Metapool - Rust Smart Contract Auditing

Requisite

Audit Smart Contracts for Metapool Staking Pool (https://github.com/Narwallets/meta-pool)

Approaches

Since there are still no known tools available for Rust Smart Contract auditing, two different options were analyzed:

Option 1

Develop a Source Analyzer for Smart Contracts in Rust similar to Slither, (https://github.com/crytic/slither) which is available for Solidity.

The following rust parsers were analyzed:

- Pest the elegant Parser: https://lib.rs/crates/pest
- Lexical Core: https://lib.rs/crates/lexical-core
- Combine: https://lib.rs/crates/combine

Conclusion

Development is too complex for the time available.

Option 2

Perform a manual analysis of contracts using the following Slither detectors (https://github.com/crytic/slither) as a basis.
Note: As Rust and Solidity are two different languages in their architecture, there will be detectors that cannot be used

Detectors

https://github.com/crytic/slither#detectors

Conclusion

This kind of analysis could be carried out on the timeframe available.
Based on the control points, an analysis report will be elaborated.

This report will include the following items: