SPEEDEX:

A **S**calable, **P**arallelizable, and **E**conomically **E**fficient **D**istributed **EX**change

GEOFFREY RAMSEYER, DAVID MAZIÈRES, ASHISH GOEL

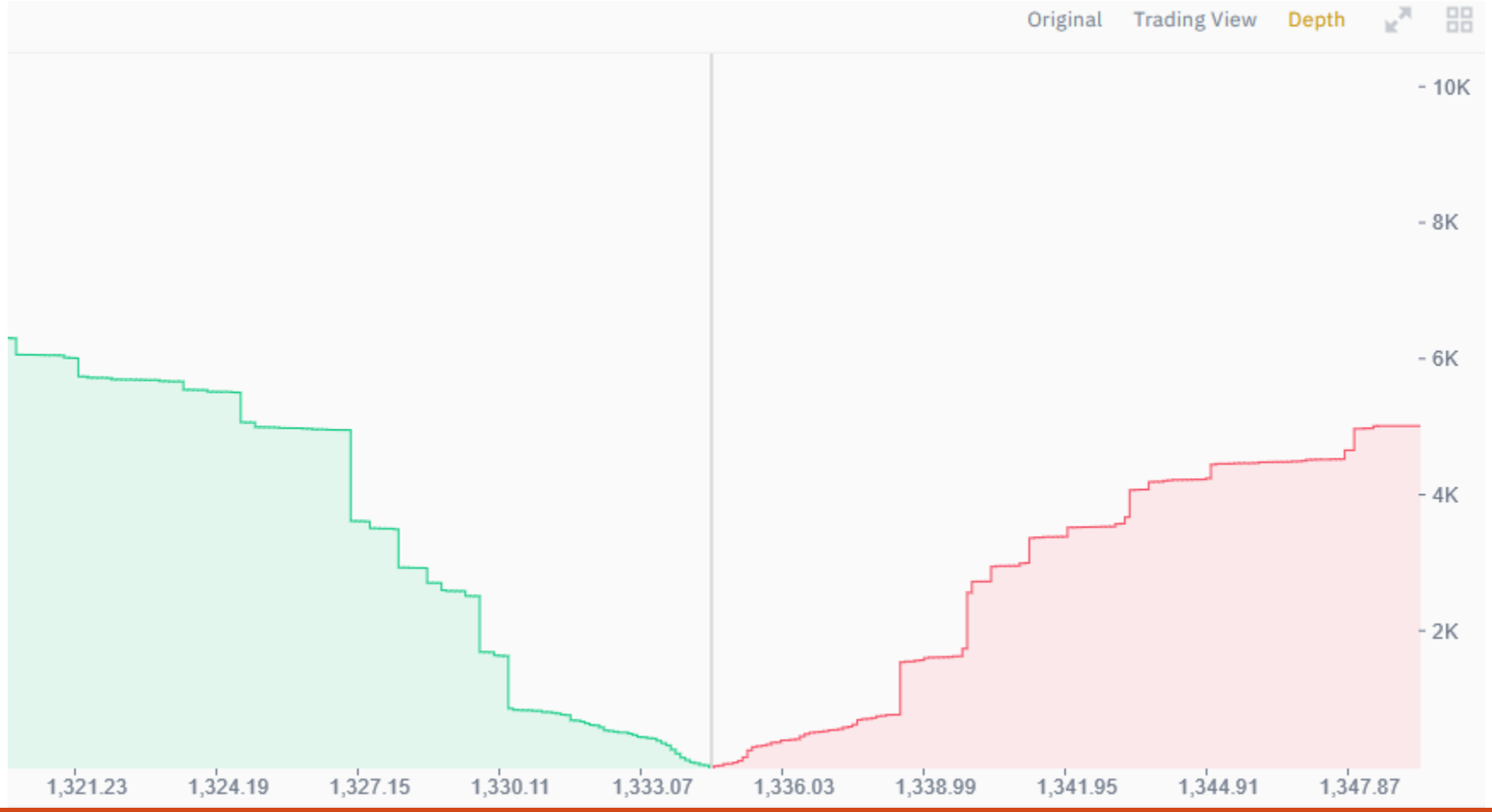
Digital Currency Infrastructure for the next 100 years

- Interoperability
  - Efficiently Exchangeable
- Scalable Infrastructure
- Auditability, Reliability

Outline

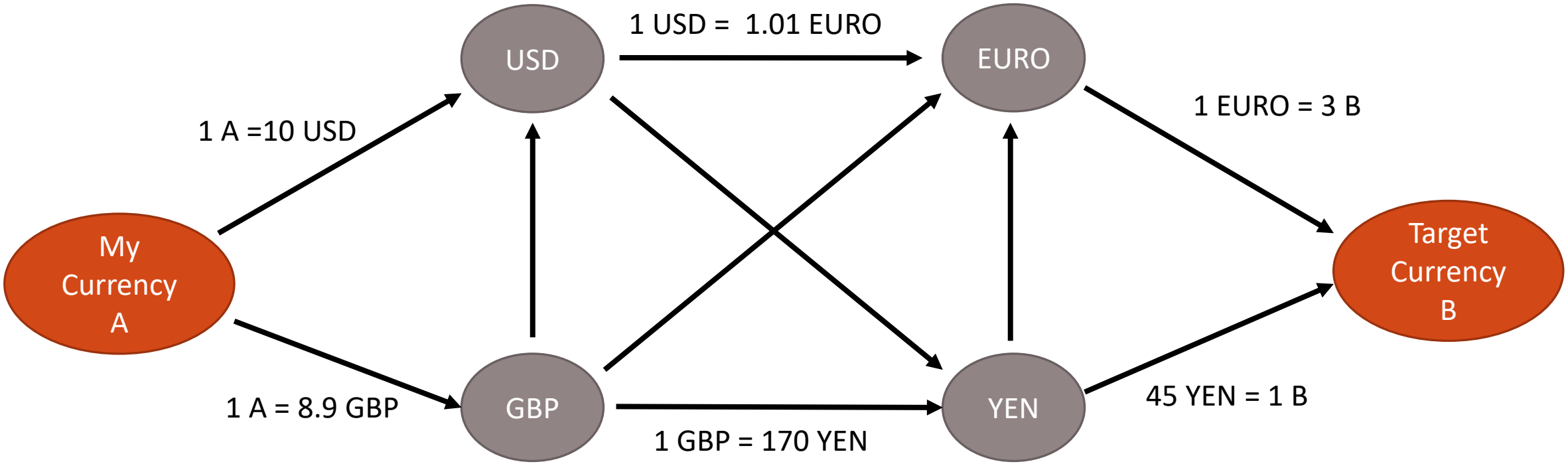
- Challenges in Existing DEX design
- What is SPEEDEX?
  - Many-Asset Batch Exchange
  - Scalable, High Throughput
  - Replicable, Auditable ⇒ Decentralized (in a Blockchain)

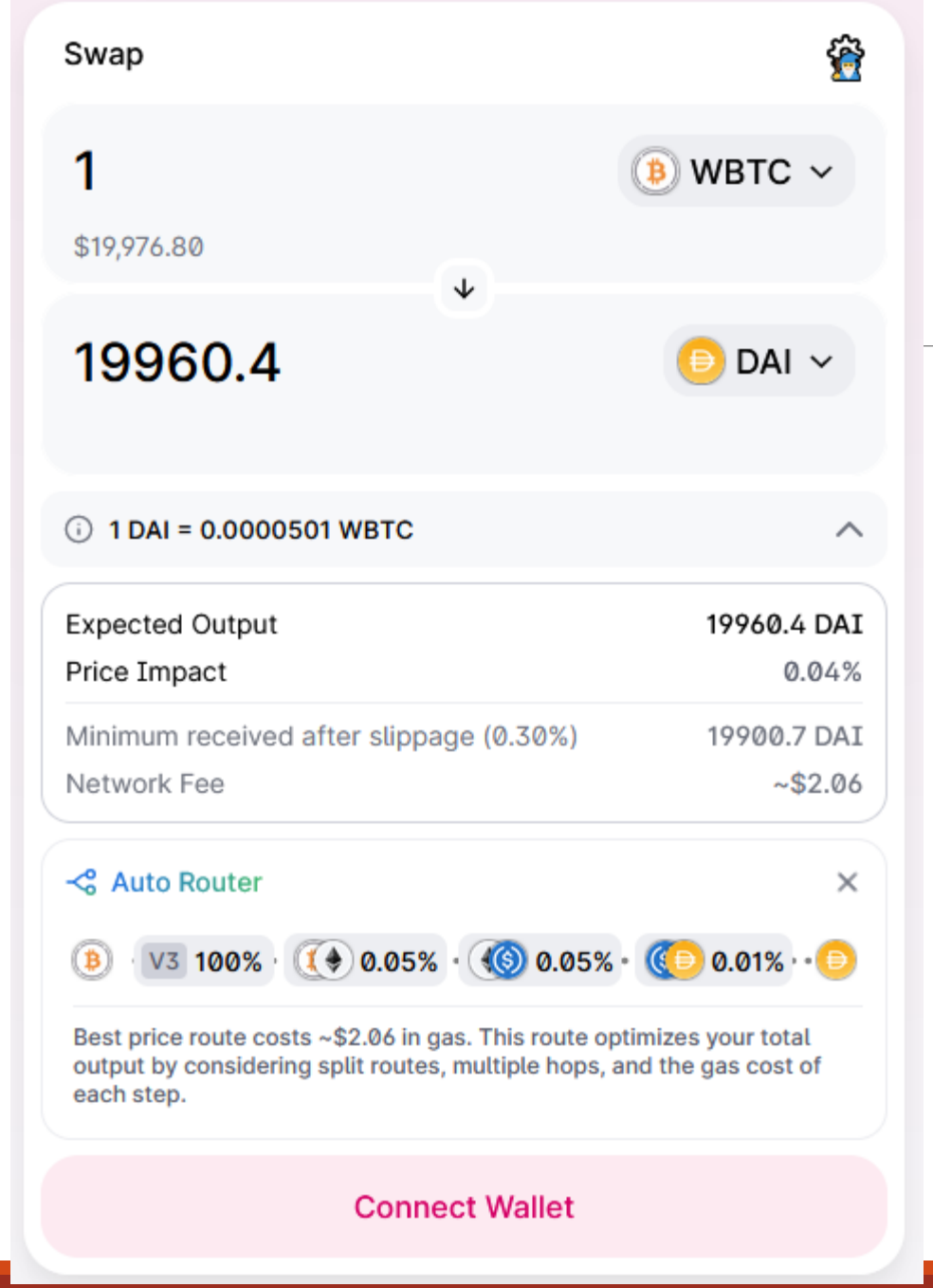
Existing Exchanges: Continuous Double-Auctions

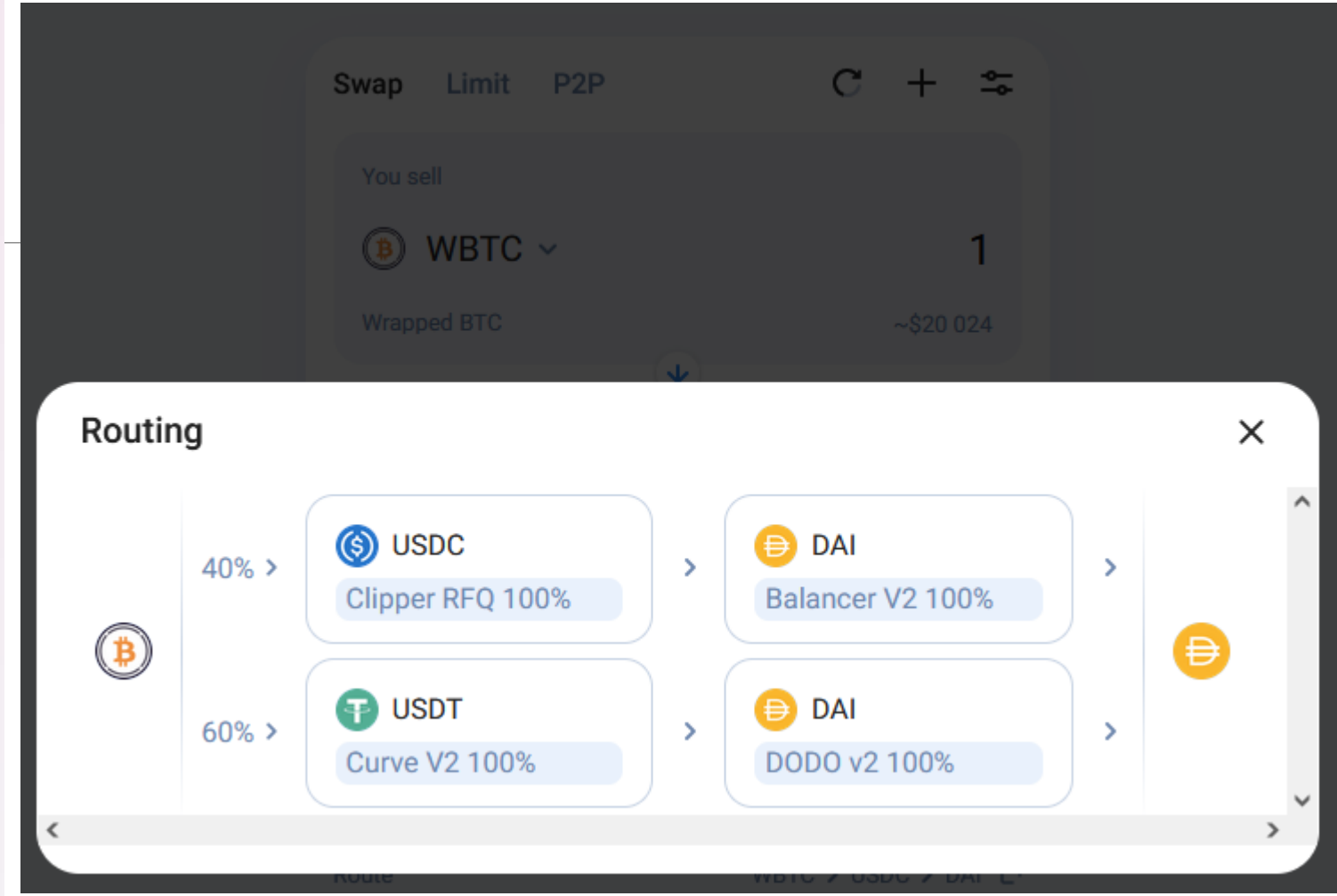


https://www.binance.com/en/trade/ETH_BUSD

Existing Exchanges: Pairwise Trading







https://app.uniswap.org/#/swap

https://app.1inch.io/#/1/unified/swap/WBTC/DAI

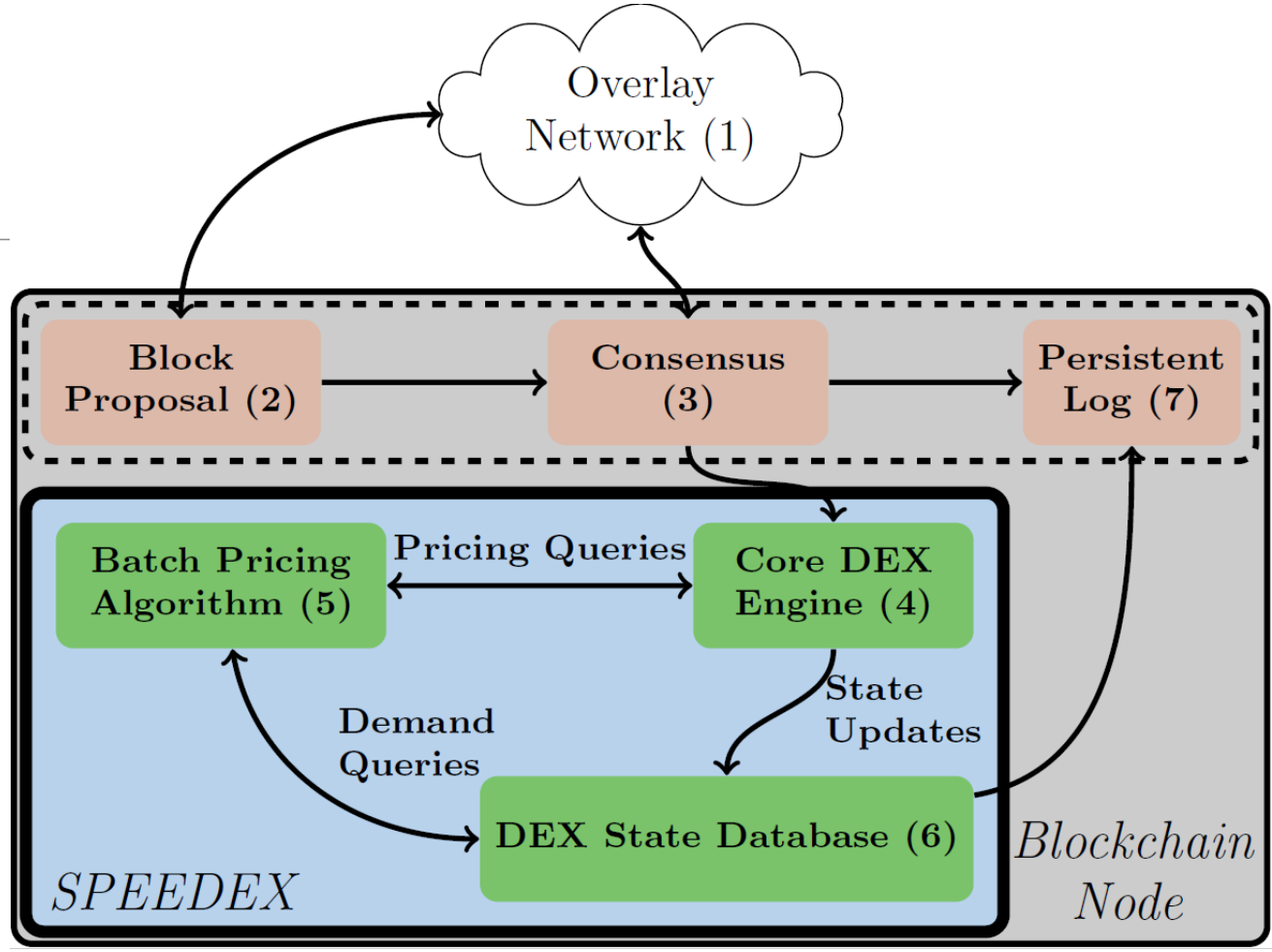
What is SPEEDEX?

Scalable

Parallelizable

Economically **E**fficient

Distributed **EX**change



SPEEDEX Batch Trading

- How can we trade many assets all in one batch?
- Answer:
  - Model a batch as an Arrow-Debreu Exchange Market
  - Compute Equilibrium (Prices $\{p\}$, Allocations $\{x\})$

Sell $10 for at least €1.20/$1

$$u(x) = 1.2\, x_{€} + \mathrm{x}_{\$}$$

$$x_{\$} + \frac{p_{€}}{p_{\$}} x_{€} \leq 10$$

Why Many-Asset Batch Trading?

- No Risk-Free Front Running
  - Trade at equilibrium price, not limit price
- No Routing Problem, No Internal Arbitrage
  - No reason to hold intermediate assets
  - $\frac{p_A}{p_B} * \frac{p_B}{p_C} = \frac{p_A}{p_C}$
- Liquidity between infrequently traded assets

Why Many-Asset Batch Trading?

- SPEEDEX trading logic is unaffected by trade ordering
  - Trade offers in one block *commute* with one another
  - Scalability through Parallelism

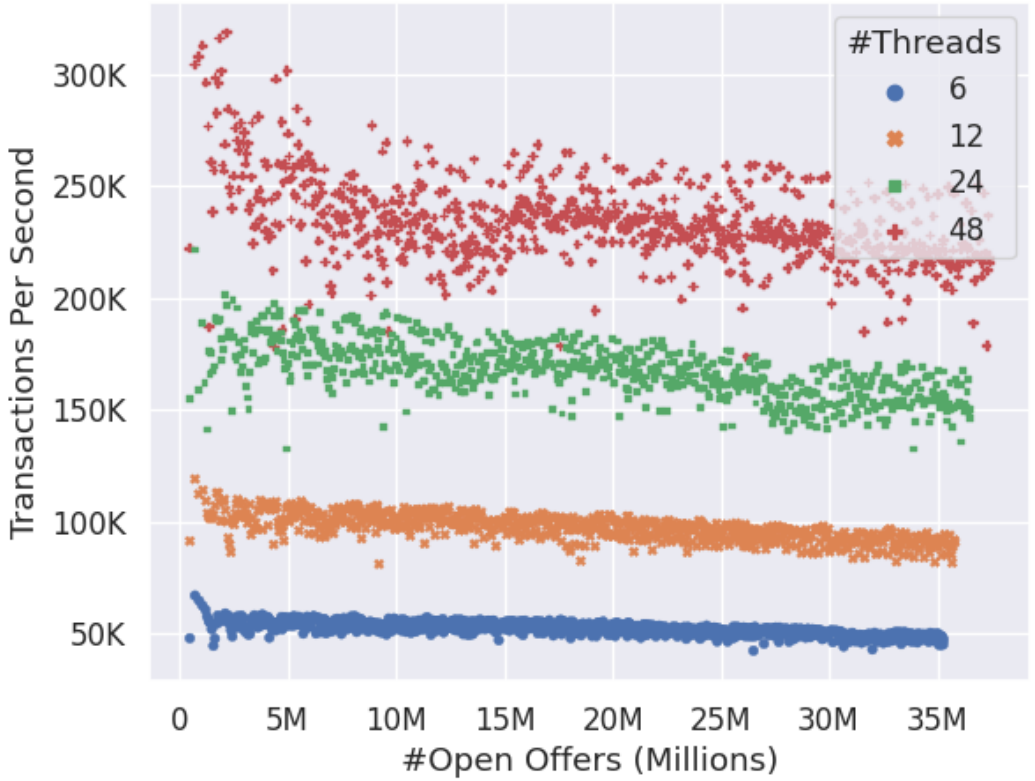
Core Challenge: Equilibrium Computation

- Number of assets << Number of Trade Offers
- ∃ Convex Program [DGV16]
- Iterative method: Tâtonnement [CMV05]
  - Query “How close is a set of prices to equilibrium?”
  - Adjust (Economics 101)
  - Repeat
- Round Results with Linear Program

Core Challenge: Equilibrium Computation

- Need ~1,000-10,000 loop repetitions for high accuracy
- Expensive: “Try to clear market with candidate valuations”
  - Sort + preprocess + binary search: O*(log(#offers)* * $\#assets^2$)
- Linear program size: $O(\#assets^2)$

Overall Transaction Rate



SPEEDEX: A New Distributed Exchange

- Batch offer matching eliminates internal arbitrage and front-running.
- Replicable and Auditable: Can run in a blockchain “Layer-1”
- Scalability via a transaction semantics and a trading engine in which operations **commute**.
- More than **200,000 transactions/second** on a 48-core machine with 10s of millions of open offers

Open Questions

- Efficient Market-Making?
- Cost of Liquidity Provision?
- Batch Frequency?

geoff.ramseyer@cs.stanford.edu