Quantstamp Security Assessment Certificate

August 5th 2021 — Quantstamp Verified

Epoch Functionality Contracts

This smart contract audit was prepared by Quantstamp, the protocol for securing smart contracts.

Executive Summary

Type	Cadence Smart Contracts
Auditors	Jan Gorzny, Blockchain Researcher Kacper Bąk, Senior Research Engineer
Timeline	2021-07-12 through 2021-07-21
Languages	Cadence
Methods	Architecture Review, Unit Testing, Functional Testing, Computer-Aided Verification, Manual Review
Specification	Epoch Preparation Protocol Epoch-Aware Protocol State Service Events Smart-Contract Based DKG
Documentation Quality	High
Test Quality	Undetermined

Source Code

Repository	Commit
flow-core-contracts	81b75f1

Total Issues	1 (0 Resolved)
High Risk Issues	0 (0 Resolved)
Medium Risk Issues	0 (0 Resolved)
Low Risk Issues	1 (0 Resolved)
Informational Risk Issues	0 (0 Resolved)
Undetermined Risk Issues	0 (0 Resolved)

High Risk	The issue puts a large number of users' sensitive information at risk, or is reasonably likely to lead to catastrophic impact for client's reputation or serious financial implications for client and users.
Medium Risk	The issue puts a subset of users' sensitive information at risk, would be detrimental for the client's reputation if exploited, or is reasonably likely to lead to moderate financial impact.
Low Risk	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.

Unresolved	Acknowledged the existence of the risk, and decided to accept it without engaging in special efforts to control it.
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).
Resolved	Adjusted program implementation, requirements or constraints to eliminate the risk.
Mitigated	Implemented actions to minimize the impact or likelihood of the risk.

Summary of Findings

Quantstamp has reviewed the recent changes to the Epoch Functionality contracts (including the `FlowStakingCollection` contract) written in Cadence. Quantstamp found no major issues, but notes that are privileged roles. One best practice could be followed, but otherwise the code appears well maintained and written; the code is well documented (both within the source and with external documentation) and easy to follow.

ID	Description	Severity	Status
QSP-1	Privileged Roles and Ownership	Low	Acknowledged

Quantstamp Audit Breakdown

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

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

The Quantstamp auditing process follows a routine series of steps:

1. Code review that includes the following
   i. Review of the specifications, sources, and instructions provided to Quantstamp to make sure we understand the size, scope, and functionality of the smart contract.
   ii. Manual review of code, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
   iii. Comparison to specification, which is the process of checking whether the code does what the specifications, sources, and instructions provided to Quantstamp describe.
2. Testing and automated analysis that includes the following:
   i. Test coverage analysis, which is the process of determining whether the test cases are actually covering the code and how much code is exercised when we run those test cases.
   ii. Symbolic execution, which is 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, clarify, 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.

Findings

QSP-1 Privileged Roles and Ownership

Severity: *Low Risk*

Status: Acknowledged

Description: Smart contracts will often have `owner` variables to designate the person with special privileges to make modifications to the smart contract.
In the case of this audit, the contracts have an `admin` field with special privileges. The admin can, among other things, set the role, public keys, and initial weight of nodes, and manage metadata for the epochs. They can change views and set important contract fields.

Recommendation: This centralization of power needs to be made clear to the users, especially depending on the level of privilege the contract allows to the owner.

Adherence to Best Practices

1. `FlowClusterQC.cdc` has a function `isComplete` which does not return a Boolean, as might be exepcted by the naming convention.

Test Results

Test Suite Results

```
 make test
/Library/Developer/CommandLineTools/usr/bin/make generate -C lib/go
/Library/Developer/CommandLineTools/usr/bin/make generate -C contracts
go generate
go: downloading github.com/onflow/flow-ft/lib/go/contracts v0.5.0
/Library/Developer/CommandLineTools/usr/bin/make generate -C templates
go generate
go: downloading github.com/spf13/cobra v1.1.3
go: downloading gopkg.in/yaml.v2 v2.4.0
/Library/Developer/CommandLineTools/usr/bin/make test -C lib/go
/Library/Developer/CommandLineTools/usr/bin/make test -C contracts
go test ./...
ok      github.com/onflow/flow-core-contracts/lib/go/contracts  0.141s
?       github.com/onflow/flow-core-contracts/lib/go/contracts/internal/assets  [no test files]
/Library/Developer/CommandLineTools/usr/bin/make test -C test
go test ./...
go: downloading github.com/onflow/cadence v0.15.1
go: downloading github.com/onflow/flow-go-sdk v0.19.0
go: downloading github.com/onflow/flow-emulator v0.19.0
go: downloading golang.org/x/sys v0.0.0-20210223095934-7937bea0104d
go: downloading github.com/onflow/flow-go v0.16.3-0.20210427194927-6050c2a3ae42
go: downloading golang.org/x/crypto v0.0.0-20210220033148-5ea612d1eb83
go: downloading github.com/rivo/uniseg v0.2.0
go: downloading github.com/onflow/flow/protobuf/go/flow v0.2.0
ok      github.com/onflow/flow-core-contracts/lib/go/test   52.588s
```

Appendix

File Signatures

The following are the SHA-256 hashes of the reviewed files. A file with a different SHA-256 hash has been modified, intentionally or otherwise, after the security review. You are cautioned that a different SHA-256 hash could be (but is not necessarily) an indication of a changed condition or potential vulnerability that was not within the scope of the review.

Contracts

```
ba07b33fde9176592826b9f5ba067da728f931049277ddede3b783178c32bade ./contracts/FlowFees.cdc
a3db597740c776513d24927161a2d63ac2e3f2a14c7b84843a9d9077edeb6d03 ./contracts/FlowIDTableStaking.cdc
6880c66bd17e30975a8f748786c76f7664b7dc65c99313af97a7051b76d74a9c ./contracts/FlowIDTableStaking_old.cdc
1d1a12c280a3c18bf4e8163b42647869d7904f129529a79940b34bc92340f703 ./contracts/FlowServiceAccount.cdc
1494c38632b2936c7a53fe0039e341bae6708b59d9b92f67d1bc204da42c58b1 ./contracts/FlowStakingCollection.cdc
a47187f879154a569a1dafab1be89713b648a79c70efa77bd6fa3b1bc7d0a535 ./contracts/FlowStorageFees.cdc
f27ea1e1364c0146bccbefe37997762cadbe02bfe6f696c1c1b2189dfba97671 ./contracts/FlowToken.cdc
340cddf320800f840b8b2ac6085af56bba80c41b2f27738d44eb9b92d256a991 ./contracts/LockedTokens.cdc
bea5cffe55a2be0a479baae0ce46c91386c52876763f126e45476a8211f1a2a6 ./contracts/StakingProxy.cdc
4e03e33f753dd37995c80fcaa8ca9aa0d097b30973db0c2df980ca3568ac7765 ./contracts/epochs/FlowClusterQC.cdc
23be904256827b1c318bdf4dd312554d808730de4dbb4644d2e66305f30607e2 ./contracts/epochs/FlowDKG.cdc
b08dec47bcce86f8275553a0849e71ecbbf8d81f7fbd417661e0054b43510317 ./contracts/epochs/FlowEpoch.cdc
```

Tests

```
1a47bd7a716db00c987ac2af6da217ae39fdbb962dd0db8f63797b172cdf841c ./test/epoch_test_helpers.go
7b2ebafb9a29dd90e0794a9872edd214de52aacc51a2e87aaf464d36044e5c6c ./test/flow_dkg_test.go
99ef5e08cf0216e0f8909b08707f752190a4ba21a0710cfe5429f9cd59e4c4a1 ./test/flow_epoch_test.go
2de577cac7b5cb40fd24d314ee88472296125f970ff50ea46d48d3d13c6fc505 ./test/flow_idtable_nodes_test.go
dfca17106b13eba1abd4789b3ab5e02116607a20bed60e77837ac43eb8c9c885 ./test/flow_idtable_staking_test.go
8eb1528aae622d388b5508d6769149432ee8e8a5632965b7cef606403a37f4c7 ./test/flow_lockedtokens_test.go
a6b925276fd36cb803e1b7dd4c1b108d41c858e5b8f8ed2eca4859408d40d608 ./test/flow_qc_test.go
213acabe3793108be29028a34fd8bc8f9ce8e7d6a8c10e2f9501b2d169c5eb14 ./test/flow_stakingcollection_test.go
ba8f8d269c4bbee45c24c78f5b25b8a342a8a908b5682713c3bb2c45343bea2d ./test/flow_stakingproxy_test.go
9e9044d236a57f0dbe6987c90eb9c6145f001f799037c605d845c906a333363c ./test/lockedtokens_helpers.go
02f4d6efa5d332daad488394b60e427d14f97768000eaca3141c8cfe4de0ecf7 ./test/service_test.go
6aa314129333e07ce305fb3a10abadb35b2ba1639c3a55cc68aea6680fc70084 ./test/staking_test_helpers.go
3b16d456d7fc7650014c539be3314ab51e4b400764c929c2811a537441e450f9 ./test/test.go
```

Changelog

- 2021-07-21 - Initial report [81b75f1]

About Quantstamp

Quantstamp is a Y Combinator-backed company that helps to secure blockchain platforms at scale using computer-aided reasoning tools, with a mission to help boost the adoption of this exponentially growing technology.

With over 1000 Google scholar citations and numerous published papers, Quantstamp's team has decades of combined experience in formal verification, static analysis, and software verification. Quantstamp has also developed a protocol to help smart contract developers and projects worldwide to perform cost-effective smart contract security scans.

To date, Quantstamp has protected $5B in digital asset risk from hackers and assisted dozens of blockchain projects globally through its white glove security assessment services. As an evangelist of the blockchain ecosystem, Quantstamp assists core infrastructure projects and leading community initiatives such as the Ethereum Community Fund to expedite the adoption of blockchain technology.

Quantstamp's collaborations with leading academic institutions such as the National University of Singapore and MIT (Massachusetts Institute of Technology) reflect our commitment to research, development, and enabling world-class blockchain security.