Quantstamp Security Assessment Certificate

July 8th 2022 — Quantstamp Verified

Sweat Economy

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

Executive Summary

Type	Fungible Token
Auditors	Souhail Mssassi, Research Engineer Marius Guggenmos, Senior Research Engineer Fayçal Lalidji, Senior Security Engineer
Timeline	2022-05-31 through 2022-06-21
Languages	Rust
Methods	Architecture Review, Unit Testing, Functional Testing, Computer-Aided Verification, Manual Review
Specification	Sweat Litepaper
Documentation Quality	Medium
Test Quality	High

Source Code

Repository	Commit
sweat-near	5189277
sweat-near	f898246

Total Issues	**7** (3 Resolved)
High Risk Issues	**1** (0 Resolved)
Medium Risk Issues	0 (0 Resolved)
Low Risk Issues	**1** (0 Resolved)
Informational Risk Issues	**4** (3 Resolved)
Undetermined Risk Issues	**1** (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).
Fixed	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

Initial audit:
Through reviewing the code, we found **7 potential issues** of various levels of severity: 1 high-severity, 1 low-severity, 4 informational-severity and 1 undetermined issues. We recommend addressing all the issues before deploying the code.
After the re-audit:
The Sweat team has fixed the majority of the issues and the contracts are ready to be deployed.

ID	Description	Severity	Status
QSP-1	Outdated Vulnerable Packages In The Project	High	Acknowledged
QSP-2	Possible Overflow & Underflow In The Contract	Low	Acknowledged
QSP-3	Adding Oracle Doesn't Revert On An Existent Element	Informational	Fixed
QSP-4	Redundant Verification On Private Functions	Informational	Acknowledged
QSP-5	Hardcoded Length Check	Informational	Fixed
QSP-6	Unclear Name `steps_from_tge`	Informational	Fixed
QSP-7	The Batch Mint Function Can Panic	Undetermined	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:

- Cargo Audit 0.16.0
- Cargo Geiger 0.11.1

Steps taken to run the tools:

1. Installed via `cargo install cargo-audit`
2. Ran `cargo audit`
3. cargo install cargo-geiger

Findings

QSP-1 Outdated Vulnerable Packages In The Project

Severity: *High Risk*

Status: Acknowledged

File(s) affected: `Cargo.toml`

Description: During our code review, we used the `cargo audit` tool to check if any of the dependencies contain known vulnerabilities. The tool reported two critical vulnerabilities in the `regex` and the `time` crates. Refer to the `Cargo Audit` section of this report for details.

Recommendation:

- Consider updating the `time` package to a version greater than 0.2.23.
- Consider updating the `regex`package to a version greater than 1.5.5.

Update: The team has acknowledged the risk knowing that the dependencies are used only in the workspace test framework.

QSP-2 Possible Overflow & Underflow In The Contract

Severity: *Low Risk*

Status: Acknowledged

File(s) affected: `sweat/src/lib.rs`, `sweat/src/math.rs`

Description: In the `formula` function (see file `sweat/lib.rs` file, L4), the `last_trillion` is incremented by one using the `+` operator, which can cause an overflow. The overflow-check is enabled in the `Cargo.toml` which is a good practice however it's better to verify it also from the code.

- Same issue in math.rs(L9,L16)
- Same issue in lib.rs(L84,L85,L86,L88)

Recommendation:

- Instead of using the `+`operator, we recommend using the `checked_add` function to prevent an overflow.
- Instead of using the `-`operator, we recommend using the `checked_sub` function to prevent an underflow.
- Instead of using the `/`operator, we recommend using the `checked_div` function.
- Instead of using the `*`operator, we recommend using the `checked_mul` function to prevent an overflow.

Update: The team has acknowledged the issue knowing they already do the verification for the overflow-check in TOML file.

QSP-3 Adding Oracle Doesn't Revert On An Existent Element

Severity: *Informational*

Status: Fixed

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

Description: The `add_oracle` function is used to add new oracles to the set oracles using the `insert` method. When adding a duplicate oracle to the set, `insert` will return `false` and not revert. Similarly, removing a non-existing oracle will not revert.

Recommendation: Consider wrapping the output of the `insert` method in the `assert!` macro, if the output is `false` revert the transaction.

Update: The team has fixed the issue using a `require` and reverting the transaction if the oracle already exist.

QSP-4 Redundant Verification On Private Functions

Severity: *Informational*

Status: Acknowledged

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

Description: The following functions `add_oracle`, `remove_oracle`,`tge_mint` , `tge_mint_batch` with the `#[private]` decorator verify also if the method is only called by the contract itself using the common pattern of validation that the direct caller matches the contract's account. The `#[private]` macro is already performs this check.

Recommendation: Consider removing the following line from the private functions

```
assert_eq!(env::predecessor_account_id(), env::current_account_id());
```

Update: The team has acknowledged the issue knowing that they are using it for testing purposes.

QSP-5 Hardcoded Length Check

Severity: *Informational*

Status: Fixed

File(s) affected: `sweat/src/math.rs`

Description: In `math.rs:formula`, there is a check whether the lookup table should be used in the form of `if trillion < 400`. Should there be any modifications to the length of the lookup tables, it would be easy to miss that this check has to be adjusted as well since there is no reference to the arrays.

Recommendation: Replace the hard-coded length with the length of one of the arrays. Since the size is statically known and fixed, the compiler will generate the same code. Additionally, consider adding a static assertion that makes sure the KS and BS arrays have the same length like this:

```
#[allow(dead_code)]
const fn assert_lookup_lengths() {
    const_assert_eq!(KS.len(), BS.len());
}
```

Update: The team has fixed the issue by verification `trillion` with `KLS.len()`.

QSP-6 Unclear Name `steps_from_tge`

Severity: *Informational*

Status: Fixed

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

Description: The member `Contract.steps_from_tge` records the steps that have been reported through `record_batch`, i.e., presumably the steps since after the TGE event. The name `steps_from_tge` suggests it records the number of steps that were recorded at the TGE event and not since.

Recommendation: Rename the variable to `steps_since_tge` to clear up any potential confusion.

Update: The team has fixed the issue by changing the name of the variable.

QSP-7 The Batch Mint Function Can Panic

Severity: *Undetermined*

Status: Acknowledged

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

Description: The `tge_mint_batch(...)` function calls `FungibleToken.internal_register_account(...)` which panics if the account already exists in the token accounts list rather than continuing execution as `tge_mint` does.

Recommendation: If this behavior is intended, consider documenting it. Otherwise, it is advised to remove the verification.

Automated Analyses

Cargo Audit

```
   Fetching advisory database from `https://github.com/RustSec/advisory-db.git`
      Loaded 417 security advisories (from C:\Users\atq\.cargo\advisory-db)
    Updating crates.io index
    Scanning Cargo.lock for vulnerabilities (319 crate dependencies)
Crate:         regex
Version:       1.5.4
Title:         Regexes with large repetitions on empty sub-expressions take a very long time to parse
Date:          2022-03-08
ID:            RUSTSEC-2022-0013
URL:           https://rustsec.org/advisories/RUSTSEC-2022-0013
Solution:      Upgrade to >=1.5.5
Dependency tree:
regex 1.5.4
├── validator 0.12.0
│   └── near-primitives 0.10.0
├── prometheus 0.11.0
│   └── near-metrics 0.12.0
│       └── near-jsonrpc-primitives 0.12.0
│           ├── workspaces 0.2.0
│           │   └── examples 0.0.0
│           └── near-jsonrpc-client 0.3.0
│               └── workspaces 0.2.0
├── near-units-core 0.2.0
│   ├── near-units-macro 0.2.0
│   │   └── near-units 0.2.0
│   │       └── examples 0.0.0
│   └── near-units 0.2.0
└── near-primitives 0.10.0

Crate:         time
Version:       0.1.43
Title:         Potential segfault in the time crate
Date:          2020-11-18
ID:            RUSTSEC-2020-0071
URL:           https://rustsec.org/advisories/RUSTSEC-2020-0071
Solution:      Upgrade to >=0.2.23
Dependency tree:
time 0.1.43
├── zip 0.5.13
│   └── binary-install 0.0.2
│       └── near-sandbox-utils 0.2.0
│           └── workspaces 0.2.0
│               └── examples 0.0.0
└── chrono 0.4.19
    ├── workspaces 0.2.0
    ├── near-sandbox-utils 0.2.0
    ├── near-primitives 0.12.0
    ├── near-primitives 0.10.0
    ├── near-network-primitives 0.12.0
    │   ├── near-jsonrpc-primitives 0.12.0
    │   │   ├── workspaces 0.2.0
    │   │   └── near-jsonrpc-client 0.3.0
    │   │       └── workspaces 0.2.0
    │   └── near-client-primitives 0.12.0
    │       └── near-jsonrpc-primitives 0.12.0
    ├── near-client-primitives 0.12.0
    ├── near-chain-primitives 0.12.0
    │   ├── near-client-primitives 0.12.0
    │   └── near-chunks-primitives 0.12.0
    │       └── near-client-primitives 0.12.0
    └── near-chain-configs 0.12.0
        ├── near-jsonrpc-primitives 0.12.0
        ├── near-jsonrpc-client 0.3.0
        └── near-client-primitives 0.12.0

Crate:         failure
Version:       0.1.8
Warning:       unmaintained
```

```
Title:         failure is officially deprecated/unmaintained
Date:          2020-05-02
ID:            RUSTSEC-2020-0036
URL:           https://rustsec.org/advisories/RUSTSEC-2020-0036
Dependency tree:
failure 0.1.8
├── near-chain-primitives 0.12.0
│   ├── near-client-primitives 0.12.0
│   │   └── near-jsonrpc-primitives 0.12.0
│   │       ├── workspaces 0.2.0
│   │       │   └── examples 0.0.0
│   │       └── near-jsonrpc-client 0.3.0
│   │           └── workspaces 0.2.0
│   └── near-chunks-primitives 0.12.0
│       └── near-client-primitives 0.12.0
└── binary-install 0.0.2
    └── near-sandbox-utils 0.2.0
        └── workspaces 0.2.0

Crate:         sha2
Version:       0.9.8
Warning:       yanked
Dependency tree:
sha2 0.9.8
├── near-vm-logic 0.10.0
│   └── near-sdk 4.0.0-pre.7
│       ├── sweat 0.1.0
│       ├── near-contract-standards 4.0.0-pre.7
│       │   └── sweat 0.1.0
│       └── examples 0.0.0
├── near-primitives-core 0.12.0
├── near-primitives-core 0.10.0
├── near-primitives 0.10.0
├── near-chain-configs 0.12.0
│   ├── near-jsonrpc-primitives 0.12.0
│   │   ├── workspaces 0.2.0
│   │   │   └── examples 0.0.0
│   │   └── near-jsonrpc-client 0.3.0
│   │       └── workspaces 0.2.0
│   ├── near-jsonrpc-client 0.3.0
│   └── near-client-primitives 0.12.0
│       └── near-jsonrpc-primitives 0.12.0
└── ed25519-dalek 1.0.1
    ├── near-crypto 0.12.0
    └── near-crypto 0.10.0

error: 2 vulnerabilities found!
warning: 2 allowed warnings found
```

Cargo Geiger

```
Metric output format: x/y
    x = unsafe code used by the build
    y = total unsafe code found in the crate

Symbols:
     ✓  = No `unsafe` usage found, declares #![forbid(unsafe_code)]
     ✓  = No `unsafe` usage found, missing #![forbid(unsafe_code)]
     ✓ ✓   = `unsafe` usage found

Functions  Expressions  Impls  Traits  Methods  Dependency

0/0        0/0          0/0    0/0     0/0       ✓ sweat 0.1.0
0/0        0/0          0/0    0/0     0/0       ✓ ├── near-contract-standards 4.0.0-pre.7
53/53      460/478      0/0    0/0     0/0       ✓ ✓ │   ├── near-sdk 4.0.0-pre.7
0/0        0/0          0/0    0/0     0/0       ✓ │   │   ├── base64 0.13.0
0/0        7/7          0/0    0/0     0/0       ✓ ✓ │   │   ├── borsh 0.9.1
0/0        0/0          0/0    0/0     0/0       ✓ │   │   │   ├── borsh-derive 0.9.1
0/0        0/0          0/0    0/0     0/0       ✓ │   │   │   │   ├── borsh-derive-internal 0.9.1
0/0        0/0          0/0    0/0     0/0       ✓ │   │   │   │   │   ├── proc-macro2 1.0.32
0/0        0/0          0/0    0/0     0/0       ✓ │   │   │   │   │   │   └── unicode-xid 0.2.2
0/0        0/0          0/0    0/0     0/0       ✓ │   │   │   │   │   ├── quote 1.0.10
0/0        0/0          0/0    0/0     0/0       ✓ │   │   │   │   │   │   └── proc-macro2 1.0.32
0/0        45/45        3/3    0/0     2/2       ✓ ✓ │   │   │   │   │   └── syn 1.0.78
0/0        0/0          0/0    0/0     0/0       ✓ │   │   │   │   │       ├── proc-macro2 1.0.32
0/0        0/0          0/0    0/0     0/0       ✓ │   │   │   │   │       ├── quote 1.0.10
0/0        0/0          0/0    0/0     0/0       ✓ │   │   │   │   │       └── unicode-xid 0.2.2
0/0        0/0          0/0    0/0     0/0       ✓ │   │   │   │   ├── borsh-schema-derive-internal 0.9.1
0/0        0/0          0/0    0/0     0/0       ✓ │   │   │   │   │   ├── proc-macro2 1.0.32
0/0        0/0          0/0    0/0     0/0       ✓ │   │   │   │   │   ├── quote 1.0.10
0/0        45/45        3/3    0/0     2/2       ✓ ✓ │   │   │   │   │   └── syn 1.0.78
0/0        0/0          0/0    0/0     0/0       ✓ │   │   │   │   ├── proc-macro-crate 0.1.5
0/0        0/0          0/0    0/0     0/0       ✓ │   │   │   │   │   └── toml 0.5.8
0/0        37/42        1/1    0/0     0/0       ✓ ✓ │   │   │   │   │       ├── indexmap 1.7.0
2/2        1082/1198    19/22  1/1     51/58     ✓ ✓ │   │   │   │   │       │   ├── hashbrown 0.11.2
0/0        5/5          0/0    0/0     0/0       ✓ ✓ │   │   │   │   │       │   │   └── serde 1.0.136
0/0        0/0          0/0    0/0     0/0       ✓ │   │   │   │   │       │   │       └── serde_derive 1.0.136
0/0        0/0          0/0    0/0     0/0       ✓ │   │   │   │   │       │   │           ├── proc-macro2 1.0.32
0/0        0/0          0/0    0/0     0/0       ✓ │   │   │   │   │       │   │           ├── quote 1.0.10
0/0        45/45        3/3    0/0     2/2       ✓ ✓ │   │   │   │   │       │   │           └── syn 1.0.78
0/0        5/5          0/0    0/0     0/0       ✓ ✓ │   │   │   │   │       │   └── serde 1.0.136
0/0        5/5          0/0    0/0     0/0       ✓ ✓ │   │   │   │   │       └── serde 1.0.136
0/0        0/0          0/0    0/0     0/0       ✓ │   │   │   │   ├── proc-macro2 1.0.32
0/0        45/45        3/3    0/0     2/2       ✓ ✓ │   │   │   │   └── syn 1.0.78
2/2        1006/1098    16/19  0/0     35/39     ✓ ✓ │   │   │   └── hashbrown 0.9.1
0/0        16/20        0/0    0/0     0/0       ✓ ✓ │   │   │       ├── ahash 0.4.7
0/0        5/5          0/0    0/0     0/0       ✓ ✓ │   │   │       └── serde 1.0.136
0/0        1/1          0/0    0/0     0/0       ✓ ✓ │   │   ├── bs58 0.4.0
12/12      231/231      0/0    0/0     0/0       ✓ ✓ │   │   └── sha2 0.9.8
0/0        6/6          0/0    0/0     0/0       ✓ ✓ │   │       ├── block-buffer 0.9.0
0/0        3/3          0/0    0/0     0/0       ✓ ✓ │   │       │   ├── block-padding 0.2.1
1/1        295/295      20/20  8/8     5/5       ✓ ✓ │   │       │   └── generic-array 0.14.4
0/0        5/5          0/0    0/0     0/0       ✓ ✓ │   │       │       ├── serde 1.0.136
0/0        0/0          0/0    0/0     0/0       ✓ │   │       │       └── typenum 1.14.0
0/0        0/0          0/0    0/0     0/0       ✓ │   │       ├── cfg-if 1.0.0
0/1        0/14         0/0    0/0     0/0       ✓ │   │       ├── cpufeatures 0.2.1
0/0        0/0          0/0    0/0     0/0       ✓ │   │       ├── digest 0.9.0
1/1        295/295      20/20  8/8     5/5       ✓ ✓ │   │       │   └── generic-array 0.14.4
0/0        0/0          0/0    0/0     0/0       ✓ │   │       └── opaque-debug 0.3.0
0/0        0/0          0/0    0/0     0/0       ✓ │   ├── near-primitives-core 0.10.0
0/0        0/0          0/0    0/0     0/0       ✓ │   │   ├── base64 0.11.0
0/0        7/7          0/0    0/0     0/0       ✓ ✓ │   │   ├── borsh 0.9.1
0/0        1/1          0/0    0/0     0/0       ✓ ✓ │   │   ├── bs58 0.4.0
0/0        0/0          0/0    0/0     0/0       ✓ │   │   ├── derive_more 0.99.16
0/0        0/0          0/0    0/0     0/0       ✓ │   │   │   ├── convert_case 0.4.0
0/0        15/15        0/0    0/0     0/0       ✓ ✓ │   │   │   └── rand 0.7.3
2/4        50/150       1/1    0/0     3/3       ✓ ✓ │   │   │       ├── getrandom 0.1.16
0/0        0/0          0/0    0/0     0/0       ✓ │   │   │       │   ├── cfg-if 1.0.0
0/20       12/353       0/2    0/0     2/38      ✓ ✓ │   │   │       │   └── libc 0.2.122
0/20       12/353       0/2    0/0     2/38      ✓ ✓ │   │   │       ├── libc 0.2.122
0/0        0/0          0/0    0/0     0/0       ✓ │   │   │       ├── rand_chacha 0.2.2
2/2        636/712      0/0    0/0     17/25     ✓ ✓ │   │   │       │   ├── ppv-lite86 0.2.16
0/0        22/22        0/0    0/0     0/0       ✓ ✓ │   │   │       │   └── rand_core 0.5.1
2/4        50/150       1/1    0/0     3/3       ✓ ✓ │   │   │       │       ├── getrandom 0.1.16
0/0        5/5          0/0    0/0     0/0       ✓ ✓ │   │   │       │       └── serde 1.0.136
0/0        22/22        0/0    0/0     0/0       ✓ ✓ │   │   │       └── rand_core 0.5.1
0/0        0/0          0/0    0/0     0/0       ✓ │   │   ├── proc-macro2 1.0.32
0/0        0/0          0/0    0/0     0/0       ✓ │   │   ├── quote 1.0.10
0/0        45/45        3/3    0/0     2/2       ✓ ✓ │   │   │   └── syn 1.0.78
0/0        0/0          0/0    0/0     0/0       ✓ │   │   ├── hex 0.4.3
0/0        5/5          0/0    0/0     0/0       ✓ ✓ │   │   │   └── serde 1.0.136
0/0        7/7          1/1    0/0     0/0       ✓ ✓ │   │   ├── lazy_static 1.4.0
0/0        0/0          0/0    0/0     0/0       ✓ │   │   ├── near-account-id 0.10.0
0/0        7/7          0/0    0/0     0/0       ✓ ✓ │   │   │   ├── borsh 0.9.1
0/0        5/5          0/0    0/0     0/0       ✓ ✓ │   │   │   └── serde 1.0.136
0/0        0/0          0/0    0/0     0/0       ✓ │   │   ├── num-rational 0.3.2
0/0        6/11         0/0    0/0     0/0       ✓ ✓ │   │   │   ├── num-bigint 0.3.3
0/0        0/0          0/0    0/0     0/0       ✓ │   │   │   │   ├── num-integer 0.1.44
0/0        4/10         0/0    0/0     0/0       ✓ ✓ │   │   │   │   │   └── num-traits 0.2.14
0/0        4/10         0/0    0/0     0/0       ✓ ✓ │   │   │   │   ├── num-traits 0.2.14
0/0        15/15        0/0    0/0     0/0       ✓ ✓ │   │   │   │   ├── rand 0.7.3
0/0        5/5          0/0    0/0     0/0       ✓ ✓ │   │   │   │   │   └── serde 1.0.136
0/0        0/0          0/0    0/0     0/0       ✓ │   │   │   ├── num-integer 0.1.44
0/0        4/10         0/0    0/0     0/0       ✓ ✓ │   │   │   │   ├── num-traits 0.2.14
0/0        5/5          0/0    0/0     0/0       ✓ ✓ │   │   │   │   └── serde 1.0.136
0/0        5/5          0/0    0/0     0/0       ✓ ✓ │   │   │   ├── serde 1.0.136
0/0        4/7          0/0    0/0     0/0       ✓ ✓ │   │   │   ├── serde_json 1.0.71
0/0        37/42        1/1    0/0     0/0       ✓ ✓ │   │   │   │   ├── indexmap 1.7.0
0/0        1/1          0/0    0/0     0/0       ✓ ✓ │   │   │   │   ├── itoa 0.4.8
8/12       674/921      0/0    0/0     2/2       ✓ ✓ │   │   │   │   ├── ryu 1.0.5
0/0        5/5          0/0    0/0     0/0       ✓ ✓ │   │   │   │   └── serde 1.0.136
12/12      231/231      0/0    0/0     0/0       ✓ ✓ │   │   │   └── sha2 0.9.8
0/0        0/0          0/0    0/0     0/0       ✓ │   │   ├── near-sdk-macros 4.0.0-pre.7
0/0        0/0          0/0    0/0     0/0       ✓ │   │   │   ├── Inflector 0.11.4
0/0        7/7          1/1    0/0     0/0       ✓ ✓ │   │   │   │   ├── lazy_static 1.4.0
0/0        34/34        1/2    0/0     2/2       ✓ ✓ │   │   │   │   └── regex 1.5.4
19/19      678/678      0/0    0/0     22/22     ✓ ✓ │   │   │   │       ├── aho-corasick 0.7.18
36/37      2067/2140    0/0    0/0     16/16     ✓ ✓ │   │   │   │       │   └── memchr 2.4.1
0/20       12/353       0/2    0/0     2/38      ✓ ✓ │   │   │   │       │       └── libc 0.2.122
36/37      2067/2140    0/0    0/0     16/16     ✓ ✓ │   │   │   │       ├── memchr 2.4.1
0/0        0/0          0/0    0/0     0/0       ✓ │   │   │   │       └── regex-syntax 0.6.25
0/0        0/0          0/0    0/0     0/0       ✓ │   │   │   ├── proc-macro2 1.0.32
```

```
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   ├── quote 1.0.10
0/0        45/45        3/3    0/0     2/2       ✓ ✓   |   |   |   └── syn 1.0.78
1/1        1/1          0/0    0/0     0/0       ✓ ✓   |   |   ├── near-sys 0.1.0
0/0        9/9          0/0    0/0     0/0       ✓ ✓   |   |   ├── near-vm-logic 0.10.0
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   ├── base64 0.13.0
0/0        7/7          0/0    0/0     0/0       ✓ ✓   |   |   |   ├── borsh 0.9.1
0/0        1/1          0/0    0/0     0/0       ✓ ✓   |   |   |   ├── bs58 0.4.0
1/1        193/193      0/0    0/0     0/0       ✓ ✓   |   |   |   ├── byteorder 1.4.3
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   ├── near-account-id 0.10.0
0/0        1/1          0/0    0/0     0/0       ✓ ✓   |   |   |   |   ├── near-crypto 0.10.0
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   |   ├── arrayref 0.3.6
0/0        12/21        13/13  1/1     0/0       ✓ ✓   |   |   |   |   ├── blake2 0.9.2
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   |   ├── crypto-mac 0.8.0
1/1        295/295      20/20  8/8     5/5       ✓ ✓   |   |   |   |   |   |   ├── generic-array 0.14.4
0/0        3/3          0/0    0/0     0/0       ✓ ✓   |   |   |   |   |   |   └── subtle 2.4.1
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   |   ├── digest 0.9.0
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   |   └── opaque-debug 0.3.0
0/0        7/7          0/0    0/0     0/0       ✓ ✓   |   |   |   ├── borsh 0.9.1
0/0        1/1          0/0    0/0     0/0       ✓ ✓   |   |   |   ├── bs58 0.4.0
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   ├── c2-chacha 0.3.3
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   ├── cipher 0.2.5
1/1        295/295      20/20  8/8     5/5       ✓ ✓   |   |   |   |   |   └── generic-array 0.14.4
2/2        636/712      0/0    0/0     17/25     ✓ ✓   |   |   |   |   └── ppv-lite86 0.2.16
0/2        0/857        0/0    0/0     0/0       ✓ |   |   |   |   ├── curve25519-dalek 3.2.0
1/1        193/193      0/0    0/0     0/0       ✓ ✓   |   |   |   |   |   ├── byteorder 1.4.3
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   |   ├── digest 0.9.0
0/0        22/22        0/0    0/0     0/0       ✓ ✓   |   |   |   |   |   ├── rand_core 0.5.1
0/0        5/5          0/0    0/0     0/0       ✓ ✓   |   |   |   |   |   ├── serde 1.0.136
0/0        3/3          0/0    0/0     0/0       ✓ ✓   |   |   |   |   |   ├── subtle 2.4.1
1/1        22/22        0/0    0/0     0/0       ✓ ✓   |   |   |   |   |   └── zeroize 1.4.3
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   |       └── zeroize_derive 1.2.2
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   |           ├── proc-macro2 1.0.32
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   |           ├── quote 1.0.10
0/0        45/45        3/3    0/0     2/2       ✓ ✓   |   |   |   |           |   ├── syn 1.0.78
0/0        0/0          1/1    0/0     0/0       ✓ ✓   |   |   |   |           |   └── unicode-xid 0.2.2
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |           └── synstructure 0.12.6
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |               ├── proc-macro2 1.0.32
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |               ├── quote 1.0.10
0/0        45/45        3/3    0/0     2/2       ✓ ✓   |   |   |               |   ├── syn 1.0.78
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |               |   └── unicode-xid 0.2.2
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   ├── derive_more 0.99.16
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   ├── ed25519-dalek 1.0.1
0/2        0/857        0/0    0/0     0/0       ✓ |   |   |   |   ├── curve25519-dalek 3.2.0
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   ├── ed25519 1.3.0
0/0        5/5          0/0    0/0     0/0       ✓ ✓   |   |   |   |   |   ├── serde 1.0.136
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   |   ├── signature 1.5.0
0/0        15/15        0/0    0/0     0/0       ✓ ✓   |   |   |   |   |   |   └── rand_core 0.6.3
2/4        50/149       1/1    0/0     3/3       ✓ ✓   |   |   |   |   |   |       ├── getrandom 0.2.3
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   |   |   |       |   ├── cfg-if 1.0.0
0/20       12/353       0/2    0/0     2/38      ✓ ✓   |   |   |   |   |   |       |   └── libc 0.2.122
0/0        5/5          0/0    0/0     0/0       ✓ ✓   |   |   |   |   |   |       └── serde 1.0.136
1/1        22/22        0/0    0/0     0/0       ✓ ✓   |   |   |   |   |   └── zeroize 1.4.3
0/0        15/15        0/0    0/0     0/0       ✓ ✓   |   |   |   |   ├── rand 0.7.3
0/0        22/22        0/0    0/0     0/0       ✓ ✓   |   |   |   |   ├── rand_core 0.5.1
0/0        5/5          0/0    0/0     0/0       ✓ ✓   |   |   |   |   ├── serde 1.0.136
12/12      231/231      0/0    0/0     0/0       ✓ ✓   |   |   |   |   ├── sha2 0.9.8
1/1        22/22        0/0    0/0     0/0       ✓ ✓   |   |   |   |   └── zeroize 1.4.3
0/0        7/7          1/1    0/0     0/0       ✓ ✓   |   |   |   ├── lazy_static 1.4.0
0/20       12/353       0/2    0/0     2/38      ✓ ✓   |   |   |   ├── libc 0.2.122
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   ├── near-account-id 0.10.0
0/0        215/215      2/2    0/0     0/0       ✓ ✓   |   |   |   ├── parity-secp256k1 0.7.0
4/4        295/295      2/2    1/1     5/5       ✓ ✓   |   |   |   |   ├── arrayvec 0.5.2
0/0        5/5          0/0    0/0     0/0       ✓ ✓   |   |   |   |   |   └── serde 1.0.136
0/0        15/15        0/0    0/0     0/0       ✓ ✓   |   |   |   |   └── rand 0.7.3
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   ├── primitive-types 0.10.1
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   |   ├── fixed-hash 0.7.0
1/1        193/193      0/0    0/0     0/0       ✓ ✓   |   |   |   |   |   |   ├── byteorder 1.4.3
0/0        14/30        0/0    0/0     0/0       ✓ ✓   |   |   |   |   |   |   ├── rand 0.8.4
0/20       12/353       0/2    0/0     2/38      ✓ ✓   |   |   |   |   |   |   |   ├── libc 0.2.122
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   |   |   |   |   ├── rand_chacha 0.3.1
2/2        636/712      0/0    0/0     17/25     ✓ ✓   |   |   |   |   |   |   |   |   |   ├── ppv-lite86 0.2.16
0/0        15/15        0/0    0/0     0/0       ✓ ✓   |   |   |   |   |   |   |   |   |   ├── rand_core 0.6.3
0/0        5/5          0/0    0/0     0/0       ✓ ✓   |   |   |   |   |   |   |   |   |   └── serde 1.0.136
0/0        15/15        0/0    0/0     0/0       ✓ ✓   |   |   |   |   |   |   |   |   ├── rand_core 0.6.3
0/0        5/5          0/0    0/0     0/0       ✓ ✓   |   |   |   |   |   |   |   |   └── serde 1.0.136
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   |   |   |   ├── rustc-hex 2.1.0
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   |   |   └── static_assertions 1.1.0
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   |   ├── impl-codec 0.5.1
0/0        4/4          0/0    0/0     0/0       ✓ ✓   |   |   |   |   |   └── parity-scale-codec 2.3.1
2/2        350/350      2/2    0/0     7/7       ✓ ✓   |   |   |   |   |       ├── arrayvec 0.7.2
0/0        5/5          0/0    0/0     0/0       ✓ ✓   |   |   |   |   |       |   └── serde 1.0.136
15/15      1105/1108    14/14  1/1     62/62     ✓ ✓   |   |   |   |   |       ├── bitvec 0.20.4
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   |   |       |   ├── funty 1.1.0
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   |   |       |   ├── radium 0.6.2
0/0        5/5          0/0    0/0     0/0       ✓ ✓   |   |   |   |   |   |       |   ├── serde 1.0.136
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   |   |       |   ├── tap 1.0.1
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   |   |       |   └── wyz 0.2.0
0/0        0/0          2/2    3/3     0/0       ✓ ✓   |   |   |   |   |       ├── byte-slice-cast 1.2.0
1/1        295/295      20/20  8/8     5/5       ✓ ✓   |   |   |   |   |       ├── generic-array 0.14.4
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   |   |       ├── impl-trait-for-tuples 0.2.1
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   |   |       ├── proc-macro2 1.0.32
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   |   |       ├── quote 1.0.10
0/0        45/45        3/3    0/0     2/2       ✓ ✓   |   |   |   |   |   |       └── syn 1.0.78
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   |   |       ├── parity-scale-codec-derive 2.3.1
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   |   |       |   ├── proc-macro-crate 1.1.0
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   |   |       |   |   ├── thiserror 1.0.30
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   |   |       |   |   |   └── thiserror-impl 1.0.30
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   |   |       |   |   |       ├── proc-macro2 1.0.32
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   |   |       |   |   |       ├── quote 1.0.10
0/0        45/45        3/3    0/0     2/2       ✓ ✓   |   |   |   |   |   |       |   |   |       └── syn 1.0.78
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   |   |       |   |   └── toml 0.5.8
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   |   |       |   ├── proc-macro2 1.0.32
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   |   |       |   ├── quote 1.0.10
0/0        45/45        3/3    0/0     2/2       ✓ ✓   |   |   |   |   |   |       |   └── syn 1.0.78
0/0        5/5          0/0    0/0     0/0       ✓ ✓   |   |   |   |   |   |       └── serde 1.0.136
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   |   └── uint 0.9.1
1/1        193/193      0/0    0/0     0/0       ✓ ✓   |   |   |   |   |       ├── byteorder 1.4.3
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   |       ├── crunchy 0.2.2
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   |       ├── hex 0.4.3
0/0        15/15        0/0    0/0     0/0       ✓ ✓   |   |   |   |       ├── rand 0.7.3
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   |       └── static_assertions 1.1.0
0/0        15/15        0/0    0/0     0/0       ✓ ✓   |   |   |   ├── rand 0.7.3
0/0        22/22        0/0    0/0     0/0       ✓ ✓   |   |   |   ├── rand_core 0.5.1
0/0        5/5          0/0    0/0     0/0       ✓ ✓   |   |   |   ├── serde 1.0.136
0/0        4/7          0/0    0/0     0/0       ✓ ✓   |   |   |   ├── serde_json 1.0.71
0/0        3/3          0/0    0/0     0/0       ✓ ✓   |   |   |   ├── subtle 2.4.1
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   └── thiserror 1.0.30
0/0        0/0          0/0    0/0     0/0       ✓ |   |   ├── near-primitives 0.10.0
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   ├── base64 0.13.0
0/0        7/7          0/0    0/0     0/0       ✓ ✓   |   |   |   ├── borsh 0.9.1
0/0        1/1          0/0    0/0     0/0       ✓ ✓   |   |   |   ├── bs58 0.4.0
1/1        193/193      0/0    0/0     0/0       ✓ ✓   |   |   |   ├── byteorder 1.4.3
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   ├── bytesize 1.1.0
0/0        5/5          0/0    0/0     0/0       ✓ ✓   |   |   |   |   └── serde 1.0.136
1/1        44/90        2/2    0/0     0/0       ✓ ✓   |   |   |   ├── chrono 0.4.19
0/20       12/353       0/2    0/0     2/38      ✓ ✓   |   |   |   |   ├── libc 0.2.122
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   ├── num-integer 0.1.44
0/0        4/10         0/0    0/0     0/0       ✓ ✓   |   |   |   |   |   ├── num-traits 0.2.14
0/0        5/5          0/0    0/0     0/0       ✓ ✓   |   |   |   |   |   ├── serde 1.0.136
1/1        216/216      0/0    0/0     0/0       ✓ ✓   |   |   |   |   |   └── time 0.1.43
0/20       12/353       0/2    0/0     2/38      ✓ ✓   |   |   |   |   |       └── libc 0.2.122
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   ├── derive_more 0.99.16
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   ├── easy-ext 0.2.9
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   ├── hex 0.4.3
0/0        1/1          0/0    0/0     0/0       ✓ ✓   |   |   |   ├── near-crypto 0.10.0
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   ├── near-primitives-core 0.10.0
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   ├── near-rpc-error-macro 0.10.0
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   |   ├── near-rpc-error-core 0.10.0
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   |   |   ├── proc-macro2 1.0.32
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   |   |   ├── quote 1.0.10
0/0        5/5          0/0    0/0     0/0       ✓ ✓   |   |   |   |   |   |   ├── serde 1.0.136
0/0        45/45        3/3    0/0     2/2       ✓ ✓   |   |   |   |   |   |   └── syn 1.0.78
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   |   ├── proc-macro2 1.0.32
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   |   ├── quote 1.0.10
0/0        5/5          0/0    0/0     0/0       ✓ ✓   |   |   |   |   |   ├── serde 1.0.136
0/0        4/7          0/0    0/0     0/0       ✓ ✓   |   |   |   |   |   ├── serde_json 1.0.71
0/0        45/45        3/3    0/0     2/2       ✓ ✓   |   |   |   |   |   └── syn 1.0.78
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   ├── near-vm-errors 0.10.0
0/0        7/7          0/0    0/0     0/0       ✓ ✓   |   |   |   |   ├── borsh 0.9.1
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   ├── hex 0.4.3
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   ├── near-account-id 0.10.0
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   ├── near-rpc-error-macro 0.10.0
0/0        5/5          0/0    0/0     0/0       ✓ ✓   |   |   |   |   └── serde 1.0.136
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   ├── num-rational 0.3.2
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   ├── primitive-types 0.10.1
0/0        15/15        0/0    0/0     0/0       ✓ ✓   |   |   |   ├── rand 0.7.3
0/0        151/151      0/0    0/0     0/0       ✓ ✓   |   |   |   ├── reed-solomon-erasure 4.0.2
0/20       12/353       0/2    0/0     2/38      ✓ ✓   |   |   |   |   ├── libc 0.2.122
1/1        392/392      7/7    1/1     13/13     ✓ ✓   |   |   |   |   └── smallvec 1.7.0
0/0        5/5          0/0    0/0     0/0       ✓ ✓   |   |   |   |       └── serde 1.0.136
0/0        34/34        1/2    0/0     2/2       ✓ ✓   |   |   |   ├── regex 1.5.4
0/0        5/5          0/0    0/0     0/0       ✓ ✓   |   |   |   ├── serde 1.0.136
0/0        4/7          0/0    0/0     0/0       ✓ ✓   |   |   |   ├── serde_json 1.0.71
12/12      231/231      0/0    0/0     0/0       ✓ ✓   |   |   |   ├── sha2 0.9.8
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   ├── smart-default 0.6.0
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   ├── proc-macro2 1.0.32
0/0        0/0          0/0    0/0     0/0       ✓ |   |   |   |   ├── quote 1.0.10
```

```
0/0         45/45        3/3    0/0     2/2       ✓ ✓  |   |   |   |   |   └── syn 1.0.78
0/0          0/0          0/0    0/0     0/0        ✓ |   |   |   |   |   └── validator 0.12.0
0/0          0/0          0/0    0/0     0/0        ✓ |   |   |   |   |       ├── idna 0.2.3
0/0          0/0          0/0    0/0     0/0        ✓ |   |   |   |   |       |   ├── matches 0.1.9
0/0          0/0          0/0    0/0     0/0       ✓ |   |   |   |   |       |   ├── unicode-bidi 0.3.7
0/0          5/5          0/0    0/0     0/0       ✓ ✓  |   |   |   |       |   |   └── serde 1.0.136
0/0         20/20         0/0    0/0     0/0       ✓ ✓  |   |   |   |       |   └── unicode-normalization 0.1.19
0/0          0/0          0/0    0/0     0/0       ✓ |   |   |   |       |       └── tinyvec 1.5.1
0/0          5/5          0/0    0/0     0/0       ✓ ✓  |   |   |   |       |           ├── serde 1.0.136
0/0          0/0          0/0    0/0     0/0        ✓ |   |   |   |       |           └── tinyvec_macros 0.1.0
0/0          7/7          1/1    0/0     0/0       ✓ ✓  |   |   |   |       ├── lazy_static 1.4.0
0/0         34/34         1/2    0/0     2/2       ✓ ✓  |   |   |   |       ├── regex 1.5.4
0/0          5/5          0/0    0/0     0/0       ✓ ✓  |   |   |   |       ├── serde 1.0.136
0/0          0/0          0/0    0/0     0/0        ✓ |   |   |   |       ├── serde_derive 1.0.136
0/0          4/7          0/0    0/0     0/0       ✓ ✓  |   |   |   |       ├── serde_json 1.0.71
0/0          0/0          0/0    0/0     0/0        ✓ |   |   |   |       ├── url 2.2.2
0/0          2/2          0/0    0/0     0/0       ✓ ✓  |   |   |   |       |   ├── form_urlencoded 1.0.1
0/0          0/0          0/0    0/0     0/0        ✓ |   |   |   |       |   |   ├── matches 0.1.9
0/0          3/3          0/0    0/0     0/0       ✓ ✓  |   |   |   |       |   |   └── percent-encoding 2.1.0
0/0          0/0          0/0    0/0     0/0        ✓ |   |   |   |       |   ├── idna 0.2.3
0/0          0/0          0/0    0/0     0/0        ✓ |   |   |   |       |   ├── matches 0.1.9
0/0          3/3          0/0    0/0     0/0       ✓ ✓  |   |   |   |       |   ├── percent-encoding 2.1.0
0/0          5/5          0/0    0/0     0/0       ✓ ✓  |   |   |   |       |   └── serde 1.0.136
0/0          0/0          0/0    0/0     0/0        ✓ |   |   |   |       └── validator_types 0.12.0
0/0          0/0          0/0    0/0     0/0        ✓ |   |   |   |   ├── near-primitives-core 0.10.0
0/0          0/0          0/0    0/0     0/0        ✓ |   |   |   |   ├── near-vm-errors 0.10.0
0/0          0/0          0/0    0/0     0/0        ✓ |   |   |   |   ├── ripemd160 0.9.1
0/0          6/6          0/0    0/0     0/0       ✓ ✓  |   |   |   |   ├── block-buffer 0.9.0
0/0         0/0          0/0    0/0     0/0       ✓ |   |   |   |   ├── digest 0.9.0
0/0          0/0          0/0    0/0     0/0        ✓ |   |   |   |   └── opaque-debug 0.3.0
0/0          5/5          0/0    0/0     0/0       ✓ ✓  |   |   |   ├── serde 1.0.136
12/12      231/231        0/0    0/0     0/0       ✓ ✓  |   |   |   ├── sha2 0.9.8
0/0         14/14         0/0    0/0     0/0       ✓ ✓  |   |   |   └── sha3 0.9.1
0/0          6/6          0/0    0/0     0/0       ✓ ✓  |   |   |       ├── block-buffer 0.9.0
0/0          0/0          0/0    0/0     0/0       ✓ |   |   |       ├── digest 0.9.0
0/0          0/0          0/0    0/0     0/0        ✓ |   |   |       |   ├── keccak 0.1.0
0/0          0/0          0/0    0/0     0/0        ✓ |   |   |       |   └── opaque-debug 0.3.0
0/0          5/5          0/0    0/0     0/0       ✓ ✓  |   |   ├── serde 1.0.136
0/0          4/7          0/0    0/0     0/0       ✓ ✓  |   |   ├── serde_json 1.0.71
3/5        460/570        4/4    1/1     21/25     ✓ ✓  |   |   └── wee_alloc 0.4.5
0/0          0/0          0/0    0/0     0/0        ✓ |   |       ├── cfg-if 0.1.10
0/20        12/353        0/2    0/0     2/38      ✓ ✓  |   |       ├── libc 0.2.122
0/0          0/0          0/0    0/0     0/0        ✓ |   |       └── memory_units 0.4.0
0/0          5/5          0/0    0/0     0/0       ✓ ✓  |   ├── serde 1.0.136
0/0          4/7          0/0    0/0     0/0       ✓ ✓  |   └── serde_json 1.0.71
53/53      460/478        0/0    0/0     0/0       ✓ ✓  └── near-sdk 4.0.0-pre.7

169/203     10995/13235  112/121 17/17   268/327

error: Found 12 warnings
```

Adherence to Best Practices

1. Use `require!` with a higher level error message instead of plain assert statements without messages, e.g. in `lib.rs:record_batch`.
2. Use rust's `..=` syntax in `math.rs:formula` for iterating when the upper bound should be included in the `for` loop.
3. Consider checking whether using the borsh serializer for encoding the vector arguments can cut down on bandwidth required for calling the `*_batch` functions.
4. Consider checking whether `tge_mint_batch` can use smaller integers than `U128` as arguments and scale them up in the function to save bandwidth and speed up the minting process.
5. Consider using a simplified version of `math.rs:formula` for use with `lib.rs:record_batch`. Since the `steps` input to this function is bound by the type of the argument to `record_batch`, the value cannot exceed `std::u16::MAX`, which is `65535`. The current `formula` implementation splits the token computation into slices of trillions of steps recorded since the `tge` event. Due to the aforementioned limit on the input value, the split path will almost never be taken. By modifying the function to always use the first trillion, the code can be made significantly easier to read by introducing a small deviation whenenver the next trillion steps are recorded.
   With the following implementation, the error is small enough for inputs less than `std::u16::MAX` that the tests still pass.

```
pub fn formula_simplified(steps_from_tge: f64, steps: f64) -> u128 {
    let trillion = (steps_from_tge / 1e+12).floor() as usize;
    if trillion < KS.len() {
        (area_under_line(
            KS[trillion],
            BS[trillion],
            steps_from_tge,
            steps_from_tge + steps) * 1e+18) as u128
    } else {
        (exp_decay(steps_from_tge, steps) * 1e+18) as u128
    }
}
```

1. Consider emitting an event when adding and removing an oracle.

Test Results

Test Suite Results

cargo test

```
running 1 test
test math::tests::formula_test ... ok

test result: ok. 1 passed; 0 failed; 0 ignored; 0 measured; 0 filtered out; finished in 0.00s
```

Code Coverage

We used cargo-tarpaulin for coverage, we recommend you to add more tests to achieve more than 90% in the coverage.

```
INFO cargo_tarpaulin::report: Coverage Results:
|| Uncovered Lines:
|| sweat/src/lib.rs: 24, 26-28, 32-34, 38-40, 43-44, 48-50, 54-58, 62-64, 66, 73-74, 77-86, 88, 91-92, 102-104, 106-108, 111, 114, 124, 126-129
|| Tested/Total Lines:
|| sweat/src/lib.rs: 0/52
|| sweat/src/math.rs: 32/32
||
```

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

```
8eccc460c6608d72df5d55c5cf6ffa008a468c410fb72e334c444dabae9381e1 ./sweat/src/lib.rs

32c6f209a822034ad63f29c2f30987f96f96af145cd36e2aa8875c9ea0e9fd64 ./sweat/src/math.rs
```

Changelog

- 2022-06-22 - Initial report
- 2022-07-08 - Final Report

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.