Quantstamp Security Assessment Certificate

QUANTSTAMP VERIFIED SECURITY CERTIFICATE

October 16th 2020 — Quantstamp Verified

Dock Network

This security assessment was prepared by Quantstamp, the leader in blockchain security

Executive Summary

Type	Substrate-Based Blockchain + SDK
Auditors	Shunsuke Tokoshima, Software Engineer Alex Murashkin, Senior Software Engineer Luís Fernando Schultz Xavier da Silveira, Security Consultant
Timeline	2020-09-14 through 2020-10-16
Languages	Rust, Javascript
Methods	Architecture Review, Unit Testing, Functional Testing, Computer-Aided Verification, Manual Review
Specification	Dock documentation Dock DID method specification Dock SDK Tutorial
Documentation Quality	High
Test Quality	Medium

Source Code

Repository	Commit
dock-substrate	bbdc31a
sdk	3d5b79a

Total Issues	**15** (8 Resolved)
High Risk Issues	0 (0 Resolved)
Medium Risk Issues	**4** (2 Resolved)
Low Risk Issues	**9** (6 Resolved)
Informational Risk Issues	**2** (0 Resolved)
Undetermined Risk Issues	0 (0 Resolved)

0 Unresolved
7 Acknowledged
8 Resolved

FAST RESPONSE TIMES

ALL ISSUES ADDRESSED

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

This report contains the results of our assessment of Dock Network's Substrate-based blockchain and the corresponding SDK.

When reviewing the code, we found **15 potential issues** of various levels of severity: four medium, nine low, and two informational severity. Of significant concern, we have identified a risk to system functionality, a few risks that the root entity may misunderstand the effect of their transactions on the blockchain, and a few risks regarding storage on the chain. Examples of less significant concerns include lack of input validation, unexpected behavior, and potential for excessive reward emissions and incorrect number handling in the SDK.

In addition, we have also identified multiple places in which the code may not meet its specification and some documentation problems. The details are in the corresponding sections. We made **20 best practices suggestions** on how to apply best practices to the code and raise some points worth additional consideration.

The code, overall, looks to be well-written. However, some areas of the code are not very intuitive. For example, the code of the POA pallet is not very well organized. The functions do not have a clear abstraction boundary and interact with storage in non-obvious ways. This, combined with the complexity of the Substrate framework, makes it difficult to establish the full correctness of the code.

And finally, we measured test coverage of the pallets and runtime items of the Substrate portion of the audit. While the test coverage, in terms of lines, is high, some improvement would be beneficial.

We recommend addressing the findings before using in production.

Udpate: Most findings have been marked as addressed or acknowledged. The outstanding items include `QSP-10` (partially fixed) and several best practices recommendations.
Udpate: All issues have been addressed.

ID	Description	Severity	Status
QSP-1	Denial-of-Service (DoS)	^ Medium	Acknowledged
QSP-2	Unexpected behavior of the queue of validators	^ Medium	Fixed
QSP-3	`AllowDeath` for treasury transfers	^ Medium	Acknowledged
QSP-4	Lack of TLS enforcement in the SDK	^ Medium	Fixed
QSP-5	Potentially incorrect method visibility modifier	⌄ Low	Fixed
QSP-6	Potentially incorrect handling of big numbers in the SDK	⌄ Low	Acknowledged
QSP-7	Excessive rewards	⌄ Low	Fixed
QSP-8	Lack of re-entrancy guard	⌄ Low	Acknowledged
QSP-9	No input validation on DID's controller	⌄ Low	Acknowledged
QSP-10	Insufficient test coverage	⌄ Low	Fixed
QSP-11	Epoch and validator stats not updated in certain cases	⌄ Low	Fixed
QSP-12	Unexpected weight	⌄ Low	Fixed
QSP-13	Unexpected behavior of `swap_validator()`	⌄ Low	Fixed
QSP-14	`u32` range potentially insufficient	○ Informational	Acknowledged
QSP-15	Insufficient error handling	○ Informational	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.

Toolset

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

Setup

Tool Setup:

- Rust-Clippy Latest
- Tarpaulin 0.14.2
- Rust Audit v0.12.0
- Sonar-JS Latest

Steps taken to run the tools:

1. `rustup component add clippy`
2. `cargo clippy`
3. `cargo install cargo-tarpaulin` (on a Linux environment)
4. `cargo tarpaulin --verbose -o=Html --output-dir='..'`
5. `cargo install cargo-audit`
6. `cargo audit`
7. `npm install eslint-plugin-sonarjs@0.5.0`

Findings

QSP-1 Denial-of-Service (DoS)

Severity: *Medium Risk*

Status: Acknowledged

File(s) affected: `dock-substrate/runtime/src/did.rs`

Description: A Denial-of-Service (DoS) attack is a situation which an attacker renders a service unusable. In this case, a spiteful agent can perform a denial of service attack against a target by “squatting” DIDs, i.e., by making a request for a DID with a slightly larger transaction fee whenever the target requests it. If the validators are oblivious to this behavior, they might repeatedly include the attacker's transaction first, denying the legitimate user's transaction. This is worse if validators sort transactions by their fees. Furthermore, the attacker spends only about as much as the target is wasting with erring transactions.

Recommendation: It is recommended to evaluate the possibility of this attack. We do not have a specific recommendation at the moment.
Update: According to the Dock Network team, there is no incentive in performing the attack because the vanity DIDs (such as “JohnSmith123” or “USAGov09") are not considered valuable.

QSP-2 Unexpected behavior of the queue of validators

Severity: *Medium Risk*

Status: Fixed

File(s) affected: `dock-substrate/pallets/poa/src/lib.rs`

Description: The comment at L664 is actually not accurate because of hot swaps. Due to the code in the `else` branch at L663 not being outside the `if` branch, a validator marked for removal may remain queued and even be inserted in the same function call at L685.

Recommendation: The behaviors of removals and swaps should be orthogonal: a previous swap-in should not allow removed validators to remain queued.

Update: The Dock Network team has updated the code comments to explain the behavior as of the commit `620daed`.

QSP-3 `AllowDeath` for treasury transfers

Severity: *Medium Risk*

Status: Acknowledged

File(s) affected: `dock-substrate/pallets/poa/lib.rs`

Description: In `dock-substrate/pallets/poa/lib.rs`. The treasury account may be erased in `withdraw_from_treasury_` due to `AllowDeath`.

Recommendation: Checking if the behavior is desired.

Update: The Dock Network team has added a comment to explain the behavior as of the commit `620daed`. It reads "AllowDeath is fine as the account would be back in state when it gets rewards"

QSP-4 Lack of TLS enforcement in the SDK

Severity: *Medium Risk*

Status: Fixed

Description: The SDK does not require TLS(wss://) for websocket connections. If the code allows HTTP or WS and does not complain, it could expose sensitive data to MITM attacks.

Recommendation: It is recommended to ensure websocket connections to be encrypted with TLS protocol.

Update: A functionality to warn users in case that the endpoint's address does not begin with 'wss://' has been inplemented as of the commit `620daed`.

QSP-5 Potentially incorrect method visibility modifier

Severity: *Low Risk*

Status: Fixed

File(s) affected: `dock-substrate/pallets/poa/src/lib.rs`

Description: `withdraw_from_treasury_()` is declared as a public function. The purpose of doing so is unclear. If the `pub` access control modifier allows the method to be called in public, a malicious user could invoke this function bypassing the check `ensure_root(origin)?;` and transfer the asset to an arbitrary destination.

Recommendation: It is recommended to remove `pub` keyword of the function.

Update: Addressed as of the commit `620daed`.

QSP-6 Potentially incorrect handling of big numbers in the SDK

Severity: Low Risk

Status: Acknowledged

File(s) affected: sdk/scripts/queries.js, sdk/scripts/master_voting/submit.js, etc.

Description: The SDK handles u64 values such as Balance, vote_requirement, round_no, and SlotNo as Int in Javascript. However, Javascript Number type can only handle integers up to 2^53 - 1, which is not suitable for handling u64 value.

Recommendation: It is recommended to use string or BigNumber types for handling such values. Also, it would be safer to check for integer overflow/underflow.

Update: The Dock Network team has recognized issue. They have prioritized it as low because the scripts are still experimental.

QSP-7 Excessive rewards

Severity: Low Risk

Status: Fixed

File(s) affected: dock-substrate/pallets/poa/src/lib.rs

Description: In L1014, block_count > slots_per_validatorpossibly happens. In that case rewards could be more than max_em.

Recommendation: It is recommended to check if this behaviour is desired.

Update: Fixed as of the commit 620daed.

QSP-8 Lack of re-entrancy guard

Severity: Low Risk

Status: Acknowledged

File(s) affected: dock-substrate/runtime/src/master.rs

Description: A reentrancy vulnerability is a scenario where an attacker can repeatedly call a function from itself, unexpectedly leading to potentially disastrous results. It is, in theory, possible to re-enter execute_method in dock-substrate/runtime/src/master.rs through dispatching it. However, considering that the caller of the method (of the Master role) as a whole is assumed to be non-malicious, the risk is estimated to be low.

Recommendation: As a general best practice, it is recommended to increment rounds(nonces) after a call is dispatched.

Update: Acknowledged. The Dock Network team have added some comments explaining why the risk is negligible in L233-238.

QSP-9 No input validation on DID's controller

Severity: Low Risk

Status: Acknowledged

File(s) affected: dock-substrate/runtime/src/did.rs

Description: There is currently no restriction on what controller DID could be. It could be the did itself, an arbitrary DID, or a non-existent DID.

Recommendation: It is recommended to clarify the intention and add input validation in the blockchain layer as necessary.

Update: Acknowledged. The Dock Network team have added some comments explaining why it is not validated in L326-327 and L343-344.

QSP-10 Insufficient test coverage

Severity: Low Risk

Status: Fixed

Description: It would be beneficial to improve the test coverage. For example:

1. Tests confirming that only a migrator can do the migration.
2. Tests for current_slot_no() in pallets/poa/src/lib.rs. In case it returns None, Substrate runtime would panic, therefore, would be good to have a test coverage for this method, to confirm its expected behavior and edge cases.

QSP-11 Epoch and validator stats not updated in certain cases

Severity: Low Risk

Status: Fixed

File(s) affected: `dock-substrate/pallets/poa/src/lib.rs`

Description: In case that `emission_status` is `false` or `emission_supply == 0`, `EpochDetail` and `ValidatorStats` are not updated. However, although the severity of the risk is high, it is commented that "Emission is enabled, move on" in `L1119`, the overall risk is estimated to be low.

Recommendation: If desired, it is recommended to add some logic to update `EpochDetail` and `ValidatorStats`to if-branches for the cases of `!Self::emission_status()` and `emission_supply == 0`.

Update: Addressed as of the commit `620daed`.

QSP-12 Unexpected weight

Severity: *Low Risk*

Status: Fixed

File(s) affected: `dock-substrate/runtime/src/did.rs`

Description: `DidSignature::Secp256k1(_) => SR25519_WEIGHT,` in `L179` is mistyped.

Recommendation: It is recommended to replace the line with `DidSignature::Secp256k1(_) => SECP256K1_WEIGHT,`.

Update: Fixed as of the commit `620daed`.

QSP-13 Unexpected behavior of `swap_validator()`

Severity: *Low Risk*

Status: Fixed

File(s) affected: `dock-substrate/pallets/poa/src/lib.rs`

Description: If two or more `swap_validator()` transactions are placed in the same block, only the last swap will be performed even though multiple events will be emitted.

Recommendation: We recommend the root account user to be conscious of this behavior.

Update: Addressed as of the commit `620daed`.

QSP-14 `u32` range potentially insufficient

Severity: *Informational*

Status: Acknowledged

File(s) affected: `runtime/src/lib.rs`

Description: In `runtime/src/lib.rs`, it is conceivable that the blockchain will reach its end since `BlockNumber` is `u32`. At the same time, `Index`, the transaction index, is `u32`, which may cause issues if the blockchain is heavily used.

Recommendation: Checking if this hard-limit is expected.

Update: From the Dock Network team: "Not changing: Assuming a minimum block time of 3 seconds, a 32 byte block number should let us run for over 408 years ((2^32 - 1)*3 / (3600*24*365)), so should be sufficient."

QSP-15 Insufficient error handling

Severity: *Informational*

Status: Acknowledged

File(s) affected: `dock-substrate/pallets/poa/src/lib.rs`

Description: In Substrate, the runtime may never panic. However, in `L791`, a panic will occur if `current_slot_no()` returns None. This is particularly concerning since there is an assumption documented in `L772`. Furthermore, if this function doesn't return monotonic results, there is a risk of underflow at `L802`.

Update: From the Dock Network team: "We have a couple of places where we panic but those areas of code should never have been reached". Additionally, "`current_slot_no` is only `None` when no block under processing like when network starting and it is set in `block initialize` (`on_initialize`). We checked and there is a block being processed whenever we fetch it (after `on_initialize`)."

Automated Analyses

Rust-Clippy

Some minor warnings (e.g. `redundant clone`, `useless conversion to the same type`) were raised for `dock-substrate`. The full output is below:

```
warning: using `clone` on a `Copy` type
   --> runtime/src/did.rs:517:42
    |
517 |                 let pk = sr25519::Public(bytes.value.clone());
    |                                          ^^^^^^^^^^^^^^^^^^^ help: try removing the `clone` call:
`bytes.value`
    |
    = note: `#[warn(clippy::clone_on_copy)]` on by default
    = help: for further information visit https://rust-lang.github.io/rust-
clippy/master/index.html#clone_on_copy

warning: using `clone` on a `Copy` type
   --> runtime/src/did.rs:527:42
    |
527 |                 let pk = ed25519::Public(bytes.value.clone());
    |                                          ^^^^^^^^^^^^^^^^^^^ help: try removing the `clone` call:
`bytes.value`
    |
    = help: for further information visit https://rust-lang.github.io/rust-
clippy/master/index.html#clone_on_copy

warning: using `clone` on a `Copy` type
   --> runtime/src/did.rs:537:50
    |
537 |                 let pk = ecdsa::Public::from_raw(bytes.value.clone());
    |                                                  ^^^^^^^^^^^^^^^^^^^ help: try removing the `clone`
call: `bytes.value`
    |
    = help: for further information visit https://rust-lang.github.io/rust-
clippy/master/index.html#clone_on_copy

warning: useless conversion to the same type
   --> runtime/src/master.rs:254:13
    |
254 |             proposal.into(),
    |             ^^^^^^^^^^^^^^^ help: consider removing `.into()`: `proposal`
    |
    = note: `#[warn(clippy::useless_conversion)]` on by default
    = help: for further information visit https://rust-lang.github.io/rust-
clippy/master/index.html#useless_conversion

warning: 4 warnings emitted

    Checking dock-node v0.1.0 (/home/ubuntu/dock-substrate/node)
warning: redundant clone
  --> node/src/rpc.rs:55:15
   |
55 |         client.clone(),
   |               ^^^^^^^^ help: remove this
   |
   = note: `#[warn(clippy::redundant_clone)]` on by default
note: this value is dropped without further use
  --> node/src/rpc.rs:55:9
   |
55 |         client.clone(),
   |         ^^^^^^
   = help: for further information visit https://rust-lang.github.io/rust-
clippy/master/index.html#redundant_clone

warning: very complex type used. Consider factoring parts into `type` definitions
  --> node/src/service.rs:30:6
   |
30 |   ) -> Result<
   |  ______^
31 | |     sc_service::PartialComponents<
32 | |         FullClient,
33 | |         FullBackend,
...  |
47 | |     ServiceError,
48 | | > {
   | |_^
   |
   = note: `#[warn(clippy::type_complexity)]` on by default
   = help: for further information visit https://rust-lang.github.io/rust-
clippy/master/index.html#type_complexity

warning: redundant clone
   --> node/src/service.rs:127:66
    |
127 |             finality_proof_provider: Some(finality_proof_provider.clone()),
    |                                                                  ^^^^^^^^ help: remove this
    |
note: this value is dropped without further use
   --> node/src/service.rs:127:43
    |
127 |             finality_proof_provider: Some(finality_proof_provider.clone()),
    |                                           ^^^^^^^^^^^^^^^^^^^^^^^
    = help: for further information visit https://rust-lang.github.io/rust-
clippy/master/index.html#redundant_clone

warning: 3 warnings emitted

warning: redundant clone
  --> node/src/rpc.rs:55:15
   |
55 |         client.clone(),
   |               ^^^^^^^^ help: remove this
   |
   = note: `#[warn(clippy::redundant_clone)]` on by default
note: this value is dropped without further use
```

```
  --> node/src/rpc.rs:55:9
   |
55 |         client.clone(),
   |         ^^^^^^
   = help: for further information visit https://rust-lang.github.io/rust-
clippy/master/index.html#redundant_clone

warning: very complex type used. Consider factoring parts into `type` definitions
  --> node/src/service.rs:30:6
   |
30 |   ) -> Result<
   |  ______^
31 | |     sc_service::PartialComponents<
32 | |         FullClient,
33 | |         FullBackend,
...  |
47 | |     ServiceError,
48 | | > {
   | |_^
   |
   = note: `#[warn(clippy::type_complexity)]` on by default
   = help: for further information visit https://rust-lang.github.io/rust-
clippy/master/index.html#type_complexity

warning: redundant clone
   --> node/src/service.rs:127:66
    |
127 |             finality_proof_provider: Some(finality_proof_provider.clone()),
    |                                                                  ^^^^^^^^ help: remove this
    |
note: this value is dropped without further use
   --> node/src/service.rs:127:43
    |
127 |             finality_proof_provider: Some(finality_proof_provider.clone()),
    |                                           ^^^^^^^^^^^^^^^^^^^^^^^
    = help: for further information visit https://rust-lang.github.io/rust-
clippy/master/index.html#redundant_clone

warning: 3 warnings emitted

    Finished dev [unoptimized + debuginfo] target(s) in 2m 00s
```

Rust Audit

Rust-audit identified a vulnerable crate. However, it was found to be false-positive.

Sonar-JS

Sonar-JS made several findings. All of the items are of the "Code Smell" category and no bugs were detected.

```
docknetwork/sdk/example/blob.js
  27:21  error  Immediately return this expression instead of assigning it to the temporary variable
"chainBlob"  sonarjs/prefer-immediate-return
docknetwork/sdk/example/dock-did.js
  35:23  error  Immediately return this expression instead of assigning it to the temporary variable
"transaction"  sonarjs/prefer-immediate-return
  54:23  error  Immediately return this expression instead of assigning it to the temporary variable
"transaction"  sonarjs/prefer-immediate-return
  77:23  error  Immediately return this expression instead of assigning it to the temporary variable
"transaction"  sonarjs/prefer-immediate-return
docknetwork/sdk/example/standard_schemas.js
   15:5   error  Define a constant instead of duplicating this literal 7 times  sonarjs/no-duplicate-string
   16:5   error  Define a constant instead of duplicating this literal 6 times  sonarjs/no-duplicate-string
   28:14  error  Define a constant instead of duplicating this literal 7 times  sonarjs/no-duplicate-string
   94:17  error  Define a constant instead of duplicating this literal 5 times  sonarjs/no-duplicate-string
  126:5   error  Define a constant instead of duplicating this literal 4 times  sonarjs/no-duplicate-string
  129:7   error  Define a constant instead of duplicating this literal 4 times  sonarjs/no-duplicate-string
  136:12  error  Define a constant instead of duplicating this literal 4 times  sonarjs/no-duplicate-string
  181:20  error  Define a constant instead of duplicating this literal 3 times  sonarjs/no-duplicate-string
  183:18  error  Define a constant instead of duplicating this literal 3 times  sonarjs/no-duplicate-string
  184:24  error  Define a constant instead of duplicating this literal 3 times  sonarjs/no-duplicate-string
docknetwork/sdk/src/api.js
  195:20  error  Immediately return this expression instead of assigning it to the temporary variable "result"
sonarjs/prefer-immediate-return
docknetwork/sdk/src/modules/schema.js
  174:22  error  Immediately return this expression instead of assigning it to the temporary variable "schema"
sonarjs/prefer-immediate-return
docknetwork/sdk/src/utils/vc/contexts/credential-v1-updated.js
   19:15  error  Define a constant instead of duplicating this literal 4 times   sonarjs/no-duplicate-string
   20:14  error  Define a constant instead of duplicating this literal 11 times  sonarjs/no-duplicate-string
   21:14  error  Define a constant instead of duplicating this literal 5 times   sonarjs/no-duplicate-string
   41:66  error  Define a constant instead of duplicating this literal 15 times  sonarjs/no-duplicate-string
   98:20  error  Define a constant instead of duplicating this literal 5 times   sonarjs/no-duplicate-string
   99:27  error  Define a constant instead of duplicating this literal 5 times   sonarjs/no-duplicate-string
  100:17  error  Define a constant instead of duplicating this literal 5 times   sonarjs/no-duplicate-string
  101:27  error  Define a constant instead of duplicating this literal 5 times   sonarjs/no-duplicate-string
  105:18  error  Define a constant instead of duplicating this literal 5 times   sonarjs/no-duplicate-string
  116:39  error  Define a constant instead of duplicating this literal 5 times   sonarjs/no-duplicate-string
  117:38  error  Define a constant instead of duplicating this literal 5 times   sonarjs/no-duplicate-string
  120:21  error  Define a constant instead of duplicating this literal 5 times   sonarjs/no-duplicate-string
  121:38  error  Define a constant instead of duplicating this literal 5 times   sonarjs/no-duplicate-string
docknetwork/sdk/src/utils/vc/contexts/did-v1-updated.js
  38:46  error  Define a constant instead of duplicating this literal 3 times  sonarjs/no-duplicate-string
docknetwork/sdk/src/utils/vc/document-loader.js
  11:16  warning  Unexpected unnamed function  func-names
docknetwork/sdk/src/utils/vc/schemas/schema-draft-07.js
   17:17  error  Define a constant instead of duplicating this literal 4 times  sonarjs/no-duplicate-string
   92:24  error  Define a constant instead of duplicating this literal 3 times  sonarjs/no-duplicate-string
  101:17  error  Define a constant instead of duplicating this literal 4 times  sonarjs/no-duplicate-string
docknetwork/sdk/src/verifiable-credential.js
  44:10  error  Refactor this function to reduce its Cognitive Complexity from 17 to the 15 allowed
sonarjs/cognitive-complexity
 ✓ 35 problems (34 errors, 1 warning)
  6 errors and 0 warnings potentially fixable with the `--fix` option.
```

Adherence to Specification

1. **Update: Not an issue.** From the Dock Network team: "If you mean that if a validator is accidentally added to remove list then because remove takes priority over add, it won't be added in the next epoch, then yes, we understand. There is always a way to short circuit an epoch using master though so such mistakes can be fixed. Because PoA is relatively short term, we didn't want to add logic to manage the queues too much." The `remove_validator` extrinsic in `dock-substrate/pallets/poa/src/lib.rs` doesn't check the validator is active or queued. In these situations, it bans the validator from being added until the next epoch.

2. **Update: Not an issue.** From the Dock Network team: "Reading a vector or a primitive from storage has same DB weight as pointed out in the hackmd doc". `L284`, `L318` and other places in `dock-substrate/pallets/poa/src/lib.rs`: reading `ActiveValidators`, a vector of `T::AccountId`, from storage carries the same weight as reading `EpochEndsAt`, a `SlotNo` (`u64`).

3. **Update: Fixed as of the commit `620daed`.** The weight of `set_min_epoch_length` in `dock-substrate/pallets/poa/src/lib.rs` should not include the read of `MinEpochLengthTentative` since that cost is incurred independently of whether the extrinsic was called. The same holds for `set_max_active_validators`.

4. **Update: Fixed as of the commit `44bdc6f`.** It is not clear how each epoch length is set to 10 days.

Code Documentation

1. **Update: Fixed as of the commit `620daed`.** `dock-substrate/pallets/token_migrations/src/lib.rs`, `L197`: a typo: "change" -> "chance".
2. **Update: Fixed as of the commit `620daed`.** `dock-substrate/runtime/src/blob.rs`, `L34`: a typo: "token" -> "blob".
3. **Update: Fixed as of the commit `620daed`.** `dock-substrate/runtime/src/did.rs`, `L26`: a typo: "token" -> "did".
4. **Update: Fixed as of the commit `620daed`.** `dock-substrate/pallets/poa/lib.rs`, `L812`: the current epoch actually has not ended yet and may not end for a few more slots. Replace "ended" with "ending".
5. **Update: Fixed as of the commit `620daed`.** `dock-substrate/pallets/poa/lib.rs`, `L866`: probably meant `2^32` rather than `2^64`. An alternative explanation of why overflow will not happen is that no validator can produce more blocks in an epoch than the length of the epoch.
6. **Update: Fixed as of the commit `620daed`.** `dock-substrate/pallets/poa/lib.rs`: comments in lines `1235` and `1236` are not clear.
7. **Update: Fixed as of the commit `620daed`.** `dock-substrate/pallets/poa/lib.rs`: `L1150`. Error message is incorrect. It should be `slots_per_validator + 1 < max_blocks.to_number()` instead.
8. **Update: Fixed as of the commit `620daed`.** `dock-substrate/pallets/poa/lib.rs`, `L1199`: the function actually doesn't set the last slot of the previous epoch.
9. **Update: Fixed as of the commit `620daed`.** `dock-substrate/pallets/poa/lib.rs`, `L1147`: a typo: "panicking" → "panicing".
10. **Update: Fixed as of the commit `620daed`.** `dock-substrate/runtime/src/did.rs`, `L206`: "...might be same as did" - unspecified what `did` refers to.
11. **Update: Fixed as of the commit `620daed`.** `dock-substrate/runtime/src/did.rs`, `L441`: "KeyUpdate" → "DidRemoval".
12. **Update: Acknowledged.** The validator count written in the documentation of `10` is too little: 4 compromises can already break GRANDPA. It is suggested to check the documentation and acknowledge the potential risk.
13. **Update: Fixed in `3c82cfd`.** `sdk/tutorials/src/tutorial_did.md`, `L116`: "removing" → "removed".
14. **Update: Fixed in `eedaaf7`.** `sdk/tutorials/src/tutorial_did.md`, `L128`: "createKeyUpdate" → "createDidRemoval".

Adherence to Best Practices

1. **Update: Not an issue.** According to the Dock network team, this behaviour is intentional. `new()` method in `runtime/src/did.rs` : if desired, it is recommended to require providing a signature and validate it, confirm that the user indeed owns the private key for the provided public key.

2. **Update: Fixed as of the commit `620daed`.** `L435-L442` in `node/src/chainspec.rs`: it would be safer to use `checked_mul()`.

3. **Update: Fixed as of the commit `620daed`.** `runtime/src/master.rs`: it would be safer to remove `pub` keyword from `execute_()` and `set_members_()`.

4. **Update: Fixed as of the commit `620daed`.** In `L913` of `dock-substrate/pallets/poa/src/lib.rs`, the proper type of current_epoch_no is `EpochNo`.

5. **Update: Acknowledged, unlikely to be an issue.** From Dock Network: "Even with double the emission reward, double the epoch duration and only 1 validator (maximizing blocks per validator), we have output size as 56 bits". In several places of `dock-substrate/pallets/poa/src/lib.rs`, the mathematical integer `floor(x*(p/q))`, where `q>0` and `0<=p<=q`, is sought. The code used for this is `x.saturating_mul(p)/q`, which carries a risk of loss of precision. For these occasions, we recommend the following code instead, which is guaranteed not to overflow so long as `p(q-1) <= q(q-1)` fits in the integer type.

   ```
   let (a, b) = (x/q, x%q);
   ```

```
return p*a + (p*b)/q;
```

6. **Update: Fixed as of the commit** `620daed`. A typo in `runtime/src/revoke.rs` L168: “ RevokeId” -> “RegistryId”.

7. **Update: Acknowledged(c.f. QSP-14).**In `runtime/src/lib.rs`,data type of `BlockNumber` and `Index` are defined as `u32`. consider using other types capable of handling bigger values such as `u128`.

8. **Update: Fixed in 8834a56**. From the Dock Network team: "We need to upgrade our benchmarks as per the new way of doing benchmarking in Substrate." `dock-substrate/runtime/src/did.rs`, `L355-361`: it is recommended to use `signature.weight()` or the previously defined weight constants.

9. **Update: Acknowledged.** From Dock Network: "Not fixing as `static_assertions` library cannot handle generic types". `dock-substrate/pallets/poa/lib.rs`: there is copious amounts of debugging code that should be removed. There should be a compile time assertion that the types `Balance`, `BalanceOf<T>`, `NegativeImbalanceOf<T>` and `T::Currency::Balance` are all the same unsigned numeric type (`u64`). Without this check, the logic becomes harder to understand and, although the programmer was careful to insert saturations when converting among these types, this could result in unintended loss of precision, particularly if these types are of less precision that `Balance`.

10. **Update: Acknowledged.** From the Dock Network team: "It has to consider min epoch length as well." `dock-substrate/pallets/poa/lib.rs`. Consider inserting invariant checks in `EpochDetail::new()`, even though they should not trigger for this code:

    ```
    assert!(validator_count > 0);
    assert!((expected_ending_slot - starting_slot + 1)% validator_count as SlotNo == 0);
    ```

11. **Update: Fixed as of the commit** `2f3f8eb`. `dock-substrate/pallets/poa/lib.rs`. The field `total_emission` of `EpochDetail` is redundant. Use a method to convey that meaning instead.

12. **Update: Fixed as of the commit** `620daed`. `dock-substrate/pallets/poa/lib.rs`. Why not `(true, new_count)` instead of lines `1237` to `1242`?

13. **Update: Not an issue.** From the Dock Network team: "These are printing different values". `dock-substrate/pallets/poa/lib.rs`. Lines `1148` and `1149` are redundant.

14. **Update: False-positive.** `dock-substrate/pallets/poa/lib.rs`. The code assumes that `::take()` puts a default value (`0`, `None` or `vec!()`) back into the storage slot. Substrate docs indicate the storage slot is deleted.

15. **Update: Not an issue.** `dock-substrate/pallets/poa/lib.rs`. `ValidatorStats` is not initialized for a new epoch, but that may be fine if querying an empty entry in the `double_map` produces a `block_count` of zero.

16. **Update: Fixed.** From the Dock Network team: "That is for genesis. Added a comment." `dock-substrate/pallets/poa/lib.rs`. The non-emptiness of the validator set is an invariant throughout but not on line `1350`, apparently.

17. **Update: Fixed as of the commit** `620daed`. `dock-substrate/pallets/poa/lib.rs`. By the logic in lines `891` to `905`, if all validators are incompetent, they will all be well rewarded.

18. **Update: Acknowledged.** From Dock Network: "Not fixing as `static_assertions` library cannot handle generic types". `dock-substrate/runtime/src/did.rs`, lines `243` and `244`: use a compile-time assertion instead.

19. **Update: Acknowledged, low priority.** `dock-substrate/runtime/src/did.rs`. Having `Dids` be a map of `Did => (Option<KeyDetail>, Nonce)` would be a clean solution to having many DID updates in a single block. It would be very nice to have an expiry time in `KeyUpdate` and `DidRemoval` so users can “give up” on transactions.

20. **Update: Fixed as of the commit** `620daed`. `sdk/package.json`. Configuring the version of node.js to be greater than or equal to 10 in `engines` would be safer for developing Polkadot-based project (c.f. Polkadot.js github).

Test Results

Test Suite Results

All tests pass.

```
Blockchain:

running 1 test
test chain_spec::test::expected_did_from_seed ... ok

test result: ok. 1 passed; 0 failed; 0 ignored; 0 measured; 0 filtered out

     Running target/debug/deps/dock_node-0f4c73a2b6926ce2

running 1 test
test chain_spec::test::expected_did_from_seed ... ok

test result: ok. 1 passed; 0 failed; 0 ignored; 0 measured; 0 filtered out

     Running target/debug/deps/dock_runtime-3a451cea03ee5945

running 42 tests
test __construct_runtime_integrity_test::runtime_integrity_tests ... ok
test blob::tests::err_did_does_not_exist ... ok
test blob::tests::err_blob_already_exists ... ok
test did::tests::did_creation ... ok
test blob::tests::err_blob_too_big ... ok
test did::tests::did_key_update_for_unregistered_did ... ok
```

```
test blob::tests::err_invalid_sig ... ok
test blob::tests::add_blob ... ok
test did::tests::did_key_update_with_ecdsa_key ... ok
test did::tests::did_key_update_replay_protection ... ok
test did::tests::did_remove ... ok
test did::tests::signature_verification ... ok
test did::tests::did_key_update_with_sr25519_ed25519_keys ... ok
test master::test::all_members_vote ... ok
test master::test::err_bad_sig ... ok
test master::test::err_insufficient_votes ... ok
test master::test::err_not_member ... ok
test master::test::err_zero_vote_requirement ... ok
test master::test::non_root_impossible ... ok
test master::test::execute_set_members ... ok
test master::test::round_inc ... ok
test master::test::err_vote_requirement_to_high ... ok
test master::test::no_members ... ok
test master::test::replay_protec ... ok
test revoke::calls::new_registry ... ok
test revoke::calls::remove_registry ... ok
test revoke::calls::revoke ... ok
test master::test::two_successful_rounds_of_voting ... ok
test master::test::valid_call ... ok
test revoke::errors::differentblocknumber ... ok
test revoke::errors::invalidpolicy ... ok
test revoke::errors::noreg ... ok
test revoke::calls::unrevoke ... ok
test revoke::errors::addonly ... ok
test revoke::errors::regexists ... ok
test master::test::test_events ... ok
test revoke::test::get_revocation_registry ... ok
test revoke::errors::notauthorized_wrong_command ... ok
test test_common::meta_in_ext ... ok
test revoke::test::get_revocation_status ... ok
test revoke::errors::notauthorized ... ok
test revoke::test::ensure_auth ... ok

test result: ok. 42 passed; 0 failed; 0 ignored; 0 measured; 0 filtered out

     Running target/debug/deps/poa-8d21c4540109d502

running 21 tests
test tests::config_set_by_master ... ok
test tests::add_validator_basic ... ok
test tests::add_remove_validator ... ok
test tests::add_remove_swap_validator ... ok
test tests::emission_reward_for_shorter_epoch ... ok
test tests::expected_treasury_account_id ... ok
test tests::epoch_details_and_block_count ... ok
test tests::current_epoch_end ... ok
test tests::remove_validator_basic ... ok
test tests::short_circuit_epoch ... ok
test tests::emission_rewards_status ... ok
test tests::swap_validator ... ok
test tests::rewards_for_non_empty_epoch ... ok
test tests::slots_per_validator ... ok
test tests::treasury_emission_reward ... ok
test tests::treasury_withdrawal ... ok
test tests::validator_rewards_credit ... ok
test tests::validator_block_counts ... ok
test tests::txn_fees ... ok
test tests::validator_set_change_on_max_active_validator_change ... ok
test tests::validator_rewards_for_non_empty_epoch ... ok

test result: ok. 21 passed; 0 failed; 0 ignored; 0 measured; 0 filtered out

     Running target/debug/deps/token_migration-61a29644ddf2a6ef

running 5 tests
test tests::add_migrator ... ok
test tests::expand_migrator ... ok
test tests::contract_migrator ... ok
test tests::migrate ... ok
test tests::remove_migrator ... ok

test result: ok. 5 passed; 0 failed; 0 ignored; 0 measured; 0 filtered out

   Doc-tests dock-node

running 0 tests

test result: ok. 0 passed; 0 failed; 0 ignored; 0 measured; 0 filtered out

   Doc-tests dock-runtime

running 3 tests
test src/master.rs - master (line 26) ... ok
test src/master.rs - master (line 39) ... ok
test src/master.rs - master (line 7) ... ok

test result: ok. 3 passed; 0 failed; 0 ignored; 0 measured; 0 filtered out

   Doc-tests token_migration

running 0 tests

test result: ok. 0 passed; 0 failed; 0 ignored; 0 measured; 0 filtered out

   Doc-tests poa
```

```
running 0 tests

test result: ok. 0 passed; 0 failed; 0 ignored; 0 measured; 0 filtered out

==================================
SDK:
==================================

RUNS  tests/unit/issuing.test.js
 PASS  tests/unit/utils.test.js (8.689s)
  Testing isHexWithGivenByteSize
     ✓ isHexWithGivenByteSize rejects strings not starting with 0x (2ms)
     ✓ isHexWithGivenByteSize rejects strings with invalid hex
     ✓ isHexWithGivenByteSize rejects strings with non-full byte (1ms)
     ✓ isHexWithGivenByteSize rejects strings with byte size 0
     ✓ isHexWithGivenByteSize rejects strings not matching expected byte size
     ✓ isHexWithGivenByteSize accepts correct hex string with full bytes (1ms)
     ✓ isHexWithGivenByteSize accepts correct hex string matching expected byte size
  Testing public key and signature instantiation from keyring
     ✓ getCorrectPublicKeyFromKeyringPair returns correct public key from ed25519 pair (13ms)
     ✓ getCorrectPublicKeyFromKeyringPair returns correct public key from sr25519 pair (1ms)
     ✓ getCorrectPublicKeyFromKeyringPair returns correct public key from secp256k1 pair (128ms)
     ✓ getCorrectSignatureFromKeyringPair returns correct signature from ed25519 pair (3ms)
     ✓ getCorrectSignatureFromKeyringPair returns correct signature from sr25519 pair (17ms)
     ✓ getCorrectSignatureFromKeyringPair returns correct signature from secp256k1 pair (84ms)
  Testing Ecdsa with secp256k1
     ✓ Signing and verification works (1054ms)
 PASS  tests/unit/did.test.js
  DID utilities
     ✓ On input as 40 byte hex, validateDockDIDIdentifier throws error (6ms)
     ✓ On input as 30 byte hex, validateDockDIDIdentifier throws error (1ms)
     ✓ On input as 32 byte hex, validateDockDIDIdentifier does not throw error
     ✓ On input as 33 byte hex, getHexIdentifierFromDID throws error (4ms)
     ✓ On input as 32 byte hex, getHexIdentifierFromDID returns the input
     ✓ On input valid SS58 but without qualifier, getHexIdentifierFromDID throws error (1ms)
     ✓ On input invalid SS58 but with qualifier, getHexIdentifierFromDID throws error (1ms)
     ✓ On input fully qualified Dock DID, getHexIdentifierFromDID returns valid hex representation (1ms)
     ✓ On input valid SS58 and with qualifier but smaller than 32 bytes, getHexIdentifierFromDID throws error
(1ms)
     ✓ On input valid SS58 and with qualifier but larger than 32 bytes, getHexIdentifierFromDID throws error
(2ms)
     ✓ On input valid SS58 identifier but smaller than 32 bytes, validateDockDIDSS58Identifier throws error
(1ms)
     ✓ On input valid SS58 identifier but larger than 32 bytes, validateDockDIDSS58Identifier throws error
(3ms)
     ✓ On input valid SS58 identifier, validateDockDIDSS58Identifier does not throw error (1ms)
 PASS  tests/unit/serialize.test.js
  Serialization
     ✓ VerifiableCredential fromJSON should fail if no type is provided (11ms)
     ✓ VerifiableCredential fromJSON should fail if no context is provided (1ms)
     ✓ VerifiablePresentation fromJSON should fail if no type is provided (6ms)
     ✓ VerifiablePresentation fromJSON should fail if no context is provided (1ms)
     ✓ VerifiableCredential from/to JSON serialization (1ms)
     ✓ VerifiablePresentation from/to JSON serialization (1ms)
     ✓ Schema from/to JSON serialization (12ms)
  console.log src/verifiable-credential.js:157
    expanded {
      'https://www.w3.org/2018/credentials#credentialSchema': [ { '@id': 'blob:dock:5C78GCA', '@type': [Array]
} ],
      'https://www.w3.org/2018/credentials#credentialSubject': [
        {
          'https://schema.org/alumniOf': [Array],
          'https://schema.org/email': [Array],
          '@id': 'did:dock:5GL3xbkr3vfs4qJ94YUHwpVVsPSSAyvJcafHz1wNb5zrSPGi'
        }
      ],
      '@id': 'uuid:0x9b561796d3450eb2673fed26dd9c07192390177ad93e0835bc7a5fbb705d52bc',
      'https://www.w3.org/2018/credentials#issuanceDate': [
        {
          '@type': 'http://www.w3.org/2001/XMLSchema#dateTime',
          '@value': '2020-09-30T05:32:17.141Z'
        }
      ],
      '@type': [ 'https://www.w3.org/2018/credentials#VerifiableCredential' ]
    }
 PASS  tests/unit/cred-revocation.test.js
  Check isRevocationCheckNeeded
     ✓ isRevocationCheckNeeded returns true when credentialStatus is present and forceRevocationCheck is true
and revocation API is not given (1ms)
     ✓ isRevocationCheckNeeded returns true when credentialStatus is present and forceRevocationCheck is true
and revocation API is given
     ✓ isRevocationCheckNeeded returns true when credentialStatus is present and forceRevocationCheck is false
but revocation API is given
     ✓ isRevocationCheckNeeded returns true when credentialStatus is present and forceRevocationCheck is false
but revocation API is empty object (1ms)
     ✓ isRevocationCheckNeeded returns false when credentialStatus is present and forceRevocationCheck is false
and revocation API is not given
     ✓ isRevocationCheckNeeded returns false when credentialStatus is not present and forceRevocationCheck is
true and revocation API is not given
     ✓ isRevocationCheckNeeded returns true when credentialStatus is not present and forceRevocationCheck is
true and revocation API is given
 PASS  tests/unit/schema.test.js (25.199s)
  VerifiableCredential Tests
     ✓ VerifiableCredential's setSchema should appropriately set credentialSchema. (3ms)
     ✓ VerifiableCredential's validateSchema should validate the credentialSubject with given JSON schema.
(4143ms)
  Basic Schema Tests
     ✓ accepts the id optionally and generates id of correct size when id is not given
     ✓ setAuthor will set the author and accepts a DID identifier or full DID (1ms)
     ✓ setJSONSchema will only accept valid JSON schema and set the schema key of the object. (20ms)
     ✓ validateSchema will check that the given schema is a valid JSON-schema. (7ms)
     ✓ toJSON will generate a JSON that can be sent to chain.
     ✓ toBlob will generate a JSON that can be sent to written with blob module (2ms)
  Validate Credential Schema utility
     ✓ credentialSubject has same fields and fields have same types as JSON-schema (1ms)
     ✓ credentialSubject has same fields but fields have different type than JSON-schema (1842ms)
     ✓ credentialSubject is missing required fields from the JSON-schema and it should fail to validate.
(1839ms)
     ✓ The schema's properties is missing the required key and credentialSubject can omit some of the
properties. (1856ms)
     ✓ credentialSubject has extra fields than given schema specifies and additionalProperties has certain
type. (1829ms)
     ✓ credentialSubject has nested fields and given schema specifies the nested structure. (1825ms)
 PASS  tests/unit/issuing.test.js (73.68s)
  Verifiable Credential Issuing
     ✓ Issuing should return an object with a proof, and it must pass validation. (8368ms)
  Verifiable Credential Verification
     ✓ The sample signed credential should pass verification. (4563ms)
  Verifiable Presentation creation
     ✓ A proper verifiable presentation should be created from two valid sample credentials. (2ms)
     ✓ A verifiable presentation should contain a proof once signed, and it should pass verification. (11719ms)
  Verifiable Credential incremental creation
     ✓ VC creation with only id should be possible, yet bring default values (1ms)
     ✓ VC creation with an object context should be possible
     ✓ JSON representation of a VC should bring the proper keys (1ms)
     ✓ Incremental VC creation should be possible (1ms)
     ✓ Duplicates in context, types and subjects are omitted. (1ms)
     ✓ Incremental VC creations runs basic validation (19ms)
     ✓ Issuing an incrementally-created VC should return an object with a proof, and it must pass validation.
(8930ms)
  Verifiable Presentation incremental creation
     ✓ VP creation with only id should be possible, yet bring default values (1ms)
     ✓ VP creation with an object context should be possible
     ✓ The JSON representation of a VP should bring the proper keys (1ms)
     ✓ Incremental VP creation should be possible
     ✓ Incremental VP creations runs basic validation (12ms)
     ✓ Incremental VP creation from external VCs should be possible (11982ms)
     ✓ Issuing an incrementally-created VP from an incrementally created VC should return an object with a
proof, and it must pass validation. (17916ms)
     ✓ Support contexts without @context key (1ms)
Test Suites: 6 passed, 6 total
Tests:       74 passed, 74 total
Snapshots:   0 total
Time:        74.11s
Ran all test suites matching /.\/tests\/unit/i.
 ✓  Done in 77.15s.

Unknown signed extensions OnlyMigrator found, treating them as no-effect
 PASS  tests/integration/schema.test.js (101.959s)
  Schema Blob Module Integration
     ✓ setSignature will only accept signature of the supported types and set the signature key of the object.
(9ms)
     ✓ sign will generate a signature on the schema detail, this signature is verifiable. (14ms)
     ✓ Schema.get will return schema in correct format. (7ms)
     ✓ Schema.get throws error when schema not in correct format. (12ms)
     ✓ Schema.get throws error when no blob exists at the given id. (7ms)
     ✓ Utility method verifyCredential should pass if the subject is compatible with the schema in
credentialSchema. (6992ms)
     ✓ The verify method should pass if the subject is compatible with the schema in credentialSchema. (7132ms)
     ✓ Utility method verifyCredential should check if schema is incompatible with the credentialSubject.
(6479ms)
     ✓ The verify method should detect a subject with incompatible schema in credentialSchema. (4411ms)
     ✓ Utility method verifyPresentation should check if schema is incompatible with the credentialSubject.
(18959ms)
     ✓ Utility method verifyPresentation should check if schema is compatible with the credentialSubject.
(11164ms)
     ✓ VerifiablePresentation's verify should check if the schema is incompatible with the credentialSubject.
(19035ms)
     ✓ VerifiablePresentation's verify should check if the schema is compatible with the credentialSubject.
(10865ms)
  console.warn node_modules/@polkadot/types/create/registry.js:430
    Unknown signed extensions OnlyMigrator found, treating them as no-effect
 PASS  tests/integration/master.test.js (26.671s)
  Master Module
     ✓ control: set and get bytes as sudo (1161ms)
     ✓ Root call with no votes (3047ms)
     ✓ Root call with invalid votes (2994ms)
     ✓ Root call with valid votes (2973ms)
     ✓ Root call with valid votes but insufficient vote count (6011ms)
     ✓ Root call with valid votes and oversufficient vote count (3021ms)
     ✓ Root call with votes not sorted lexically (3078ms)
     ✓ Use a master call to modify master membership. (2924ms)
  console.warn node_modules/@polkadot/types/create/registry.js:430
    Unknown signed extensions OnlyMigrator found, treating them as no-effect
 PASS  tests/integration/presenting.test.js (99.848s)
  Verifiable Presentation where both issuer and holder have a Dock DID
     ✓ Holder creates a verifiable presentation with single credential and verifier verifies it (50872ms)
     ✓ Holder creates a verifiable presentation with 2 credentials and verifier verifies it (24591ms)
  console.warn node_modules/@polkadot/types/create/registry.js:430
    Unknown signed extensions OnlyMigrator found, treating them as no-effect
 PASS  tests/integration/revocation.test.js (38.095s)
  Revocation Module
     ✓ Can create a registry with multiple controllers (8978ms)
     ✓ Can create a registry with a OneOf policy (3018ms)
     ✓ Can revoke from a registry (2980ms)
     ✓ Can unrevoke from a registry (2994ms)
     ✓ Can remove a registry (3046ms)
     ✓ Can create an add only registry (2952ms)
     ✓ Can revoke from an add only registry (3000ms)
     ✓ Can not unrevoke from an add only registry (6028ms)
```

```
      ✓ Can not remove an add only registry (2998ms)
  console.warn node_modules/@polkadot/types/create/registry.js:430
    Unknown signed extensions OnlyMigrator found, treating them as no-effect
 PASS  tests/integration/credential-revocation.test.js (47.171s)
  Credential revocation with issuer as the revocation authority
      ✓ Issuer can issue a revocable credential and holder can verify it successfully when it is not revoked
else the verification fails (12406ms)
      ✓ Holder can create a presentation and verifier can verify it successfully when it is not revoked else the
verification fails (21193ms)
  console.warn node_modules/@polkadot/types/create/registry.js:430
    Unknown signed extensions OnlyMigrator found, treating them as no-effect
 PASS  tests/integration/issuing.test.js (32.658s)
  Verifiable Credential issuance where issuer has a Dock DID
      ✓ Issue a verifiable credential with ed25519 key and verify it (7733ms)
      ✓ Issue a verifiable credential with secp256k1 key and verify it (7683ms)
      ✓ Issue a verifiable credential with sr25519 key and verify it (7476ms)
  console.warn node_modules/@polkadot/types/create/registry.js:430
    Unknown signed extensions OnlyMigrator found, treating them as no-effect
 PASS  tests/integration/blob.test.js (86.749s)
  Blob Module
      ✓ Can create and read a JSON Blob. (12235ms)
      ✓ Can create and read a string Blob. (12033ms)
      ✓ Can create and read a hex Blob. (11945ms)
      ✓ Can create and read a Vector Blob. (12007ms)
      ✓ Fails to write blob with size greater than allowed. (12005ms)
      ✓ Fails to write blob with id already used. (15067ms)
      ✓ Should throw error when cannot read blob with given id from chain. (10562ms)
  console.warn node_modules/@polkadot/types/create/registry.js:430
    Unknown signed extensions OnlyMigrator found, treating them as no-effect
 PASS  tests/integration/did.test.js (16.368s)
  DID Module
      ✓ Has keyring and account (21ms)
      ✓ Can create a DID (3175ms)
      ✓ Can get a DID document (6ms)
      ✓ Can update a DID controller (6019ms)
      ✓ Can update a DID key to ed25519 key (2940ms)
      ✓ Can remove a DID (3033ms)
 PASS  tests/integration/dock-sdk.test.js
  Config on NodeJS environment
      ✓ Is running in NodeJS environment
  Dock API
      ✓ Can connect to node (697ms)
      ✓ Has DID Module
      ✓ Has Revocation Module (1ms)
      ✓ Can disconnect from node
Test Suites: 9 passed, 9 total
Tests:       55 passed, 55 total
Snapshots:   0 total
Time:        450.721s
```

Code Coverage

Rust: Test coverage (only Line Coverage) of the Rust code was calculated with `tarpaulin`. Overall the code features good coverage, but it would be beneficial to improve the coverage for some part as noted in `QSP-10`.

File	% Lines
pallets/	
token_migration/src/lib.rs	78.13
poa/src/lib.rs	71.68
runtime/	
src/blob.rs	98.90
src/did.rs	87.57
src/lib.rs	2.60
src/master.rs	95.79
src/revoke.rs	91.65
src/blob.rs	98.90

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

```
973049d0654a8813506ba50c8a3d165af113c422cbf4d199939453e545ea3c7a ./webpack.config.js

c8fe0ced4a1f126c5aa413b56398761fabbe48165eb8f643a07b8cc894523f57 ./rollup.config.js

e31d24f21a33d3972963a97578c251b56f14c5a4340bb3c23b2ffa16747a6a61 ./dock-resolver.js

2f0f386ea9caf280d172276a0e0b3c79fb968166ea5b7fa49eb0cd9b5a9d91da ./poa-rpc-defs.js

ff172847d15f2a479ae0accc831eb87c35cab7018e2dbaab783119de9f8ee234 ./multi-resolver.js

fba6e45437b5768bd3e3db3810e7ea09810122c858db4bdf0020b673f879af4e ./verifiable-presentation.js

58f83376018c1f9571706193d2f6a6cda2622aa671011e872cbe4598a50d966b ./universal-resolver.js

bb5e29630593c804b14c956c78af69d53edb8ae12100a193b48b268acfbadb56 ./verifiable-credential.js

fc88a8fc734bcfc6ad3bb75454770f4c2e183736b709851de30f0b0ebaff5a22 ./public-keys.js

9a5c14e7326c5f9568be3c0c3fadcc50e917c38368f11e41d5eae7e64b5b0cc9 ./did-resolver.js

296df7c77b78bc39dff031bf1a1b2642f10b298ae56c2a52155c8ff041c73e36 ./api.js

e28a30c24214839b0c353053c625d813f842b21be29314eecb2037719bb3b663 ./resolver.js

5d8ca6f1e661d1b99ecb813e1a38c07016ea7c7637a40662612c89ec9981d896 ./signatures.js

0e407f28adb54c89f11abdffae314c412bc24c6412d6f1c301c05c95e9dcb0bf ./public-key.js

1aec0bf08ccfdc3f29cfcd316c4f013f9591ad4acaaf14fccf6f330e2c67ed1a ./public-key-sr25519.js

7c4707cfdd314d8dfad576d96a85f9716382d3a263ddfab0ccc3433d9497eedc ./public-key-secp256k1.js

3fb3d6f5d13e5c12ae44d979445a1bf2a34f421ba164a178cc8fa70338da5abe ./public-key-ed25519.js

7ef7b095ded17530cbbae3609b07e95b06927252b97709fa05e3f6590d938692 ./poa.js

1a35a93a1b10c281ff64a3df0b98e7abacb532b49cdc8af27284e5208929b5dd ./did.js

6434ab439cff99e3d0998db3a565ed168fa4c35fb104392fb64fa71a6813da34 ./migration.js

c351fa96f73b97831afb8389283ea377c102a5d19afc4b60158c3f468f2a1a61 ./schema.js

df8c3493214e80fc26fa42efe69b62da98e3041201cb1ce28aecaf86e6bb5788 ./blob.js

4e20451c0cbdc6a2b68246a32307a808135ef89524ba3458daeb1d9790ffb166 ./revocation.js

193818a8efe13228acac3d1888156d1ea2f0295bd1b36c898c46cf5107eb3a0a ./did.js

e3fca2c24cbe26fc7075558740a7f20ca7fee02a61ff55a4646d3cddce614581 ./vc.js

14f85db1c6f3f3d261ff86120d8125c3495e5c34d87d853a90b14315db66600b ./misc.js

ba7d38ba0695d38d44833dd908c6bc68986b99342987e97704e2181278407eed ./type-helpers.js

979f63c18dd71b8841bc2b3c372598bb7773857099a45e7c92f21827de9851bf ./codec.js

86d2b74fd88995814067e65c0f3d68d2d31a71e18584f78352bbe4e8d5e64460 ./revocation.js

fcbe70278dd2febb934ca51fed9898fc9ebc7a6892ddc508a08e98a1c3f1a754 ./no-blob-error.js

b3e1534b51967d61adfa9e8f15879e456da3c8da30aea4bcabf23f7f9dabfa99 ./policy.js

ca25a366aa6afd0c000c855cf26748fd537a0379fbcc9041c838087d093b0cd7 ./keyring-pair-did-keys.js

7c83c818d068613bfceca11d39d034d6453f1708b61fcfbfce781c46aa309d47 ./did-keys.js

2cea4d5f4f165ece49273af01031d7a966f481f063677caa0bca80a24ced86bc ./one-of-policy.js

f711aebd59e3c3539fd2216adc3386b1a321cb188c9d7b897e35b162d5520468 ./custom_crypto.js

3fa996d566bd1dff8bbca119ddf66ec5594072686fb29aa00b5413b0f8a8f95e ./contexts.js

e6f1c0797fb639b5105ac8b552999d3cad5a5273a6aa27097f250be1a518f560 ./document-loader.js

663d679a7ffa1e516875f398379259e40425f05f6722660bc99dac61c7c6f30f ./helpers.js

df5701b8c0227547e744f86a586382a53c6fde0e6164563c9d1e42a8284170c5 ./pr_card.js

fbcd20c9d307ddcd7a8221d095ddf4b310605e57d21706373887fc094ddd5f71 ./schema-draft-07.js

cf4069ad6e3a9d7e76a4f7f125a9c8c20fb67ab4f17321d4c6d0fd872d652d0a ./qp_inbond.js

d6a22184b8f7bee89b8da8ec72538ac8d306aa654fc2d2df154f3efc8a800eb7 ./immunity_event_record.js

943069ec28dacc83eae280f84105d61a91073f96a0eacaf84afc8dc972deb34e ./non_infection_check.js

ca32e35b4d59e016aa03251d227a0b575a56954725ef2cd4ee68258b205e42c2 ./infection_diagnosis.js

270aa59d8f3b610286a666f9933b9d3377041edc541da131a1e9d997d77fa6bd ./proof_of_health_core.js

464e246f0a5612a924ef07ba7dd9ca51139adf54e49ab54e7953497b2b8a55c1 ./bol.js

49748a35ea606b7a866ed1f0ac06456282759e822df3eb94211b12579f6c771c ./health_worker_passport.js

470db28b003e18cd2144de343bbdfdf2685d682b787617995ec849518a7815d3 ./vc-examples-v1.js

742ba9cc424ff14bdd9e2a9d6d39ac7b71774aa3cc3fe6ca32f98a3aba3e2a35 ./security_context.js
```

```
f8590dd490c41b085c77a1c998a4f80ff23e9a8315976ae183f2eeaab31ff2eb ./constants.js
2b24fa24e6e6389d09289d34a5d87632fcb13ae721503c1157499d0ab2447a9e ./EcdsaSepc256k1Signature2019.js
98eddfdc85842d84c99b8a213164e07d7ff720850072b79ad6868f2dcc6bc83e ./Ed25519Signature2018.js
8eafdb750b554ca249781595d87dec18b75cb9390fca423b63acb6f99e294417 ./Sr25519VerificationKey2020.js
a3318d8d22fb7c974f93610a212cf058361fc873fb553c57e2fc068fbda9fbb6 ./EcdsaSecp256k1VerificationKey2019.js
3cefd1dff815796da7baf0d14c012bfe226d4e1e4afad6ded4a1b8bbc03fb61e ./Sr25519Signature2020.js
05acb5aa41512c9b0cba970d52e8d50c8cec84df0941e93b1a52e89d0b6513a3 ./Ed25519VerificationKey2018.js
970dedb2ca2961a535d62e08685814a33b66cbdba9852b31b9fe06234a3f7e27 ./signature-sr25519.js
6b9f2b6ee20eedd0ec50ace98014f35653d0c43d765d389ac1d6c7fae937f7c7 ./signature.js
f5ee8b99d9842cad5efcdace9caed54c0275703cbb71d35e4ae75753f000a86d ./signature-secp256k1.js
cbbfbf66d2d582d4ea6a2e6c08f90e6d84db8b657c7c59c54b3d66290391bd53 ./signature-ed25519.js
9f57cc1d9f37e04a65f8b6c756bf3873c2c6c36ba5d27813ff3608f8c1280232 ./get_session_keys.js
062ee5264b9905c2b1328a4657c0f4cf6098b9db03ce165a0b7469a708c85a88 ./change_did_key.js
5f6b5529954a6dde9f90e0eb43034fa515d27e9ee2e6df0eb77256870382642a ./runtime_upgrade_with_sudo.js
3be1cde49d278fd7d403a38ca533dd56dafe03fad442af591a8da3945500113b ./insert_session_key_with_seed.js
14557dd6a1e8615f5a082db0452fc643f6ce7ee980a936375c5f5b498ff44d1b ./add_session_key_with_sudo.js
578983a98f141e815d8433f727dbcb72afbdfc07dc647287b03d4c5b20b9b5ff ./get_did_doc.js
e9c8115d2a7360c0896c53eba9c2ae56740a55bd4dc9fe879ffe6f8950cf3a4f ./remove_validator_with_sudo.js
5f8b5adbc91de6b416dc46b3a96fad6dd44c85b6fc549f287dd853d5f91ffcfb ./hit_1.js
64a6fbb78830c24f36574830e7071d9e5c261b7e9b97dd58df0031d424b5ec9e ./get_summary.js
8a745732538ef8c9f2355a8f4f64e98c55450a84ed5bedf473f79f2517c19697 ./onboard_validator_with_sudo.js
91fbd0855f9c8870e84dc67df50902cb895db37ac736e9a0b682e2f6113ceb21 ./helpers.js
526e72e926ca80344bab2863273aff0c6b5a9032122fb23bd5d88970273a0afd ./queries.js
f642379a1d0da549e2ae8bcd6a3ab1c0a820a0810471c3a76cdf29e530da16d9 ./add_validator_with_sudo.js
3cbaf4f542b966134563a6d13712ae161a9080d769e58a3feb09f7ed8658a539 ./epoch_detail.js
1caed8525c8d60174bef3b319ad9c2cb3cbe431c857c13148c8f615fe4799a25 ./swap_validator_with_sudo.js
7915f14dbe100ab28d8d8482dc2dcc2e5f70c3db090cf37d970f61e3b0ee7f49 ./submit.js
09ae6c58e23f0c963d3a1c92f5f81d8b31d705b17d658b621110a33ab205a7b4 ./vote.js
5ae72e2d554e6aef6300839f0f90299246e2892511eb04d95fdb61a394f389a1 ./example-credential.js
380aeb625bfe8e518f0ca708757ad88cf9e53018b40d2dd761d2779685892ba9 ./example-schema.js
7bbfdf65e551cdfe72c83011a5b7ec005c80b48809b2aa75c7cf115085b17b55 ./test-constants.js
4ebf82999ea80f048f216130640998b72a36fc01afc7e4fe4cced4832edae453 ./fee_payment.test.js
adbbc768f1c522fdd66f84c148a70726cd473e5a638d55605fc3cdc751f81671 ./validator_set_add_remove.test.js
ad08b2a2afe3539da22846a6864d368550a66ce5f9f955bc9fc590e50a7fb73a ./validator_swap.test.js
60f9d94609892c24f5cd8641b761cce55488791a38bec66b6ffd3f1c4a257327 ./helpers.js
75223cdf9434dd42ad65857113fc01975eb149594e6f8ccd4a2fd52d6d388a65 ./token_migration.test.js
7ae2f9ea295c490610afa0510975ff93d5534ec2b037ff65afc87339a176a117 ./did.test.js
c5f800036252171eea89d76ff3f570af8905936c49d9767416a81d90c80d93fc ./presenting.test.js
2fc45806813127d647e825b4196dd94c10da14bcff7cb561dc37ea6a4b2aa583 ./issuing.test.js
9e5ff7eaefe1379aaeef7e969a7aca5aa0beaa9a93b731f452f011186c4b2e81 ./dock-sdk.test.js
fe0fdb4cb0061c7864d3c1d174b92a15d4539757b54005a7103116846944b858 ./blob.test.js
f8ce5d13148c6f93008e1a0a524471b0cc09787e8e3333fe7c1112d0ac619d75 ./helpers.js
2751a64fe8b6e078b3444074a6c6924b3d422bbc7cf9d19cebb6c86d86bcff31 ./schema.test.js
ad15e59573f835df3418b593e52d066ed48f12e8c3231b66f4e8d4e12de04912 ./master.test.js
56c0053a27ccaca8680ae3b682de5b36ab8a3892304529c6102d4080b3f5a013 ./credential-revocation.test.js
67e33153488fb1c2fe4d31c529a361b5963cb071d857035b01271aa9a3ff4942 ./revocation.test.js
c61fbc769afd5f68f17b1d35233af1768d2f9c41d738862f7e6a1d3745c4ef16 ./did.test.js
1a7565cd98c7eda38643a79d2930df67aa7cd32fa693d806028e5fc09825543c ./cred-revocation.test.js
448462c62b84fe73ee8d5f7fccf4b8f1f239e283056680d31f93c30220a91831 ./issuing.test.js
```

```
827b54780eca7e71f8ebc883159db138ddd2ce4f710269dbfc5cb53bece8c1bf ./schema.test.js
9fa8c3391b38250ae49cf881d9f5d0e172c756cfe913b40e29035373c264fe14 ./serialize.test.js
4b66beb20e44ca4d387b5e344ec438c5754a00995b06fec16ad9cd8a5975afc1 ./utils.test.js
6173b40b3e5f72ed7c6e0694da803a9bdbc2b06bd2d1e67a4cf9322413dcd2d0 ./standard_schemas.js
5b05b0ef43cd43883ee01191211b9d1941366991c41caeee5ef97d9461b4720d ./dock-did.js
5c0ffd6ac3619fcf4a4ab01eb727f3c63dde5cdea6120d80534e79a9ae59f798 ./vcdm.js
5d40ddd335f99befc5c86acff9c66549dde045cae0213e2664a8ec94af615c8d ./create_master_proposal.js
d4db58b192480f53be3d799196171bbf63b3191a26dfadd8b479ae6fa5e56a29 ./schema-validation.js
93fd3c14577fda9e15689b17d4f7fa8407baa6eaf4dbdffc6c771762df6f165a ./schema.js
95c8d5e7ab626c818164def68e8dcafc4d0ad26bfd05603a51d070e88db42218 ./blob.js
a7b0c95aa2dd7e70bad16d6b687daa4b627cc3aa6ca1bf70b5c68e0bc2b480c4 ./revocation.js
f1c100ce0a3b00738e8f22c7874b8dedff6b193b82ddbaa17c8dfaf348cc0516 ./resolver.js
700b757d28ddfaa482711b00488fc8a405b58f72f77467732ceae215b7a38a97 ./build.rs
ecd0bf74a464f6a0ec1c662f6a61cf8ff96fa27ed040bd7789c1e45ee6c715d9 ./did.rs
03fa69a66c0dc706ae34038668c3f707825a7a2ad3cc676fa6987988fedc6f96 ./lib.rs
c7cbb0e858c077182fe6f62f8fe823e78bdc6923f9c1eb41c0a28b61a5ee7c37 ./test_common.rs
d99376dcacfe400869013b92518074d3b900c1fe710f93ddc9f27b97c3f4fefd ./blob.rs
fb2158915ea19d42bee4394319f3dd235653a4f677bac3b9e1f41cd2a16c6c39 ./benchmark_utils.rs
3e5f07c49508120141ddea7bdef92feeec40c79bbb75cbd610f043576a1e8a99 ./revoke.rs
3171616ba0c95a8122fc1c3392a1ebc5cbfada2b7ea50d1c134e8b42bf42fee0 ./master.rs
7d254f0ceabcd414f38343614ea0a6b578aceb645493c28166cbbcd6e0cc96c4 ./pallets/token_migration/src/lib.rs
ff3eba6d64281cdb05f04ac929a9d41c3158b756d072f3dfa9d498e9fb004af8 ./pallets/token_migration/src/benchmarking.rs
86b8ff0fb4482d2c9a079338f9371a82a958d366bd9c2a34efbc4b18fbbb69a3 ./pallets/token_migration/src/tests.rs
5dbdb93cb7e2551cf24960357f35b030bb5c3be171529eea928927c45a83a811 ./pallets/poa/src/runtime_api.rs
1ef7ad9c9cdd7aaa78556300be6c5d93722d9e811430c5163c419d92c3520a0d ./pallets/poa/src/lib.rs
10eadc5c7261ab305ef7b95888911881a744ff67ae6cd259f3abd281aed6ec95 ./pallets/poa/src/tests.rs
b56a3453b05f9c3681bc3554816bb471f5fffb7ed3be1dd3e7b0c2853da9f773 ./pallets/poa/rpc/src/lib.rs
```

Changelog

- 2020-09-30 - Initial report
- 2020-10-07 - Updated based on commit 620daed (dock-substrate) and c1df500 (sdk)
- 2020-10-08 - Revised report as per Slack conversation
- 2020-10-09 - Revised report as per the new fixes
- 2020-10-16 - Final revision

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.