20 (token0Native=false,token1Native=false,token0Type=true,
token1Type=false,token0NotEnoughAllowance=true,token1NotEnoughAllowance=true)
591 [PASS] Invalid front - not enough allowance erc-20 (token0Native=false,token1Native=false,token0Type=false,
token1Type=true,token0NotEnoughAllowance=true,token1NotEnoughAllowance=true)
592 [PASS] Invalid front - not enough allowance erc-20 (token0Native=false,token1Native=false,token0Type=true,
token1Type=true,token0NotEnoughAllowance=true,token1NotEnoughAllowance=true)
593 [PASS] Invalid front - not enough msg.value (token0Native=true,token1Native=false,token0Type=false,
token1Type=false,token0NotEnoughMsgValue=true,token1NotEnoughMsgValue=false)
594 [PASS] Invalid front - not enough msg.value (token0Native=true,token1Native=true,token0Type=false,
token1Type=false,token0NotEnoughMsgValue=true,token1NotEnoughMsgValue=false)
595 [PASS] Invalid front - not enough msg.value (token0Native=true,token1Native=false,token0Type=false,
token1Type=true,token0NotEnoughMsgValue=true,token1NotEnoughMsgValue=false)
596 [PASS] Invalid front - not enough msg.value (token0Native=false,token1Native=true,token0Type=false,
token1Type=false,token0NotEnoughMsgValue=false,token1NotEnoughMsgValue=true)
597 [PASS] Invalid front - not enough msg.value (token0Native=true,token1Native=true,token0Type=false,
token1Type=false,token0NotEnoughMsgValue=false,token1NotEnoughMsgValue=true)
598 [PASS] Invalid front - not enough msg.value (token0Native=false,token1Native=true,token0Type=true,
token1Type=false,token0NotEnoughMsgValue=false,token1NotEnoughMsgValue=true)
599 [PASS] Invalid front - not enough msg.value (token0Native=true,token1Native=true,token0Type=false,
token1Type=false,token0NotEnoughMsgValue=true,token1NotEnoughMsgValue=true)
600 [PASS] Invalid front - msg.value only enough for one deposit
601 [PASS] Invalid front - vault not opened
602 [PASS] Invalid front - vault got closed
603 [PASS] Invalid front - already fronted
604 [PASS] Invalid front - already claimed
605 [PASS] Invalid front - amount0 overflow 64-bits
606 Claim
607 [PASS] Valid claim (token0Native=false,token1Native=false,token0Type=false,token1Type=false,thirdPartyFront
=false,noToken0=false,noToken1=false,usesExecution=false)
608 [PASS] Valid claim (token0Native=true,token1Native=false,token0Type=false,token1Type=false,thirdPartyFront=
=false,noToken0=false,noToken1=false,usesExecution=false)
609 [PASS] Valid claim (token0Native=false,token1Native=true,token0Type=false,token1Type=false,thirdPartyFront=
=false,noToken0=false,noToken1=false,usesExecution=false)
610 [PASS] Valid claim (token0Native=true,token1Native=true,token0Type=false,token1Type=false,thirdPartyFront=
=false,noToken0=false,noToken1=false,usesExecution=false)
611 [PASS] Valid claim (token0Native=false,token1Native=false,token0Type=true,token1Type=false,thirdPartyFront=
=false,noToken0=false,noToken1=false,usesExecution=false) (38ms)
612 [PASS] Valid claim (token0Native=true,token1Native=true,token0Type=true,token1Type=false,thirdPartyFront=
=false,noToken0=false,noToken1=false,usesExecution=false)
613 [PASS] Valid claim (token0Native=false,token1Native=false,token0Type=false,token1Type=true,thirdPartyFront=
=false,noToken0=false,noToken1=false,usesExecution=false)
614 [PASS] Valid claim (token0Native=true,token1Native=false,token0Type=false,token1Type=true,thirdPartyFront=
=false,noToken0=false,noToken1=false,usesExecution=false)
615 [PASS] Valid claim (token0Native=false,token1Native=false,token0Type=false,token1Type=false,thirdPartyFront
=false,noToken0=false,noToken1=true,usesExecution=false)
616 [PASS] Valid claim (token0Native=true,token1Native=false,token0Type=false,token1Type=false,thirdPartyFront=
=false,noToken0=false,noToken1=true,usesExecution=false)
617 [PASS] Valid claim (token0Native=false,token1Native=true,token0Type=false,token1Type=false,thirdPartyFront=
=false,noToken0=false,noToken1=true,usesExecution=false)
618 [PASS] Valid claim (token0Native=true,token1Native=true,token0Type=false,token1Type=false,thirdPartyFront=
=false,noToken0=false,noToken1=true,usesExecution=false)
619 [PASS] Valid claim (token0Native=false,token1Native=false,token0Type=true,token1Type=false,thirdPartyFront=
=false,noToken0=false,noToken1=true,usesExecution=false)
620 [PASS] Valid claim (token0Native=false,token1Native=true,token0Type=true,token1Type=false,thirdPartyFront=
=false,noToken0=false,noToken1=true,usesExecution=false)
621 [PASS] Valid claim (token0Native=false,token1Native=false,token0Type=false,token1Type=true,thirdPartyFront=
=false,noToken0=false,noToken1=true,usesExecution=false)
622 [PASS] Valid claim (token0Native=true,token1Native=false,token0Type=false,token1Type=true,thirdPartyFront=
=false,noToken0=false,noToken1=true,usesExecution=false)
623 [PASS] Valid claim (token0Native=false,token1Native=true,token0Type=true,token1Type=true,thirdPartyFront=
=false,noToken0=false,noToken1=true,usesExecution=false)
624 [PASS] Valid claim (token0Native=false,token1Native=false,token0Type=false,token1Type=false,thirdPartyFront
=true,noToken0=false,noToken1=true,usesExecution=false)
625 [PASS] Valid claim (token0Native=true,token1Native=false,token0Type=false,token1Type=false,thirdPartyFront=
=true,noToken0=false,noToken1=true,usesExecution=false)
626 [PASS] Valid claim (token0Native=false,token1Native=true,token0Type=false,token1Type=false,thirdPartyFront=
=true,noToken0=false,noToken1=true,usesExecution=false)

```

29

30

---

31





```
732 [PASS] Valid claim - fronted (token0Native=false,token1Native=false,token0Type=true,token1Type=false,
733 thirdPartyFront=true,noToken0=false,noToken1=true,usesExecution=true) (43ms)
734 [PASS] Valid claim - fronted (token0Native=false,token1Native=true,token0Type=true,token1Type=false,
735 thirdPartyFront=true,noToken0=false,noToken1=true,usesExecution=true)
736 [PASS] Valid claim - fronted (token0Native=false,token1Native=false,token0Type=false,token1Type=true,
737 thirdPartyFront=true,noToken0=false,noToken1=true,usesExecution=true)
738 [PASS] Invalid claim - vault not opened
739 [PASS] Invalid claim - invalid tx confirmations
740 [PASS] Invalid claim - invalid merkle proof
741 [PASS] Invalid claim - invalid merkle proof (position)
742 [PASS] Invalid claim - btc tx empty inputs
743 [PASS] Invalid claim - btc tx empty inputs
744 [PASS] Invalid claim (vault close) - output 1 not found
745 [PASS] Invalid claim (vault close) - input 1 not found
746 [PASS] Invalid claim (vault close) - output 1 empty script
747 [PASS] Invalid claim (vault close) - output 1 not OP_RETURN
748 [PASS] Invalid claim (vault close) - output 1 invalid len
749 [PASS] Invalid claim (vault close) - caller fee 0 overflow
750 [PASS] Invalid claim (vault close) - fronting fee 0 overflow
751 [PASS] Invalid claim (vault close) - execution fee 0 overflow
752 [PASS] Invalid claim (vault close) - caller fee 1 overflow
753 [PASS] Invalid claim (vault close) - fronting fee 1 overflow
754 [PASS] Invalid claim (vault close) - amount 0 sum overflow
755 [PASS] Invalid claim (vault close) - amount 1 sum overflow
756 [PASS] Invalid claim (vault close) - withdraw too much token0
757 [PASS] Invalid claim (vault close) - withdraw too much token1
758 BitcoinNoncedOutputClaimHandler
759 [PASS] Valid random witness (87ms)
760 [PASS] Valid real witness (4322ms)
761 [PASS] Invalid empty witness
762 [PASS] Invalid incorrect commitment witness
763 [PASS] Invalid block confirmations
764 [PASS] Invalid merkle proof, root doesn't match
765 [PASS] Invalid blockheader, provided header is not known to the btc relay
766 [PASS] Invalid vout of bounds
767 [PASS] Invalid txoHash doesn't match (due to wrong outputAmount)
768 [PASS] Invalid txoHash doesn't match (due to wrong outputScript)
769 [PASS] Invalid txoHash doesn't match (due to wrong nonce)
770
771 BitcoinOutputClaimHandler
772 [PASS] Valid random witness (106ms)
773 [PASS] Valid real witness (6354ms)
774 [PASS] Invalid empty witness
775 [PASS] Invalid incorrect commitment witness
776 [PASS] Invalid block confirmations
777 [PASS] Invalid merkle proof, root doesn't match
778 [PASS] Invalid blockheader, provided header is not known to the btc relay
779 [PASS] Invalid vout of bounds
780 [PASS] Invalid txoHash doesn't match (due to wrong outputAmount)
781 [PASS] Invalid txoHash doesn't match (due to wrong outputScript)
782
783 CompactBlockHeader
784 [PASS] Valid verify out of bounds
785 [PASS] Valid verify out of bounds with offset
786 [PASS] Invalid verify out of bounds
787 [PASS] Valid read values
788 [PASS] Existing blockheaders (3335ms)
789
790 Difficulty
791 [PASS] Get chainwork random data
792 [PASS] Compute new target real adjustments (9160ms)
793 [PASS] Get chainwork real data (6726ms)
794
795 Nbits
796 [PASS] Nbits to target
```



```
797 [PASS] Target to nbits
798 [PASS] Bitcoin core test vector
799 [PASS] Bitcoin core negative nbits test vector
800 [PASS] Random targets
801
802 StoredBlockHeader
803 [PASS] Valid from calldata
804 [PASS] Valid from calldata with offset
805 [PASS] Invalid from calldata with offset
806 [PASS] Valid read values
807 [PASS] Existing blockheaders (6548ms)
808 [PASS] Valid parse random (62ms)
809 [PASS] Valid update random (567ms)
810 [PASS] Valid update random block on PoW readjustment (1211ms)
811 [PASS] Valid update random block on PoW readjustment, too fast (1496ms)
812 [PASS] Valid update random block on PoW readjustment, too slow (796ms)
813 [PASS] Valid update random block, with timestamp larger than median of last 11 blocks (591ms)
814 [PASS] Invalid update random block, due to low PoW (3131ms)
815 [PASS] Invalid update random block, due to wrong nBits (231ms)
816 [PASS] Invalid update random block, due to wrong nBits during difficulty retarget (215ms)
817 [PASS] Invalid update random block, due to wrong previous blockhash (589ms)
818 [PASS] Invalid update random block, due to timestamp not being larger than median of last 11 blocks (547ms)
819 [PASS] Invalid update random block, due to timestamp being too far in the future (420ms)
820 [PASS] Valid update real (9008ms)
821 [PASS] Valid update real on PoW readjustment (965ms)
822 [PASS] Valid update real on PoW readjustment, too fast (964ms)
823
824 BitcoinTxIdClaimHandler
825 [PASS] Valid random witness (96ms)
826 [PASS] Valid real witness (4334ms)
827 [PASS] Invalid empty witness
828 [PASS] Invalid incorrect commitment witness
829 [PASS] Invalid block confirmations
830 [PASS] Invalid merkle proof, root doesn't match
831 [PASS] Invalid blockheader, provided header is not known to the btc relay
832
833 BitcoinMerkleTree
834 [PASS] Randomly generated tests
835 [PASS] Real data tests (4171ms)
836
837 BitcoinTx
838 [PASS] Valid random bitcoin txs (515ms)
839 getRealRandomTransactionTest(): 455ef3447d4be1d1c5ea78082828a2a5b5abc52d13d21233d44baa919bc79bcb
840 getRealRandomTransactionTest(): acbd6110dc9e3ab7692631d46e045b5ca5d698ea2d1aee27d8d33e045ff2414b
841 getRealRandomTransactionTest(): 76075dc0b066ece54fba8d5634b4da7cdea7b94be66d7267440207de34522fcd
842 getRealRandomTransactionTest(): 45709232aa6257ef37be7d8d26a271307f481d72002e9e63f84c5b1f96d4b344
843 getRealRandomTransactionTest(): f74bec3437c4150341aae406346b77fc2c795de259ba5377da64a9e2c39e4a3a
844 getRealRandomTransactionTest(): dd86a8383f64bb8d57a8b84326ff3e01b3bde6d6dd9d3b007d745d05a5b776d9
845 getRealRandomTransactionTest(): 9ee76d0ec593361a6a1388e4b6e1c9f8c119482bce9cb71f364c54a3b56d0bba
846 getRealRandomTransactionTest(): 83e68be11340f6055477edb4e8a0fbf436e9fd90122bf22253ae6594311773bc
847 getRealRandomTransactionTest(): aaf0b8b717a8fba7c6d2a0d4aa42494c2ac4941583c5c14e9ef62bf7da59bf54
848 getRealRandomTransactionTest(): 9ab4423c919b861a510937df06a76ead71cef4c84e71af543fd6fa4fb19e45c6
849 [PASS] Valid real bitcoin txs (5675ms)
850 [PASS] Invalid witness not stripped
851 [PASS] Invalid tx more than expected data
852 [PASS] Invalid tx length exactly 64 bytes
853
854 Endianness
855 [PASS] Reverse uint32
856 [PASS] Reverse uint64
857 [PASS] Reverse bytes32
858
859 EIP712Sighash
860 [PASS] Random valid init (359ms)
861 [PASS] Random valid refund (168ms)
862
863 Escrow
864 [PASS] Parse flags (49ms)
865 [PASS] Total deposit calculation
866 [PASS] Random hash
```



```
867
868 EscrowStorage
869     [PASS] Commit
870     [PASS] Invalid commit twice
871     [PASS] Commit 2 different
872     [PASS] Commit & finalize success
873     [PASS] Commit & finalize not success
874     [PASS] Invalid commit, finalize, try to re-commit
875     [PASS] Invalid finalize, not committed
876     [PASS] Commit 2 different, finalize 1
877
878 LpVault
879     [PASS] Deposit
880     [PASS] 2 Deposits
881     [PASS] Invalid deposit not enough funds
882     [PASS] Invalid deposit not enough allowance
883     [PASS] Deposit ETH
884     [PASS] Deposit ETH, more than required
885     [PASS] Invalid deposit ETH, too low tx.value
886     [PASS] Invalid deposit ETH, not enough balance
887     [PASS] Withdraw
888     [PASS] Withdraw ETH
889     [PASS] Withdraw all
890     [PASS] Invalid withdraw more than deposited
891     [PASS] Invalid withdraw more than deposited (contract has enough token)
892     [PASS] Transfer out
893     [PASS] Transfer in
894     [PASS] Transfer in all
895     [PASS] Invalid transfer in, more than owned
896
897 ReputationState
898     [PASS] Test updates
899     [PASS] Test overflowing
900
901 ReputationTracker
902     [PASS] Update reputation
903     [PASS] Update reputation multiple types
904     [PASS] Update reputation multiple tokens
905     [PASS] Update reputation multiple claim handlers
906     [PASS] Update reputation multiple tokens & claim handlers
907     [PASS] Update reputation type out of bounds
908
909 Execution
910     [PASS] Random hash
911
912 ExecutionProxy
913     [PASS] Valid execute
914     [PASS] Valid execute (payable)
915     [PASS] Valid execute (revert)
916     [PASS] Valid execute (contract doesn't exist)
917     [PASS] Valid execute (out of gas) (16505ms)
918     [PASS] Valid drainAll (erc-20) (257ms)
919     [PASS] Valid drainAll (erc-20)
920     [PASS] Valid drainAll (native)
921     [PASS] Valid drainAll (native & 2x erc-20) (5949ms)
922     [PASS] Valid drainAll (native & 2x erc-20, with contract having 0 balance of 1 of the token) (41ms)
923
924 Executor
925     [PASS] Valid execute (success) (268ms)
926     [PASS] Valid execute (success, multiple calls)
927     [PASS] Valid execute (run out of gas)
928     [PASS] Valid execute (rejection in contract call)
929     [PASS] Valid execute (erc-20)
930     [PASS] Valid execute (native token)
931     [PASS] Valid execute payable (native token)
932     [PASS] Valid execute payable (native token & other erc20)
933
934 HashlockClaimHandler
935     [PASS] Valid witness
936     [PASS] Invalid witness with more than 32 bytes
```



```
937 [PASS] Invalid witness
938 [PASS] Random valid witnesses
939
940 BitcoinVaultTransactionData
941 [PASS] Parse valid (amount1 and execution) (74ms)
942 [PASS] Parse valid (execution)
943 [PASS] Parse valid (amount1)
944 [PASS] Parse valid
945 [PASS] Invalid single output only
946 [PASS] Invalid 2nd output empty script
947 [PASS] Invalid 2nd output not OP_RETURN
948 [PASS] Invalid no input
949 [PASS] Invalid just 1 input
950 [PASS] Invalid 2nd output invalid length
951 [PASS] Invalid caller fee 0 overflow
952 [PASS] Invalid fronting fee 0 overflow
953 [PASS] Invalid execution fee 0 overflow
954 [PASS] Invalid caller fee 1 overflow
955 [PASS] Invalid fronting fee 1 overflow
956 [PASS] Valid get full amounts
957 [PASS] Invalid get full amounts (overflow amount0)
958 [PASS] Invalid get full amounts (overflow amount1)
959 [PASS] Valid get hash
960
961 SpvVaultParameters
962 [PASS] Valid from raw token0
963 [PASS] Valid from raw token1
964 [PASS] Valid from raw
965 [PASS] Valid hash
966
967 SpvVaultState
968 [PASS] Valid open (42ms)
969 [PASS] Valid close
970 [PASS] Valid is opened (true)
971 [PASS] Valid is opened (false)
972 [PASS] Valid check opened and params
973 [PASS] Invalid check opened and params (not opened)
974 [PASS] Invalid check opened and params (invalid params)
975 [PASS] Valid withdraw
976 [PASS] Invalid withdraw (amount 0 withdraw too much)
977 [PASS] Invalid withdraw (amount 1 withdraw too much)
978 [PASS] Valid deposit
979 [PASS] Invalid deposit (amount 0 overflow)
980 [PASS] Invalid deposit (amount 1 overflow)
981 [PASS] Invalid deposit (deposit count overflow)
982
983 Utils
984 [PASS] Valid pack address and vault id
985 [PASS] Valid calculate fee
986 [PASS] Invalid calculate fee (overflow)
987 [PASS] Calculate fee random (142ms)
988
989 TimelockRefundHandler
990 [PASS] Valid refund
991 [PASS] Invalid refund, non-empty witness
992 [PASS] Invalid refund, not expired yet
993
994 TransferUtils
995 [PASS] Valid balance of (erc-20) (65ms)
996 [PASS] Valid balance of (native token)
997 [PASS] Valid transfer in (erc-20)
998 [PASS] Valid transfer in (erc-20 not from caller)
999 [PASS] Invalid transfer in, not enough balance (erc-20)
1000 [PASS] Invalid transfer in, not enough allowance (erc-20)
1001 [PASS] Valid transfer in (native token)
1002 [PASS] Invalid transfer in (native token not from caller)
1003 [PASS] Invalid transfer in not enough msg.value provided (native token)
1004 [PASS] Valid transfer out (erc-20)
1005 [PASS] Invalid transfer out not enough balance (erc-20)
1006 [PASS] Valid transfer out (native token)
```



```
1007 [PASS] Invalid transfer out not enough balance (native token)
1008 [PASS] Invalid transfer out, target reverted or ran out of gas (native token)
1009 [PASS] Valid transfer out (no revert) (erc-20)
1010 [PASS] Invalid transfer out not enough balance (no revert) (erc-20)
1011 [PASS] Valid transfer out (no revert) (native token)
1012 [PASS] Invalid transfer out not enough balance (no revert) (native token)
1013 [PASS] Invalid transfer out, target reverted or ran out of gas (no revert) (native token)
1014
1015 MathUtils
1016 [PASS] Valid castToUint64
1017 [PASS] Valid castToUint64 overflow
1018 [PASS] Valid uncheckedAddUint64
1019 [PASS] Invalid uncheckedAddUint64, overflow (unchecked so simply just returns the lower bits of the value)
1020 [PASS] Valid checkedSubUint64
1021 [PASS] Valid checkedSubUint64, result 0
1022 [PASS] Valid checkedSubUint64, underflow
1023 [PASS] Valid checkedSubUint64, big underflow
1024 [PASS] Valid saturatingAddOneUint32
1025 [PASS] Valid saturatingAddOneUint32, saturated
1026 [PASS] Valid saturatingAddUint224
1027 [PASS] Valid saturatingAddUint224, exact saturated
1028 [PASS] Valid saturatingAddUint224, saturated
1029 [PASS] Valid saturatingAddUint224, saturated, big summand
1030 [PASS] Valid maxUint256, first is bigger
1031 [PASS] Valid maxUint256, second is bigger
1032 [PASS] Valid maxUint256, equal
1033 [PASS] Valid maxUint256, zero
1034
1035
1036 1246 passing (3m)
```