On the Just-In-Time Discovery of Profit-Generating Transactions in DeFi Protocols

Liyi Zhou, Kaihua Qin, Antoine Cully, Benjamin Livshits and Arthur Gervais

DeFi Composability

DeFiPoser-ARB
- build a directed DeFi market graph
- identify negative cycles
- BellmanFord-Moore algorithm

DeFiPoser-SMT
- state transition model
- prune search space
- theorem prover

Evaluation
- Ethereum: 96 actions from the Uniswap, Bancor, and MakerDAO, with a total of 25 assets.
- Block 9100000 (Dec-13-2019) to 10050000 (May-12-2020)
- Validation by concrete execution
- Weekly revenue estimate:
  - DeFiPoser-ARB: 191.48 ETH (76,592 USD)
  - DeFiPoser-SMT: 72.44 ETH (28,976 USD)

DeFiPoser-ARB
- Formulate DeFi actions into symbolic models.
- Apply heuristics to reduce search space. E.g., a path must not include any loops.

DeFiPoser-SMT
- Model
- Path Pruning
- Objective constraint — final profit greater than target value
- Optimization
- Apply a binary search to find the optimal value.

Complexity

DeFiPoser-ARB
- $\mathcal{O}(|N|^3 \cdot |E|)$

DeFiPoser-SMT
- $\mathcal{O}(\log p! \times \log p!)$

One transaction

(1) 100 DAI
(2) 100 DAI
(3) 101 USDT
(4) 100 DAI
profit: 2 DAI

Transaction

DeFiProtocols
Models
Path Pruning
Theorem Prover
Transaction A
Transaction B
Transaction C
Block i
Block i+1

Negative Cycle Detection
Greedy Search
Strategic/Transaction Validation through concrete execution

DeFiPoser-SMT
- Formulate DeFi actions into symbolic models.
- Apply heuristics to reduce search space. E.g., a path must not include any loops.

Transaction

DeFiProtocols
Models
Path Pruning
Theorem Prover
Transaction A
Transaction B
Transaction C
Block i
Block i+1

Negative Cycle Detection
Greedy Search
Strategic/Transaction Validation through concrete execution

Model

Path Pruning

SMT Solver

Optimization

Objective constraint — final profit greater than target value
- Apply a binary search to find the optimal value.

Cumulative revenue/transaction fee in ETH

Jan-02-2020 Feb-02-2020 Mar-03-2020 Apr-03-2020 May-04-2020
0 1000000 2000000 3000000 4000000
9200000 9400000 9600000 9800000 10000000

DeFiPoser-SMT: best strategy per block found
DeFiPoser-SMT: validated revenue by concrete execution
DeFiPoser-SMT: transaction fee
DeFiPoser-ARB: validated revenue by concrete execution
DeFiPoser-ARB: transaction fee