Quantstamp Security Assessment Certificate

Hedgehog

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

Executive Summary

Type	Decentralized Prediction Markets
Auditors	Souhail Mssassi, Research Engineer
Timeline	2021-09-08 through 2021-10-08
Languages	Rust
Methods	Architecture Review, Unit Testing, Functional Testing, Computer-Aided Verification, Manual Review
Specification	Leaderboard Structure No-Loss Vault Parimutuel Architecture
Documentation Quality	Medium
Test Quality	Medium

Source Code

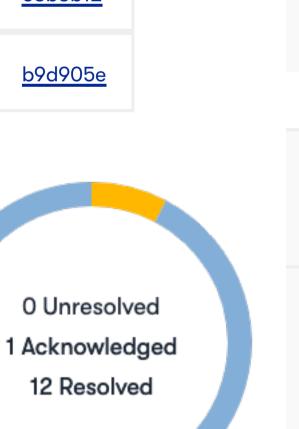| Repository	Commit
Hedgehog	53b3b12
None	b9d905e

Total Issues	13 (12 Resolved)
High Risk Issues	1 (1 Resolved)
Medium Risk Issues	5 (5 Resolved)
Low Risk Issues	5 (4 Resolved)
Informational Risk Issues	2 (2 Resolved)
Undetermined Risk Issues	0 (0 Resolved)

0 Unresolved
1 Acknowledged
12 Resolved

⌃ High Risk	The issue puts a large number of users' sensitive information at risk, or is reasonably likely to lead to catastrophic impact for client's reputation or serious financial implications for client and users.
⌃ Medium Risk	The issue puts a subset of users' sensitive information at risk, would be detrimental for the client's reputation if exploited, or is reasonably likely to lead to moderate financial impact.
⌄ Low Risk	The risk is relatively small and could not be exploited on a recurring basis, or is a risk that the client has indicated is low-impact in view of the client's business circumstances.
○ Informational	The issue does not post an immediate risk, but is relevant to security best practices or Defence in Depth.
? Undetermined	The impact of the issue is uncertain.

○ Unresolved	Acknowledged the existence of the risk, and decided to accept it without engaging in special efforts to control it.
○ Acknowledged	The issue remains in the code but is a result of an intentional business or design decision. As such, it is supposed to be addressed outside the programmatic means, such as: 1) comments, documentation, README, FAQ; 2) business processes; 3) analyses showing that the issue shall have no negative consequences in practice (e.g., gas analysis, deployment settings).
○ Resolved	Adjusted program implementation, requirements or constraints to eliminate the risk.
○ Mitigated	Implemented actions to minimize the impact or likelihood of the risk.

Summary of Findings

We have reviewed the code, documentation, and test suite and found several issues of various severities. Overall, we consider the code to be well-written and with sufficient documentation and a good test suite . We have outlined suggestions to better follow best practices, and recommend addressing all the findings to tighten the contracts for future deployments or contract updates. The team has addressed all the **13** issues found by QuantStamp.

ID	Description	Severity	Status
QSP-1	Address of the Parimutuel Program not Verified	⌃ High	Fixed
QSP-2	Overflow In The Find_User_Reward Function	⌃ Medium	Fixed
QSP-3	Overflow in the Output Msg	⌃ Medium	Mitigated
QSP-4	Overflow in the Output Reward Sources Variable	⌃ Medium	Fixed
QSP-5	Overflow in the Sponsor_Token_Amount and Amount Variable	⌃ Medium	Fixed
QSP-6	Overflow/Underflow In The Total Amount Deposited and Sponsored	⌃ Medium	Fixed
QSP-7	Lack of Verification in the Market Expiry	⌄ Low	Fixed
QSP-8	Lack of Verification in the LockUp Expiry	⌄ Low	Fixed
QSP-9	Lack of Verification in the Amount and Pool ID	⌄ Low	Fixed
QSP-10	Unnecessary Verification on Expiry_Unix	⌄ Low	Acknowledged
QSP-11	Lack of Verifcation on the Amount Variable	⌄ Low	Fixed
QSP-12	Comments Left In the Code	○ Informational	Fixed
QSP-13	Deprecated Functions Left In the Code	○ Informational	Fixed

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:

- [Tarpaulin](#) 0.14.2
- [Rust Audit](#) v0.12.0

- Cargo Geiger 0.11.1

Steps taken to run the tools:

```
cargo install cargo-tarpaulin (on a Linux environment) ` cargo tarpaulin --verbose -o=Html --output-dir='..' cargo install cargo-audit cargo audit cargo install
cargo-geiger
```

Findings

QSP-1 Address of the Parimutuel Program not Verified

Severity: *High Risk*

Status: Fixed

File(s) affected: `/hh-programs-anchor/hh-parimutuel/src/lib.rs`

Description: In the `lib.rs` file (L2677), located in `hh-paramitiuel` module, the address of the parimutuel is not verified; thus an attacker can execute remote code .

Recommendation: Declare the program id and verify that the parimutuel address matches the public key of the canonical program.

Update: The `parimutuel_program's` id is set using `solana_program::declare_id`, and the verification of the correct `parimutuel_program` account is passed in to `mint_game_token` by matching against the stated id.

QSP-2 Overflow In The Find_User_Reward Function

Severity: *Medium Risk*

Status: Fixed

File(s) affected: `/hh-programs-anchor/hh-parimutuel/src/lib.rs`

Description: The `find_user_reward` function in `hh-parimutuel/src/lib.rs` calculates the reward user, but in line 1722 it compares two variables: `FINAL_LEADERBOARD_LENGTH` and `counter + n`. The problem is that the addition is done with the `+` operator, which can cause an overflow. If one uses the debug build it can cause a panic; however in release build it will overflow silently. Same issue on L1741.

Recommendation: Instead of using the `+`operator, we recommend using the `checked_add` function to prevent an overflow.

Update: The team used `checked_add` in `find_user_reward` function to guard against overflow.

QSP-3 Overflow in the Output Msg

Severity: *Medium Risk*

Status: Mitigated

File(s) affected: `/hh-programs-anchor/hh-parimutuel/src/lib.rs`

Description: In the `lib.rs` file (L465), located in `hh-paramitiuel` module, there is a an output print of the sum of `collection_amount_pool_a` and `collection_amount_pool_b`. The problem here is that the addition is done using the `+` operator, which can cause an overflow. If one uses debug build, it can cause a panic; however, in release build it will overflow silently.

Recommendation: Instead of using the `+`operator, we recommend using the `checked_add` function to prevent an overflow.

Update: The team removed the unnecessary log message with potential for overflow.

QSP-4 Overflow in the Output Reward Sources Variable

Severity: *Medium Risk*

Status: Fixed

File(s) affected: `/hh-programs-anchor/hh-vault/src/lib.rs`

Description: In the `init_reward_info` function (see file `hh-vault/src/lib.rs` file, L1038), the `vault.reward_sources` is incremented by one using the `+` operator, which can cause an overflow. If one uses the debug build, it can cause a panic; however, in release build it will overflow silently.

Recommendation: Instead of using the `+`operator, we recommend using the `checked_add` function to prevent an overflow.

Update: The team used `checked_add` when incrementing `reward_sources`.

QSP-5 Overflow in the Sponsor_Token_Amount and Amount Variable

Severity: *Medium Risk*

Status: Fixed

File(s) affected: `/hh-programs-anchor/hh-vault/src/lib.rs`

Description: In the `handle_deposit` function (file `/hh-vault/src/lib.rs`, L2994 and 2995), the `state.sponsor_tokens_owned` and `state.amount` variables are incremented using the `+` operator, which can cause an overflow. If one uses the debug build, it can cause a panic; however, in release build it will overflow silently.

Recommendation: Instead of using the `+`operator, we recommend using the `checked_add` function to prevent an overflow.

Update: The team used `checked_add` in `SponsorState::handle_deposit`.

QSP-6 Overflow/Underflow In The Total Amount Deposited and Sponsored

Severity: *Medium Risk*

Status: Fixed

File(s) affected: `/hh-programs-anchor/hh-vault/src/lib.rs`

Description: In the `deposit_to_vault`/`withdraw_from_vault` function, the `vault.total_amount_deposited` and `vault.total_amount_sponsored` variables are incremented/decremented using the `+/-` operators, which can cause an overflow and underflow, respectively. If one uses the debug build, it can cause a panic; however, in release build it will overflow silently. This appears in `/hh-vault/src/lib.rs`, lines 1856, 1858, 2326, and 2328.

Recommendation: Instead of using the `+/-`operators, we recommend using the `checked_add`/`checked_sub` functions to prevent an overflow.

Update: The team used `checked_add` in `deposit_to_vault`.

QSP-7 Lack of Verification in the Market Expiry

Severity: *Low Risk*

Status: Fixed

File(s) affected: `/hh-programs-anchor/hh-parimutuel/src/lib.rs`

Description: The `lib.rs` file (L199), located in `hh-paramitiuel` module, contains the `init_market` public function. With the help of this function, one can initialize a market with some parameters. Amongst these parameters, we have the `_expiry_unix`, which is a timestamp that refers to the state of the market . The problem here is that there is no verification of the value of this variable; in fact, one can initialize the market with a `expiry_unix` that is lower than the current time. In the latter case, one will harm the logic of the program.

Recommendation: Verify that the `_expiry_unix` is greater than the current time .

Update: The team verified that `market.expiry_unix` is not set to a timestamp in the past using this comparaison `if _expiry_unix != 0 && current_time >= _expiry_unix`.

QSP-8 Lack of Verification in the LockUp Expiry

Severity: *Low Risk*

Status: Fixed

File(s) affected: `/hh-programs-anchor/hh-vault/src/lib.rs`

Description: The `lib.rs` file (L39), located in the `hh-vault` module, contains the `init_vault` public function. With the help of this function one can initialize a vault with some parameters. Amongst these parameters is the `_lockup_expiry`, which is a timestamp . The problem here is that there is no verification of this variable; in fact one can initialize a vault with a `_lockup_expiry` lower than the current time. In the latter case, one can harm the logic of the program.

Recommendation: Verify that the `_lockup_expiry` is greater than the current time .

Update: Since `_entry_deadline` is already verified to be before `_lockup_expiry`, the `_lockup_expiry` will also be ahead of current timestamp.

QSP-9 Lack of Verification in the Amount and Pool ID

Severity: *Low Risk*

Status: Fixed

File(s) affected: `/hh-programs-anchor/hh-vault/src/apricot.rs`

Description: The `add_user_and_deposit_full` function in `hh-vault/src/apricot.rs` takes two parameters, `amount` and `pool_id`. These parameters are not verified; also, one can inject an ID of a non-existent pool . See lines 60, 61, 102, and 103.

Recommendation: Verify if the `amount` is greater than zero; also verify if `pool_id` matches an existing pool.

Update: The team have added a verification to `_deposit_ticket_amount`, to ensure that it is greater than zero. This is the value that is passed in as the amount to the apricot instruction.

QSP-10 Unnecessary Verification on Expiry_Unix

Severity: *Low Risk*

Status: Acknowledged

File(s) affected: `/hh-programs-anchor/hh-parimutuel/src/lib.rs`

Description: Lines 364 and 381 in `lib.rs`, located in the `hh-paramitiuel` module, compares `market.expiry_unix` against zero. If the verification is performed using the comparison between `market.expiry_unix` and the current time, there is no need to verify against zero .

Recommendation: Verify that the `_expiry_unix` is greater than the current time. No other verification is needed for that variable.

Update: The team claims that the zero value serves as the default null value, and it indicates that the `expiry_unix` is unset.

QSP-11 Lack of Verifcation on the Amount Variable

Severity: *Low Risk*

Status: Fixed

File(s) affected: `/hh-programs-anchor/hh-parimutuel/src/lib.rs`

Description: In the `enter_prediction` function in `lib.rs` file (L256), located in the `hh-paramitiuel` module, one enters a prediction for a specified market, as well as an amount. The amount variable, however, is not verified and it can be given the zero value.

Recommendation: The Team should verify if the amount is greater than zero.

Update: The team verified that the amount submitted to `enter_prediction` is non zero.

QSP-12 Comments Left In the Code

Severity: *Informational*

Status: Fixed

File(s) affected: `/hh-programs-anchor/hh-vault/src/lib.rs`

Description: The `lib.rs` file, located in the `hh-vault` module, contains code that is completely commented out--see L883 and 1441. This is currently dead code.

Recommendation: Remove the commented out code as it has no purpose.

Update: The team removed the commented code.

QSP-13 Deprecated Functions Left In the Code

Severity: *Informational*

Status: Fixed

File(s) affected: `/hh-programs-anchor/hh-vault/src/lib.rs`

Description: We found some functions marked as deprecated; if these functions are not used anymore, the team should consider removing them. This appears in `hh-vault/src/lib.rs`, on lines 843, 919, 1315, 2538, 2562, and 2777.

Recommendation: The Team should remove the deprecated functions.

Update: The team removed the deprecated code.

Automated Analyses

Tarpaulin

hh-Parimutuel

```
Compiling proc-macro2 v1.0.27
Compiling unicode-xid v0.2.2
Compiling syn v1.0.73
Compiling serde_derive v1.0.126
Compiling serde v1.0.126
Compiling typenum v1.13.0
Compiling version_check v0.9.3
Compiling cfg-if v1.0.0
Compiling block-padding v0.2.1
Compiling libc v0.2.97
Compiling opaque-debug v0.3.0
Compiling cpufeatures v0.1.4
Compiling subtle v2.4.0
Compiling bs58 v0.3.1
Compiling semver-parser v0.7.0
Compiling ryu v1.0.5
Compiling anyhow v1.0.41
Compiling memchr v2.4.0
Compiling serde_json v1.0.64
Compiling crunchy v0.2.2
Compiling unicode-segmentation v1.7.1
Compiling getrandom v0.1.16
Compiling itoa v0.4.7
Compiling yansi v0.5.0
Compiling autocfg v1.0.1
Compiling log v0.4.14
Compiling regex-syntax v0.6.25
Compiling feature-probe v0.1.1
Compiling ucd-trie v0.1.3
Compiling cc v1.0.68
Compiling humantime v2.1.0
Compiling termcolor v1.1.2
Compiling rustversion v1.0.5
Compiling ppv-lite86 v0.2.10
Compiling lazy_static v1.4.0
Compiling ahash v0.4.7
Compiling arrayref v0.3.6
Compiling keccak v0.1.0
Compiling constant_time_eq v0.1.5
Compiling base64 v0.12.3
Compiling zeroize v1.3.0
Compiling cfg-if v0.1.10
Compiling either v1.6.1
Compiling arrayvec v0.5.2
Compiling byteorder v1.4.3
Compiling hex v0.4.3
Compiling alloc-traits v0.1.1
Compiling bytemuck v1.7.0
Compiling base64 v0.13.0
Compiling safe-transmute v0.11.2
Compiling static_assertions v1.1.0
Compiling generic-array v0.14.4
Compiling proc-macro2-diagnostics v0.9.1
Compiling semver v0.9.0
Compiling heck v0.3.3
Compiling num-traits v0.2.14
Compiling memoffset v0.6.4
Compiling bv v0.11.1
Compiling pest v2.1.3
Compiling blake3 v0.3.8
Compiling hashbrown v0.9.1
Compiling itertools v0.9.0
Compiling without-alloc v0.2.1
Compiling rustc_version v0.2.3
Compiling semver-parser v0.10.2
Compiling quote v1.0.9
Compiling generic-array v0.12.4
Compiling atty v0.2.14
Compiling memmap2 v0.1.0
Compiling solana-frozen-abi-macro v1.7.11
Compiling solana-frozen-abi v1.7.11
Compiling solana-program v1.7.11
Compiling aho-corasick v0.7.18
Compiling semver v0.11.0
Compiling digest v0.8.1
Compiling rand_core v0.5.1
Compiling regex v1.5.4
Compiling rustc_version v0.3.3
Compiling rand_chacha v0.2.2
Compiling curve25519-dalek v2.1.2
Compiling env_logger v0.8.4
Compiling borsh-derive-internal v0.9.1
Compiling borsh-schema-derive-internal v0.9.1
Compiling field-offset v0.3.4
Compiling rand v0.7.3
Compiling solana-logger v1.7.11
Compiling thiserror-impl v1.0.25
Compiling solana-sdk-macro v1.7.11
Compiling num-derive v0.3.3
Compiling derivative v2.2.0
Compiling enumflags2_derive v0.6.4
Compiling thiserror v1.0.25
Compiling enumflags2 v0.6.4
Compiling toml v0.5.8
Compiling bincode v1.3.3
Compiling serde_bytes v0.11.5
Compiling digest v0.9.0
Compiling block-buffer v0.9.0
Compiling crypto-mac v0.8.0
Compiling proc-macro-crate v0.1.5
Compiling libsecp256k1-core v0.2.2
Compiling hmac v0.8.1
Compiling sha2 v0.9.5
Compiling sha3 v0.9.1
Compiling libsecp256k1-gen-genmult v0.2.1
Compiling libsecp256k1-gen-ecmult v0.2.1
Compiling borsh-derive v0.9.1
Compiling hmac_num_derive v0.5.1
Compiling hmac-drbg v0.3.0
Compiling anchor-syn v0.11.1
Compiling libsecp256k1 v0.5.0
Compiling borsh v0.9.1
Compiling num_enum v0.5.1
Compiling anchor-attribute-event v0.11.1
Compiling anchor-attribute-program v0.11.1
Compiling anchor-attribute-state v0.11.1
```

```
   Compiling anchor-attribute-error v0.11.1
   Compiling anchor-derive-accounts v0.11.1
   Compiling anchor-attribute-interface v0.11.1
   Compiling anchor-attribute-account v0.11.1
   Compiling anchor-attribute-access-control v0.11.1
   Compiling anchor-lang v0.11.1
   Compiling spl-token v3.2.0
   Compiling serum_dex v0.3.1
   Compiling anchor-spl v0.11.1
   Compiling hh-parimutuel v0.1.0 (/root/hh-programs-anchor/programs/hh-parimutuel)
    Finished test [unoptimized + debuginfo] target(s) in 2m 33s
Oct 01 16:51:28.474  INFO cargo_tarpaulin::process_handling::linux: Launching test
Oct 01 16:51:28.474  INFO cargo_tarpaulin::process_handling: running /root/hh-programs-anchor/target/debug/deps/hh_parimutuel-f84f912c77c52bbc

running 1 test
test test_id ... ok

test result: ok. 1 passed; 0 failed; 0 ignored; 0 measured; 0 filtered out; finished in 0.01s

Oct 01 16:51:29.457  INFO cargo_tarpaulin::report: Coverage Results:
|| Tested/Total Lines:
|| ../../node_modules/@project-serum/serum/node_modules/@solana/web3.js/examples/bpf-rust-noop/src/lib.rs: 0/1
|| src/lib.rs: 1/402
|| ../hh-vault/src/lib.rs: 0/235
||
0.16% coverage, 1/638 lines covered
```

hh-vault

```
  Compiling proc-macro2 v1.0.27
   Compiling unicode-xid v0.2.2
   Compiling syn v1.0.73
   Compiling serde_derive v1.0.126
   Compiling serde v1.0.126
   Compiling version_check v0.9.3
   Compiling typenum v1.13.0
   Compiling autocfg v1.0.1
   Compiling cfg-if v1.0.0
   Compiling block-padding v0.2.1
   Compiling opaque-debug v0.3.0
   Compiling libc v0.2.97
   Compiling cpufeatures v0.1.4
   Compiling bs58 v0.3.1
   Compiling subtle v2.4.0
   Compiling semver-parser v0.7.0
   Compiling crunchy v0.2.2
   Compiling memchr v2.4.0
   Compiling getrandom v0.1.16
   Compiling ryu v1.0.5
   Compiling anyhow v1.0.41
   Compiling serde_json v1.0.64
   Compiling yansi v0.5.0
   Compiling unicode-segmentation v1.7.1
   Compiling regex-syntax v0.6.25
   Compiling itoa v0.4.7
   Compiling log v0.4.14
   Compiling feature-probe v0.1.1
   Compiling ppv-lite86 v0.2.10
   Compiling rustversion v1.0.5
   Compiling cc v1.0.68
   Compiling termcolor v1.1.2
   Compiling humantime v2.1.0
   Compiling lazy_static v1.4.0
   Compiling ahash v0.4.7
   Compiling arrayref v0.3.6
   Compiling ucd-trie v0.1.3
   Compiling constant_time_eq v0.1.5
   Compiling either v1.6.1
   Compiling base64 v0.12.3
   Compiling arrayvec v0.5.2
   Compiling zeroize v1.3.0
   Compiling keccak v0.1.0
   Compiling byteorder v1.4.3
   Compiling cfg-if v0.1.10
   Compiling hex v0.4.3
   Compiling bytemuck v1.7.0
   Compiling alloc-traits v0.1.1
   Compiling safe-transmute v0.11.2
   Compiling base64 v0.13.0
   Compiling static_assertions v1.1.0
   Compiling generic-array v0.14.4
   Compiling proc-macro2-diagnostics v0.9.1
   Compiling num-traits v0.2.14
   Compiling memoffset v0.6.4
   Compiling num-integer v0.1.44
   Compiling num-bigint v0.4.0
   Compiling num-rational v0.4.0
   Compiling num-iter v0.1.42
   Compiling semver v0.9.0
   Compiling heck v0.3.3
   Compiling bv v0.11.1
   Compiling blake3 v0.3.8
   Compiling hashbrown v0.9.1
   Compiling pest v2.1.3
   Compiling itertools v0.9.0
   Compiling without-alloc v0.2.1
   Compiling rustc_version v0.2.3
   Compiling semver-parser v0.10.2
   Compiling quote v1.0.9
   Compiling generic-array v0.12.4
   Compiling aho-corasick v0.7.18
   Compiling atty v0.2.14
   Compiling memmap2 v0.1.0
   Compiling solana-frozen-abi-macro v1.7.11
   Compiling solana-frozen-abi v1.7.11
   Compiling solana-program v1.7.11
   Compiling semver v0.11.0
   Compiling digest v0.8.1
   Compiling num-complex v0.4.0
   Compiling regex v1.5.4
   Compiling rand_core v0.5.1
   Compiling rustc_version v0.3.3
   Compiling env_logger v0.8.4
   Compiling borsh-schema-derive-internal v0.9.1
   Compiling borsh-derive-internal v0.9.1
   Compiling rand_chacha v0.2.2
   Compiling curve25519-dalek v2.1.2
   Compiling field-offset v0.3.4
   Compiling thiserror-impl v1.0.25
   Compiling solana-sdk-macro v1.7.11
   Compiling num-derive v0.3.3
   Compiling derivative v2.2.0
   Compiling enumflags2_derive v0.6.4
   Compiling solana-logger v1.7.11
   Compiling rand v0.7.3
   Compiling num v0.4.0
   Compiling thiserror v1.0.25
   Compiling enumflags2 v0.6.4
   Compiling toml v0.5.8
   Compiling bincode v1.3.3
   Compiling serde_bytes v0.11.5
   Compiling digest v0.9.0
   Compiling block-buffer v0.9.0
   Compiling crypto-mac v0.8.0
   Compiling proc-macro-crate v0.1.5
   Compiling libsecp256k1-core v0.2.2
   Compiling sha2 v0.9.5
   Compiling sha3 v0.9.1
   Compiling hmac v0.8.1
   Compiling borsh-derive v0.9.1
   Compiling num_enum_derive v0.5.1
   Compiling anchor-syn v0.11.1
   Compiling libsecp256k1-gen-genmult v0.2.1
   Compiling libsecp256k1-gen-ecmult v0.2.1
   Compiling hmac-drbg v0.3.0
   Compiling borsh v0.9.1
   Compiling num_enum v0.5.1
   Compiling libsecp256k1 v0.5.0
   Compiling anchor-attribute-program v0.11.1
   Compiling anchor-derive-accounts v0.11.1
   Compiling anchor-attribute-error v0.11.1
   Compiling anchor-attribute-event v0.11.1
   Compiling anchor-attribute-state v0.11.1
   Compiling anchor-attribute-account v0.11.1
running 1 test
   Compiling anchor-attribute-access-control v0.11.1
   Compiling anchor-attribute-interface v0.11.1
   Compiling anchor-lang v0.11.1
   Compiling spl-token v3.2.0
   Compiling serum_dex v0.3.1
   Compiling port-variable-rate-lending-instructions v0.1.1
   Compiling apricot-client v0.14.0
   Compiling anchor-spl v0.11.1
   Compiling hh-parimutuel v0.1.0 (/root/hh-programs-anchor/programs/hh-parimutuel)
   Compiling hh-vault v0.1.0 (/root/hh-programs-anchor/programs/hh-vault)
    Finished test [unoptimized + debuginfo] target(s) in 2m 45s
Oct 01 17:00:51.375  INFO cargo_tarpaulin::process_handling::linux: Launching test
```

```
Oct 01 17:00:51.375  INFO cargo_tarpaulin::process_handling: running /root/hh-programs-anchor/target/debug/deps/hh_vault-ae332ef558a0349c

running 0 tests

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

Oct 01 17:00:52.434  INFO cargo_tarpaulin::report: Coverage Results:
|| Tested/Total Lines:
|| ../../node_modules/@project-serum/serum/node_modules/@solana/web3.js/examples/bpf-rust-noop/src/lib.rs: 0/1
|| ../hh-parimutuel/src/lib.rs: 0/402
|| src/apricot.rs: 0/69
|| src/lib.rs: 0/782
|| src/port_finance.rs: 0/63
||
0.00% coverage, 0/1317 lines covered
```

Rust Audit

Fetching advisory database from https://github.com/RustSec/advisory-db.git Loaded 362 security advisories (from /root/.cargo/advisory-db) Updating crates.io index Scanning Cargo.lock for vulnerabilities (142 crate dependencies) Crate: bytemuck Version: 1.7.0 Warning: yanked Dependency tree: bytemuck 1.7.0 😊😊😊 serum_dex 0.3.1 😊 😊😊😊 anchor-spl 0.11.1 😊 😊😊😊 hh-vault 0.1.0 😊 😊😊😊 hh-parimutuel 0.1.0 😊 😊😊😊 hh-vault 0.1.0 😊😊😊 anchor-lang 0.11.1 😊😊😊 hh-vault 0.1.0 😊😊😊 hh-parimutuel 0.1.0 😊😊😊 anchor-spl 0.11.1 warning: 1 allowed warning found

Cargo Geiger

hh-parimutuel

```
WARNING: Dependency file was never scanned: /root/hh-programs-anchor/target/debug/build/rustversion-e250664088361652/out/version.rs
WARNING: Dependency file was never scanned: /root/hh-programs-anchor/target/debug/build/crunchy-e0fcbdfe1190469c/out/lib.rs
WARNING: Dependency file was never scanned: /root/hh-programs-anchor/target/debug/build/typenum-3c0c9c4a497d91de/out/consts.rs
WARNING: Dependency file was never scanned: /root/hh-programs-anchor/target/debug/build/libsecp256k1-b85ded6a2ae5e32f/out/const.rs
WARNING: Dependency file was never scanned: /root/hh-programs-anchor/target/debug/build/typenum-3c0c9c4a497d91de/out/op.rs
WARNING: Dependency file was never scanned: /root/hh-programs-anchor/target/debug/build/libsecp256k1-b85ded6a2ae5e32f/out/const_gen.rs

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)]
    S  = 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      S hh-parimutuel 0.1.0
0/0        0/0          0/0    0/0     0/0      S    anchor-lang 0.11.1
0/0        0/0          0/0    0/0     0/0      S        anchor-attribute-access-control 0.11.1
0/0        8/8          0/0    0/0     0/0      "            anchor-syn 0.11.1
15/18      428/435      3/3    0/0     11/11    "                anyhow 1.0.41
0/0        1/1          0/0    0/0     0/0      "                bs58 0.3.1
0/0        0/0          0/0    0/0     0/0      S                heck 0.3.3
0/0        0/0          0/0    0/0     0/0      S                    unicode-segmentation 1.7.1
0/0        0/0          0/0    0/0     0/0      S                proc-macro2 1.0.27
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      S                proc-macro2-diagnostics 0.9.1
0/0        0/0          0/0    0/0     0/0      S                    proc-macro2 1.0.27
0/0        0/0          0/0    0/0     0/0      S                    quote 1.0.9
0/0        0/0          0/0    0/0     0/0      S                        proc-macro2 1.0.27
0/0        45/45        3/3    0/0     2/2      "                    syn 1.0.73
0/0        0/0          0/0    0/0     0/0      S                        proc-macro2 1.0.27
0/0        0/0          0/0    0/0     0/0      S                        quote 1.0.9
0/0        0/0          0/0    0/0     0/0      =                        unicode-xid 0.2.2
3/3        34/34        0/0    0/0     0/0      "                    yansi 0.5.0
0/0        0/0          0/0    0/0     0/0      S                quote 1.0.9
0/0        4/4          0/0    0/0     0/0      "                serde 1.0.126
0/0        0/0          0/0    0/0     0/0      S                    serde_derive 1.0.126
0/0        0/0          0/0    0/0     0/0      S                        proc-macro2 1.0.27
0/0        0/0          0/0    0/0     0/0      S                        quote 1.0.9
0/0        45/45        3/3    0/0     2/2      "                        syn 1.0.73
0/0        4/6          0/0    0/0     0/0      "                serde_json 1.0.64
0/0        1/1          0/0    0/0     0/0      "                    itoa 0.4.7
8/12       674/921      0/0    0/0     2/2      "                    ryu 1.0.5
0/0        4/4          0/0    0/0     0/0      "                    serde 1.0.126
2/2        73/73        0/0    0/0     0/0      "                sha2 0.9.5
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        4/4          0/0    0/0     0/0      "                            serde 1.0.126
0/0        0/0          0/0    0/0     0/0      =                            typenum 1.13.0
0/0        0/0          0/0    0/0     0/0      S                    cfg-if 1.0.0
0/1        0/14         0/0    0/0     0/0      S                    cpufeatures 0.1.4
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      S                    opaque-debug 0.3.0
0/0        45/45        3/3    0/0     2/2      "                    syn 1.0.73
0/0        0/0          0/0    0/0     0/0      S                thiserror 1.0.25
0/0        0/0          0/0    0/0     0/0      S                    thiserror-impl 1.0.25
0/0        0/0          0/0    0/0     0/0      S                        proc-macro2 1.0.27
0/0        0/0          0/0    0/0     0/0      S                        quote 1.0.9
0/0        45/45        3/3    0/0     2/2      "                        syn 1.0.73
15/18      428/435      3/3    0/0     11/11    "            anyhow 1.0.41
0/0        0/0          0/0    0/0     0/0      S            proc-macro2 1.0.27
0/0        0/0          0/0    0/0     0/0      S            quote 1.0.9
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 2.4.0
0/19       12/313       0/0    0/0     2/29     "                    libc 0.2.97
36/37      2067/2140    0/0    0/0     16/16    "                memchr 2.4.0
0/0        0/0          0/0    0/0     0/0      =                regex-syntax 0.6.25
0/0        45/45        3/3    0/0     2/2      "                syn 1.0.73
0/0        0/0          0/0    0/0     0/0      S            anchor-attribute-account 0.11.1
0/0        8/8          0/0    0/0     0/0      "                anchor-syn 0.11.1
15/18      428/435      3/3    0/0     11/11    "                anyhow 1.0.41
0/0        0/0          0/0    0/0     0/0      S                proc-macro2 1.0.27
0/0        0/0          0/0    0/0     0/0      S                quote 1.0.9
0/0        45/45        3/3    0/0     2/2      "                syn 1.0.73
0/0        0/0          0/0    0/0     0/0      S            anchor-attribute-error 0.11.1
0/0        8/8          0/0    0/0     0/0      "                anchor-syn 0.11.1
0/0        0/0          0/0    0/0     0/0      S                proc-macro2 1.0.27
0/0        0/0          0/0    0/0     0/0      S                quote 1.0.9
0/0        45/45        3/3    0/0     2/2      "                syn 1.0.73
0/0        0/0          0/0    0/0     0/0      S            anchor-attribute-event 0.11.1
0/0        8/8          0/0    0/0     0/0      "                anchor-syn 0.11.1
15/18      428/435      3/3    0/0     11/11    "                anyhow 1.0.41
0/0        0/0          0/0    0/0     0/0      S                proc-macro2 1.0.27
0/0        0/0          0/0    0/0     0/0      S                quote 1.0.9
0/0        45/45        3/3    0/0     2/2      "                syn 1.0.73
0/0        0/0          0/0    0/0     0/0      S            anchor-attribute-interface 0.11.1
```

```
0/0        8/8        0/0    0/0    0/0     "          anchor-syn 0.11.1
15/18      428/435    3/3    0/0    11/11   "          anyhow 1.0.41
0/0        0/0        0/0    0/0    0/0     S          heck 0.3.3
0/0        0/0        0/0    0/0    0/0     S          proc-macro2 1.0.27
0/0        0/0        0/0    0/0    0/0     S          quote 1.0.9
0/0        45/45      3/3    0/0    2/2     "          syn 1.0.73
0/0        0/0        0/0    0/0    0/0     S      anchor-attribute-program 0.11.1
0/0        8/8        0/0    0/0    0/0     "          anchor-syn 0.11.1
15/18      428/435    3/3    0/0    11/11   "          anyhow 1.0.41
0/0        0/0        0/0    0/0    0/0     S          proc-macro2 1.0.27
0/0        0/0        0/0    0/0    0/0     S          quote 1.0.9
0/0        45/45      3/3    0/0    2/2     "          syn 1.0.73
0/0        0/0        0/0    0/0    0/0     S      anchor-attribute-state 0.11.1
0/0        8/8        0/0    0/0    0/0     "          anchor-syn 0.11.1
15/18      428/435    3/3    0/0    11/11   "          anyhow 1.0.41
0/0        0/0        0/0    0/0    0/0     S          proc-macro2 1.0.27
0/0        0/0        0/0    0/0    0/0     S          quote 1.0.9
0/0        45/45      3/3    0/0    2/2     "          syn 1.0.73
0/0        0/0        0/0    0/0    0/0     S      anchor-derive-accounts 0.11.1
0/0        8/8        0/0    0/0    0/0     "          anchor-syn 0.11.1
15/18      428/435    3/3    0/0    11/11   "          anyhow 1.0.41
0/0        0/0        0/0    0/0    0/0     S          proc-macro2 1.0.27
0/0        0/0        0/0    0/0    0/0     S          quote 1.0.9
0/0        45/45      3/3    0/0    2/2     "          syn 1.0.73
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     S          borsh-derive 0.9.1
0/0        0/0        0/0    0/0    0/0     S              borsh-derive-internal 0.9.1
0/0        0/0        0/0    0/0    0/0     S                  proc-macro2 1.0.27
0/0        0/0        0/0    0/0    0/0     S                  quote 1.0.9
0/0        45/45      3/3    0/0    2/2     "                  syn 1.0.73
0/0        0/0        0/0    0/0    0/0     S              borsh-schema-derive-internal 0.9.1
0/0        0/0        0/0    0/0    0/0     S                  proc-macro2 1.0.27
0/0        0/0        0/0    0/0    0/0     S                  quote 1.0.9
0/0        45/45      3/3    0/0    2/2     "                  syn 1.0.73
0/0        0/0        0/0    0/0    0/0     S              proc-macro-crate 0.1.5
0/0        0/0        0/0    0/0    0/0     =                  toml 0.5.8
0/0        4/4        0/0    0/0    0/0     "                      serde 1.0.126
0/0        0/0        0/0    0/0    0/0     S              proc-macro2 1.0.27
0/0        45/45      3/3    0/0    2/2     "              syn 1.0.73
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        4/4        0/0    0/0    0/0     "          serde 1.0.126
0/0        97/109     104/104 4/4    0/0     "  bytemuck 1.7.0
3/3        340/340    1/1    0/0    2/2     "  solana-program 1.7.11
0/0        22/22      0/0    0/0    0/0     "      bincode 1.3.3
0/0        4/4        0/0    0/0    0/0     "          serde 1.0.126
10/78      71/3969    0/0    0/0    0/0     "      blake3 0.3.8
0/0        0/0        0/0    0/0    0/0     S          arrayref 0.3.6
4/4        295/295    2/2    1/1    5/5     "          arrayvec 0.5.2
0/0        4/4        0/0    0/0    0/0     "              serde 1.0.126
0/0        0/0        0/0    0/0    0/0     S          cfg-if 0.1.10
0/0        0/0        0/0    0/0    0/0     S          constant_time_eq 0.1.5
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 2.4.0
0/0        0/0        0/0    0/0    0/0     =          digest 0.9.0
0/0        7/7        0/0    0/0    0/0     "              borsh 0.9.1
0/0        0/0        0/0    0/0    0/0     S          borsh-derive 0.9.1
0/0        1/1        0/0    0/0    0/0     "          bs58 0.3.1
2/2        206/206    0/0    0/0    7/7     "          bv 0.11.1
0/0        4/4        0/0    0/0    0/0     "              serde 1.0.126
0/2        0/857      0/0    0/0    0/0     S          curve25519-dalek 2.1.2
1/1        193/193    0/0    0/0    0/0     "              byteorder 1.4.3
0/0        0/0        0/0    0/0    0/0     S              digest 0.8.1
1/1        223/223    18/18  8/8    5/5     "                  generic-array 0.12.4
0/0        4/4        0/0    0/0    0/0     "                      serde 1.0.126
0/0        0/0        0/0    0/0    0/0     =                  typenum 1.13.0
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        0/0        0/0    0/0    0/0     S                  cfg-if 1.0.0
0/19       12/313     0/0    0/0    2/29    "                  libc 0.2.97
1/1        16/16      1/1    0/0    0/0     "                  log 0.4.14
0/0        0/0        0/0    0/0    0/0     S                      cfg-if 1.0.0
0/0        4/4        0/0    0/0    0/0     "                      serde 1.0.126
0/0        4/4        0/0    0/0    0/0     "              serde 1.0.126
0/0        3/3        0/0    0/0    0/0     "              subtle 2.4.0
1/1        23/23      0/0    0/0    0/0     "              zeroize 1.3.0
0/0        0/0        0/0    0/0    0/0     S          hex 0.4.3
0/0        4/4        0/0    0/0    0/0     "              serde 1.0.126
0/0        0/72       0/3    0/1    0/3     S          itertools 0.9.0
0/0        0/0        0/0    0/0    0/0     S              either 1.6.1
0/0        4/4        0/0    0/0    0/0     "                  serde 1.0.126
0/0        7/7        1/1    0/0    0/0     "          lazy_static 1.4.0
0/0        4/4        0/0    0/0    0/0     "          libsecp256k1 0.5.0
0/0        0/0        0/0    0/0    0/0     S              arrayref 0.3.6
0/0        0/0        0/0    0/0    0/0     =              base64 0.12.3
0/0        0/0        0/0    0/0    0/0     =              digest 0.9.0
0/0        0/0        0/0    0/0    0/0     S              hmac-drbg 0.3.0
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     =                  hmac 0.8.1
0/0        0/0        0/0    0/0    0/0     =                      crypto-mac 0.8.0
0/0        0/0        0/0    0/0    0/0     =                      digest 0.9.0
0/0        33/33      0/0    0/0    2/2     "              libsecp256k1-core 0.2.2
0/0        0/0        0/0    0/0    0/0     S                  crunchy 0.2.2
0/0        0/0        0/0    0/0    0/0     =                  digest 0.9.0
0/0        3/3        0/0    0/0    0/0     "                  subtle 2.4.0
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
0/19       12/313     0/0    0/0    2/29    "                  libc 0.2.97
1/1        16/16      1/1    0/0    0/0     "                  log 0.4.14
0/0        0/0        0/0    0/0    0/0     S                  rand_chacha 0.2.2
2/2        565/641    0/0    0/0    14/22   "                      ppv-lite86 0.2.10
0/0        22/22      0/0    0/0    0/0     "                      rand_core 0.5.1
0/0        22/22      0/0    0/0    0/0     "                  rand_core 0.5.1
0/0        4/4        0/0    0/0    0/0     "              serde 1.0.126
2/2        73/73      0/0    0/0    0/0     "              sha2 0.9.5
0/0        0/0        0/0    0/0    0/0     =              typenum 1.13.0
1/1        16/16      1/1    0/0    0/0     "          log 0.4.14
0/0        0/0        0/0    0/0    0/0     S          num-derive 0.3.3
```

```
0/0      0/0         0/0    0/0    0/0    S              proc-macro2 1.0.27
0/0      0/0         0/0    0/0    0/0    S              quote 1.0.9
0/0      45/45       3/3    0/0    2/2    "              syn 1.0.73
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
0/1      0/1         0/0    0/0    0/0    S            rustversion 1.0.5
0/0      4/4         0/0    0/0    0/0    "            serde 1.0.126
0/0      16/16       0/0    0/0    0/0    "            serde_bytes 0.11.5
0/0      4/4         0/0    0/0    0/0    "              serde 1.0.126
0/0      0/0         0/0    0/0    0/0    S              serde_derive 1.0.126
2/2      73/73       0/0    0/0    0/0    "            sha2 0.9.5
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    S            keccak 0.1.0
0/0      0/0         0/0    0/0    0/0    S          opaque-debug 0.3.0
0/0      0/0         0/0    0/0    0/0    S        solana-frozen-abi 1.7.11
0/0      1/1         0/0    0/0    0/0    "          bs58 0.3.1
2/2      206/206     0/0    0/0    7/7    "          bv 0.11.1
1/1      295/295     20/20  8/8    5/5    "          generic-array 0.14.4
1/1      16/16       1/1    0/0    0/0    "          log 0.4.14
0/0      91/212      2/4    0/0    6/6    "          memmap2 0.1.0
0/19     12/313      0/0    0/0    2/29   "            libc 0.2.97
0/0      4/4         0/0    0/0    0/0    "          serde 1.0.126
0/0      0/0         0/0    0/0    0/0    S          serde_derive 1.0.126
2/2      73/73       0/0    0/0    0/0    "          sha2 0.9.5
0/0      0/0         0/0    0/0    0/0    S          solana-frozen-abi-macro 1.7.11
0/0      0/0         0/0    0/0    0/0    S            proc-macro2 1.0.27
0/0      0/0         0/0    0/0    0/0    S            quote 1.0.9
0/0      45/45       3/3    0/0    2/2    "            syn 1.0.73
0/0      0/0         0/0    0/0    0/0    S          solana-logger 1.7.11
0/0      0/0         0/0    0/0    0/0    S            env_logger 0.8.4
2/2      45/45       0/0    0/0    0/0    "              atty 0.2.14
0/19     12/313      0/0    0/0    2/29   "              libc 0.2.97
0/0      0/0         0/0    0/0    0/0    =              humantime 2.1.0
1/1      16/16       1/1    0/0    0/0    "              log 0.4.14
0/0      34/34       1/2    0/0    2/2    "              regex 1.5.4
0/0      0/0         0/0    0/0    0/0    S              termcolor 1.1.2
0/0      7/7         1/1    0/0    0/0    "            lazy_static 1.4.0
1/1      16/16       1/1    0/0    0/0    "            log 0.4.14
0/0      0/0         0/0    0/0    0/0    S          thiserror 1.0.25
0/0      0/0         0/0    0/0    0/0    S          solana-frozen-abi-macro 1.7.11
0/0      0/0         0/0    0/0    0/0    S          solana-logger 1.7.11
0/0      0/0         0/0    0/0    0/0    S          solana-sdk-macro 1.7.11
0/0      1/1         0/0    0/0    0/0    "            bs58 0.3.1
0/0      0/0         0/0    0/0    0/0    S            proc-macro2 1.0.27
0/0      0/0         0/0    0/0    0/0    S            quote 1.0.9
0/1      0/1         0/0    0/0    0/0    S            rustversion 1.0.5
0/0      45/45       3/3    0/0    2/2    "            syn 1.0.73
0/0      0/0         0/0    0/0    0/0    S          thiserror 1.0.25
0/0      0/0         0/0    0/0    0/0    S        thiserror 1.0.25
0/0      0/0         0/0    0/0    0/0    S      anchor-spl 0.11.1
0/0      0/0         0/0    0/0    0/0    S        anchor-lang 0.11.1
0/0      7/7         1/1    0/0    0/0    "        lazy_static 1.4.0
2/2      57/57       29/29  0/0    0/0    "        serum_dex 0.3.1
0/0      0/0         0/0    0/0    0/0    S          arrayref 0.3.6
0/0      22/22       0/0    0/0    0/0    "          bincode 1.3.3
0/0      97/109      104/104 4/4   0/0    "          bytemuck 1.7.0
1/1      193/193     0/0    0/0    0/0    "          byteorder 1.4.3
0/0      31/31       0/0    0/0    1/1    "          enumflags2 0.6.4
0/0      0/0         0/0    0/0    0/0    S            enumflags2_derive 0.6.4
0/0      0/0         0/0    0/0    0/0    S              proc-macro2 1.0.27
0/0      0/0         0/0    0/0    0/0    S              quote 1.0.9
0/0      45/45       3/3    0/0    2/2    "              syn 1.0.73
0/0      4/4         0/0    0/0    0/0    "            serde 1.0.126
0/0      51/51       0/0    0/0    8/8    "          field-offset 0.3.4
0/0      0/0         0/0    0/0    0/0    S            memoffset 0.6.4
0/0      0/72        0/3    0/1    0/3    S          itertools 0.9.0
0/0      4/10        0/0    0/0    0/0    "          num-traits 0.2.14
0/0      0/0         0/0    0/0    0/0    S          num_enum 0.5.1
0/0      0/0         0/0    0/0    0/0    S            derivative 2.2.0
0/0      0/0         0/0    0/0    0/0    S              proc-macro2 1.0.27
0/0      0/0         0/0    0/0    0/0    S              quote 1.0.9
0/0      45/45       3/3    0/0    2/2    "              syn 1.0.73
0/0      0/0         0/0    0/0    0/0    S            num_enum_derive 0.5.1
0/0      0/0         0/0    0/0    0/0    S              proc-macro-crate 0.1.5
0/0      0/0         0/0    0/0    0/0    S              proc-macro2 1.0.27
0/0      0/0         0/0    0/0    0/0    S              quote 1.0.9
0/0      45/45       3/3    0/0    2/2    "              syn 1.0.73
18/20    133/162     47/47  1/1    3/3    "          safe-transmute 0.11.2
0/0      4/4         0/0    0/0    0/0    "          serde 1.0.126
3/3      340/340     1/1    0/0    2/2    "          solana-program 1.7.11
0/0      0/0         0/0    0/0    0/0    =          spl-token 3.2.0
0/0      0/0         0/0    0/0    0/0    S            arrayref 0.3.6
0/0      0/0         0/0    0/0    0/0    S            num-derive 0.3.3
0/0      4/10        0/0    0/0    0/0    "              num-traits 0.2.14
0/0      0/0         0/0    0/0    0/0    S            num_enum 0.5.1
3/3      340/340     1/1    0/0    2/2    "            solana-program 1.7.11
0/0      0/0         0/0    0/0    0/0    S            thiserror 1.0.25
0/0      0/0         0/0    0/0    0/0    S        static_assertions 1.1.0
0/0      0/0         0/0    0/0    0/0    S        thiserror 1.0.25
0/0      179/179     0/0    0/0    13/13  "        without-alloc 0.2.1
1/1      20/57       0/0    1/1    0/3    "          alloc-traits 0.1.1
3/3      340/340     1/1    0/0    2/2    "      solana-program 1.7.11
0/0      0/0         0/0    0/0    0/0    =      spl-token 3.2.0
3/3      340/340     1/1    0/0    2/2    "    solana-program 1.7.11
0/0      0/0         0/0    0/0    0/0    =    spl-token 3.2.0

136/239  8222/14171  249/258 23/24 166/211

error: Found 6 warnings
```

hh-vault

```
    Scanning done
WARNING: Dependency file was never scanned: /root/hh-programs-anchor/target/debug/build/crunchy-e0fcbdfe1190469c/out/lib.rs
WARNING: Dependency file was never scanned: /root/hh-programs-anchor/target/debug/build/num-bigint-f9fce85bff47ba7f/out/radix_bases.rs
WARNING: Dependency file was never scanned: /root/hh-programs-anchor/target/debug/build/typenum-3c0c9c4a497d91de/out/consts.rs
WARNING: Dependency file was never scanned: /root/hh-programs-anchor/target/debug/build/libsecp256k1-b85ded6a2ae5e32f/out/const_gen.rs
WARNING: Dependency file was never scanned: /root/hh-programs-anchor/target/debug/build/rustversion-e250664088361652/out/version.rs
WARNING: Dependency file was never scanned: /root/hh-programs-anchor/target/debug/build/libsecp256k1-b85ded6a2ae5e32f/out/const.rs
WARNING: Dependency file was never scanned: /root/hh-programs-anchor/target/debug/build/typenum-3c0c9c4a497d91de/out/op.rs

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)]
S   = 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	S	hh-vault 0.1.0
0/0	0/0	0/0	0/0	0/0	S	anchor-lang 0.11.1
0/0	0/0	0/0	0/0	0/0	S	anchor-attribute-access-control 0.11.1
0/0	8/8	0/0	0/0	0/0	"	anchor-syn 0.11.1
15/18	428/435	3/3	0/0	11/11	"	anyhow 1.0.41
0/0	1/1	0/0	0/0	0/0	"	bs58 0.3.1
0/0	0/0	0/0	0/0	0/0	S	heck 0.3.3
0/0	0/0	0/0	0/0	0/0	S	unicode-segmentation 1.7.1
0/0	0/0	0/0	0/0	0/0	S	proc-macro2 1.0.27
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	S	proc-macro2-diagnostics 0.9.1
0/0	0/0	0/0	0/0	0/0	S	proc-macro2 1.0.27
0/0	0/0	0/0	0/0	0/0	S	quote 1.0.9
0/0	0/0	0/0	0/0	0/0	S	proc-macro2 1.0.27
0/0	45/45	3/3	0/0	2/2	"	syn 1.0.73
0/0	0/0	0/0	0/0	0/0	S	proc-macro2 1.0.27
0/0	0/0	0/0	0/0	0/0	S	quote 1.0.9
0/0	0/0	0/0	0/0	0/0	=	unicode-xid 0.2.2
3/3	34/34	0/0	0/0	0/0	"	yansi 0.5.0
0/0	0/0	0/0	0/0	0/0	S	quote 1.0.9
0/0	4/4	0/0	0/0	0/0	"	serde 1.0.126
0/0	0/0	0/0	0/0	0/0	S	serde_derive 1.0.126
0/0	0/0	0/0	0/0	0/0	S	proc-macro2 1.0.27
0/0	0/0	0/0	0/0	0/0	S	quote 1.0.9
0/0	45/45	3/3	0/0	2/2	"	syn 1.0.73
0/0	4/6	0/0	0/0	2/2	"	serde_json 1.0.64
0/0	1/1	0/0	0/0	0/0	"	itoa 0.4.7
8/12	674/921	0/0	0/0	2/2	"	ryu 1.0.5
0/0	4/4	0/0	0/0	0/0	"	serde 1.0.126
2/2	73/73	0/0	0/0	0/0	"	sha2 0.9.5
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	4/4	0/0	0/0	0/0	"	serde 1.0.126
0/0	0/0	0/0	0/0	0/0	=	typenum 1.13.0
0/0	0/0	0/0	0/0	0/0	S	cfg-if 1.0.0
0/1	0/14	0/0	0/0	0/0	S	cpufeatures 0.1.4
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	S	opaque-debug 0.3.0
0/0	45/45	3/3	0/0	2/2	"	syn 1.0.73
0/0	0/0	0/0	0/0	0/0	S	thiserror 1.0.25
0/0	0/0	0/0	0/0	0/0	S	thiserror-impl 1.0.25
0/0	0/0	0/0	0/0	0/0	S	proc-macro2 1.0.27
0/0	0/0	0/0	0/0	0/0	S	quote 1.0.9
0/0	45/45	3/3	0/0	2/2	"	syn 1.0.73
15/18	428/435	3/3	0/0	11/11	"	anyhow 1.0.41
0/0	0/0	0/0	0/0	0/0	S	proc-macro2 1.0.27
0/0	0/0	0/0	0/0	0/0	=	quote 1.0.9
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 2.4.0
0/19	12/313	0/0	0/0	2/29	"	libc 0.2.97
36/37	2067/2140	0/0	0/0	16/16	"	memchr 2.4.0
0/0	0/0	0/0	0/0	0/0	=	regex-syntax 0.6.25
0/0	45/45	3/3	0/0	2/2	"	syn 1.0.73
0/0	0/0	0/0	0/0	0/0	S	anchor-attribute-account 0.11.1
0/0	8/8	0/0	0/0	0/0	"	anchor-syn 0.11.1
15/18	428/435	3/3	0/0	11/11	"	anyhow 1.0.41
0/0	0/0	0/0	0/0	0/0	S	proc-macro2 1.0.27
0/0	0/0	0/0	0/0	0/0	S	quote 1.0.9
0/0	45/45	3/3	0/0	2/2	"	syn 1.0.73
0/0	0/0	0/0	0/0	0/0	S	anchor-attribute-error 0.11.1
0/0	8/8	0/0	0/0	0/0	"	anchor-syn 0.11.1
0/0	0/0	0/0	0/0	0/0	S	proc-macro2 1.0.27
0/0	0/0	0/0	0/0	0/0	S	quote 1.0.9
0/0	45/45	3/3	0/0	2/2	"	syn 1.0.73
0/0	0/0	0/0	0/0	0/0	S	anchor-attribute-event 0.11.1
0/0	8/8	0/0	0/0	0/0	"	anchor-syn 0.11.1
15/18	428/435	3/3	0/0	11/11	"	anyhow 1.0.41
0/0	0/0	0/0	0/0	0/0	S	proc-macro2 1.0.27
0/0	0/0	0/0	0/0	0/0	S	quote 1.0.9
0/0	45/45	3/3	0/0	2/2	"	syn 1.0.73
0/0	0/0	0/0	0/0	0/0	S	anchor-attribute-interface 0.11.1
0/0	8/8	0/0	0/0	0/0	"	anchor-syn 0.11.1
15/18	428/435	3/3	0/0	11/11	"	anyhow 1.0.41
0/0	0/0	0/0	0/0	0/0	S	heck 0.3.3
0/0	0/0	0/0	0/0	0/0	S	proc-macro2 1.0.27
0/0	0/0	0/0	0/0	0/0	S	quote 1.0.9
0/0	45/45	3/3	0/0	2/2	"	syn 1.0.73
0/0	0/0	0/0	0/0	0/0	S	anchor-attribute-program 0.11.1
0/0	8/8	0/0	0/0	0/0	"	anchor-syn 0.11.1
15/18	428/435	3/3	0/0	11/11	"	anyhow 1.0.41
0/0	0/0	0/0	0/0	0/0	S	proc-macro2 1.0.27
0/0	0/0	0/0	0/0	0/0	S	quote 1.0.9
0/0	45/45	3/3	0/0	2/2	"	syn 1.0.73
0/0	0/0	0/0	0/0	0/0	S	anchor-attribute-state 0.11.1
0/0	8/8	0/0	0/0	0/0	"	anchor-syn 0.11.1
15/18	428/435	3/3	0/0	11/11	"	anyhow 1.0.41
0/0	0/0	0/0	0/0	0/0	S	proc-macro2 1.0.27
0/0	0/0	0/0	0/0	0/0	S	quote 1.0.9
0/0	45/45	3/3	0/0	2/2	"	syn 1.0.73
0/0	0/0	0/0	0/0	0/0	S	anchor-derive-accounts 0.11.1
0/0	8/8	0/0	0/0	0/0	"	anchor-syn 0.11.1
15/18	428/435	3/3	0/0	11/11	"	anyhow 1.0.41
0/0	0/0	0/0	0/0	0/0	S	proc-macro2 1.0.27
0/0	0/0	0/0	0/0	0/0	S	quote 1.0.9
0/0	45/45	3/3	0/0	2/2	"	syn 1.0.73
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	S	borsh-derive 0.9.1
0/0	0/0	0/0	0/0	0/0	S	borsh-derive-internal 0.9.1
0/0	0/0	0/0	0/0	0/0	S	proc-macro2 1.0.27
0/0	0/0	0/0	0/0	0/0	S	quote 1.0.9
0/0	45/45	3/3	0/0	2/2	"	syn 1.0.73
0/0	0/0	0/0	0/0	0/0	S	borsh-schema-derive-internal 0.9.1
0/0	0/0	0/0	0/0	0/0	S	proc-macro2 1.0.27

```
0/0      0/0        0/0      0/0    0/0    S              quote 1.0.9
0/0      45/45      3/3      0/0    2/2    "               syn 1.0.73
0/0      0/0        0/0      0/0    0/0    S           proc-macro-crate 0.1.5
0/0      0/0        0/0      0/0    0/0    =                toml 0.5.8
0/0      4/4        0/0      0/0    0/0    "                  serde 1.0.126
0/0      0/0        0/0      0/0    0/0    S           proc-macro2 1.0.27
0/0      45/45      3/3      0/0    2/2    "               syn 1.0.73
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      4/4        0/0      0/0    0/0    "             serde 1.0.126
0/0      97/109     104/104  4/4    0/0    "       bytemuck 1.7.0
3/3      340/340    1/1      0/0    2/2    "       solana-program 1.7.11
0/0      22/22      0/0      0/0    0/0    "         bincode 1.3.3
0/0      4/4        0/0      0/0    0/0    "           serde 1.0.126
10/78    71/3969    0/0      0/0    0/0    "         blake3 0.3.8
0/0      0/0        0/0      0/0    0/0    "           arrayref 0.3.6
4/4      295/295    2/2      1/1    5/5    "           arrayvec 0.5.2
0/0      4/4        0/0      0/0    0/0    "             serde 1.0.126
0/0      0/0        0/0      0/0    0/0    S           cfg-if 0.1.10
0/0      0/0        0/0      0/0    0/0    S           constant_time_eq 0.1.5
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 2.4.0
0/0      0/0        0/0      0/0    0/0    =           digest 0.9.0
0/0      7/7        0/0      0/0    0/0    "         borsh 0.9.1
0/0      0/0        0/0      0/0    0/0    S         borsh-derive 0.9.1
0/0      1/1        0/0      0/0    0/0    "         bs58 0.3.1
2/2      206/206    0/0      0/0    7/7    "         bv 0.11.1
0/0      4/4        0/0      0/0    0/0    "           serde 1.0.126
0/2      0/857      0/0      0/0    0/0    S         curve25519-dalek 2.1.2
1/1      193/193    0/0      0/0    0/0    "           byteorder 1.4.3
0/0      0/0        0/0      0/0    0/0    S           digest 0.8.1
1/1      223/223    18/18    8/8    5/5    "             generic-array 0.12.4
0/0      4/4        0/0      0/0    0/0    "               serde 1.0.126
0/0      0/0        0/0      0/0    0/0    =               typenum 1.13.0
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      0/0        0/0      0/0    0/0    S               cfg-if 1.0.0
0/19     12/313     0/0      0/0    2/29   "               libc 0.2.97
1/1      16/16      1/1      0/0    0/0    "               log 0.4.14
0/0      0/0        0/0      0/0    0/0    S                 cfg-if 1.0.0
0/0      4/4        0/0      0/0    0/0    "                 serde 1.0.126
0/0      4/4        0/0      0/0    0/0    "           serde 1.0.126
0/0      3/3        0/0      0/0    0/0    "           subtle 2.4.0
1/1      23/23      0/0      0/0    0/0    "           zeroize 1.3.0
0/0      0/0        0/0      0/0    0/0    S         hex 0.4.3
0/0      4/4        0/0      0/0    0/0    "           serde 1.0.126
0/0      0/72       0/3      0/1    0/3    S         itertools 0.9.0
0/0      0/0        0/0      0/0    0/0    S           either 1.6.1
0/0      4/4        0/0      0/0    0/0    "             serde 1.0.126
0/0      7/7        1/1      0/0    0/0    "         lazy_static 1.4.0
0/0      4/4        0/0      0/0    0/0    "         libsecp256k1 0.5.0
0/0      0/0        0/0      0/0    0/0    S           arrayref 0.3.6
0/0      0/0        0/0      0/0    0/0    =           base64 0.12.3
0/0      0/0        0/0      0/0    0/0    =           digest 0.9.0
0/0      0/0        0/0      0/0    0/0    S           hmac-drbg 0.3.0
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    =             hmac 0.8.1
0/0      0/0        0/0      0/0    0/0    =               crypto-mac 0.8.0
0/0      0/0        0/0      0/0    0/0    =               digest 0.9.0
0/0      33/33      0/0      0/0    2/2    "           libsecp256k1-core 0.2.2
0/0      0/0        0/0      0/0    0/0    S             crunchy 0.2.2
0/0      0/0        0/0      0/0    0/0    =             digest 0.9.0
0/0      3/3        0/0      0/0    0/0    "             subtle 2.4.0
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
0/19     12/313     0/0      0/0    2/29   "             libc 0.2.97
1/1      16/16      1/1      0/0    0/0    "             log 0.4.14
0/0      0/0        0/0      0/0    0/0    S             rand_chacha 0.2.2
2/2      565/641    0/0      0/0    14/22  "               ppv-lite86 0.2.10
0/0      22/22      0/0      0/0    0/0    "               rand_core 0.5.1
0/0      22/22      0/0      0/0    0/0    "             rand_core 0.5.1
0/0      4/4        0/0      0/0    0/0    "           serde 1.0.126
2/2      73/73      0/0      0/0    0/0    "           sha2 0.9.5
0/0      0/0        0/0      0/0    0/0    =           typenum 1.13.0
1/1      16/16      1/1      0/0    0/0    "         log 0.4.14
0/0      0/0        0/0      0/0    0/0    S         num-derive 0.3.3
0/0      0/0        0/0      0/0    0/0    S           proc-macro2 1.0.27
0/0      0/0        0/0      0/0    0/0    S           quote 1.0.9
0/0      45/45      3/3      0/0    2/2    "           syn 1.0.73
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
0/1      0/1        0/0      0/0    0/0    S         rustversion 1.0.5
0/0      4/4        0/0      0/0    0/0    "         serde 1.0.126
0/0      16/16      0/0      0/0    0/0    "         serde_bytes 0.11.5
0/0      4/4        0/0      0/0    0/0    "           serde 1.0.126
0/0      0/0        0/0      0/0    0/0    S         serde_derive 1.0.126
2/2      73/73      0/0      0/0    0/0    "         sha2 0.9.5
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    S           keccak 0.1.0
0/0      0/0        0/0      0/0    0/0    S           opaque-debug 0.3.0
0/0      0/0        0/0      0/0    0/0    S         solana-frozen-abi 1.7.11
0/0      1/1        0/0      0/0    0/0    "           bs58 0.3.1
2/2      206/206    0/0      0/0    7/7    "           bv 0.11.1
1/1      295/295    20/20    8/8    5/5    "           generic-array 0.14.4
1/1      16/16      1/1      0/0    0/0    "           log 0.4.14
0/0      91/212     2/4      0/0    6/6    "           memmap2 0.1.0
0/19     12/313     0/0      0/0    2/29   "             libc 0.2.97
0/0      4/4        0/0      0/0    0/0    "           serde 1.0.126
0/0      0/0        0/0      0/0    0/0    S           serde_derive 1.0.126
2/2      73/73      0/0      0/0    0/0    "           sha2 0.9.5
0/0      0/0        0/0      0/0    0/0    S         solana-frozen-abi-macro 1.7.11
0/0      0/0        0/0      0/0    0/0    S           proc-macro2 1.0.27
0/0      0/0        0/0      0/0    0/0    S           quote 1.0.9
0/0      45/45      3/3      0/0    2/2    "           syn 1.0.73
0/0      0/0        0/0      0/0    0/0    S         solana-logger 1.7.11
0/0      0/0        0/0      0/0    0/0    S           env_logger 0.8.4
2/2      45/45      0/0      0/0    0/0    "             atty 0.2.14
```

0/19	12/313	0/0	0/0	2/29	"	libc 0.2.97
0/0	0/0	0/0	0/0	0/0	=	humantime 2.1.0
1/1	16/16	1/1	0/0	0/0	"	log 0.4.14
0/0	34/34	1/2	0/0	2/2	"	regex 1.5.4
0/0	0/0	0/0	0/0	0/0	S	termcolor 1.1.2
0/0	7/7	1/1	0/0	0/0	"	lazy_static 1.4.0
1/1	16/16	1/1	0/0	0/0	"	log 0.4.14
0/0	0/0	0/0	0/0	0/0	S	thiserror 1.0.25
0/0	0/0	0/0	0/0	0/0	S	solana-frozen-abi-macro 1.7.11
0/0	0/0	0/0	0/0	0/0	S	solana-logger 1.7.11
0/0	0/0	0/0	0/0	0/0	S	solana-sdk-macro 1.7.11
0/0	1/1	0/0	0/0	0/0	"	bs58 0.3.1
0/0	0/0	0/0	0/0	0/0	S	proc-macro2 1.0.27
0/0	0/0	0/0	0/0	0/0	S	quote 1.0.9
0/1	0/1	0/0	0/0	0/0	S	rustversion 1.0.5
0/0	45/45	3/3	0/0	2/2	"	syn 1.0.73
0/0	0/0	0/0	0/0	0/0	S	thiserror 1.0.25
0/0	0/0	0/0	0/0	0/0	S	thiserror 1.0.25
0/0	0/0	0/0	0/0	0/0	S	anchor-spl 0.11.1
0/0	0/0	0/0	0/0	0/0	S	anchor-lang 0.11.1
0/0	7/7	1/1	0/0	0/0	"	lazy_static 1.4.0
2/2	57/57	29/29	0/0	0/0	"	serum_dex 0.3.1
0/0	0/0	0/0	0/0	0/0	S	arrayref 0.3.6
0/0	22/22	0/0	0/0	0/0	"	bincode 1.3.3
0/0	97/109	104/104	4/4	0/0	"	bytemuck 1.7.0
1/1	193/193	0/0	0/0	0/0	"	byteorder 1.4.3
0/0	31/31	0/0	0/0	1/1	"	enumflags2 0.6.4
0/0	0/0	0/0	0/0	0/0	S	enumflags2_derive 0.6.4
0/0	0/0	0/0	0/0	0/0	S	proc-macro2 1.0.27
0/0	0/0	0/0	0/0	0/0	S	quote 1.0.9
0/0	45/45	3/3	0/0	2/2	"	syn 1.0.73
0/0	4/4	0/0	0/0	0/0	"	serde 1.0.126
0/0	51/51	0/0	0/0	8/8	"	field-offset 0.3.4
0/0	0/0	0/0	0/0	0/0	S	memoffset 0.6.4
0/0	0/72	0/3	0/1	0/3	S	itertools 0.9.0
0/0	4/10	0/0	0/0	0/0	"	num-traits 0.2.14
0/0	0/0	0/0	0/0	0/0	S	num_enum 0.5.1
0/0	0/0	0/0	0/0	0/0	S	derivative 2.2.0
0/0	0/0	0/0	0/0	0/0	S	proc-macro2 1.0.27
0/0	0/0	0/0	0/0	0/0	S	quote 1.0.9
0/0	45/45	3/3	0/0	2/2	"	syn 1.0.73
0/0	0/0	0/0	0/0	0/0	S	num_enum_derive 0.5.1
0/0	0/0	0/0	0/0	0/0	S	proc-macro-crate 0.1.5
0/0	0/0	0/0	0/0	0/0	S	proc-macro2 1.0.27
0/0	0/0	0/0	0/0	0/0	S	quote 1.0.9
0/0	45/45	3/3	0/0	2/2	"	syn 1.0.73
18/20	133/162	47/47	1/1	3/3	"	safe-transmute 0.11.2
0/0	4/4	0/0	0/0	0/0	"	serde 1.0.126
3/3	340/340	1/1	0/0	2/2	"	solana-program 1.7.11
0/0	0/0	0/0	0/0	0/0	=	spl-token 3.2.0
0/0	0/0	0/0	0/0	0/0	S	arrayref 0.3.6
0/0	0/0	0/0	0/0	0/0	S	num-derive 0.3.3
0/0	4/10	0/0	0/0	0/0	"	num-traits 0.2.14
0/0	0/0	0/0	0/0	0/0	S	num_enum 0.5.1
3/3	340/340	1/1	0/0	2/2	"	solana-program 1.7.11
0/0	0/0	0/0	0/0	0/0	S	thiserror 1.0.25
0/0	0/0	0/0	0/0	0/0	S	static_assertions 1.1.0
0/0	0/0	0/0	0/0	0/0	S	thiserror 1.0.25
0/0	179/179	0/0	0/0	13/13	"	without-alloc 0.2.1
1/1	20/57	0/0	1/1	0/3	"	alloc-traits 0.1.1
3/3	340/340	1/1	0/0	2/2	"	solana-program 1.7.11
0/0	0/0	0/0	0/0	0/0	=	spl-token 3.2.0
0/0	5/5	0/0	0/0	0/0	"	apricot-client 0.14.0
0/0	0/72	0/3	0/1	0/3	S	itertools 0.9.0
3/3	340/340	1/1	0/0	2/2	"	solana-program 1.7.11
0/0	0/0	0/0	0/0	0/0	=	spl-token 3.2.0
0/0	0/0	0/0	0/0	0/0	S	hh-parimutuel 0.1.0
0/0	0/0	0/0	0/0	0/0	S	anchor-lang 0.11.1
0/0	0/0	0/0	0/0	0/0	S	anchor-spl 0.11.1
3/3	340/340	1/1	0/0	2/2	"	solana-program 1.7.11
0/0	0/0	0/0	0/0	0/0	=	spl-token 3.2.0
0/0	0/0	0/0	0/0	0/0	S	num 0.4.0
0/0	6/11	0/0	0/0	0/0	"	num-bigint 0.4.0
0/0	0/0	0/0	0/0	0/0	S	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	4/4	0/0	0/0	0/0	"	serde 1.0.126
0/0	0/0	0/0	0/0	0/0	S	num-complex 0.4.0
0/0	4/10	0/0	0/0	0/0	"	num-traits 0.2.14
0/0	4/4	0/0	0/0	0/0	"	serde 1.0.126
0/0	0/0	0/0	0/0	0/0	S	num-integer 0.1.44
0/0	0/0	0/0	0/0	0/0	S	num-iter 0.1.42
0/0	0/0	0/0	0/0	0/0	S	num-integer 0.1.44
0/0	4/10	0/0	0/0	0/0	"	num-traits 0.2.14
0/0	0/0	0/0	0/0	0/0	S	num-rational 0.4.0
0/0	6/11	0/0	0/0	0/0	"	num-bigint 0.4.0
0/0	0/0	0/0	0/0	0/0	S	num-integer 0.1.44
0/0	4/10	0/0	0/0	0/0	"	num-traits 0.2.14
0/0	4/4	0/0	0/0	0/0	"	serde 1.0.126
0/0	4/10	0/0	0/0	0/0	"	num-traits 0.2.14
0/0	0/0	0/0	0/0	0/0	S	port-variable-rate-lending-instructions 0.1.1
0/0	0/0	0/0	0/0	0/0	S	num-derive 0.3.3
0/0	4/10	0/0	0/0	0/0	"	num-traits 0.2.14
3/3	340/340	1/1	0/0	2/2	"	solana-program 1.7.11
0/0	0/0	0/0	0/0	0/0	=	spl-token 3.2.0
0/0	0/0	0/0	0/0	0/0	S	thiserror 1.0.25
136/239	8233/14187	249/258	23/24	166/211		

error: Found 7 warnings

Test Results

Test Suite Results

☺ Fails to initialize a ViewerLeaderboard with invalid seeds

☺ Successfully initializes a ViewerLeaderboard account

☺ Fails when Market is Closed

☺ Fails when Market is ClosedFails when Market is Closed

☺ Fails with incorrect UserROIInfo.

☺ Fails with incorrect UserToken account.

☺ Fails with incorrect UserMarketInfo.

☺ Fails with incorrect UserROIInfo.

☺ Fails with incorrect prediction

☺ Successfully collects correct amount of tokens from prediction

☺ Entering both sides of market yields correct amount.

☺ Invalid market status refunds correct amount of tokens

☺ Successfully enters Yes prediction

☺ Successfully enters No prediction

☺ Fails when a token account with an invalid event set is used

☺ Fails when an invalid Event is used

☺ Fails when an invalid pool is used

☺ Fails when an invalid UserMarketInfo is used

☺ Fails when an invalid UserROIInfo is used

☺ Fails to enter prediction when MarketStatus is not Open

☺ Initializes global state

☺ Initializes an event set

☺ Initializes an event

☺ Fails to initialize an event with mismatching creator

☺ Initializes a Main market

☺ Fails to update mutable Market Ipfs resource with an invalid creator

☺ Fails to update mutable Market Ipfs resource with an invalid event

☺ Succesfully updates mutable Market Ipfs resource

☺ Initializes a Micro market

☺ Initializes an Aux market

☺ Fails duplicate main market init calls

☺ Fails initialization when using invalid seed indexes

☺ Fails when correct creator does not sign

☺ Fails when incorrect event_set is provided

☺ Fails when incorrect mint is provided

☺ Succesfully increments seed index up to 10

☺ Succesfully increments seed index up to 500

☺ Initializes a UserMarketInfo account

☺ Fails UserMarketInfo initialization with invalid seeds

☺ Initializes a UserROIInfo account

☺ Fails UserROIInfo initialization with invalid seeds

☺ Fails to update UserROIInfo with an invalid mint in the event_set

☺ Fails to update UserROIInfo with invalid seeds or other invalid constraints

☺ Successfully fills ViewerLeaderboard

☺ Fails to initialize a FinalLeaderboard with invalid seeds

☺ Successfully initializes a FinalLeaderboard account

☺ Successfully fills final leaderboard

☺ Successfully replaces stale position buckets

☺ Successfully dismisses unqualified entries

☺ Fails to update Market to Closed without resolver signer

☺ Fails to update Market to Closed with invalid resolver

☺ Successfully updates to Closed status

☺ Fails to update Market to Pending status before expiry

☺ Successfully updates to Pending status

☺ Fails to update Market to Resolved status without outcome

☺ Fails to update Market to Resolved status with invalid outcome

☺ Successfully updates to Resolved status

☺ Only performs valid MarketStatus transitions

Code Coverage

For code coverage the current test code managed to to surpass the recommended value.

```
hh-Parimutuel

    Compiling proc-macro2 v1.0.27
    Compiling unicode-xid v0.2.2
    Compiling syn v1.0.73
    Compiling serde_derive v1.0.126
    Compiling serde v1.0.126
    Compiling typenum v1.13.0
    Compiling version_check v0.9.3
    Compiling cfg-if v1.0.0
    Compiling block-padding v0.2.1
    Compiling libc v0.2.97
    Compiling opaque-debug v0.3.0
    Compiling cpufeatures v0.1.4
    Compiling subtle v2.4.0
    Compiling bs58 v0.3.1
    Compiling semver-parser v0.7.0
    Compiling ryu v1.0.5
    Compiling anyhow v1.0.41
    Compiling memchr v2.4.0
    Compiling serde_json v1.0.64
    Compiling crunchy v0.2.2
    Compiling unicode-segmentation v1.7.1
    Compiling getrandom v0.1.16
    Compiling itoa v0.4.7
    Compiling yansi v0.5.0
    Compiling autocfg v1.0.1
    Compiling log v0.4.14
    Compiling regex-syntax v0.6.25
    Compiling feature-probe v0.1.1
    Compiling ucd-trie v0.1.3
    Compiling cc v1.0.68
    Compiling humantime v2.1.0
    Compiling termcolor v1.1.2
    Compiling rustversion v1.0.5
    Compiling ppv-lite86 v0.2.10
    Compiling lazy_static v1.4.0
    Compiling ahash v0.4.7
    Compiling arrayref v0.3.6
    Compiling keccak v0.1.0
    Compiling constant_time_eq v0.1.5
    Compiling base64 v0.12.3
    Compiling zeroize v1.3.0
    Compiling cfg-if v0.1.10
    Compiling either v1.6.1
    Compiling arrayvec v0.5.2
    Compiling byteorder v1.4.3
```

```
Compiling hex v0.4.3
Compiling alloc-traits v0.1.1
Compiling bytemuck v1.7.0
Compiling base64 v0.13.0
Compiling safe-transmute v0.11.2
Compiling static_assertions v1.1.0
Compiling generic-array v0.14.4
Compiling proc-macro2-diagnostics v0.9.1
Compiling semver v0.9.0
Compiling heck v0.3.3
Compiling num-traits v0.2.14
Compiling memoffset v0.6.4
Compiling bv v0.11.1
Compiling pest v2.1.3
Compiling blake3 v0.3.8
Compiling hashbrown v0.9.1
Compiling itertools v0.9.0
Compiling without-alloc v0.2.1
Compiling rustc_version v0.2.3
Compiling semver-parser v0.10.2
Compiling quote v1.0.9
Compiling generic-array v0.12.4
Compiling atty v0.2.14
Compiling memmap2 v0.1.0
Compiling solana-frozen-abi-macro v1.7.11
Compiling solana-frozen-abi v1.7.11
Compiling solana-program v1.7.11
Compiling aho-corasick v0.7.18
Compiling semver v0.11.0
Compiling digest v0.8.1
Compiling rand_core v0.5.1
Compiling regex v1.5.4
Compiling rustc_version v0.3.3
Compiling rand_chacha v0.2.2
Compiling curve25519-dalek v2.1.2
Compiling env_logger v0.8.4
Compiling borsh-derive-internal v0.9.1
Compiling borsh-schema-derive-internal v0.9.1
Compiling field-offset v0.3.4
Compiling rand v0.7.3
Compiling solana-logger v1.7.11
Compiling thiserror-impl v1.0.25
Compiling solana-sdk-macro v1.7.11
Compiling num-derive v0.3.3
Compiling derivative v2.2.0
Compiling enumflags2_derive v0.6.4
Compiling thiserror v1.0.25
Compiling enumflags2 v0.6.4
Compiling toml v0.5.8
Compiling bincode v1.3.3
Compiling serde_bytes v0.11.5
Compiling digest v0.9.0
Compiling block-buffer v0.9.0
Compiling crypto-mac v0.8.0
Compiling proc-macro-crate v0.1.5
Compiling libsecp256k1-core v0.2.2
Compiling hmac v0.8.1
Compiling sha2 v0.9.5
Compiling sha3 v0.9.1
Compiling libsecp256k1-gen-genmult v0.2.1
Compiling libsecp256k1-gen-ecmult v0.2.1
Compiling borsh-derive v0.9.1
Compiling num_enum_derive v0.5.1
Compiling hmac-drbg v0.3.0
Compiling anchor-syn v0.11.1
Compiling libsecp256k1 v0.5.0
Compiling borsh v0.9.1
Compiling num_enum v0.5.1
Compiling anchor-attribute-event v0.11.1
Compiling anchor-attribute-program v0.11.1
Compiling anchor-attribute-state v0.11.1
Compiling anchor-attribute-error v0.11.1
Compiling anchor-derive-accounts v0.11.1
Compiling anchor-attribute-interface v0.11.1
Compiling anchor-attribute-account v0.11.1
Compiling anchor-attribute-access-control v0.11.1
Compiling anchor-lang v0.11.1
Compiling spl-token v3.2.0
Compiling serum_dex v0.3.1
Compiling anchor-spl v0.11.1
Compiling hh-parimutuel v0.1.0 (/root/hh-programs-anchor/programs/hh-parimutuel)
    Finished test [unoptimized + debuginfo] target(s) in 2m 33s
Oct 01 16:51:28.474  INFO cargo_tarpaulin::process_handling::linux: Launching test
Oct 01 16:51:28.474  INFO cargo_tarpaulin::process_handling: running /root/hh-programs-anchor/target/debug/deps/hh_parimutuel-f84f912c77c52bbc

running 1 test
test test_id ... ok

test result: ok. 1 passed; 0 failed; 0 ignored; 0 measured; 0 filtered out; finished in 0.01s

Oct 01 16:51:29.457  INFO cargo_tarpaulin::report: Coverage Results:
|| Tested/Total Lines:
|| ../../node_modules/@project-serum/serum/node_modules/@solana/web3.js/examples/bpf-rust-noop/src/lib.rs: 0/1
|| src/lib.rs: 1/402
|| ../hh-vault/src/lib.rs: 0/235
||
0.16% coverage, 1/638 lines covered
```

hh-vault

```
Compiling proc-macro2 v1.0.27
Compiling unicode-xid v0.2.2
Compiling syn v1.0.73
Compiling serde_derive v1.0.126
Compiling serde v1.0.126
Compiling version_check v0.9.3
Compiling typenum v1.13.0
Compiling autocfg v1.0.1
Compiling cfg-if v1.0.0
Compiling block-padding v0.2.1
Compiling opaque-debug v0.3.0
Compiling libc v0.2.97
Compiling cpufeatures v0.1.4
Compiling bs58 v0.3.1
Compiling subtle v2.4.0
Compiling semver-parser v0.7.0
Compiling crunchy v0.2.2
Compiling memchr v2.4.0
Compiling getrandom v0.1.16
Compiling ryu v1.0.5
Compiling anyhow v1.0.41
Compiling serde_json v1.0.64
Compiling yansi v0.5.0
Compiling unicode-segmentation v1.7.1
Compiling regex-syntax v0.6.25
Compiling itoa v0.4.7
Compiling log v0.4.14
Compiling feature-probe v0.1.1
Compiling ppv-lite86 v0.2.10
Compiling rustversion v1.0.5
Compiling cc v1.0.68
Compiling termcolor v1.1.2
Compiling humantime v2.1.0
Compiling lazy_static v1.4.0
Compiling ahash v0.4.7
Compiling arrayref v0.3.6
Compiling ucd-trie v0.1.3
Compiling constant_time_eq v0.1.5
Compiling either v1.6.1
Compiling base64 v0.12.3
Compiling arrayvec v0.5.2
Compiling zeroize v1.3.0
Compiling keccak v0.1.0
Compiling byteorder v1.4.3
Compiling cfg-if v0.1.10
Compiling hex v0.4.3
Compiling bytemuck v1.7.0
Compiling alloc-traits v0.1.1
Compiling safe-transmute v0.11.2
Compiling base64 v0.13.0
Compiling static_assertions v1.1.0
Compiling generic-array v0.14.4
Compiling proc-macro2-diagnostics v0.9.1
Compiling num-traits v0.2.14
Compiling memoffset v0.6.4
Compiling num-integer v0.1.44
Compiling num-bigint v0.4.0
Compiling num-rational v0.4.0
Compiling num-iter v0.1.42
Compiling semver v0.9.0
Compiling heck v0.3.3
Compiling bv v0.11.1
Compiling blake3 v0.3.8
Compiling pest v2.1.3
Compiling itertools v0.9.0
```

```
    Compiling without-alloc v0.2.1
    Compiling rustc_version v0.2.3
    Compiling semver-parser v0.10.2
    Compiling quote v1.0.9
    Compiling generic-array v0.12.4
    Compiling aho-corasick v0.7.18
    Compiling atty v0.2.14
    Compiling memmap2 v0.1.0
    Compiling solana-frozen-abi-macro v1.7.11
    Compiling solana-frozen-abi v1.7.11
    Compiling solana-program v1.7.11
    Compiling semver v0.11.0
    Compiling digest v0.8.1
    Compiling num-complex v0.4.0
    Compiling regex v1.5.4
    Compiling rand_core v0.5.1
    Compiling rustc_version v0.3.3
    Compiling env_logger v0.8.4
    Compiling borsh-schema-derive-internal v0.9.1
    Compiling borsh-derive-internal v0.9.1
    Compiling rand_chacha v0.2.2
    Compiling curve25519-dalek v2.1.2
    Compiling field-offset v0.3.4
    Compiling thiserror-impl v1.0.25
    Compiling solana-sdk-macro v1.7.11
    Compiling num-derive v0.3.3
    Compiling derivative v2.2.0
    Compiling enumflags2_derive v0.6.4
    Compiling solana-logger v1.7.11
    Compiling rand v0.7.3
    Compiling num v0.4.0
    Compiling thiserror v1.0.25
    Compiling enumflags2 v0.6.4
    Compiling toml v0.5.8
    Compiling bincode v1.3.3
    Compiling serde_bytes v0.11.5
    Compiling digest v0.9.0
    Compiling block-buffer v0.9.0
    Compiling crypto-mac v0.8.0
    Compiling proc-macro-crate v0.1.5
    Compiling libsecp256k1-core v0.2.2
    Compiling sha2 v0.9.5
    Compiling sha3 v0.9.1
    Compiling hmac v0.8.1
    Compiling borsh-derive v0.9.1
    Compiling num_enum_derive v0.5.1
    Compiling anchor-syn v0.11.1
    Compiling libsecp256k1-gen-genmult v0.2.1
    Compiling libsecp256k1-gen-ecmult v0.2.1
    Compiling hmac-drbg v0.3.0
    Compiling borsh v0.9.1
    Compiling num_enum v0.5.1
    Compiling libsecp256k1 v0.5.0
    Compiling anchor-attribute-program v0.11.1
    Compiling anchor-derive-accounts v0.11.1
    Compiling anchor-attribute-error v0.11.1
    Compiling anchor-attribute-event v0.11.1
    Compiling anchor-attribute-state v0.11.1
    Compiling anchor-attribute-account v0.11.1
    Compiling anchor-attribute-access-control v0.11.1
    Compiling anchor-attribute-interface v0.11.1
    Compiling anchor-lang v0.11.1
    Compiling spl-token v3.2.0
    Compiling serum_dex v0.3.1
    Compiling port-variable-rate-lending-instructions v0.1.1
    Compiling apricot-client v0.14.0
    Compiling anchor-spl v0.11.1
    Compiling hh-parimutuel v0.1.0 (/root/hh-programs-anchor/programs/hh-parimutuel)
    Compiling hh-vault v0.1.0 (/root/hh-programs-anchor/programs/hh-vault)
     Finished test [unoptimized + debuginfo] target(s) in 2m 45s
Oct 01 17:00:51.375  INFO cargo_tarpaulin::process_handling::linux: Launching test
Oct 01 17:00:51.375  INFO cargo_tarpaulin::process_handling: running /root/hh-programs-anchor/target/debug/deps/hh_vault-ae332ef558a0349c

running 0 tests

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

Oct 01 17:00:52.434  INFO cargo_tarpaulin::report: Coverage Results:
|| Tested/Total Lines:
|| ../../node_modules/@project-serum/serum/node_modules/@solana/web3.js/examples/bpf-rust-noop/src/lib.rs: 0/1
|| ../hh-parimutuel/src/lib.rs: 0/402
|| src/apricot.rs: 0/69
|| src/lib.rs: 0/782
|| src/port_finance.rs: 0/63
```

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

a264915ad704a214c278993d8e419935a8356d40f3ec1ce07c2940e891f88c56 ./programs/hh-vault/src/apricot.rs

c9e32708d15e5bb1c5ef6bd3ab96b3e0eabe1be11820e9f67366e96daf11da97 ./programs/hh-vault/src/lib.rs

884e787490008f077e5fcbf7d050f9fc31368afe17f787b5bd72d1a98530fca3 ./programs/hh-vault/src/port_finance.rs

ae5df5c13b07427f8864429511db864cba415bee2b860ab5c90f672332bd7937 ./programs/hh-parimutuel/src/lib.rs

Tests

42ecac6417f6c074d2dcd0f58975a2e14baa7706beb407b1d2696f17834b9ada ./hh-programs-anchor/tests/utils.js

9474898ebac86da831e8ea1729d4d247a9246287754e6d5b3e9a56f534b5e931 ./hh-programs-anchor/tests/hh-vault/claimRewardNull.fix.js

55e756cb41bba9ad29eacf72a6d197fdbd48b25dc5e2f6b359fa44b950b9b6f6 ./hh-programs-anchor/tests/hh-vault/depositNull.test.js

824e1dc6dafed8b61f1127b0adee3be1cefc0850c27f94f5598fc395a5138df0 ./hh-programs-anchor/tests/hh-vault/initPlayerState.test.js

231babab96685c1a85bb5776eecc20630e34a2bc07d2e1ee1a8c8669bf44a105 ./hh-programs-anchor/tests/hh-vault/initRewardInfo.test.js

f24bee8266a6131eda2afa543c50670d09e48be7c75507ee866593c36c305a41 ./hh-programs-anchor/tests/hh-vault/initSponsorState.test.js

504bfb66ded64b7b3aaaaeca6b70bcdccb582a53499774c579d60387b196866d ./hh-programs-anchor/tests/hh-vault/initVault.test.js

24c3958bb82bcb7e9c0bb2aa21da5d134741c85bdb71ccc1643090363d0eff63 ./hh-programs-anchor/tests/hh-vault/mintGameToken.test.js

9e08f9c6b7f31f65b10a6b85c6dce21473c7823b1a4dd52a1d384cd615ff508a ./hh-programs-anchor/tests/hh-vault/utils.js

eb57d5425c6b641da00fc47607e71d0cec94f76ab9897c928b41b3028701be44 ./hh-programs-anchor/tests/hh-vault/withdrawNull.test.js

5670685197a939a35c3246465cb10e2306e0465b2c471ef35bdbb7bb4789c310 ./hh-programs-anchor/tests/hh-parimutuel/collectPrediction.test.js

b9708e2b03e6173e3a37af33f3bb6b00bbc492d1d034115c70f0d0f9026ee7d4 ./hh-programs-anchor/tests/hh-parimutuel/enterPrediction.test.js

204b4b0e95df8751206c6153f3e88b165baad88b0b35f773df75b2edbe2e7d11 ./hh-programs-anchor/tests/hh-parimutuel/hh-parimutuel.test.js

e4c93017b35796d0d40b4d0f8c7be30f5599ec6a4bb048ee941ce7c526cf758d ./hh-programs-anchor/tests/hh-parimutuel/leaderboard.test.js

55f93703592560e64b462c88fb0d44be10a4600d9ea8d848ffb87eab027cedb4 ./hh-programs-anchor/tests/hh-parimutuel/updateMarketStatus.test.js

81b1949b2ed7bc9f9640edef584361772f58dd0a5754c7adb10970a16947c370 ./hh-programs-anchor/migrations/deploy.js

Changelog

- 2021-10-08 - Initial report
- 2021-10-26 - 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.

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.