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

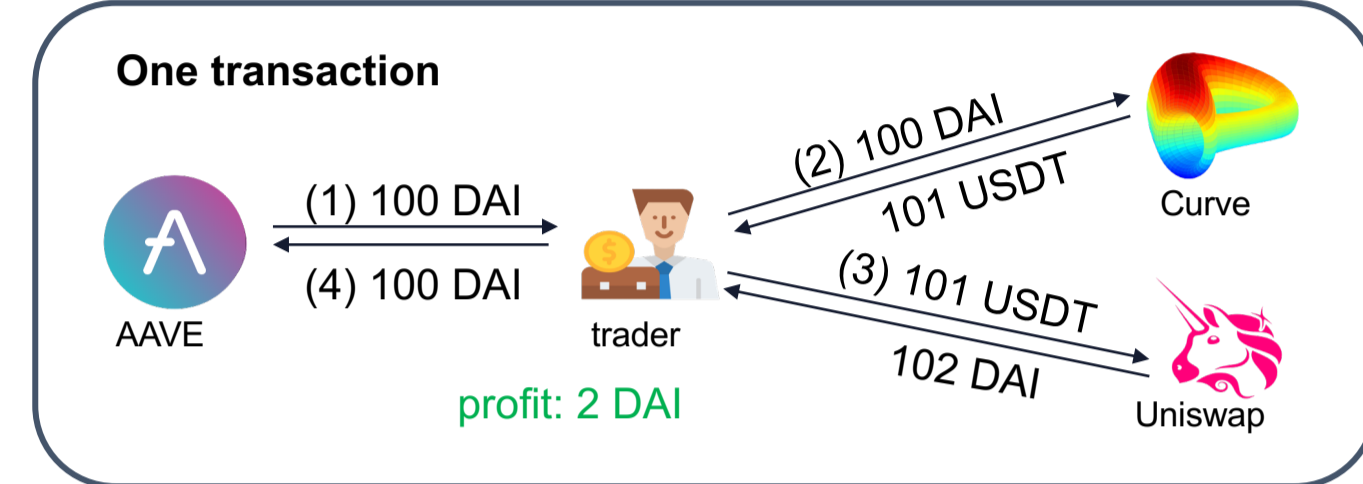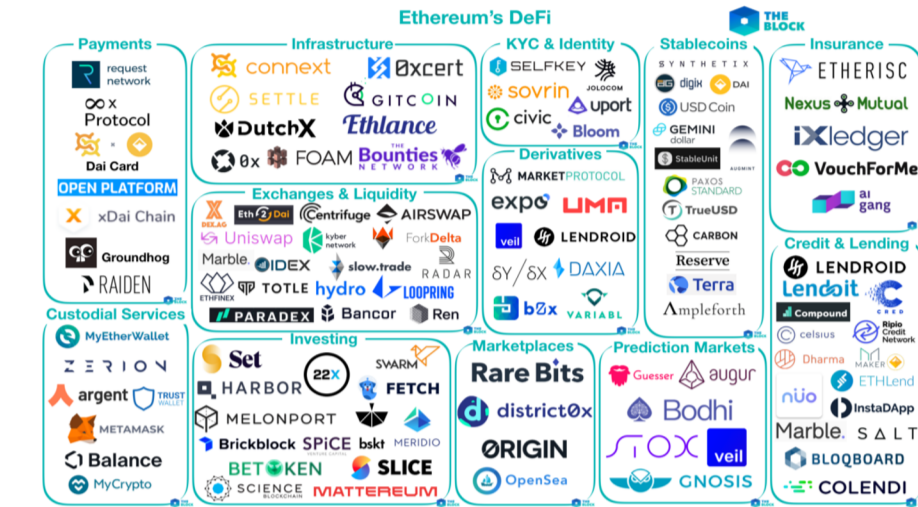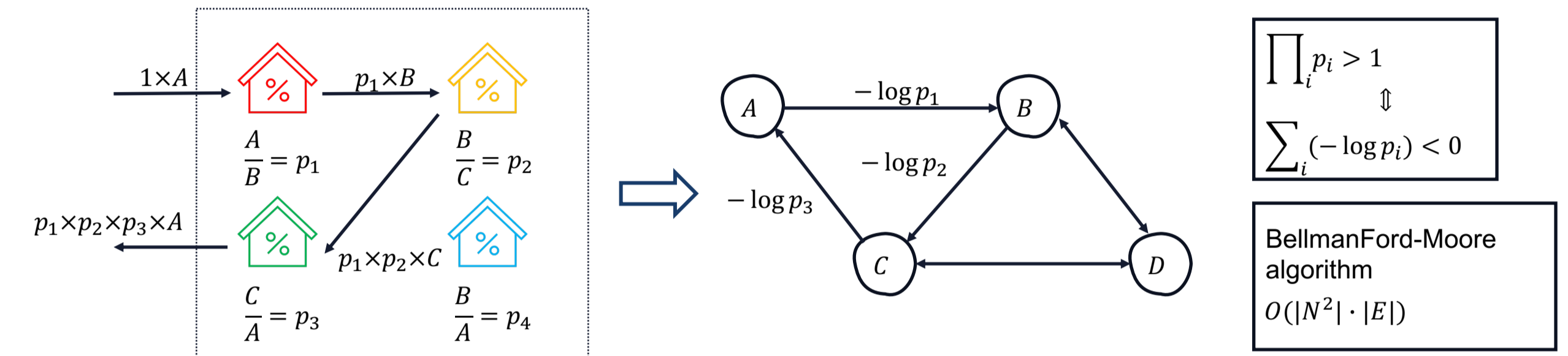Liyi Zhou, _Kaihua Qin_, Antoine Cully, Benjamin Livshits and Arthur Gervais
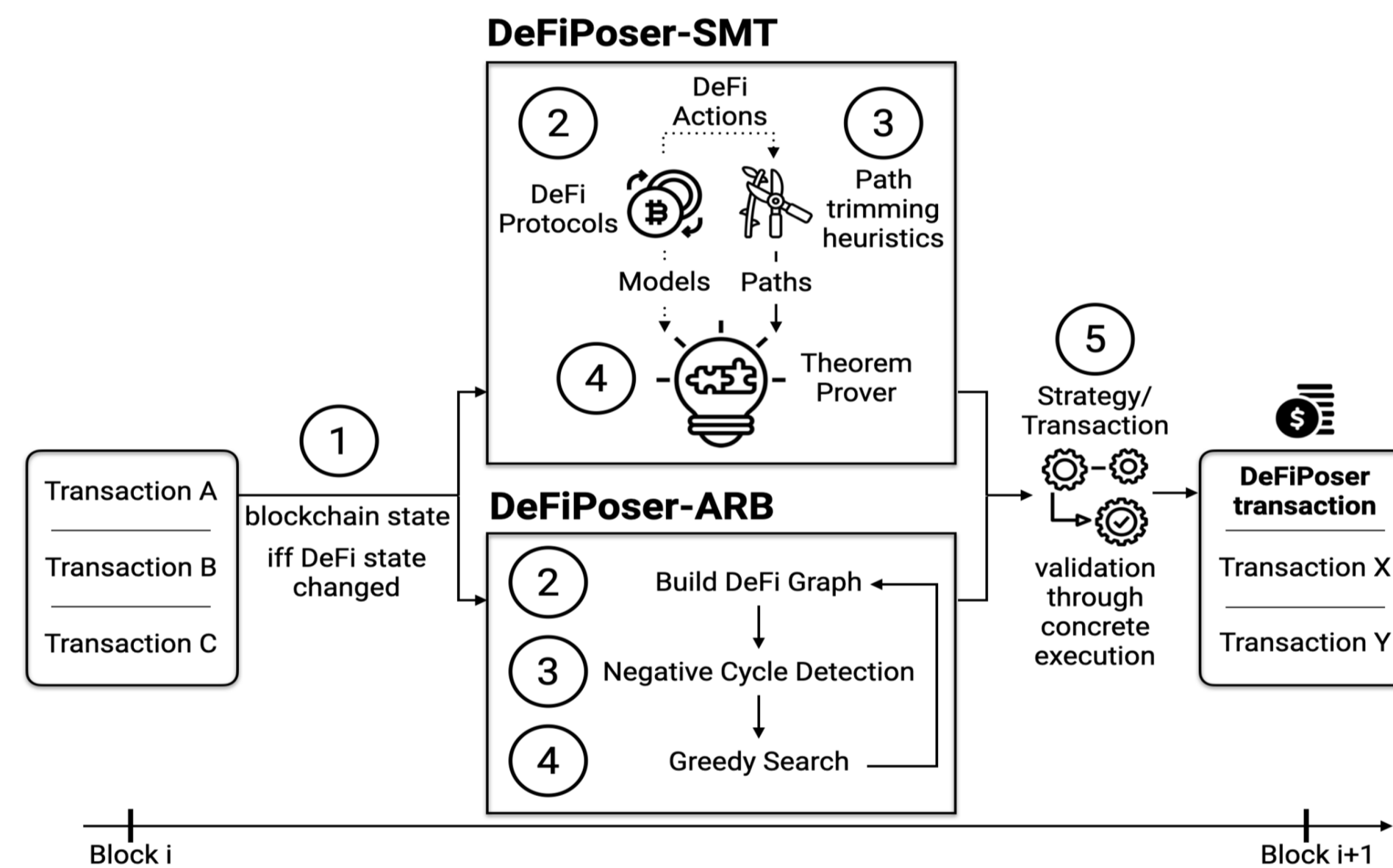
DeFi Composability
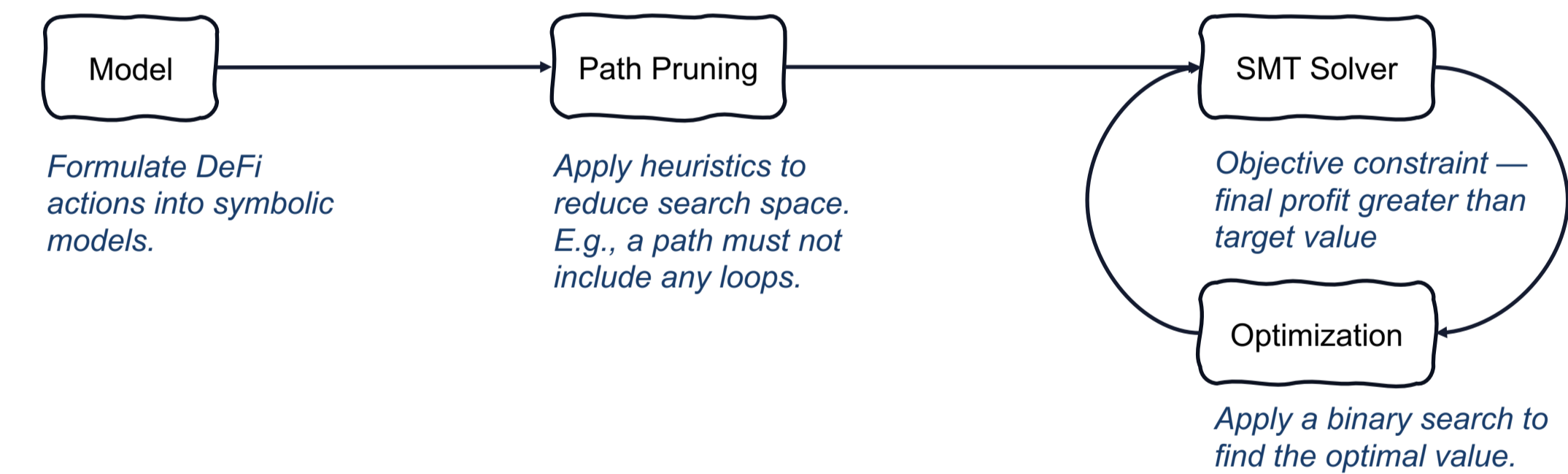

Complexity

DeFiPoser

DeFiPoser-ARB

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

DeFiPoser-SMT

- state transition model
- prune search space
- theorem prover

DeFiPoser-ARB

$$\prod_i p_i > 1$$
$$\Updownarrow$$
$$\sum_i (-\log p_i) < 0$$

BellmanFord-Moore algorithm
$O(|N^2| \cdot |E|)$

DeFiPoser-SMT

Model
Formulate DeFi actions into symbolic models.

Path Pruning
Apply heuristics to reduce search space. E.g., a path must not include any loops.

SMT Solver
Objective constraint — final profit greater than target value

Optimization
Apply a binary search to find the optimal value.

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)