

Overview

This document describes the formalization in the Rocq prover for the following article.
Strategy-aware Liquidity for Account-based Blockchains. (Accepted at SETTA 2025)

The formalization is based on the ConCert framework:

[GitHub - AU-COBRA/ConCert: A framework for smart contract verification in Coq](#)

The formalization mainly includes:

1. Model of transaction execution as driven by the strategies of the honest users and the adversary, based on the model of smart contract execution in ConCert
2. Formalization of the strategy-aware liquidity property in the article, and the meta-theoretical properties of the liquidity property (incl. monotonicity and connection with strategy-less liquidity)
3. A proof method for the verification of strategy-aware liquidity, together with the soundness proof of the method
4. A proof method for the refutation of strategy-aware liquidity, together with the soundness proof of the method
5. Formalization of the smart contracts c_{fm} , c_{fm}^x , the escrow contract, and the honeypot contract, accompanied with the proofs for verifying or refuting strategy-aware liquidity for these smart contracts

Paper-to-code Correspondence

The following table shows the correspondence between contents in the article and their mechanized counterpart in Rocq.

Part in Manuscript	Definition/Result	File in Mechanization	Entry
Section 3.1	$\sigma \xrightarrow{\beta} \sigma'$	strat_liquidity/StratModel.v	Definition transition
Section 3.1	<i>init-ctr</i>	strat_liquidity/StratModel.v	Definition is_init_state
Section 3.2	<i>Definition 1 (strategies)</i>	strat_liquidity/StratModel.v	Definition strat
Section 3.2	$\delta^{as} \vdash \pi \rightarrow \pi'$	strat_liquidity/StratModel.v	Definition stratDrive
Section 4	$(\delta_u^{as1}, \delta_a^{as2}) \vdash \pi \rightsquigarrow \pi'$	strat_liquidity/StratModel.v	Inductive interleavedExecution
Section 4	<i>usl, asl</i>	strat_liquidity/StratModel.v	Inductive userLiquidates ... with envProgress ...
Section 4	<i>Definition 2 (strategy-aware liquidity)</i>	strat_liquidity/StratModel.v	Definition strategy_aware_liquidity
Section 5.1	<i>Definition 3 (Relative strength of strategies)</i>	strat_liquidity/Mono.v	Definition strat_subset
Section 5.1	<i>Theorem 1 (monotonicity)</i>	strat_liquidity/Mono.v	Theorem strat_liquidity_mono_wrt_env
Section 5.2	<i>Definition 4 (Basic liquidity)</i>	strat_liquidity/StratModel.v	Definition basic_liquidity
Section 5.2	<i>Theorem 2 (connection between liquidity notions)</i>	strat_liquidity/Connection.v	Theorem SL_equiv_BL_with_empty_env_and_complete_user
Section 6.1	<i>Theorem 3 (soundness of</i>	strat_liquidity/ProofLib.v	Theorem soundness

	<i>verification)</i>		
Section 6.2	<i>Theorem 4 (soundness of refutation)</i>	strat_liquidity/ProofLib.v	Theorem rft_soundness
Section 7.2	<i>Theorem 5 (verification result for c_{fm})</i>	strat_liquidity/examples/ fundsManagement/ fdmgmt_sat_liq.v	Theorem fm_sat_strat_liquidity
Section 7.2	<i>Theorem 6 (refutation result for c_{fm}^x)</i>	strat_liquidity/examples/ fundsManagement/ fdmgmt_nsat_liq.v	Theorem fm_unsat_strat_liquidity
Section 7.2	<i>Verification result for escrow contract</i>	strat_liquidity/examples/ escrow/escrow_sat_liq.v	Theorem escrow_sat_liq_honest_buyer Theorem escrow_sat_liq_honest_seller
Section 7.2	<i>Refutation result for honeypot contract</i>	strat_liquidity/examples/ honeypot/honeypot_nsat_liq.v	Theorem honeypot_unsat_strat_liquidity

Building and Running the Proof Scripts

This formalization is developed using Rocq (Coq) 8.16.1

To build the proof scripts, first ensure that the “bin” folder of the Coq installation is in the system path.

A makefile should be generated from _CoqProject with the following command:

```
coq_makefile -f _CoqProject -o Makefile
```

To build the development, issue the “make” command in the top-level folder.

After the proof scripts are built, they can be run using Proof General or CoqIDE.