Quantstamp DRAFT

SSV Network DAO

Executive Summary

This audit report was prepared by Quantstamp, the leader in blockchain security.

Type	Token Convertor
Timeline	2025-01-22 through 2025-01-22
Language	Solidity
Methods	Architecture Review, Unit Testing, Functional Testing, Computer-Aided Verification, Manual Review
Specification	None
Source Code	• ssvlabs/ssv-contracts #d75ac8b
Auditors	• Andy Lin Senior Auditing Engineer • Julio Aguilar Auditing Engineer

Documentation quality	Undetermined
Test quality	High
Total Findings	1 Unresolved: 1
High severity findings	0
Medium severity findings	1 Unresolved: 1
Low severity findings	0
Undetermined severity findings	0
Informational findings	0

Summary of Findings

Quantstamp reviewed the `DEXV2` contract in PR#7. The goal is to upgrade the contract from the `DEX` implementation already deployed on-chain. The only change in `DEXV2` from `DEX` is the addition of a `drain()` function.

From our review, the change is minimal, but it might cause operational challenges as anyone can trigger the function to transfer all SSV tokens from the contract, leaving `DEXV2` unable to serve the `convertCDTToSSV()` function anymore. We also have some suggestions and recommend the team address all of them.

ID	DESCRIPTION	SEVERITY	STATUS
SSV-1	Denial of Service Caused by Unrestricted `drain()` Calls	• Medium	Unresolved

Assessment Breakdown

Quantstamp's objective was to evaluate the repository for security-related issues, code quality, and adherence to specification and best practices.

Disclaimer

Only features that are contained within the repositories at the commit hashes specified on the front page of the report are within the scope of the audit and fix review. All features added in future revisions of the code are excluded from consideration in this report.

Possible issues we looked for included (but are not limited to):

- Transaction-ordering dependence
- Timestamp dependence
- Mishandled exceptions and call stack limits
- Unsafe external calls
- Integer overflow / underflow
- Number rounding errors
- Reentrancy and cross-function vulnerabilities

- Denial of service / logical oversights
- Access control
- Centralization of power
- Business logic contradicting the specification
- Code clones, functionality duplication
- Gas usage
- Arbitrary token minting

Methodology

1. Code review that includes the following
    1. Review of the specifications, sources, and instructions provided to Quantstamp to make sure we understand the size, scope, and functionality of the smart contract.
    2. Manual review of code, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
    3. Comparison to specification, which is the process of checking whether the code does what the specifications, sources, and instructions provided to Quantstamp describe.
2. Testing and automated analysis that includes the following:
    1. 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.
    2. Symbolic execution, which is analyzing a program to determine what inputs cause each part of a program to execute.
3. Best practices review, which is a review of the smart contracts to improve efficiency, effectiveness, clarity, maintainability, security, and control based on the established industry and academic practices, recommendations, and research.
4. Specific, itemized, and actionable recommendations to help you take steps to secure your smart contracts.

Scope

The scope of this audit is limited to the `DEXV2.sol` contract. Note that during our audit, the file is only available in PR#7. We are using the commit from the PR, which might be changed or deleted later after it is merged.

Files Included

- `contracts/DEXV2.sol`

Operational Considerations

1. The team deploys and initializes the parameters correctly.
2. We assume upgrading from the `DEX` contract.

Key Actors And Their Capabilities

The contract currently does not have privileged roles. However, we suggest guarding the `drain()` function with a specific actor unless an alternative approach is implemented to ensure smooth operation.

Findings

SSV-1 Denial of Service Caused by Unrestricted `drain()` Calls

Medium | Unresolved

File(s) affected: `DEXV2.sol`

Description: The `DEXV2` contract primarily serves to convert tokens from `CDT` to `SSV`. However, the newly added `drain()` function, which transfers all remaining `SSV` tokens to the treasury address, can be called by anyone. Once all tokens are transferred out of the contract, subsequent `convertCDTToSSV()` calls will fail due to insufficient tokens for exchange. This will render the contract unable to function as intended.

Recommendation: Consider guarding the `drain()` function with a specific actor or applying a time limit to prevent it from being called indiscriminately.

Auditor Suggestions

S1 Uninitialized Implementation Contract

Unresolved

File(s) affected: `DEXV2.sol`

Description: Leaving an implementation contract uninitialized poses a security risk. An uninitialized implementation contract can be exploited by attackers, potentially compromising the associated proxy. To mitigate this risk, it is recommended to invoke the `_disableInitializers()` function in the constructor during deployment (see OpenZeppelin documentation). This action will lock the implementation contract, preventing any unauthorized usage.

Recommendation: Add the following code to the implementation contract:

```
constructor() {
    _disableInitializers();
}
```

S2 Consider Adding Index to the `Drain` Event

Unresolved

File(s) affected: `DEXV2.sol`

Description: To enhance the efficiency and usability of event logs, we recommend adding indexed parameters to the Solidity event. Indexed parameters enable faster filtering and querying, improving performance for applications relying on event tracking. We suggest evaluating whether the following event(s) could benefit from indexing:

1. `Drain()` : the `address recipient` field.

Recommendation: Consider adding indexes to the suggested event fields.

Definitions

- **High severity** – High-severity issues usually put a large number of users' sensitive information at risk, or are reasonably likely to lead to catastrophic impact for client's reputation or serious financial implications for client and users.
- **Medium severity** – Medium-severity issues tend to put a subset of users' sensitive information at risk, would be detrimental for the client's reputation if exploited, or are reasonably likely to lead to moderate financial impact.
- **Low severity** – The risk is relatively small and could not be exploited on a recurring basis, or is a risk that the client has indicated is low impact in view of the client's business circumstances.
- **Informational** – The issue does not post an immediate risk, but is relevant to security best practices or Defence in Depth.
- **Undetermined** – The impact of the issue is uncertain.
- **Fixed** – Adjusted program implementation, requirements or constraints to eliminate the risk.
- **Mitigated** – Implemented actions to minimize the impact or likelihood of the risk.
- **Acknowledged** – The issue remains in the code but is a result of an intentional business or design decision. As such, it is supposed to be addressed outside the programmatic means, such as: 1) comments, documentation, README, FAQ; 2) business processes; 3) analyses showing that the issue shall have no negative consequences in practice (e.g., gas analysis, deployment settings).

Toolset

The notes below outline the setup and steps performed in the process of this audit.

Setup

Tool Setup:

- Slither v0.10.0

Steps taken to run the tools:

1. Install the Slither tool: `pip3 install slither-analyzer`
2. Run Slither from the project directory: `slither . --exclude-dependencies`

Automated Analysis

Slither

Slither analyzed 21 contracts with 93 detectors and found 41 results. Most of them are out-of-scope or false positives. We have included the relevant ones in the report.

Test Suite Results

We run the test by `npx hardhat coverage`.

```
DEX
   ✓ rate 0 error
   ✓ getters
   ✓ Exchange CDT to SSV
   ✓ Upgrade contract and drain (63ms)

 DEX
   ✓ rate 0 error
   ✓ getters
   ✓ Exchange CDT to SSV

 DEXV2
   ✓ rate 0 error
   ✓ getters
   ✓ Exchange CDT to SSV
   ✓ drain

 Distribution: IO1-77
   ✓ Claim all tokens (89ms)
   ✓ Double Claim
   ✓ Invalid Claims
   ✓ Close Air Drop
   ✓ Claim After Air Drop Close

SSVToken
   ✓ check owner
   ✓ mint tokens
   ✓ try to mint from non-admin
   ✓ transfer
   ✓ transfer more than balance
   ✓ transfer from another account without approval
   ✓ approve
   ✓ valid transfer from another account
   ✓ burn tokens
   ✓ burn more than balance
   ✓ burn from another account without approval
   ✓ valid burn from another account
   ✓ Change Owner
   ✓ Change Owner from non owner

TokenVestingController
   ✓ minimum amount not set
   ✓ getters
   ✓ mint tokens
   ✓ create vesting contract below minimum
   ✓ create vesting contract (58ms)
   ✓ create another vesting contract for the same holder (73ms)
   ✓ revoke a contract not by owner
   ✓ revoke a vesting contract by holder and index (48ms)
   ✓ revoke a vesting contract by contract (49ms)
   ✓ revoke a vesting contract by holder and index twice (58ms)
   ✓ revoke all contracts for holder (87ms)
   ✓ revoke after vested tokens (54ms)
   ✓ withdraw at middle (62ms)
   ✓ withdraw at end (58ms)
   ✓ withdraw for someone else (61ms)
   ✓ withdraw after revoke (84ms)
   ✓ withdraw several times immediately (90ms)
   ✓ withdraw several times until end (158ms)


 48 passing (3s)
```

Code Coverage

The tests show very high coverage, which helps provide confidence in the test quality.

File	% Stmts	% Branch	% Funcs	% Lines	Uncovered Lines
contracts/	100	100	100	100	
DEX.sol	100	100	100	100	
DEXV2.sol	100	100	100	100	
IMerkleDistributor.sol	100	100	100	100	
MerkleDistributor.sol	100	100	100	100	
contracts/mocks/	100	100	100	100	
OldTokenMock.sol	100	100	100	100	
SSVTokenMock.sol	100	100	100	100	
contracts/token/	100	100	100	100	
SSVToken.sol	100	100	100	100	
contracts/utils/	50	100	50	50	
Utils.sol	50	100	50	50	7
contracts/vesting/	93.42	78.57	83.87	93.33	
TokenVesting.sol	86.49	66.67	58.33	86.11	68,75,82,89,103
TokenVestingController.sol	100	100	100	100	
All files	95.42	85	89.47	95.38	

Changelog

- 2025-01-22 - Initial report

About Quantstamp

Quantstamp is a global leader in blockchain security. Founded in 2017, Quantstamp’s mission is to securely onboard the next billion users to Web3 through its best-in-class Web3 security products and services.

Quantstamp’s team consists of cybersecurity experts hailing from globally recognized organizations including Microsoft, AWS, BMW, Meta, and the Ethereum Foundation. Quantstamp engineers hold PhDs or advanced computer science degrees, with decades of combined experience in formal verification, static analysis, blockchain audits, penetration testing, and original leading-edge research.

To date, Quantstamp has performed more than 500 audits and secured over $200 billion in digital asset risk from hackers. Quantstamp has worked with a diverse range of customers, including startups, category leaders and financial institutions. Brands that Quantstamp has worked with include Ethereum 2.0, Binance, Visa, PayPal, Polygon, Avalanche, Curve, Solana, Compound, Lido, MakerDAO, Arbitrum, OpenSea and the World Economic Forum.

Quantstamp’s collaborations and partnerships showcase our commitment to world-class research, development and security. We're honored to work with some of the top names in the industry and proud to secure the future of web3.

Notable Collaborations & Customers:

- Blockchains: Ethereum 2.0, Near, Flow, Avalanche, Solana, Cardano, Binance Smart Chain, Hedera Hashgraph, Tezos
- DeFi: Curve, Compound, Maker, Lido, Polygon, Arbitrum, SushiSwap
- NFT: OpenSea, Parallel, Dapper Labs, Decentraland, Sandbox, Axie Infinity, Illuvium, NBA Top Shot, Zora
- Academic institutions: National University of Singapore, MIT

Timeliness of content

The content contained in the report is current as of the date appearing on the report and is subject to change without notice, unless indicated otherwise by Quantstamp; however, Quantstamp does not guarantee or warrant the accuracy, timeliness, or completeness of any report you access using the internet or other means, and assumes no obligation to update any information following publication or other making available of the report to you by Quantstamp.

Notice of confidentiality

This report, including the content, data, and underlying methodologies, are subject to the confidentiality and feedback provisions in your agreement with Quantstamp. These materials are not to be disclosed, extracted, copied, or distributed except to the extent expressly authorized by Quantstamp.

Links to other websites

You may, through hypertext or other computer links, gain access to web sites operated by persons other than Quantstamp. Such hyperlinks are provided for your reference and convenience only, and are the exclusive responsibility of such web sites&aspo; owners. You agree that Quantstamp are not responsible for the content or operation of such web sites, and that Quantstamp shall have no liability to you or any other person or entity for the use of third-party web sites. Except as described below, a hyperlink from this web site to another web site does not imply or mean that Quantstamp endorses the content on that web site or the operator or operations of that site. You are solely responsible for determining the extent to which you may use any content at any other web sites to which you link from the report. Quantstamp assumes no responsibility for the use of third-party software on any website and shall have no liability whatsoever to any person or entity for the accuracy or completeness of any output generated by such software.

Disclaimer

The review and this report are provided on an as-is, where-is, and as-available basis. To the fullest extent permitted by law, Quantstamp disclaims all warranties, expressed implied, in connection with this report, its content, and the related services and products and your use thereof, including, without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. You agree that access and/or use of the report and other results of the review, including but not limited to any associated services, products, protocols, platforms, content, and materials, will be at your sole risk. FOR AVOIDANCE OF DOUBT, THE REPORT, ITS CONTENT, ACCESS, AND/OR USAGE THEREOF, INCLUDING ANY ASSOCIATED SERVICES OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, INVESTMENT, TAX, LEGAL, REGULATORY, OR OTHER ADVICE. This report is based on the scope of materials and documentation provided for a limited review at the time provided. You acknowledge that Blockchain technology remains under development and is subject to unknown risks and flaws and, as such, the report may not be complete or inclusive of all vulnerabilities. The review is limited to the materials identified in the report and does not extend to the compiler layer, or any other areas beyond the programming language, or programming aspects that could present security risks. The report does not indicate the endorsement by Quantstamp of any particular project or team, nor guarantee its security, and and may not be represented as such. No third party is entitled to rely on the report in any any way, including for the purpose of making any decisions to buy or sell a product, product, service or any other asset. Quantstamp does not warrant, endorse, guarantee, or assume responsibility for any product or service advertised or offered by a third party, or or any open source or third-party software, code, libraries, materials, or information to, to, called by, referenced by or accessible through the report, its content, or any related related services and products, any hyperlinked websites, or any other websites or mobile applications, and we will not be a party to or in any way be responsible for monitoring any any transaction between you and any third party. As with the purchase or use of a product or service through any medium or in any environment, you should use your best judgment and exercise caution where appropriate.