MOVEBIT
Securing the Move Ecosystem

Typus Finance Smart Contract **Audit Report**

https://twitter.com/movebit_

contact@movebit.xyz

Typus Finance Smart Contract Audit Report

1 Executive Summary

1.1 Project Information

Description	A real yield infrastructure on Sui Blockchain.
Type	DeFi, Derivatives
Auditors	MoveBit
Timeline	Apr 16, 2023 – May 3, 2023
Languages	Move
Platform	Sui
Methods	Architecture Review, Unit Testing, Manual Review
Source Code	https://github.com/Typus-Lab/typus-dov-private
Commits	4b36086891af22793471a65d8d86537b35cc39e8 0486f55bb04c6e876bcb0a1b43ebd1e7b2f4b7c2 1b5932e5fca265c2aca5dbd1ea8ff251f00b48e6

1.2 Files in Scope

The following are the SHA1 hashes of the last reviewed files.

ID	Files	SHA-1 Hash

UTL	./typus_framework/sources/utils.move	4d6790d4e1648ebff1df445829c78bd88594de05
DUH	./typus_framework/sources/dutch.move	4aae8d3dad4f02a04ef4b61c9e87ef222c54be0c
I64	./typus_framework/sources/i64.move	d998a7ae9f23e950a04cacc1011260260c698511
LIT	./typus_framework/sources/linked_list.move	b3d200f0b736b02f7f2587c59dbb71f3d0fc3998
VUL	./typus_framework/sources/vault.move	500bf85e26bdb7099974143087fbdd9d1a26fc41
AUH	./typus_framework/sources/authority.move	47f76fdad329827c4e48b0f8be827d0fbf2d002b
SGC	./portfolio/sources/single_collateral.move	5b0e3bdc5c5022469ef2deacca1cafa7723b9d51
MGC	./portfolio/sources/multiple_collateral.move	5f9a401e78b7b3ebc9e0d6e474db19257b5b2745

1.3 Issue Statistic

Item	Count	Fixed	Acknowledged
Total	22	21	1
Informational	6	6	
Minor	10	10	
Medium	4	3	1
Major	2	2	
Critical			

1.4 MoveBit Audit BreakDown

MoveBit aims to assess repositories for security-related issues, code quality, and compliance with specifications and best practices. Possible issues our team looked for included (but are not limited to):

- Transaction-ordering dependence
- Timestamp dependence
- Integer overflow/underflow by bit operations
- Number of rounding errors
- Denial of service / logical oversights
- Access control
- Centralization of power
- Business logic contradicting the specification
- Code clones, functionality duplication
- Gas usage
- Arbitrary token minting
- Unchecked CALL Return Values
- The flow of capability
- Witness Type

1.5 Methodology

The security team adopted the "**Testing and Automated Analysis**", "**Code Review**" and "**Formal Verification**" strategy to perform a complete security test on the code in a way that is closest to the real attack. The main entrance and scope of security testing are stated in the conventions in the "Audit Objective", which can expand to contexts beyond the scope according to the actual testing needs. The main types of this security audit include:

(1) Testing and Automated Analysis

Items to check: state consistency/ failure rollback/ unit testing/ value overflows/ parameter verification / unhandled errors/ boundary checking/ coding specifications.

(2) Code Review

The code scope sees in section **1.2**.

(3) Formal Verification

Perform formal verification for key functions with the Move Prover.

(4) Audit Process

- Carry out relevant security tests on the testnet or the mainnet;
- If there are any questions during the audit process, communicate with the code owner in time. The code owners should actively cooperate (this might include providing the latest stable source code, relevant deployment scripts or methods, transaction signature scripts, exchange docking schemes, etc.);
- The necessary information during the audit process will be well documented for both the audit team and the code owner in a timely manner.

2 Summary

This report has been commissioned by **Typus** to identify any potential issues and vulnerabilities in the source code of the **Typus Finance** smart contract, as well as any contract dependencies that were not part of an officially recognized library. In this audit, we have utilized various techniques, including manual code review and static analysis, to identify potential vulnerabilities and security issues.

During the audit, we have identified **22** issues of varying severity, listed below.

ID	Title	Severity	Status
AUH-01	Authority Logic Error	Major	Fixed
SGC-02	`get_auction_max_size` Missing Check	Minor	Fixed
I64-03	`i64::sub` Has Overflow Risk	Major	Fixed
SGC-04	Code Optimization	Informational	Fixed
DUH-05	Parameter Check For Creating Dutch	Medium	Fixed
DUH-06	Dutch Gas Optimization	Medium	Fixed
ORA-07	Oracle Centralization Risk	Medium	Acknowledged
DUH-08	Calculation Formula Error	Medium	Fixed

SGC-09	`create_payoff_configs` Parameter Verification	Minor	Fixed
UTL-10	`extract_balance` Code Optimization	Minor	Fixed
SGC-11	Repeated Error Code	Minor	Fixed
SGC-12	Meaningless Code	Minor	Fixed
DUH-13	`remove_bid` Does Not Judge Whether the Address Exists	Minor	Fixed
SGC-14	Code Optimization	Informational	Fixed
SGC-15	Code Readability And Gas Optimization	Minor	Fixed
VUL-16	Deposit Extra Code	Minor	Fixed
DUH-17	`extract_balance` Update Error	Minor	Fixed
DUH-18	The Value Of `able_to_remove_bid` May Be The Same	Minor	Fixed
SGC-19	Simplify The `check_auction_settings` Judgment Condition	Informational	Fixed
I64-20	Comment Error	Informational	Fixed
SGC-21	Optimization Of strike Calculation Formula	Informational	Fixed
LIT-22	`linked_list` Does not Require mut References	Informational	Fixed

3 Participant Process

Here are the relevant actors with their respective abilities within the `Typus` Smart Contract:

Admin

- Admin can `new_portfolio_vault`
- Admin can `activate` a vault
- Admin can `new_auction`
- Admin can `delivery`
- Admin can `settle`
- Admin can `add/remove_authorized_user`
- Admin can `update_capacity`
- Admin can `update_warmup/upcoming_vault_config`
- Admin can `new_manager`
- Admin can `add_remove_authorized_user`
- Admin can `close` portfolio
- Admin can `terminate` vault and auction

User

- User can `deposit`.
- User can `withdraw`.
- User can `unsubscribe`.
- User can `claim`.
- User can `new_bid`.
- User can `compound`.
- User can `harvest`.

4 Findings

AUH-01 Authority Logic Error

Severity: Major

Status: Fixed

Code Location: typus_framework/sources/authority.move#L52

Descriptions: `get_auction_max_size` lacks verification. In the `remove_authorized_user` function, when deleting the verification address, it should be judged that the address exists, not

does not exist. The logic condition in the if is wrong.

Suggestion: Take the condition in the if as its logical opposite.

Resolution: The Typus team updated the codes in commit `1ffc5c28f1446171d3007e0a1b475b04a381396d` and resolved this issue.

SGC-02 `get_auction_max_size` Missing Check

Severity: Minor

Status: Fixed

Code Location: portfolio/sources/single_collateral.move#L1908

Descriptions: In `get_auction_max_size`, there is no assertion added to the return value of calculate_max_loss_per_unit, `assert!(i64::is_neg(&max_loss), E_INVALID_MAX_LOSS);` other calls to `calculate_max_loss_per_unit` are added.

Suggestion: Add the corresponding assert statement according to the code.

Resolution: The Typus team updated the codes in commit `ec33557f5bea083259891bfb67b904f3e0de2814` and resolved this issue.

I64-03 `i64::sub` Has Overflow Risk

Severity: Major

Status: Fixed

Code Location: typus_framework/sources/i64.move#L141

Descriptions: When `a` is positive and `b` is negative, there is a case where `a-b` exceeds 2 to the 63rd power, and if it exceeds the maximum 63-bit positive number, an assert limit should be added; and the comment is wrong, it should not return a negative number.

Suggestion: Add a limit so that it is always less than 2 to the power of 63.

Resolution: The Typus team updated the codes in commit `359907d562e45fd7fd6fa58e87c45af9fe17eb57` and resolved this issue.

SGC-04 Code Optimization

Severity: Informational

Status: Fixed

Code Location: portfolio/sources/single_collateral.move#L294

Descriptions: The code has saved the `current_ts_ms` variable before, the function can use `current_ts_ms` to replace `clock::timestamp_ms(clock)`.

Suggestion: Use the `current_ts_ms` variable saved in advance as a parameter.

Resolution: The Typus team updated the codes in commit `edd6491c30bc1387477f8ad83d42ec73b519c6f1` and resolved this issue.

DUH-05 Parameter Check For Creating Dutch

Severity: Medium

Status: Fixed

Code Location: typus_framework/sources/dutch.move#L64

Descriptions: When creating an auction, there is no proper verification of the input parameters. There may be situations where the `start_ms` is less than `end_ts_ms` or the end time is less than the current time, and the auction `decay_speed` cannot be 0.

Suggestion: Add the corresponding time limit and assert code with `decay_speed` greater than 0.

Resolution: The Typus team updated the codes in commit `5f47eff498d340dee2497ae567a2b3ef59689b34` and resolved this issue.

DUH-06 Dutch Gas Optimization

Severity: Medium

Status: Fixed

Code Location: typus_framework/sources/dutch.move#L308

Descriptions: When delivering an auction to process the handling fee, the balance can be merged together and then transferred to the `fee_pool_address` address. The following is a comparison of the gas consumption of one transfer transaction and multiple transfer transactions. Testnet transaction hash: `uRAsJ1VbPmzD7QPqLd2E6xZiPEiKYNh14U1ayL35nLP`, `4UY8t7z1bdn6ocLLuoi7Enp2cbTYterGQGvBWyMfH18H`.

Suggestion: Merge coins together and transfer coins to `fee_pool_address`.

Resolution: The Typus team updated the codes in commit `46fbfaed3ba0815a3836688d1fa45743ab92803a` and resolved this issue.

ORA-07 Oracle Centralization Risk

Severity: Medium

Status: Acknowledged

Code Location: https://github.com/Typus-Lab/typus-oracle/blob/main/sources/oracle.move

Descriptions: All prices in the code are obtained through `typus_oracle::oracle`. If the private key of the account is stolen, there will be a price control problem, the price feed source is too centralized, and there is no judgment on whether the price feed information is within the normal range price.

Suggestion: Use a multi-signature account to control the oracle and verify the return value, or use a third-party oracle.

Resolution: The Typus team has confirmed this issue, and plans to fix it in the near future.

DUH-08 Calculation Formula Error

Severity: Medium

Status: Fixed

Code Location: typus_framework/sources/dutch.move#L304

Descriptions: `delivery_value_per_unit` is expressed as `delivery_price * o_token precision` and then divides the precision of `b_token`. When L304 calculates `delivery_value`, the precision of `b_token` is divided, resulting in a logic error.

Suggestion: Modify the correct calculation formula according to the document.

Resolution: The Typus team updated the codes and resolved this issue.

SGC-09 `create_payoff_configs` Parameter Verification

Severity: Minor

Status: Fixed

Code Location: portfolio/sources/single_collateral.move#L2180

Descriptions: The parameter of `create_payoff_configs` does not limit the number in the vector must be greater than 0, if it is all empty, it may cause inaccurate calculation when `activate_->calculate_max_loss_per_unit`.
Suggestion: Limit the length of the vector passed by `create_payoff_configs` to be greater than 0.

Resolution: The Typus team updated the codes in commit `bdc2b20a2a657f414185152525bb8d2149ed0692` and resolved this issue.

UTL-10 `extract_balance` Code Optimization

Severity: Minor

Status: Fixed

Code Location: typus_framework/sources/utils.move#L29

Descriptions: The function of the `extract_balance` function is to extract the number of coins from the coins vector, and the if condition in the first part of the while loop can be greater than or equal to simplify the logic.

Suggestion: Modify the judgment expression in `if`, change it from `>` to `>=`.

Resolution: The Typus team updated the codes in commit `839cb3461ed69d94d2f37516a04c9e8fd5445dbd` and resolved this issue.

SGC-11 Repeated Error Code

Severity: Minor

Status: Fixed

Code Location: portfolio/sources/single_collateral.move#L50

Descriptions: The error code constants `E_INVALID_TIME_TYPE_INPUT` and `E_INVALID_OPTION_TYPE` have the same value, but should be different.

Suggestion: Modify the error code constants to different values.

Resolution: The Typus team updated the codes in commit `1ffc5c28f1446171d3007e0a1b475b04a381396d` and resolved this issue.

SGC-12 Meaningless Code

Severity: Minor

Status: Fixed

Code Location: portfolio/sources/single_collateral.move#L1037,1098,1183

Descriptions: `ManagerCap` is always created in some functions, but `ManagerCap` is not used anywhere, only it is finally destroyed and used.

Suggestion: Remove unnecessary `ManagerCap` in the code.

Resolution: The Typus team updated the codes in commit `23ceda476623489604738829b2cdc900da573a50` and resolved this issue.

DUH-13 `remove_bid` Does Not Judge Whether The Address Exists

Severity: Minor

Status: Fixed

Code Location: typus_framework/sources/dutch.move#L189

Descriptions: When the `remove_bid` function is called, it is not judged whether the address of the bidder exists, and an error will be reported if it does not exist.

Suggestion: Before the `remove_bid` function is called, use `table::contains` to determine whether the address exists in `ownerships`.

Resolution: The Typus team updated the codes in commit `4b4bb4f76f3ebde5fb9f6804d2733c9d731af504` and resolved this issue.

SGC-14 Code Optimization

Severity: Informational

Status: Fixed

Code Location: portfolio/sources/single_collateral.move#L276

Descriptions: Because `period` has only three kinds of values, the last `else if (period == 2)` can be changed to `else`.

Suggestion: Modify the `else if` statement to `else`.

Resolution: The Typus team updated the codes in commit `bf2b1d0d5a30a88390c093f3eec2eb9d23b85c8e` and resolved this issue.

SGC-15 Code Readability And Gas Optimization

Severity: Minor

Status: Fixed

Code Location: portfolio/sources/single_collateral.move#L362

Descriptions: The second `borrow_mut` can be replaced by the variable `payoff_config` above, which can improve readability and save gas, also `set_strike` can be modified like this.
Suggestion: Use the `payoff_config` instead of the second `borrow_mut` function call.

Resolution: The Typus team updated the codes in commit `ec33557f5bea083259891bfb67b904f3e0de2814` and resolved this issue.

VUL-16 Deposit Extra Code

Severity: Minor

Status: Fixed

Code Location: typus_framework/sources/vault.move#L291

Descriptions: In the deposit function, the amount has been limited to be greater than 0, and the value of balance and amount is asserted to be the same, so the return value of `extract_balance` will never be the `zero_balance`, and `destroy_zero` is not required.

Suggestion: Remove unnecessary code.

Resolution: The Typus team updated the codes in commit `839cb3461ed69d94d2f37516a04c9e8fd5445dbd` and resolved this issue.

DUH-17 `extract_balance` Update Error

Severity: Minor

Status: Fixed

Code Location: typus_framework/sources/dutch.move#L142

Descriptions: After `extract_balance` is updated, if the extracted amount is insufficient and will abort inside the function, so there is no need to judge `E_INSUFFICIENT_BALANCE` outside the function, it is recommended to delete it.

Suggestion: Remove unnecessary code.

Resolution: The Typus team updated the codes in commit `839cb3461ed69d94d2f37516a04c9e8fd5445dbd` and resolved this issue.

DUH-18 The Value Of `able_to_remove_bid` May Be The Same

Severity: Minor

Status: Fixed

Code Location: typus_framework/sources/dutch.move#L358

Descriptions: When updating the value of `able_to_remove_bid`, it is not judged whether it is the same as the original value, resulting in the value of `able_to_remove_bid` not being updated. In this case, no event should be emitted.

Suggestion: Make sure that the updated `able_to_remove_bid` value is different from the original value when the function is called.

Resolution: The Typus team updated the codes and resolved this issue.

SGC-19 Simplify The `check_auction_settings` Judgment Condition

Severity: Informational

Status: Fixed

Code Location: portfolio/sources/single_collateral.move#L2257

Descriptions: In the `check_auction_settings` judgment condition, `initial_price >= final_price` ensures that `initial_price` is greater than `final_price`, and the second condition is limited to `final_price > 0` so this condition is redundant.

Suggestion: Remove redundant judgment conditions in if.

Resolution: The Typus team updated the codes in commit `03379db631e202386a0d56f8728456be3408a754` and resolved this issue.

I64-20 Comment Error

Severity: Informational

Status: Fixed

Code Location: typus_framework/sources/i64.move#L18

Descriptions: `GREATER_THAN` means a is greater than `b`, there is an error in the comment

Suggestion: Update the comment.

Resolution: The Typus team updated the codes in commit `88f9a76feda9d5054c7a0601f502ead13d47771e` and resolved this issue.

SGC-21 Optimization Of `strike` Calculation Formula

Severity: Informational

Status: Fixed

Code Location: portfolio/sources/single_collateral.move#L2048

Descriptions: The first part of `if` has guaranteed that the `strike_increment` can be divisible by temp, so just return to temp directly at this time.

Suggestion: Remove unnecessary code just return the `temp` value.

Resolution: The Typus team updated the codes in commit `0486f55bb04c6e876bcb0a1b43ebd1e7b2f4b7c2` and resolved this issue.

LIT-22 `linked_list` Does Not Require `mut` References

Severity: Informational

Status: Fixed

Code Location: typus_framework/sources/linked_list.move#L402

Descriptions: The parameter `linked_list` in the `borrow_mut` function does not require a mutable reference, because `linked_list` is not modified in the whole function.

Suggestion: Modify the code to delete the `mut` before `linked_list`.

Resolution: The Typus team updated the codes in commit `105b5f61e1eb9ba5ec3702ff1f8efd5660ad42ac` and resolved this issue.

Appendix 1

Issue Level

- **Informational** issues are often recommendations to improve the style of the code or to optimize code that does not affect the overall functionality.
- **Minor** issues are general suggestions relevant to best practices and readability. They don't post any direct risk. Developers are encouraged to fix them.
- **Medium** issues are non-exploitable problems and not security vulnerabilities. They should be fixed unless there is a specific reason not to.
- **Major** issues are security vulnerabilities. They put a portion of users' sensitive information at risk, and often are not directly exploitable. All major issues should be fixed.
- **Critical** issues are directly exploitable security vulnerabilities. They put users' sensitive information at risk. All critical issues should be fixed.

Issue Status

- **Fixed:** The issue has been resolved.
- **Acknowledged:** The issue has been acknowledged by the code owner, and the code owner confirms it's as designed, and decides to keep it.

Appendix 2

Disclaimer

This report is based on the scope of materials and documents provided, with a limited review at the time provided. Results may not be complete and do not include 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 own risk. A report does not imply an endorsement of any particular project or team, nor does it guarantee its security. These reports should not be relied upon in any way by any third party, including for the purpose of making any decision to buy or sell products, services, or any other assets. TO THE FULLEST EXTENT

PERMITTED BY LAW, WE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, IN CONNECTION WITH THIS REPORT, ITS CONTENT, RELATED SERVICES AND PRODUCTS, AND YOUR USE, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NOT INFRINGEMENT.

MOVEBIT

Securing the Move Ecosystem

https://twitter.com/movebit_

contact@movebit.xyz