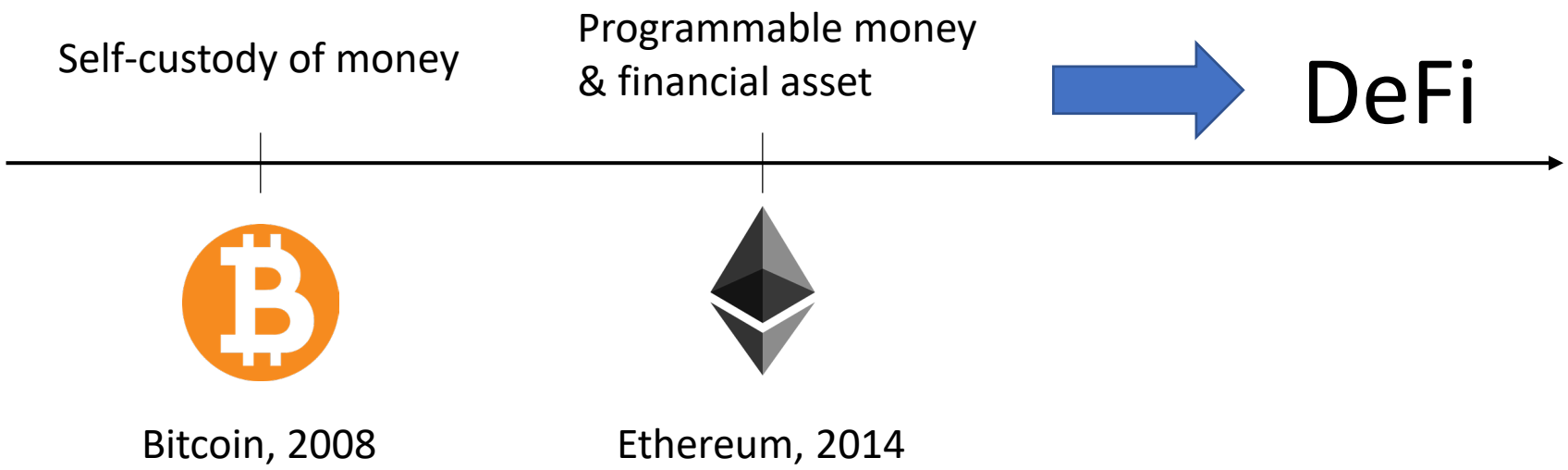
On the Just-In-Time Discovery of Profit-Generating Transactions in DeFi Protocols

Liyi Zhou, Kaihua Qin, Antoine Cully, Benjamin Livshits, and Arthur Gervais, IEEE S&P 2021

Presenter: Taeung Yoon

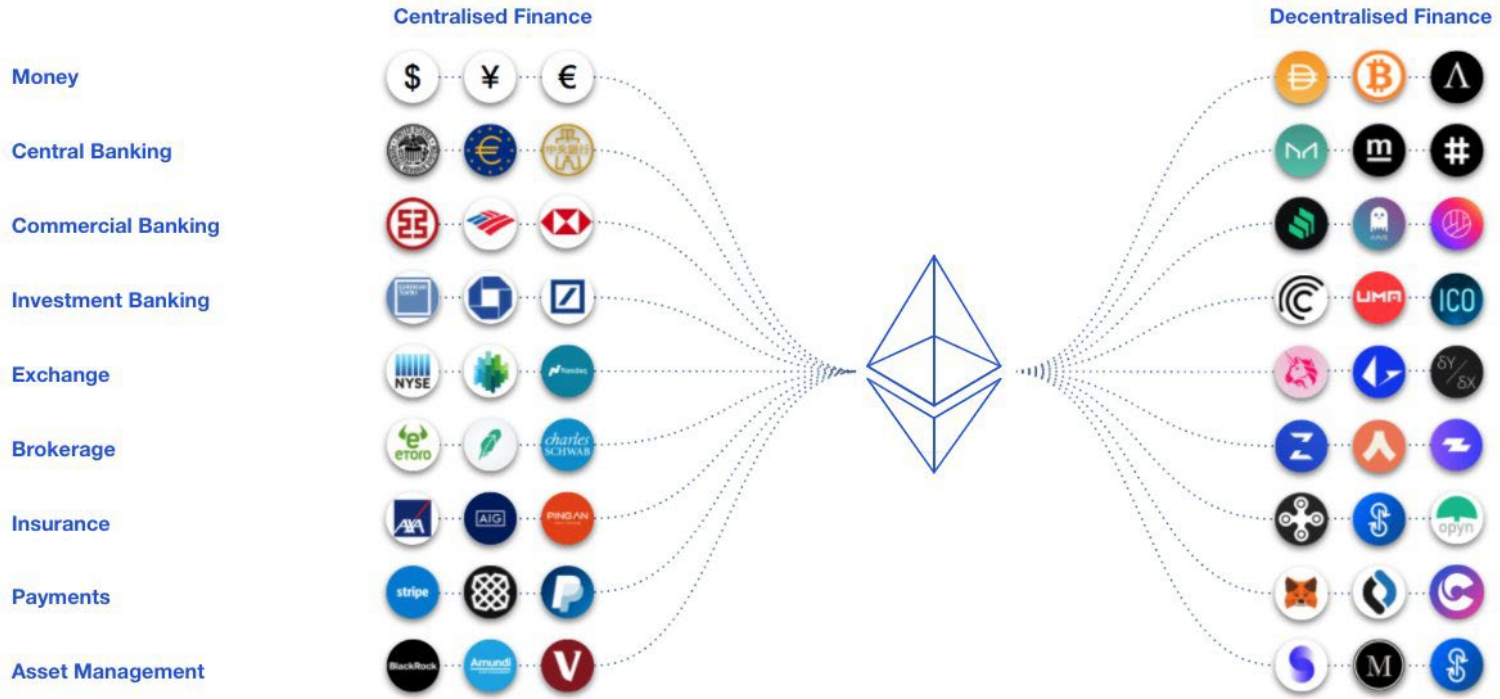
Background – Finance and public blockchains

- Centralized Finance
  - Hold custodies of customer's funds/assets
  - Customer has no privacy to service provider
- Ethereum: birth of smart contract platform



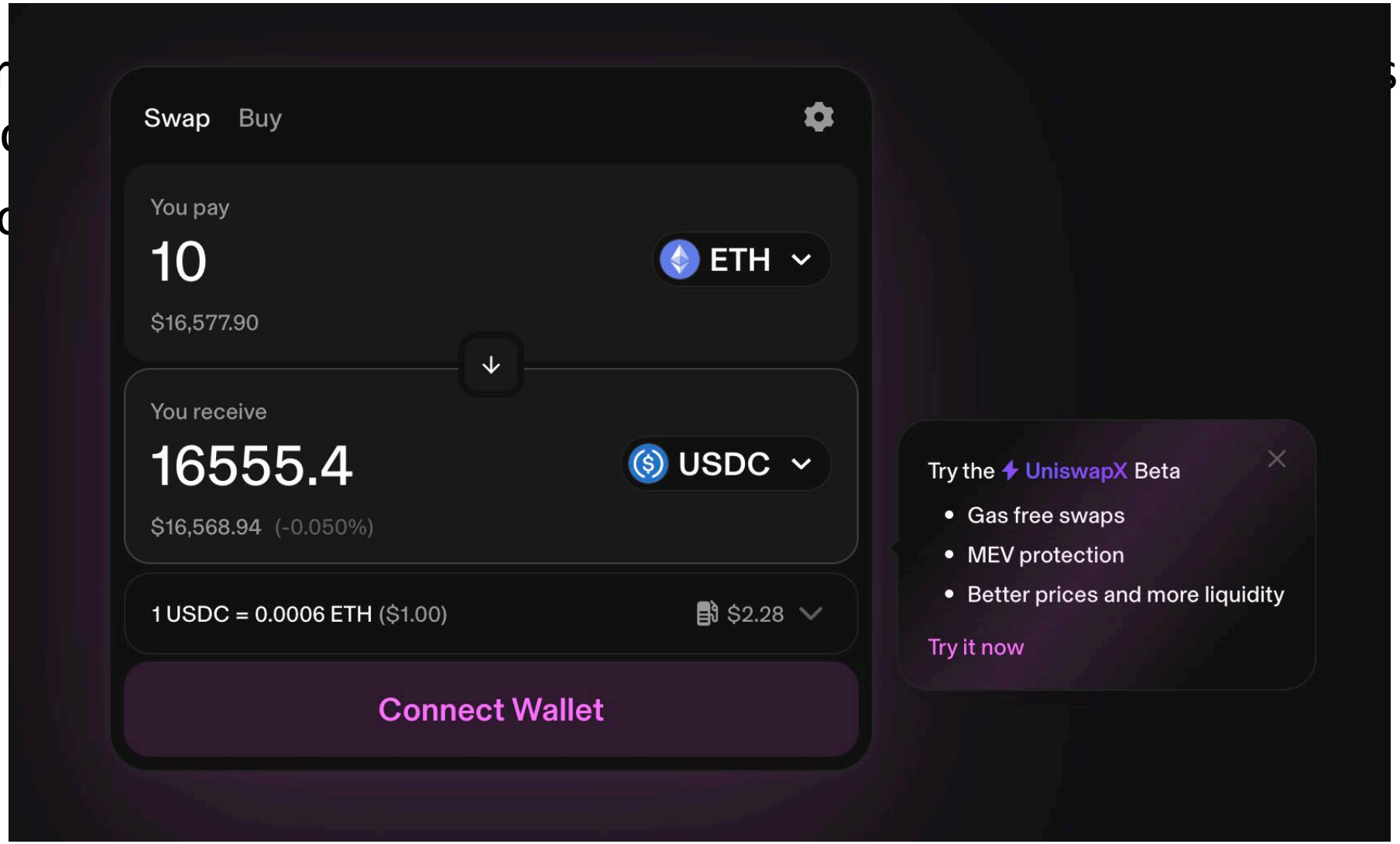
Background – What is Decentralized Finance (DeFi)?

- Financial infrastructure as an open, permissionless, and highly interoperable protocol stack built on public smart contract platforms
- Custody & settlement, Transaction execution, protocol governance



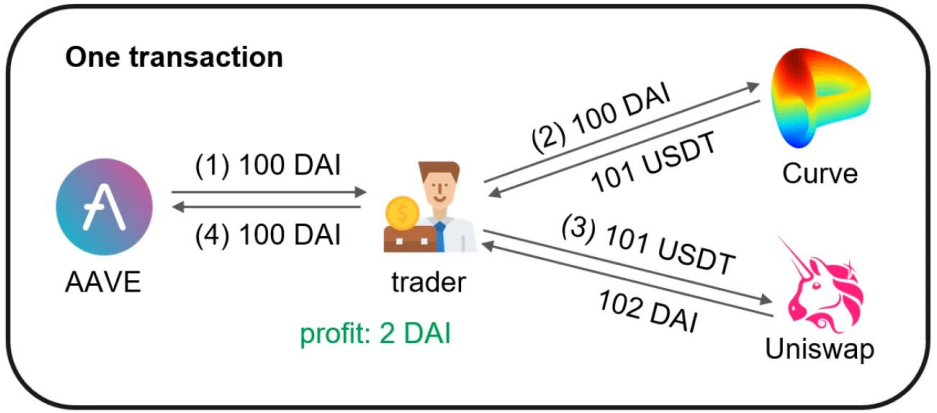
Atomic composability in DeFi

- A tr … in one bloc…
- "Ato…



Decentralized Exchange (DEX) arbitrage

- A DEX (decentralized exchange) is a peer-to-peer marketplace where users can trade cryptocurrencies in a non-custodial manner
- Multiple markets with
  - The same assets X and Y
  - Different prices for X and Y
- Prices are synchronized by “arbitrageurs”
  - Profit from the price difference
  - Requires to perform at least one transaction



Introduction

- DeFi’s explosive growth and Ethereum
- Challenges and solutions
  - DeFiPoser-ARB, DeFiPoser-SMT
- Blockchain security and MEV

Challenges

- Each DeFi protocols has different implementations, smart contracts, and pricing formulas.
  - Analyzing all DeFi systems needs a lot of efforts.

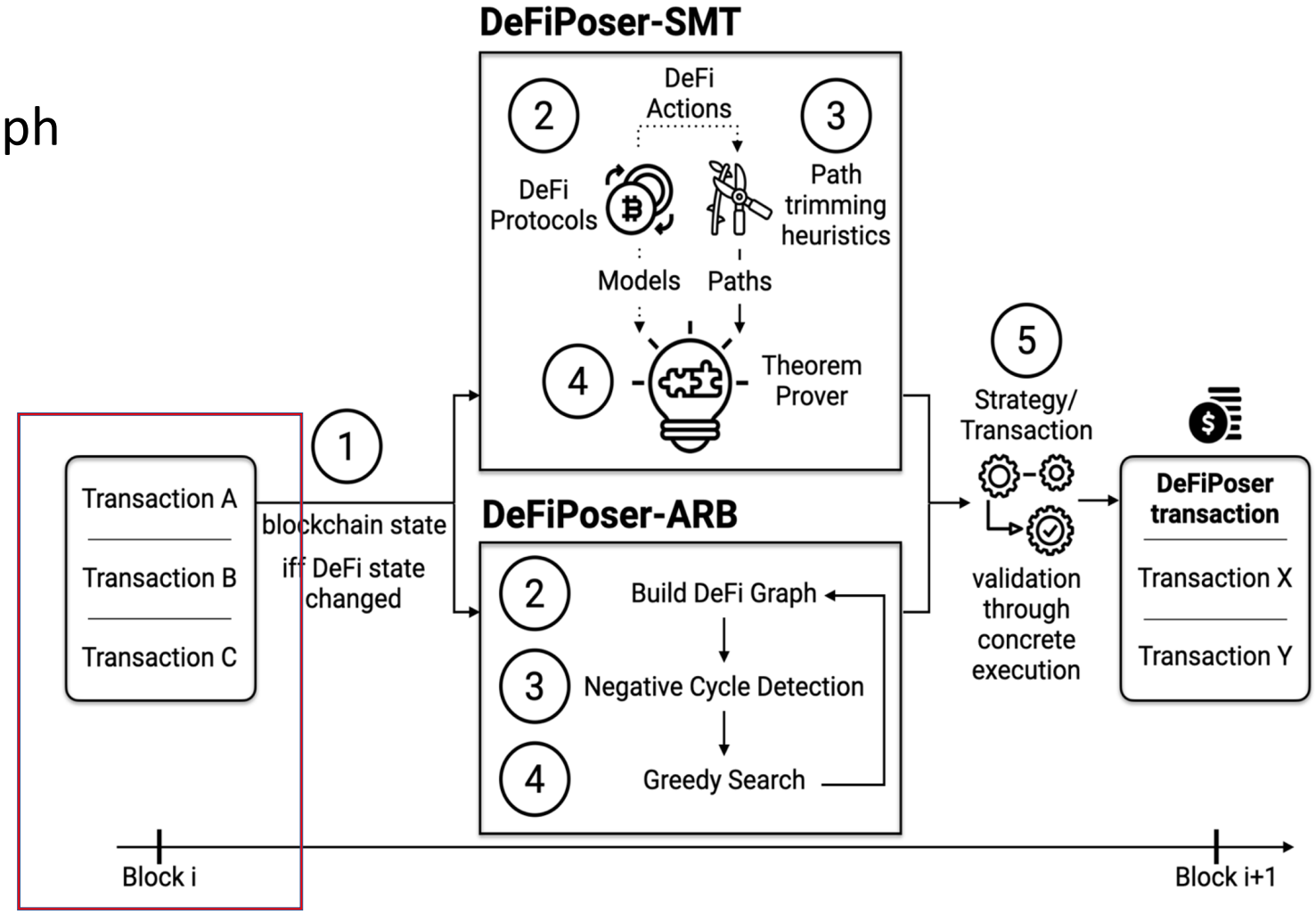
- The discovery of profitable transaction should be done in block interval (12sec).

How to detect arbitrage/profitable opportunities?

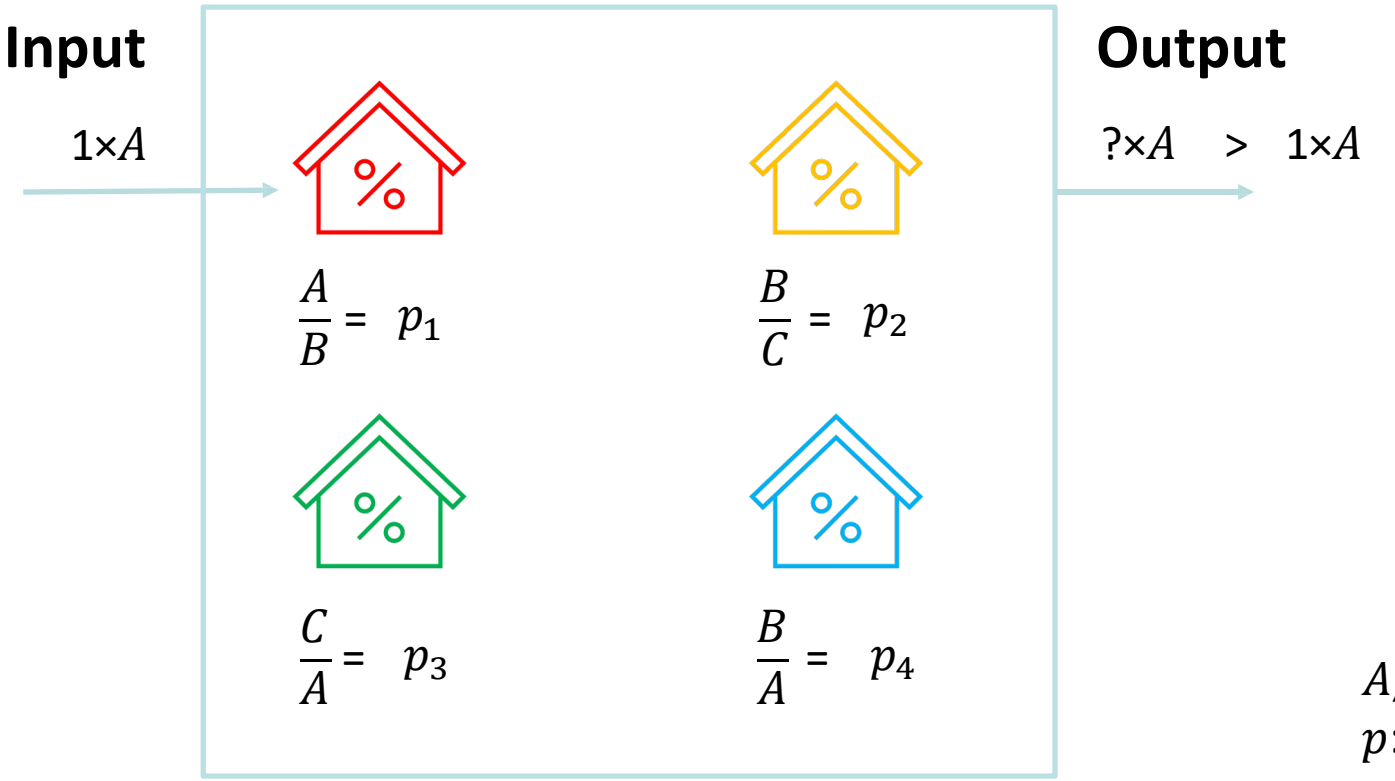
- Bellman Ford Algorithm
  - Negative cycle detection
  - Works among multiple markets
  - Used in traditional finance and DeFi
- Theorem Solver (SMT)
  - Needs to encode the DeFi model
  - Apply heuristics for path pruning

DeFiPoser-ARB and DeFiPoser-SMT

- DeFiPoser-ARB
  - Builds a directed DeFi market graph
  - Identifies negative cycles
  - Bellman Ford-Moore algorithm
- DeFiPoser-SMT
  - State transition model
  - Prunes serach space
  - Theorem prover

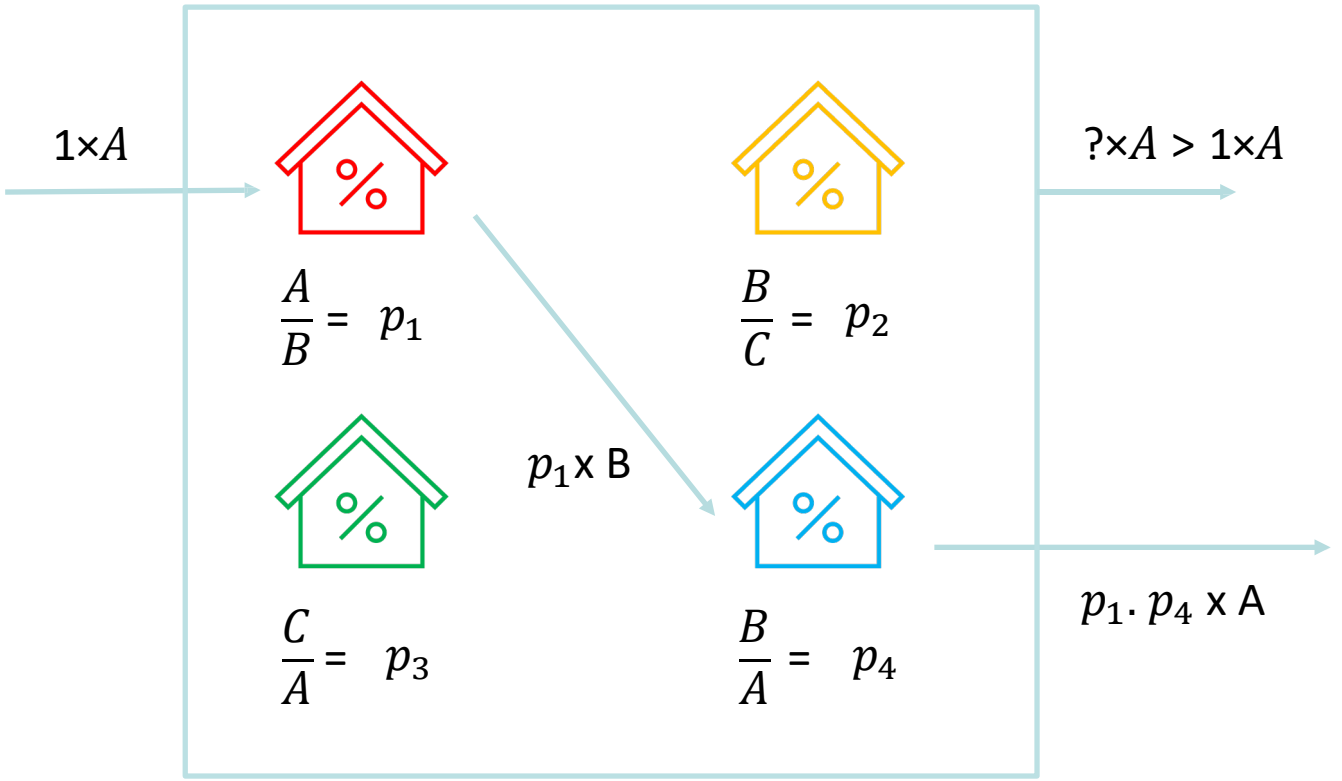


DeFiPoser-ARB



A, B : crypto asset
p: price

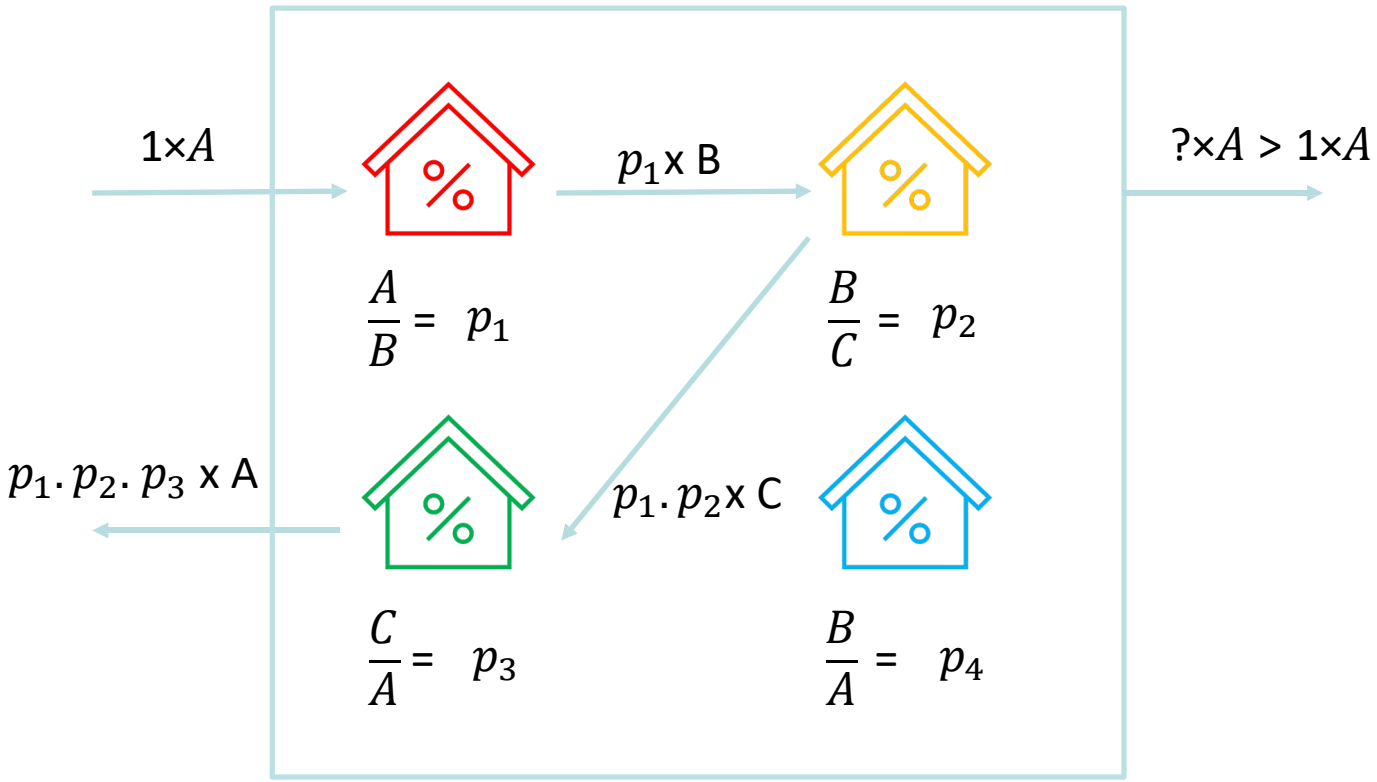
DeFiPoser-ARB



Profitable condition

$p_1 . p_4\ 1 <$

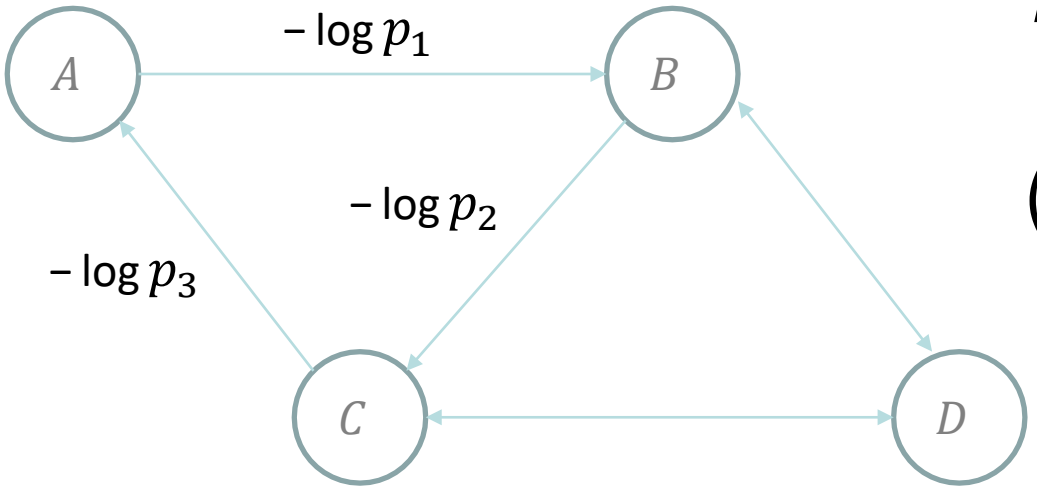
DeFiPoser-ARB



Profitable condition

$p_1.p_2.p_3 > 1$

DeFiPoser-ARB



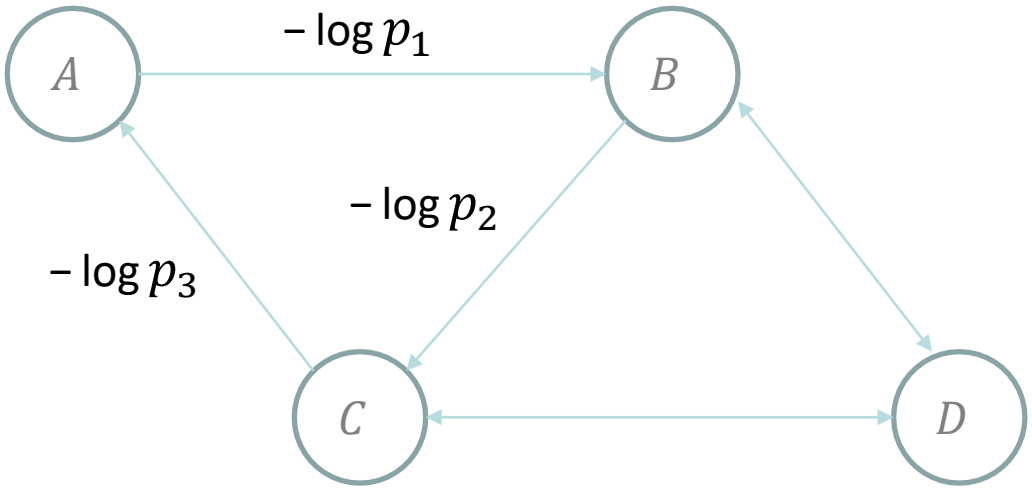
Profitable condition

$$p_1 . p_2 . p_3 \; 1 <$$

$$\Updownarrow$$

$$(- \log p_1 -) + (\log p_2 -) + (\log p_3) < 0$$

DeFiPoser-ARB



$$\prod_i p_i > 1$$

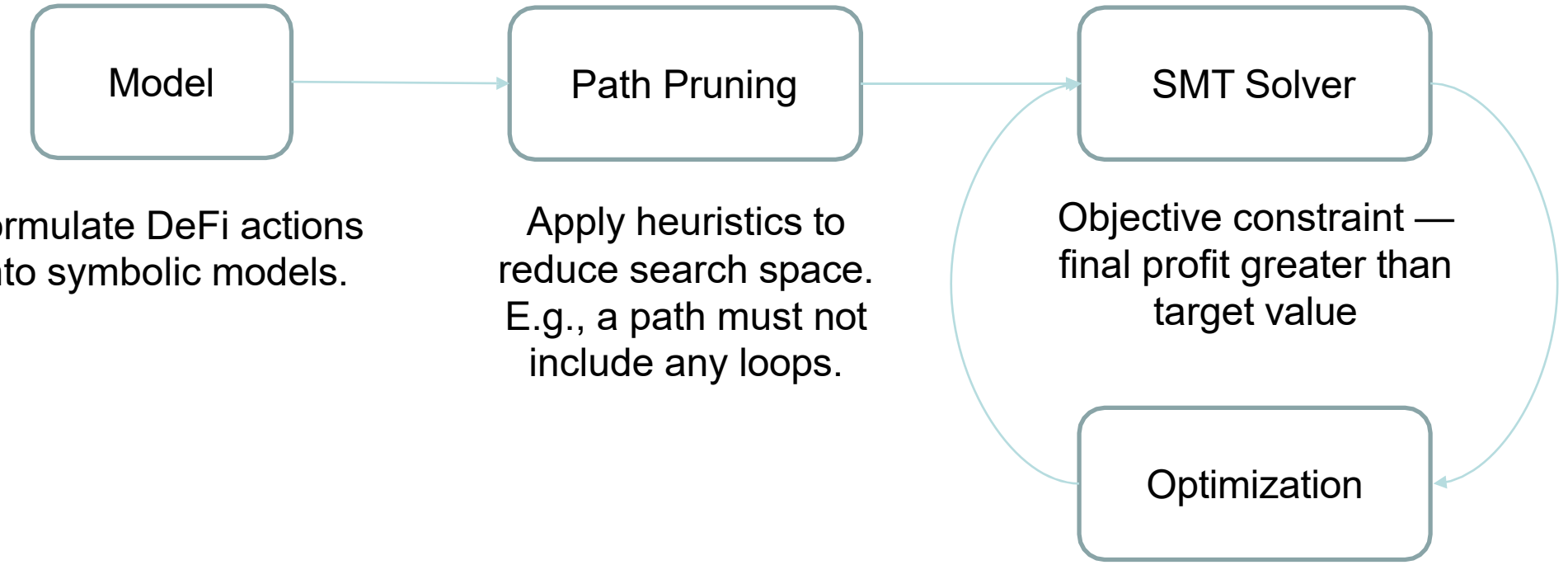
$$\Updownarrow$$

$$\sum_i (-log p_i) < 0$$

Bellman-Ford algorithm

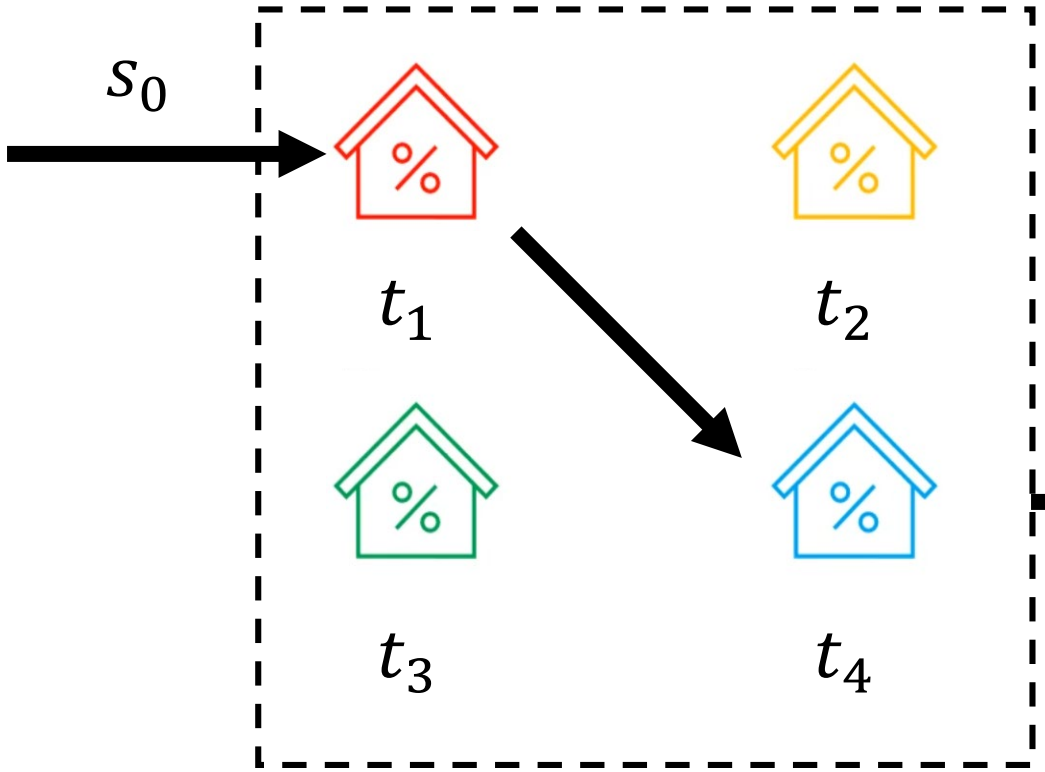
$$O(|N^2| \cdot |E|)$$

DeFiPoser-SMT



DeFiPoser-SMT

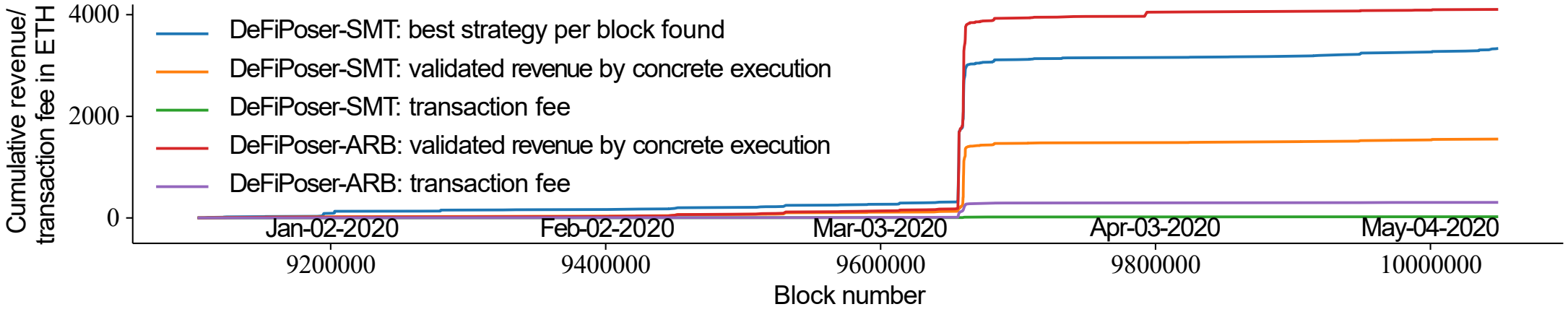
- Use symbolic models instead of prices.



$$s_1 = t_1(s_0) \ \wedge$$
$$s_2 = t_4(s_1) \ \wedge$$
$$isSAT(obj(s_2))$$

s_i: i-th state
t_i : symbolically modelled transition action
obj: symbolically modelled objective

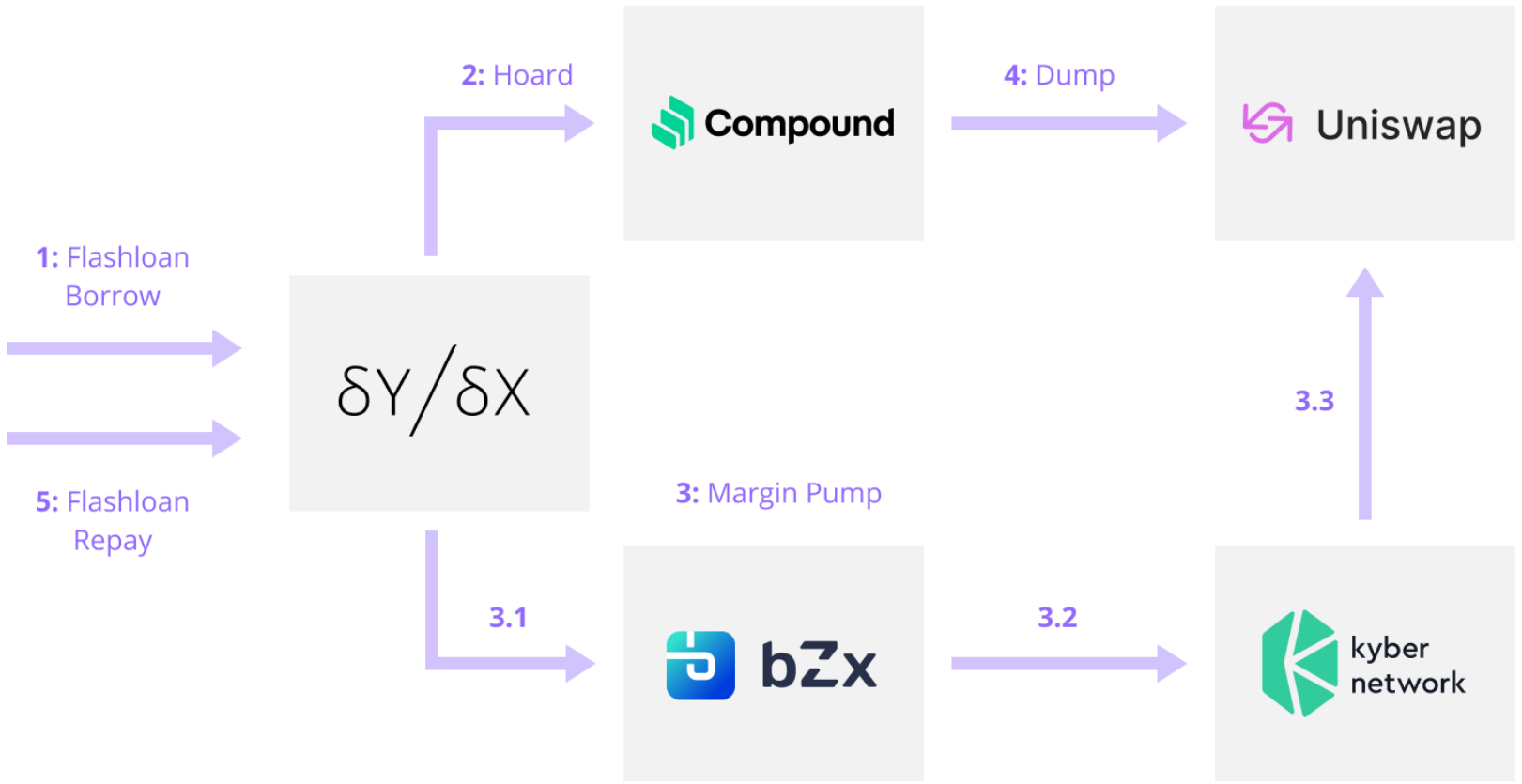
DeFiPoser Evaluation



- 96 actions on Uniswap, Bancor, MakerDAO, total of 25 assets
- Block 9,100,000 (Dec-13-2019) to 10,050,000 (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)

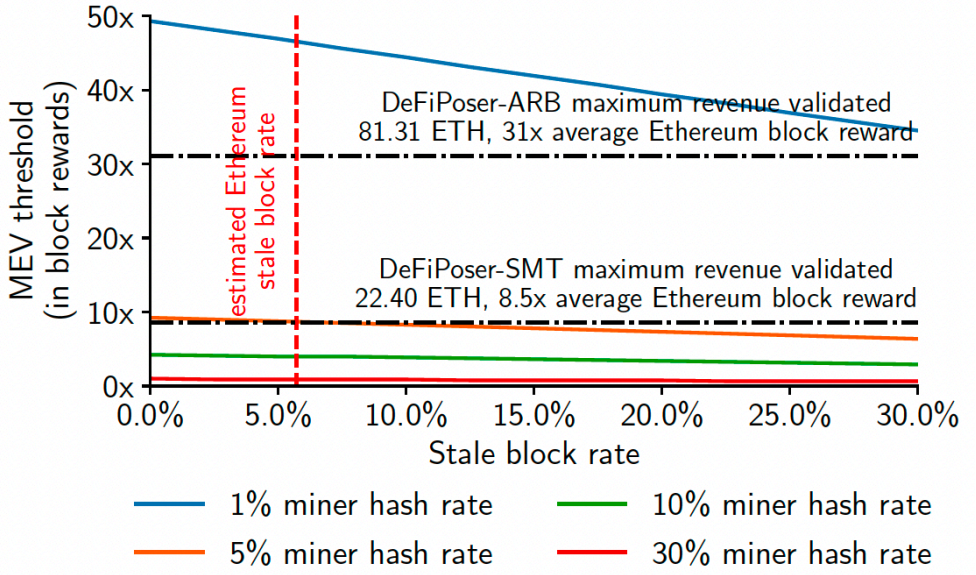
bZx attack

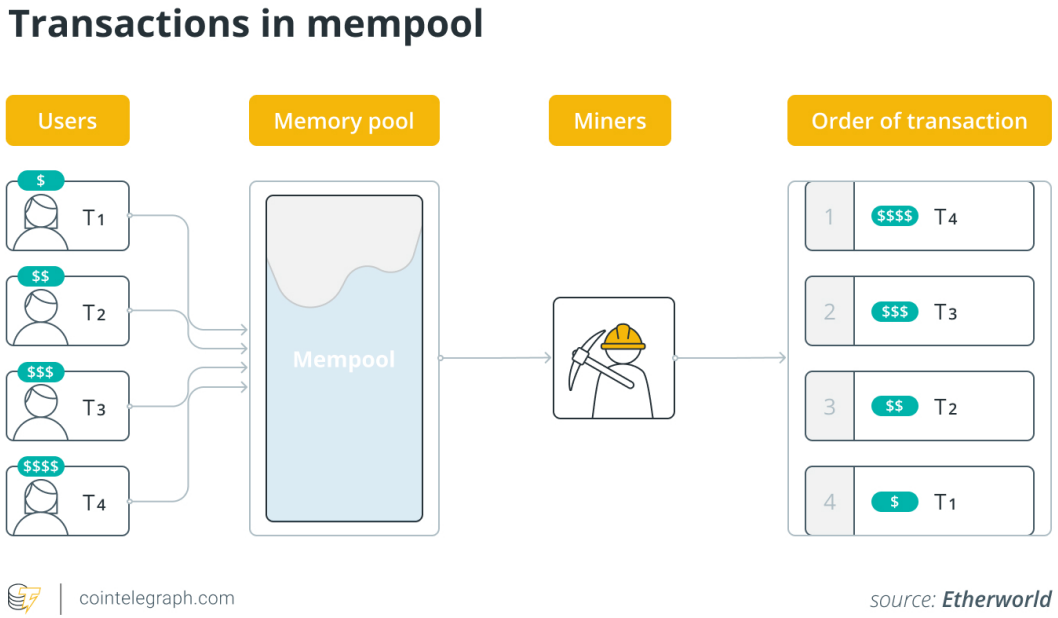
Five Composable DeFi Protocols in bZx Hack



Blockchain Security and MEV (Maximal Extractable Value)

- Quantify the value at which an MEV-aware miner would exploit an MEV opportunity by forking the blockchain
- A miner with 10% hash rate will engage to fork the chain to exploit an MEV opportunity
- MEV incentives miners to fork

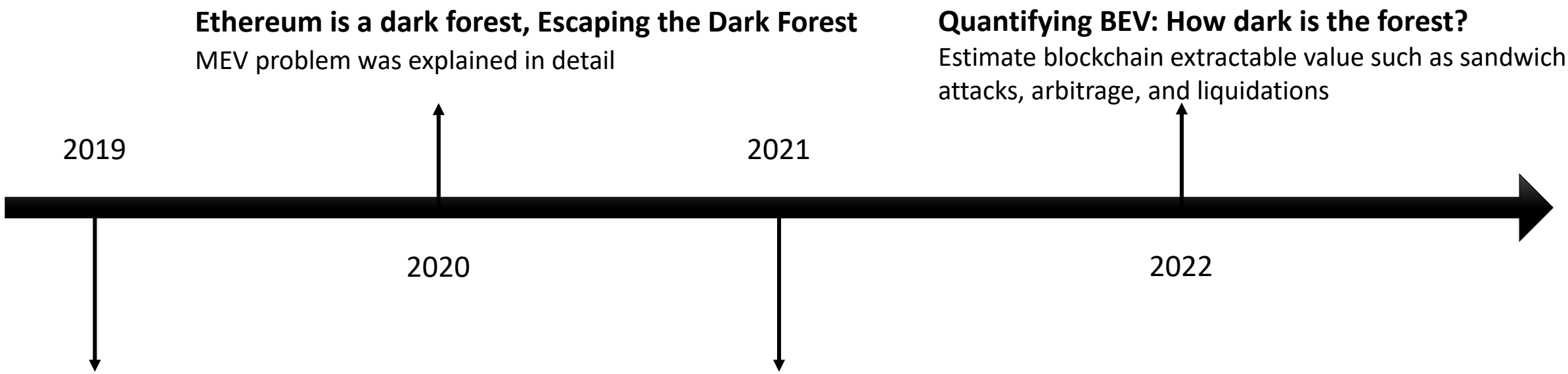




Summary, Conclusion

- Introducing DeFiPoser-ARB and DeFiPoser-SMT
- Estimated average weekly revenue
  - DeFiPoser-ARB (191.48 ETH, 76,592 USD) and DeFiPoser-SMT (72.44 ETH, 28,976 USD)
- Quantifies blockchain security challenges due to profitable transactions and Miner Extractable Value (MEV)
- Systemically documenting the process of finding profitable transaction, highlighting the potential threats by DeFi exploits

Related work



Philip Daian, Flash Boys 2.0
The word MEV was first used to explain the problem

Ethereum is a dark forest, Escaping the Dark Forest
MEV problem was explained in detail

On the Just-In-Time Discovery …

Quantifying BEV: How dark is the forest?
Estimate blockchain extractable value such as sandwich attacks, arbitrage, and liquidations

Good questions

- How can DeFiPoser contribute to the security of the ecosystem? In other words, can we prevent arbitrage using insights from this work?
- As mentioned just above, SMT could have found the bZx attack (Feb. 2020), open for 69 days, and its peak in terms of profitability (one day before the attack). So, could a SMT-like tool be used to detect and report vulnerabilities in smart contracts / DeFi Protocol and lead to a fix before the vulnerability is exploited?
- How do we categorize the bZx trade as an attack and not other similar trades that generate less profit? It exploited protocol flaws, cryptocurrency discrepancies, etc. But all traders do the same, don’t they?

Best question

- Even if arbitrage cycles were identified, there could be significant slippage during the execution process. I want to ask whether the tool can consider slippage, and if not, whether it could be improved to account for slippage. (정수환)
- Can this technique be used to assist an attacker in earning a large sum of money or execute other attack? (김호빈)
- Right now, Ethereum uses PoS, not PoW. In this case, can MEV-aware miners trigger forks similarly? If so, what could its threat model (or adversarial assumption) be? (박승민)