



# Suboptimality in DeFi

---

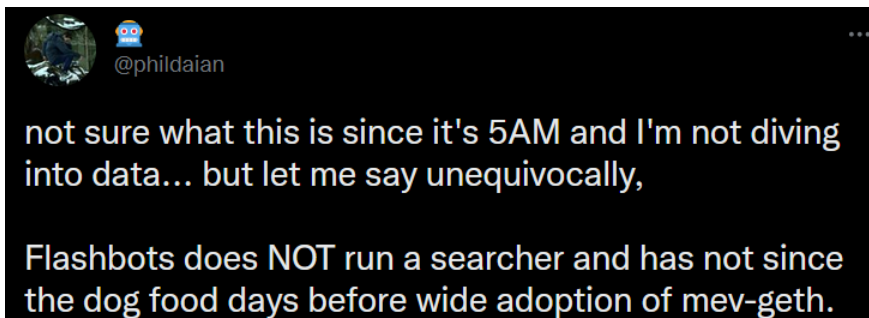
**Aviv Yaish**, Maya Dotan, Kaihua Qin, Aviv Zohar, Arthur Gervais



# Overview

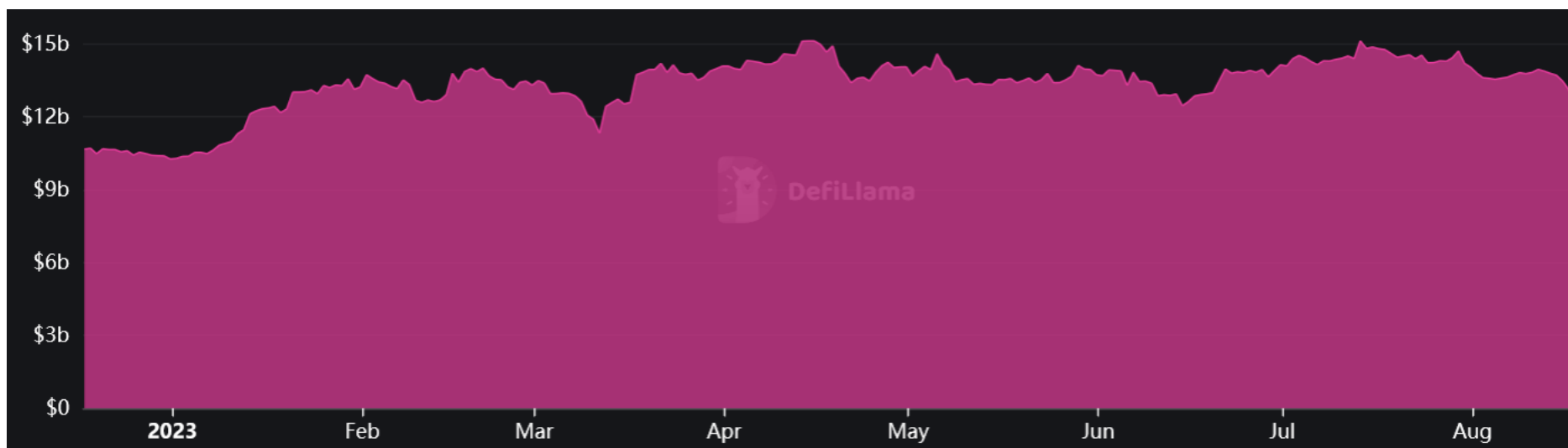
---

- DeFi users and tools perform suboptimally
  - Three primitives (TVL>\$16 bil): collateralized lending, flashswaps, flashswap-based liquidations
  - Cast each as an optimization problem
  - Suboptimality illustrated via a series of case studies
- Lenders: can increase short-term profit by over 100%
- Arbitrageurs: could improve by >4.2 million USD
  - Surprising circumstantial evidence: how do private TX channels make money?



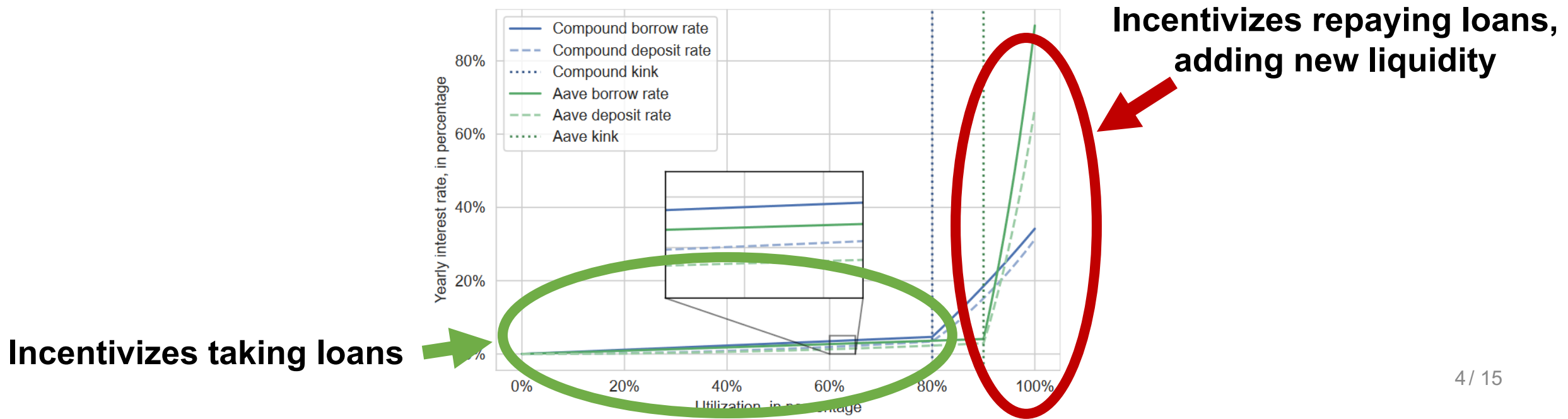
# Part I: Lending Suboptimality

- Users can lend & borrow funds
- Interest determined algorithmically



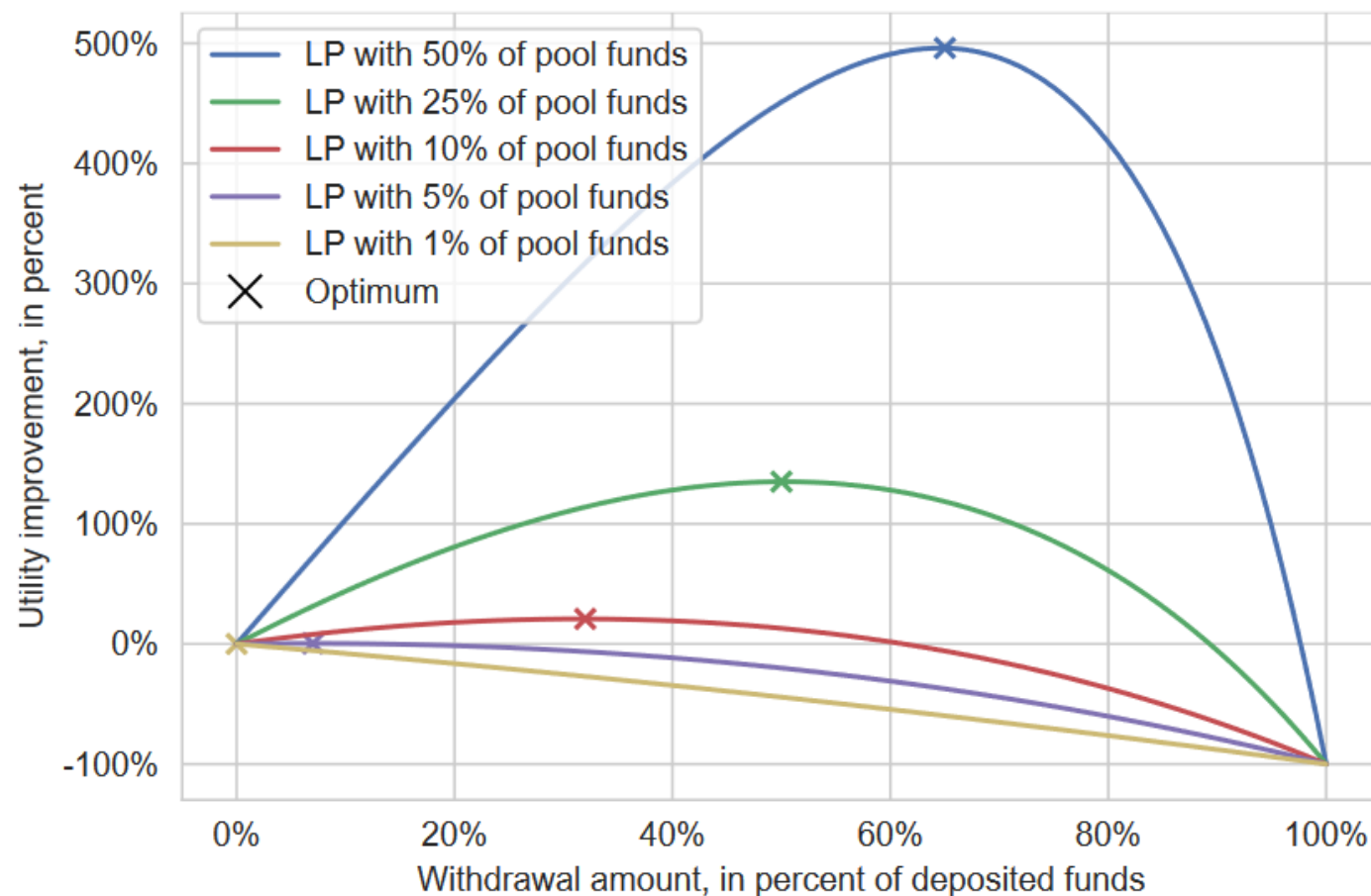
# Interest Rates

- Utilization =  $\frac{\text{borrows}}{\text{deposits}}$
- Interest = monotonically increasing in utilization



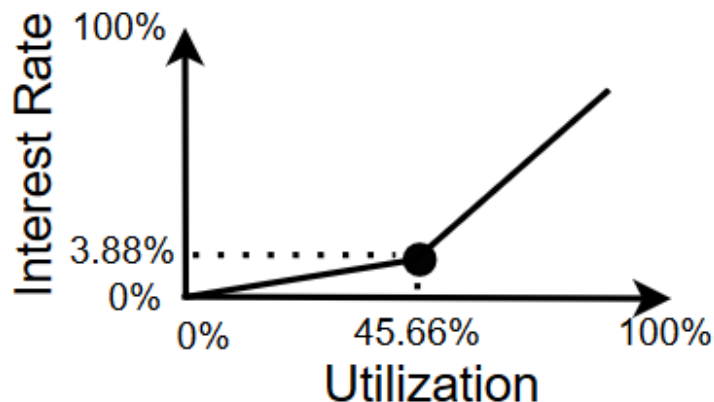
# Short-term Optimality

$$\begin{aligned} & \underset{d^*}{\text{maximize}} && d^* \cdot I_d(u) \\ & \text{subject to} && d^* \geq 0 \\ & && d^* \leq d_{max} \\ & && u = \frac{b}{d + d^*} \end{aligned}$$



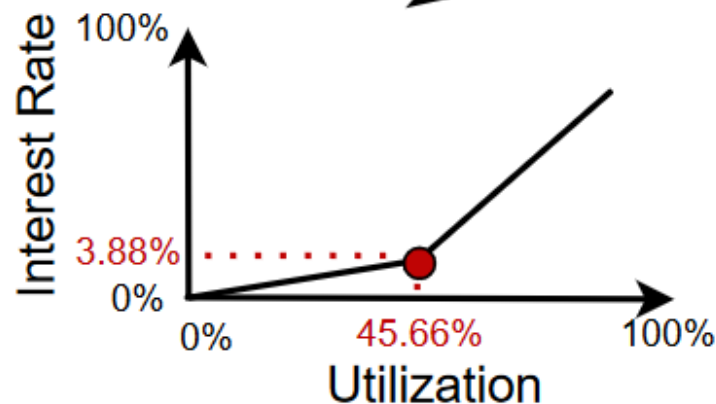
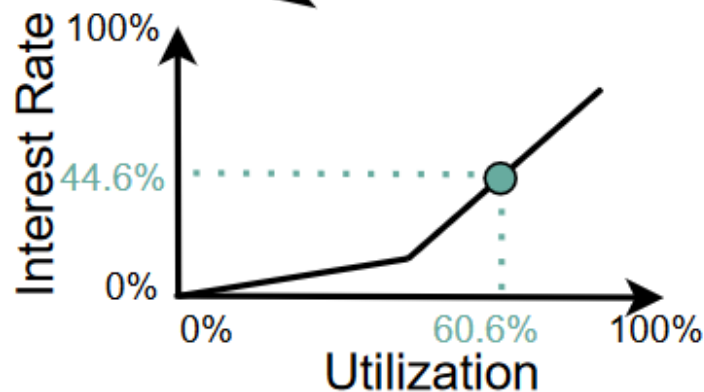
# Whales Dictate Utilization

Liquidity  
Provider



Remove liquidity

No action

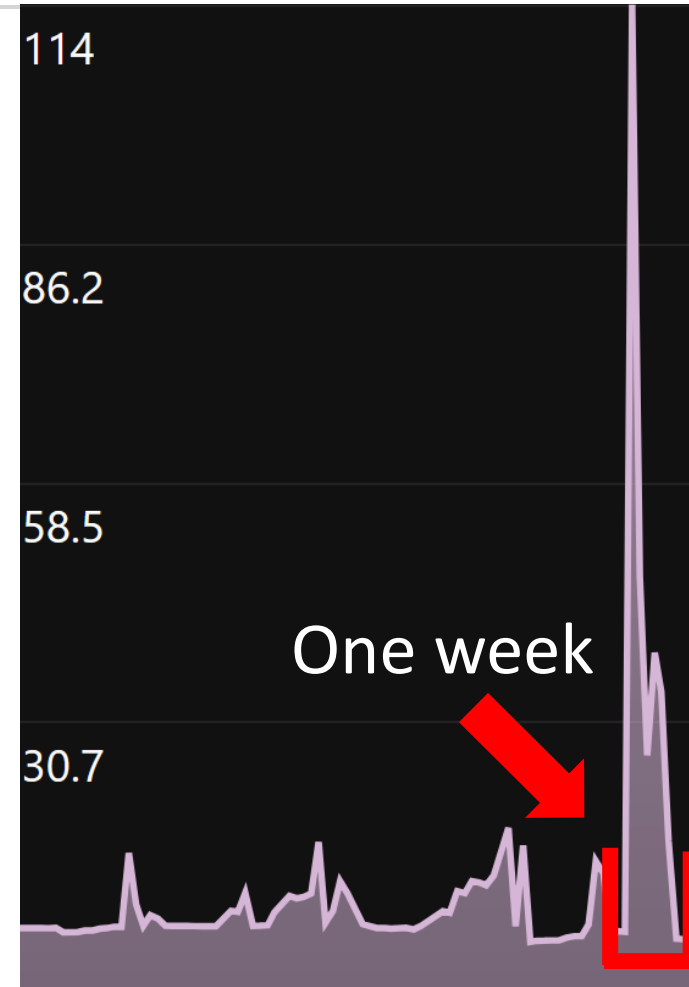


## AAVE's CRV pool, Sep '22:

- 1 user supplies 80% of liquidity
- Can withdraw 28% of funds
- Get 700% abs. *short-term* profit

# Limitations

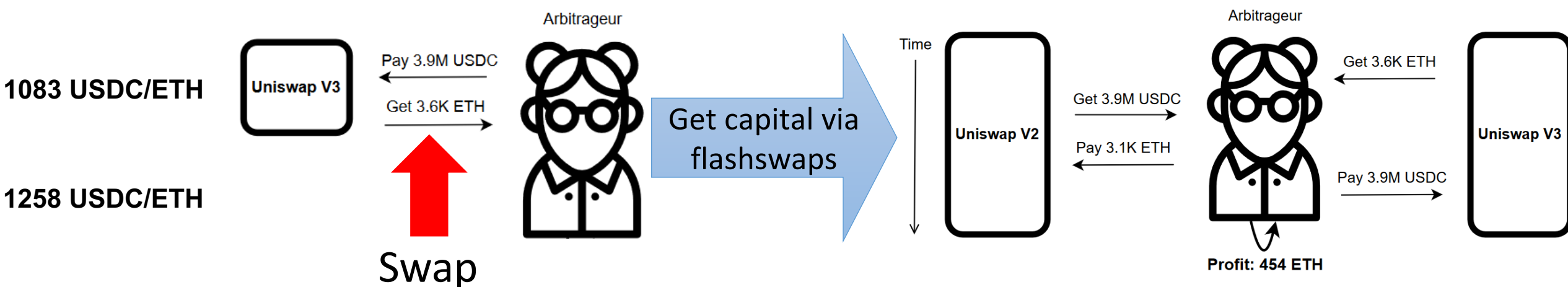
- ***Long-term sustainability not assured***
- Works for thinly-traded assets
- Proof of concept came few months after publication



Source: aavescan.com

# Part II: Flashswap Suboptimality

- Exchanges like Uniswap (& clones) have +\$4 billion TVL
- Arbitrageurs find and close arbitrage opportunities
- Some capital is needed
- Flashswap: get capital, use it, repay exchange (or TX reverts)

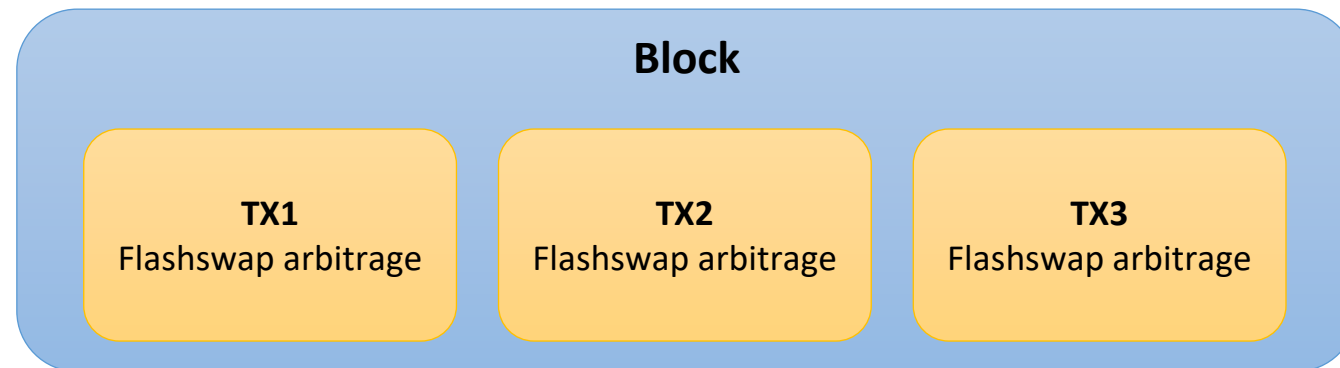




# Suboptimality Heuristic

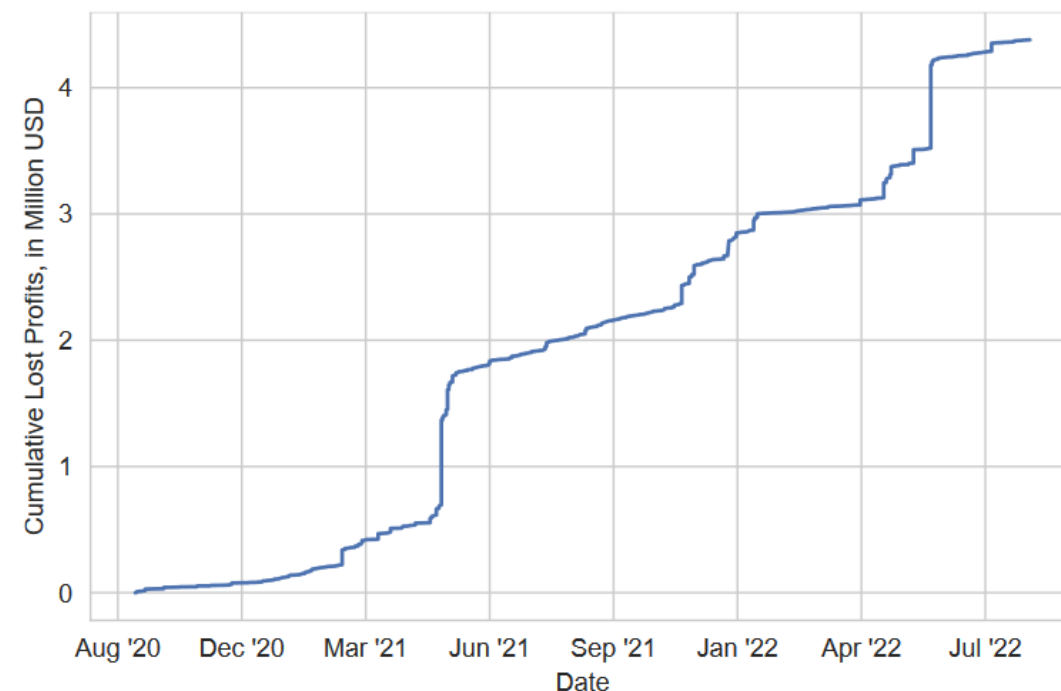
---

- Heuristic: consecutive flashswaps exploiting similar arbitrage types
- Backrunning arbitrage can't exist if 1<sup>st</sup> TX is optimal
- First TXs are suboptimal



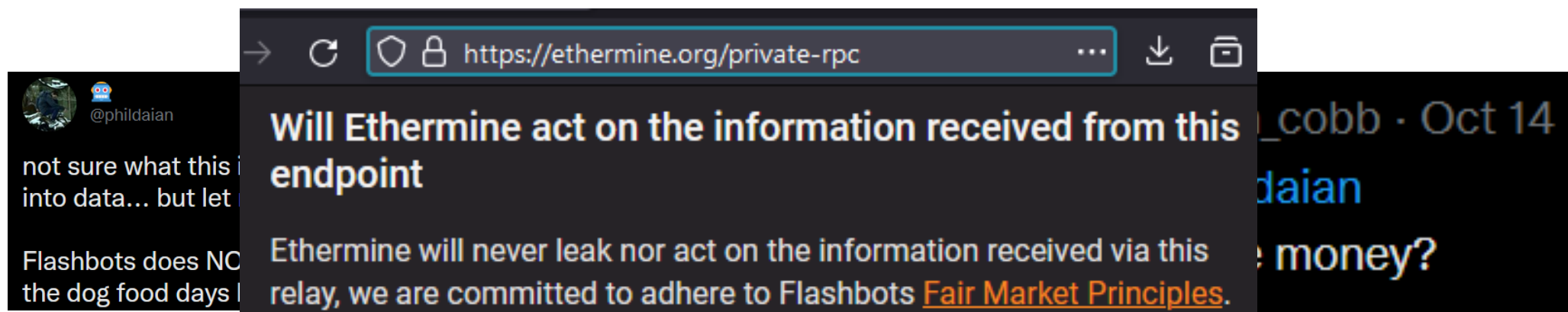
# Arbitrage Suboptimality

- Average: 2.91 ETH/day
- Total: 4.6 Million USD
- Largest cases
  - 428 ETH, ~517K USD, 94% improvement
  - 170 ETH, ~694K USD, 770% improvement
- Suboptimality is reasonable
  - Action space is huge
  - Tooling is mediocre
- The data is hiding a few other secrets!



# Private Orderflow?

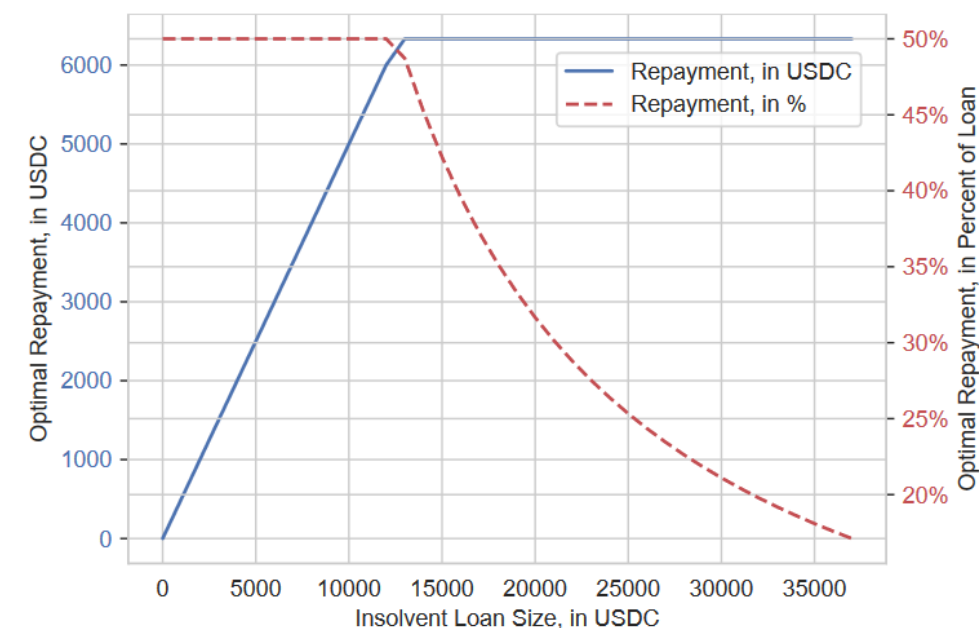
- Some builders let users send TXs in private, for free
- Ethermine: “never leak nor act on the information received via this relay”
  - Arbitrageur 0x584... appears only in Ethermine’s blocks
  - 0x584... & Ethermine’s relay started & stopped working at ~ the same time
  - Some TXs are in suboptimal TX sequences that include private orderflow



# Part III: Liquidation Suboptimality

- Repay bad collateralized debt, get collateral at a discount
- Get initial funds via flashswaps (or flashloan & swap)
- Swaps affect exchange-rates (“slippage”)
- Disincentivizes large liquidations!

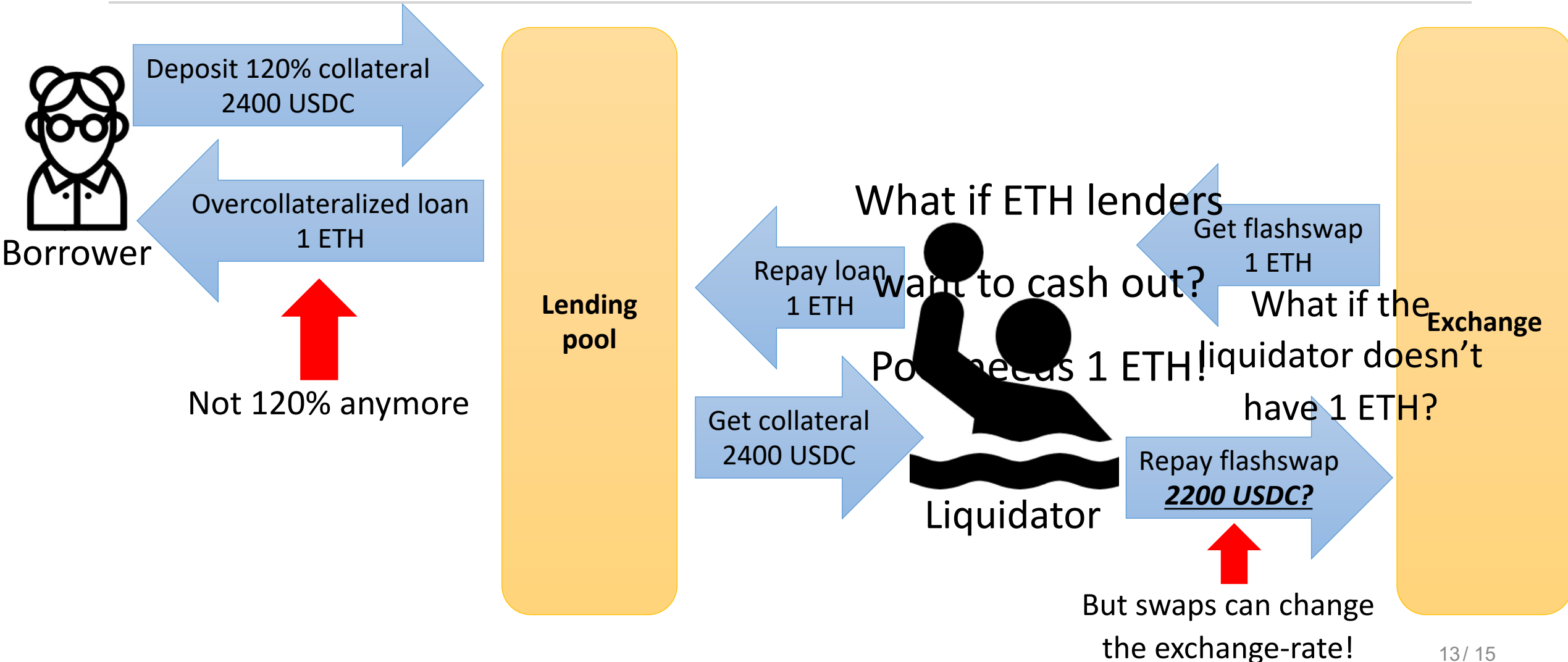
**Theorem 5.1 (Optimal liquidation).** Consider a debt position that is available for liquidation, where the debt is in cryptocurrency  $\mathcal{D}$ , and is collateralized by funds in cryptocurrency  $\mathcal{C}$ . If a user wishes to perform the liquidation using a swap obtained from a CPAMM with  $x_c$  of  $\mathcal{C}$  and  $x_d$  of  $\mathcal{D}$  reserved, then the optimal amount to repay is:  $\varrho^* = \min \left( \kappa \cdot \delta, \frac{\sqrt{p_{liq} \cdot x_c \cdot x_d} - x_c}{p_{liq}} \right)$ .



# Part III: Liquidation Suboptimality

2000 USDC ~~≠~~ 1 ETH

2200 USDC = 1 ETH



# Conclusions

---

- DeFi users behave suboptimally
  - Lack of tools, awareness → inefficient market
  - Full paper has more details, case studies
- Future work
  - Better interest rate mechanisms
  - Long-term lending

Thank you!  
Questions?