



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 Bqk, 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	<div style="width: 100%; height: 10px; background: linear-gradient(to right, #007bff, #007bff);"></div> High				
Test Quality	<div style="width: 100%; height: 10px; background: linear-gradient(to right, #007bff, #007bff);"></div> Undetermined				
Source Code	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 50%;">Repository</th> <th style="width: 50%;">Commit</th> </tr> </thead> <tbody> <tr> <td><a href="#">flow-core-contracts</a></td> <td><a href="#">81b75f1</a></td> </tr> </tbody> </table>	Repository	Commit	<a href="#">flow-core-contracts</a>	<a href="#">81b75f1</a>
Repository	Commit				
<a href="#">flow-core-contracts</a>	<a href="#">81b75f1</a>				

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)



<b>High Risk</b>	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.
<b>Medium Risk</b>	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.
<b>Low Risk</b>	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.
<b>Informational</b>	The issue does not post an immediate risk, but is relevant to security best practices or Defence in Depth.
<b>Undetermined</b>	The impact of the issue is uncertain.
<b>Unresolved</b>	Acknowledged the existence of the risk, and decided to accept it without engaging in special efforts to control it.
<b>Acknowledged</b>	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).
<b>Resolved</b>	Adjusted program implementation, requirements or constraints to eliminate the risk.
<b>Mitigated</b>	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 expected 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
- f27ea1e1364c0146bccbefef37997762cadbe02bfe6f696c1c1b2189dfba97671 ./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
- ba8f8d269c4bbe45c24c78f5b25b8a342a8a908b5682713c3bb2c45343bea2d ./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.

### 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.

### 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, Inc. (Quantstamp). Such hyperlinks are provided for your reference and convenience only, and are the exclusive responsibility of such web sites' 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 the website and shall have no liability whatsoever to any person or entity for the accuracy or completeness of any outcome generated by such software.

### Disclaimer

This report is based on the scope of materials and documentation provided for a limited review at the time provided. Results may not be complete nor inclusive of all vulnerabilities. The review and this report are provided on an as-is, where-is, and as-available basis. You agree that your access and/or use, including but not limited to any associated services, products, protocols, platforms, content, and materials, will be at your sole risk. Blockchain technology remains under development and is subject to unknown risks and flaws. The review does not extend to the compiler layer, or any other areas beyond the programming language, or other programming aspects that could present security risks. A report does not indicate the endorsement of any particular project or team, nor guarantee its security. No third party should rely on the reports in any way, including for the purpose of making any decisions to buy or sell a product, service or any other asset. To the fullest extent permitted by law, we disclaim all warranties, expressed or 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. We do not warrant, endorse, guarantee, or assume responsibility for any product or service advertised or offered by a third party through the product, any open source or third-party software, code, libraries, materials, or information linked to, called by, referenced by or accessible through the report, its content, and the related services and products, any hyperlinked websites, any websites or mobile applications appearing on any advertising, and we will not be a party to or in any way be responsible for monitoring any transaction between you and any third-party providers of products or services. 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. 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.