# Allocative Inefficiencies in Public Blockchains, MEV, and Private Transactions

Ye Wang

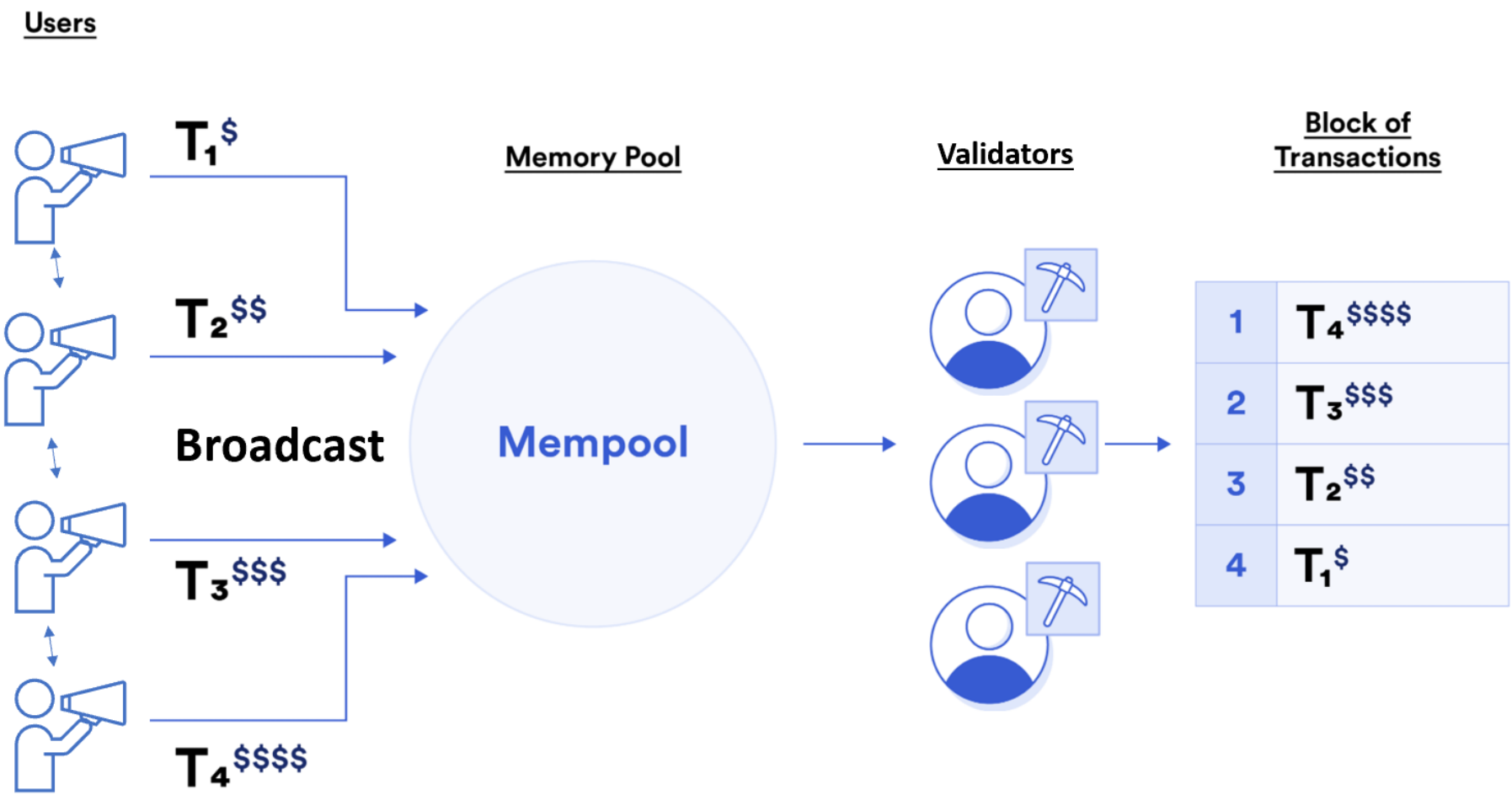
University of Macau

Web3 Young Scholars Program

joint work with Agostino Capponi (Columbia)
and Ruizhe Jia (Columbia)

# Outline

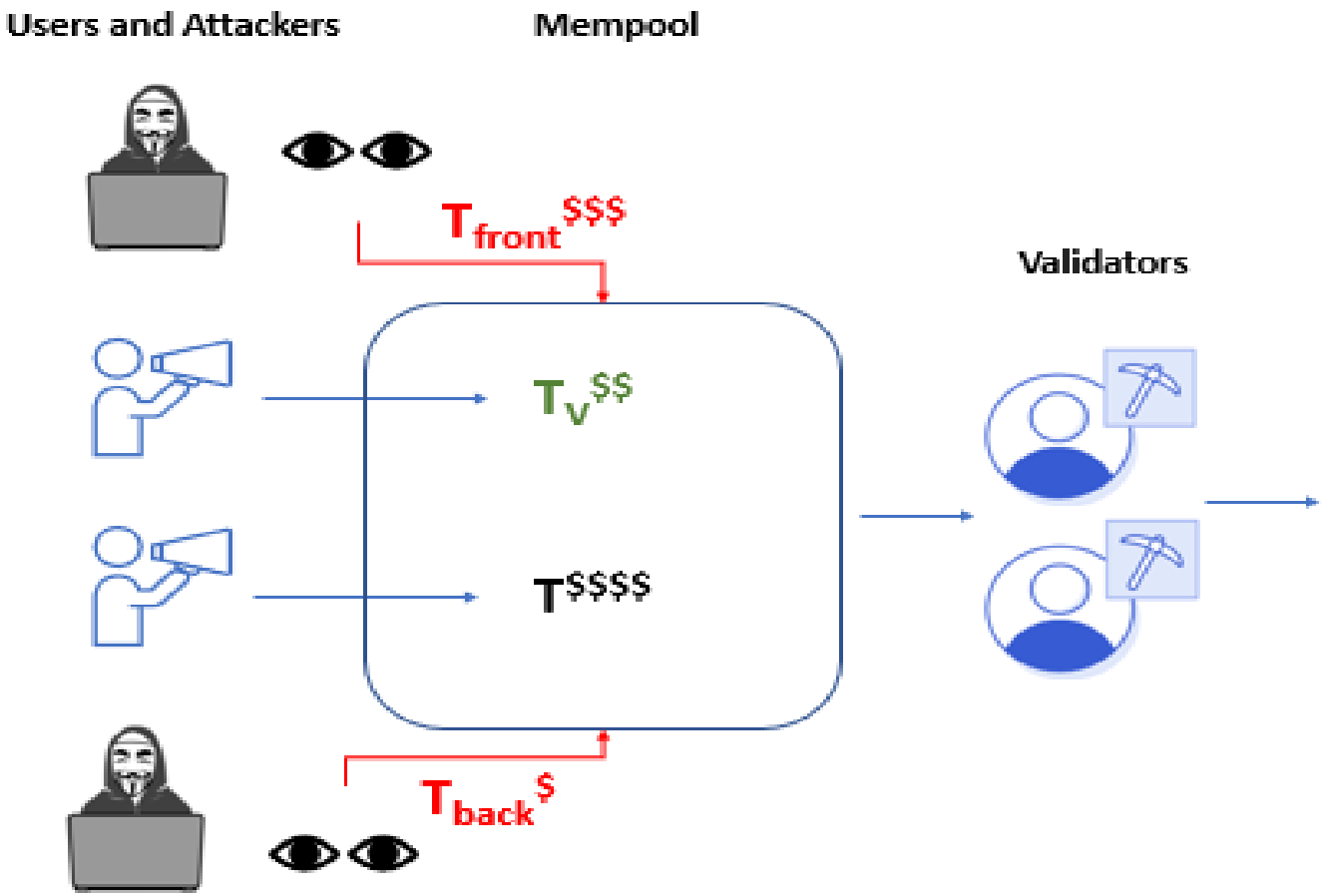
# Blockchain Architecture



# Frontrunning Attacks

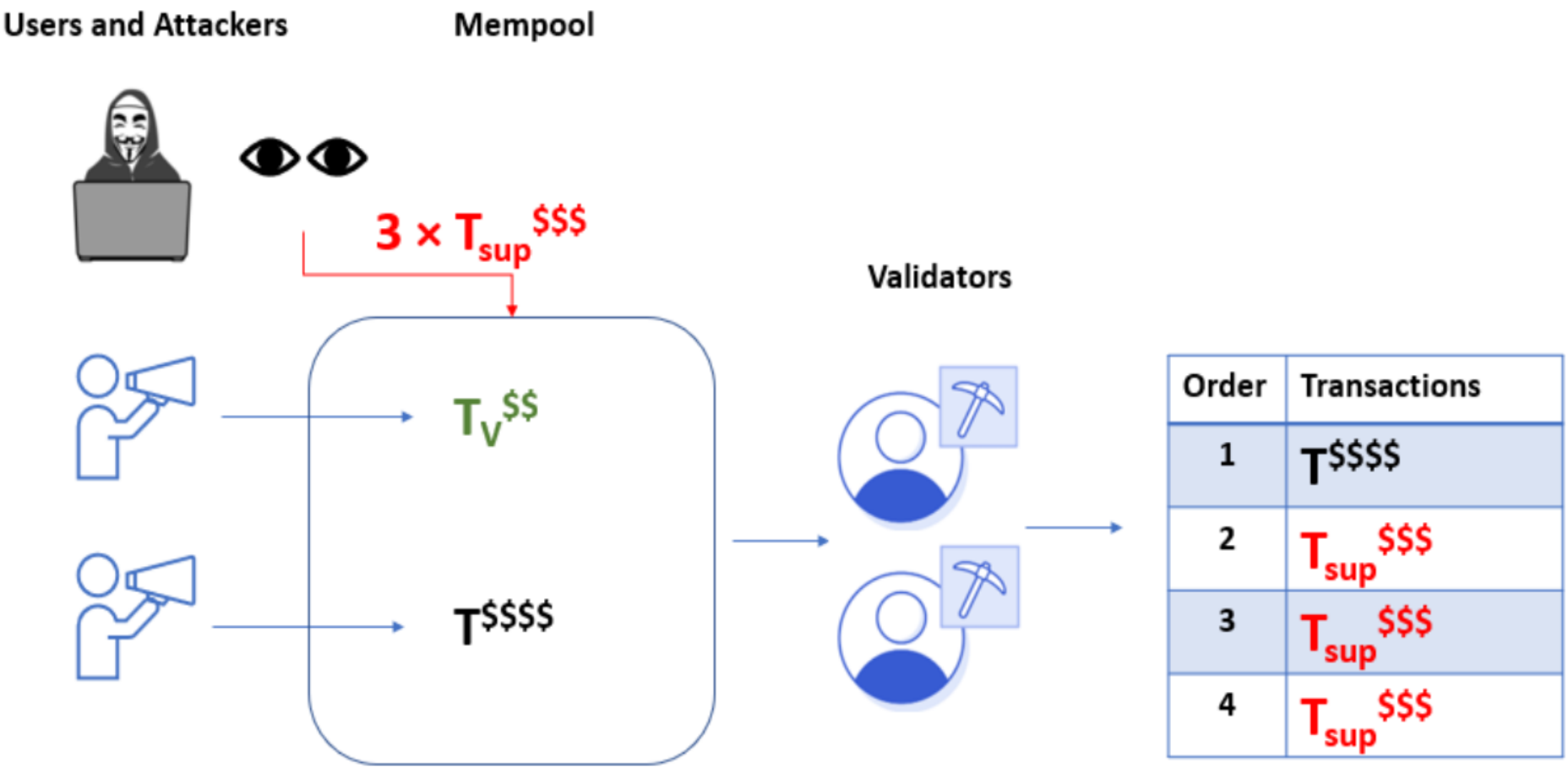
- Transparency can have unintended consequences
- Information on settled and pending transactions can be exploited by malicious attackers
- Pending transactions are revealed in the mempool before settlement, which leads to **frontrunning** attacks

# Sandwich Attack



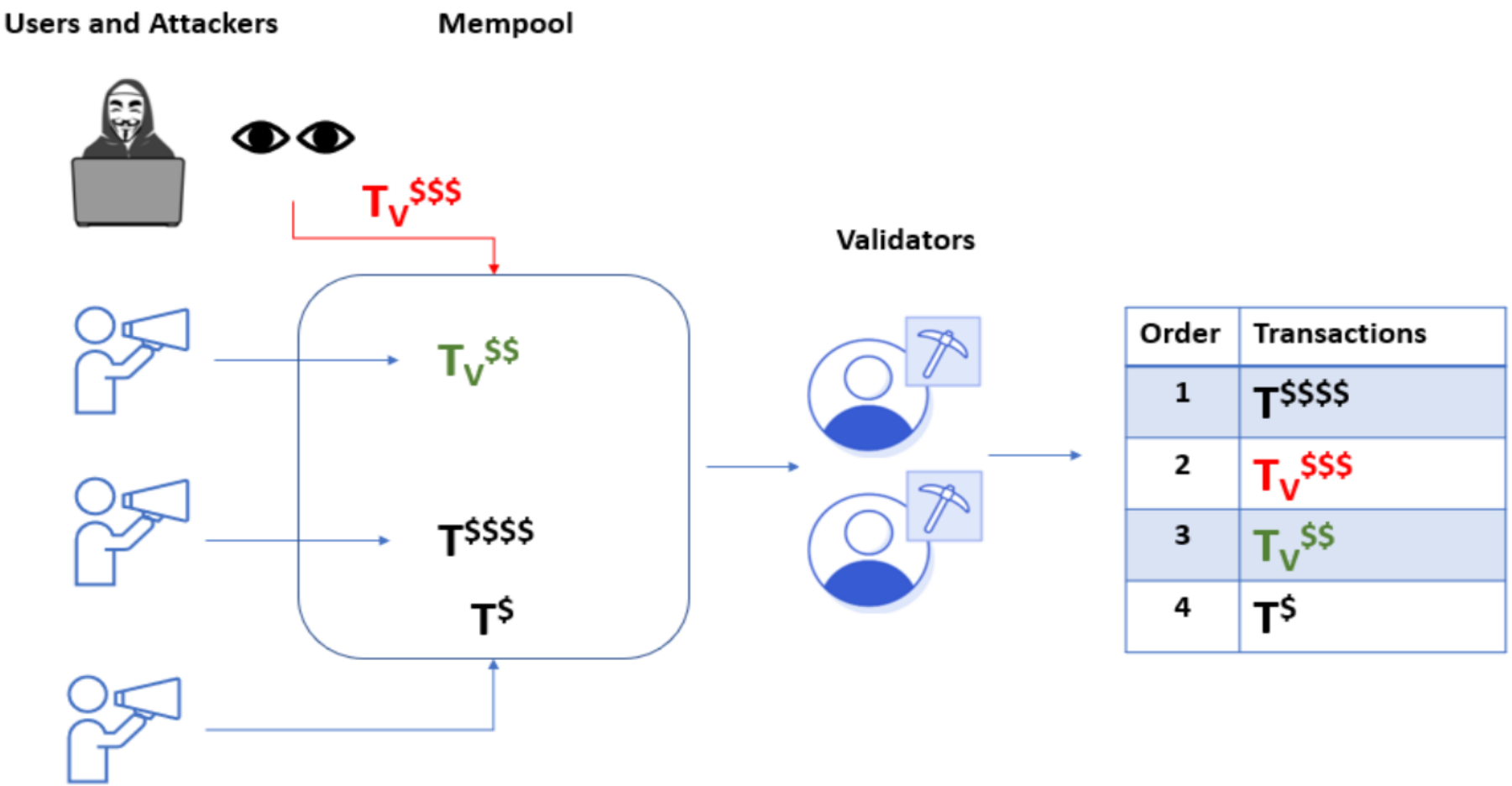

| Order | Transactions |
|---|---|
| 1 | $T^{\$\$\$\$}$ |
| 2 | $T_{front}^{\$\$\$}$ |
| 3 | $T_V^{\$\$}$ |
| 4 | $T_{back}^{\$}$ |

# Suppression Attack



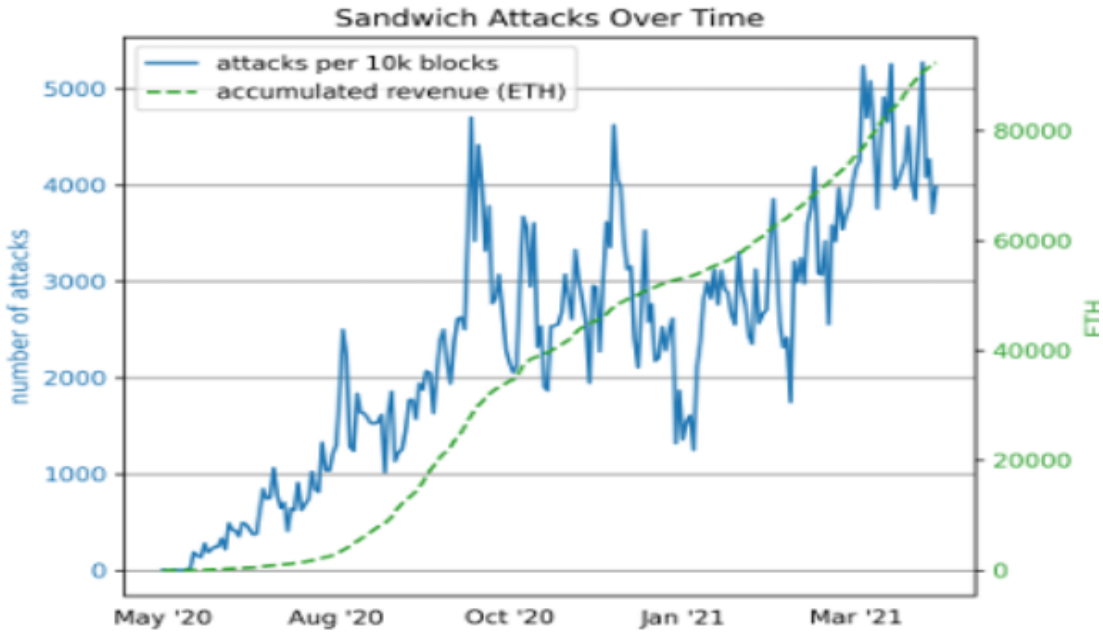

| Order | Transactions |
|---|---|
| 1 | $T^{\$\$\$\$}$ |
| 2 | $T_{sup}^{\$\$\$}$ |
| 3 | $T_{sup}^{\$\$\$}$ |
| 4 | $T_{sup}^{\$\$\$}$ |

# Displacement Attack




| Order | Transactions |
|---|---|
| 1 | $T^{\$\$\$\$}$ |
| 2 | $T_V^{\$\$\$}$ |
| 3 | $T_V^{\$\$}$ |
| 4 | $T^{\$}$ |

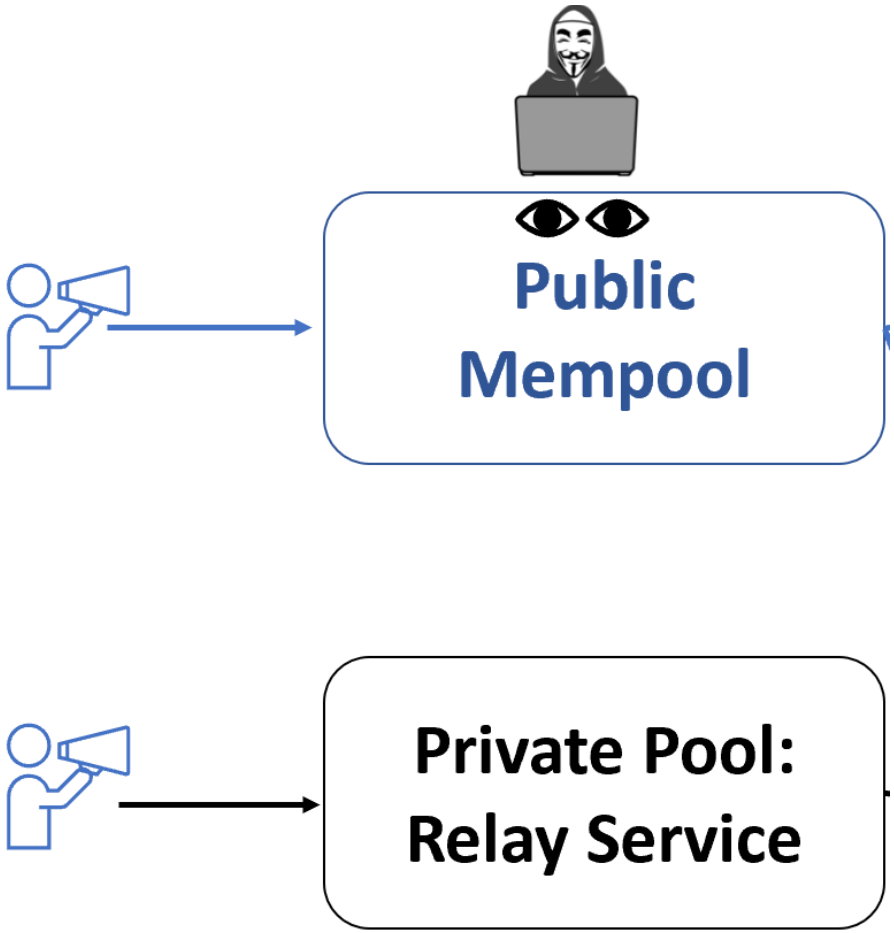
# Is Frontrunning Risk Material?




- **Direct loss for victims:** about 80,000 ETH wealth transfer from victims to attackers and validators.
- **Indirect costs:** allocative inefficiency, higher blockchain congestion and increased priority fees

# Public vs Private Pools

- Flashbots are **private** off-chain channels:
- Goal: reduce frontrunning by arbitrage bots and transaction fee surges



# Research Questions

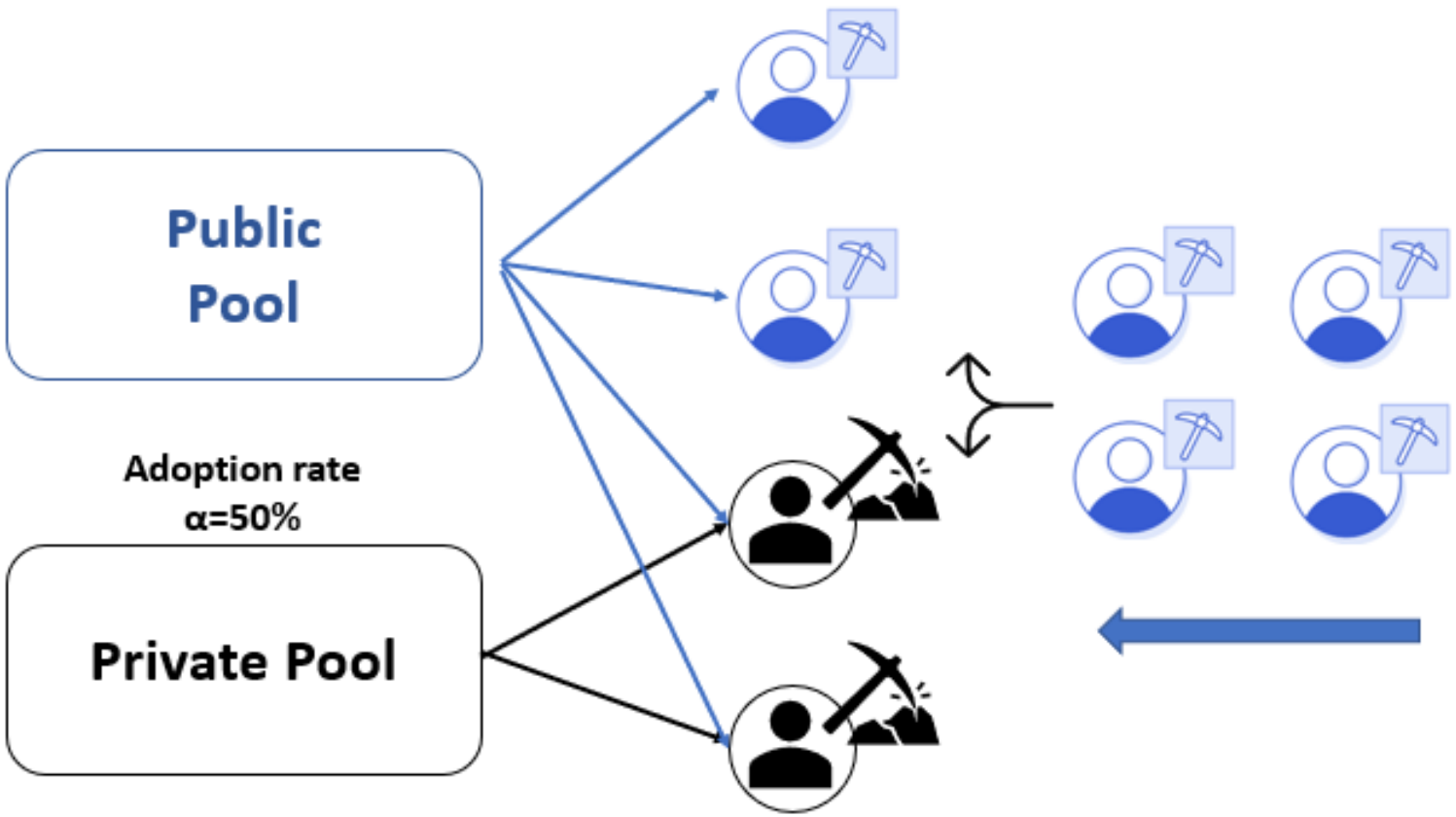
- **Adoption:** Will the private pool be adopted by users and validators?
- **Mitigation of Frontrunning:** If adopted, will it achieve the intended purpose of reducing frontrunning risk and priority fees?
- **Welfare:** Is the introduction of a private pool welfare enhancing?

# Model Setup

- 3 periods indexed by $t$, $t = 1, 2, 3$.
- 3 types of agents:
  - $N$ homogeneous and rational validators
  - A frontrunnable user and a discrete set of non-frontrunnable users who earn private values from transacting on blockchain
  - Two attackers
- Two transaction submission venues: private pool and public pool
- Each block has capacity $B$

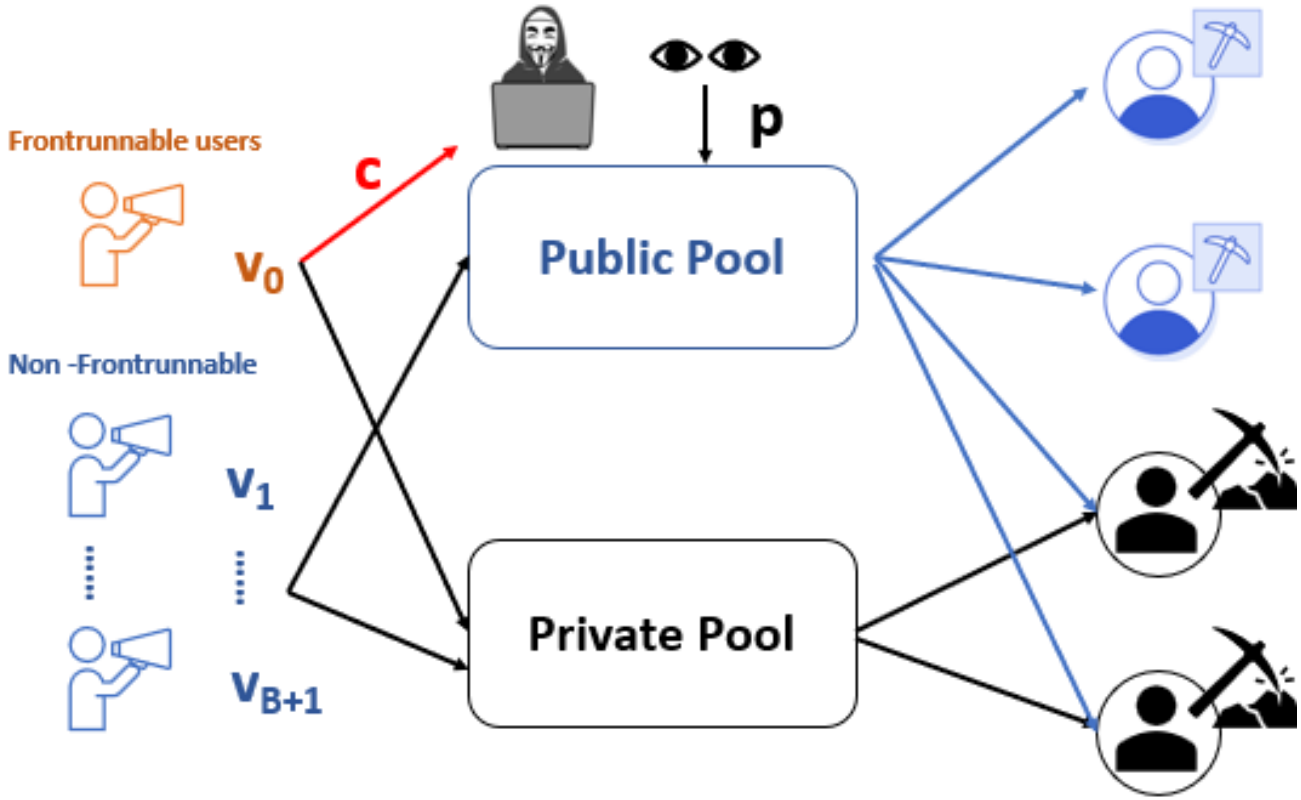
# Period $t = 1$

- Validators decide whether to monitor the private pool, in addition to the public pool. Let $\alpha$ be the fraction which monitors private pool

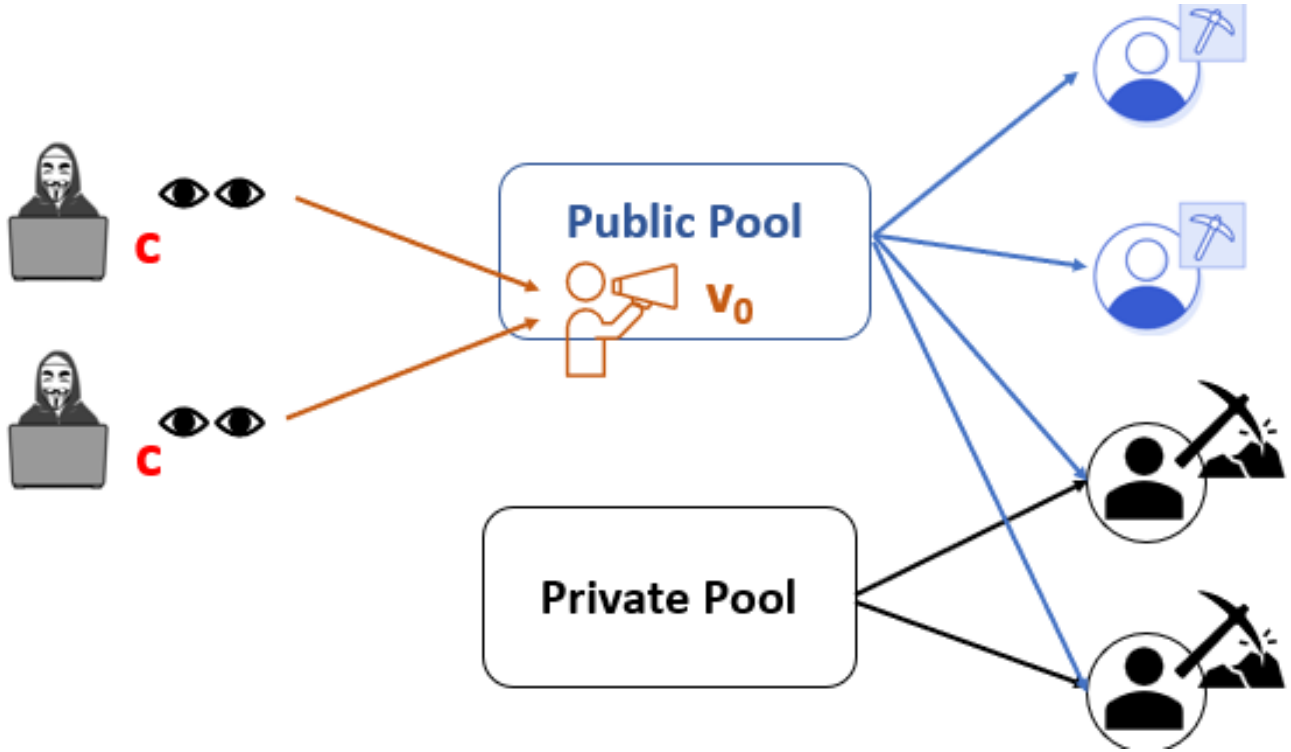


# Period $t = 2$

- Users bid the priority fee and choose the submission venue
- Users have exogenous valuation for their transactions:
  $v_0 > v_1 > \cdots > v_B$
- The frontrunnable user loses $c > 0$ if his transaction is frontrun

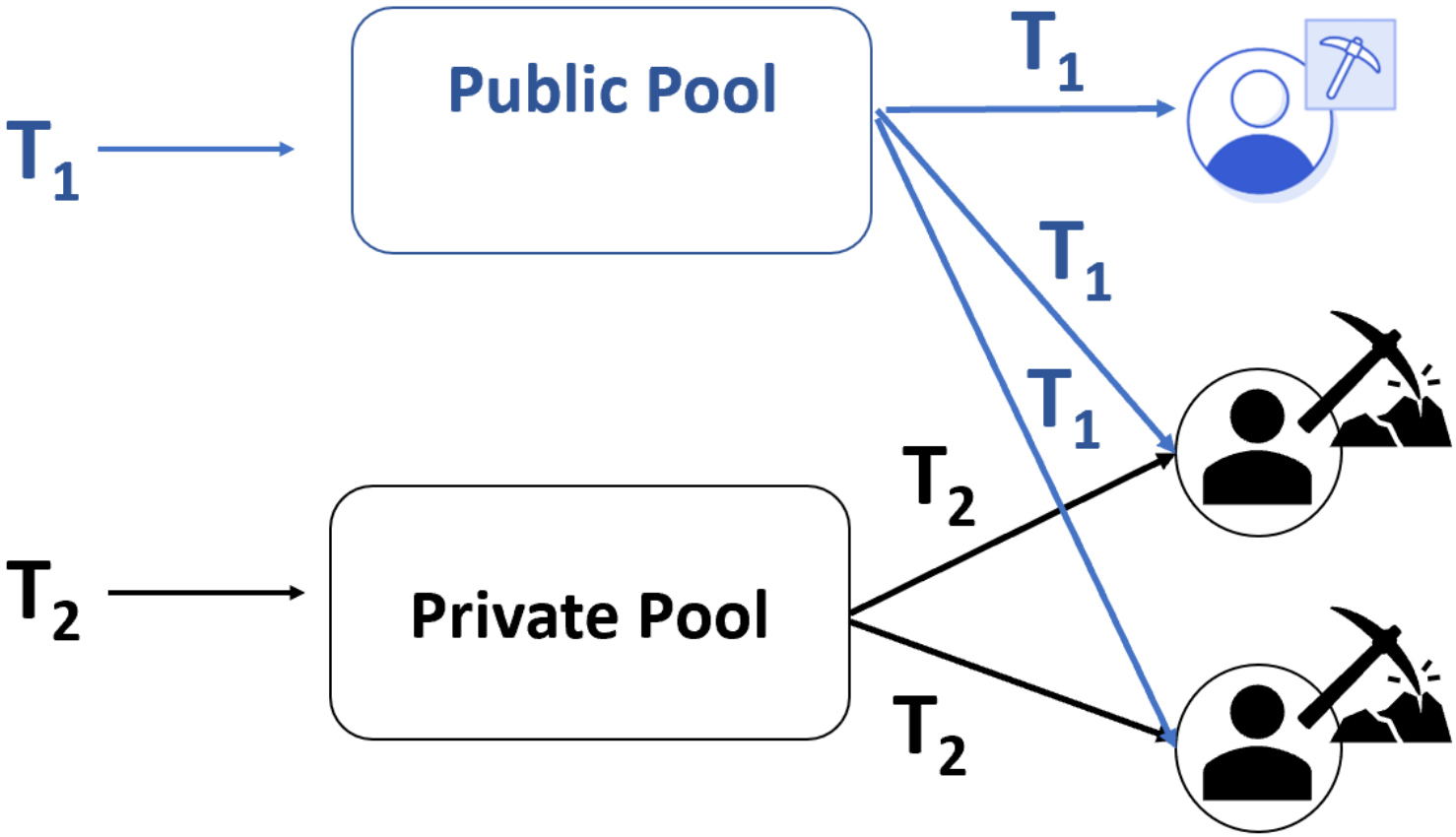


# Period $t = 3$

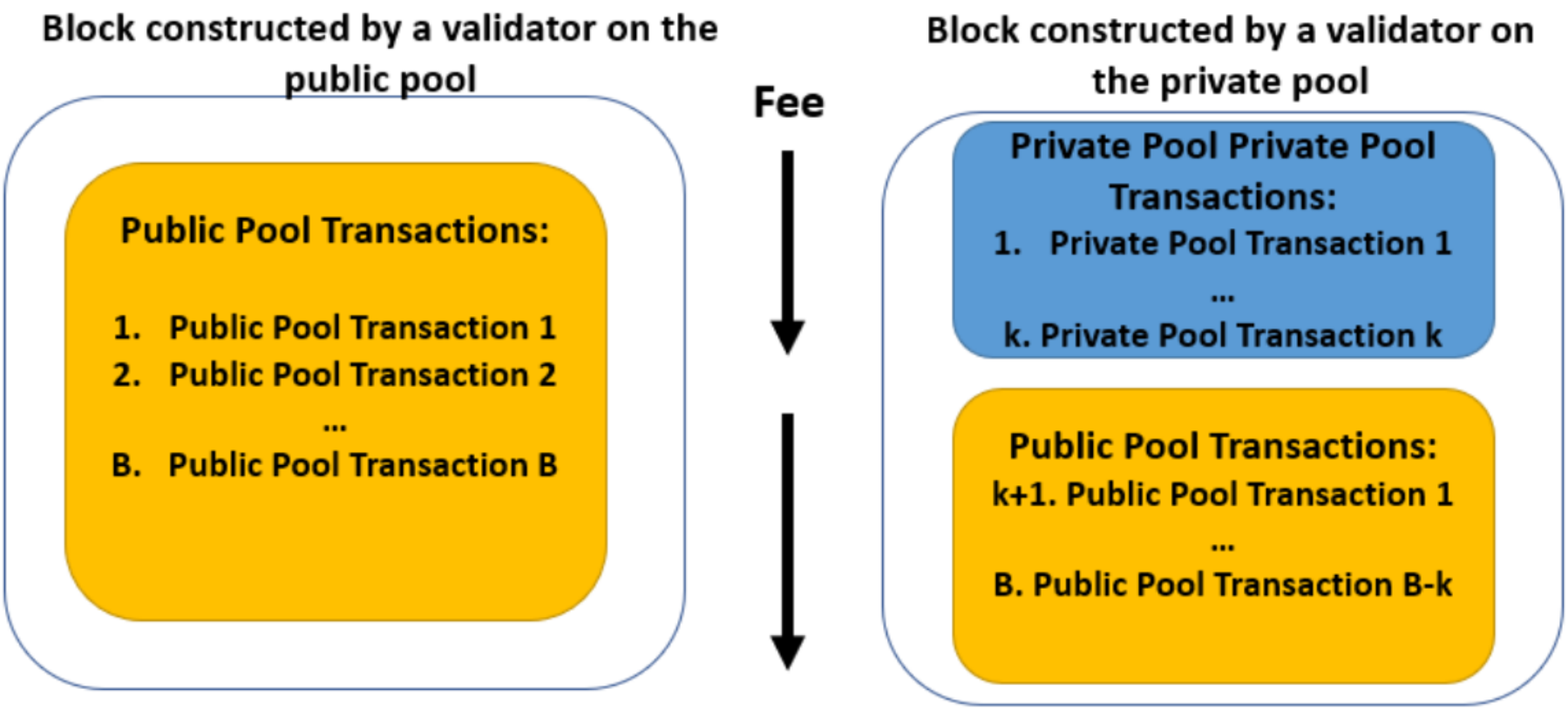



- Attackers create a frontrunning order, bid a fee and decide which venue to use: public pool, private pool, or both.
- The attacker who executes the order first earns a profit $c \geq 0$.

# Execution Risk in the Private Pool



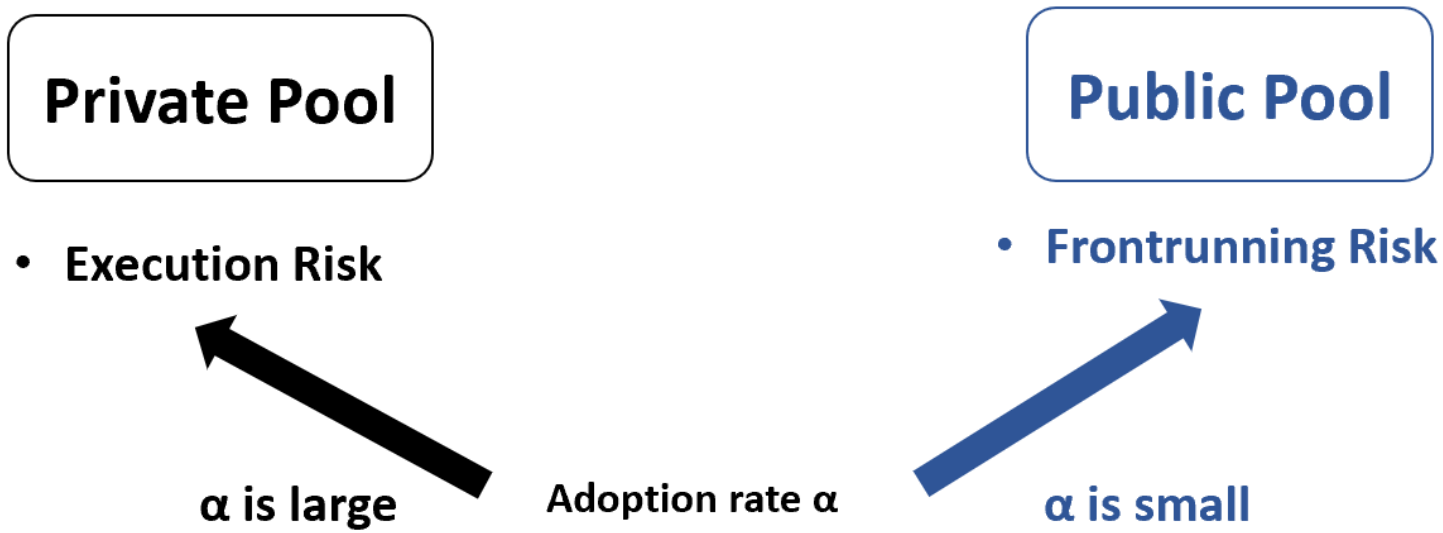
# Execution Priority



# Attackers' Choice of Submission Venue

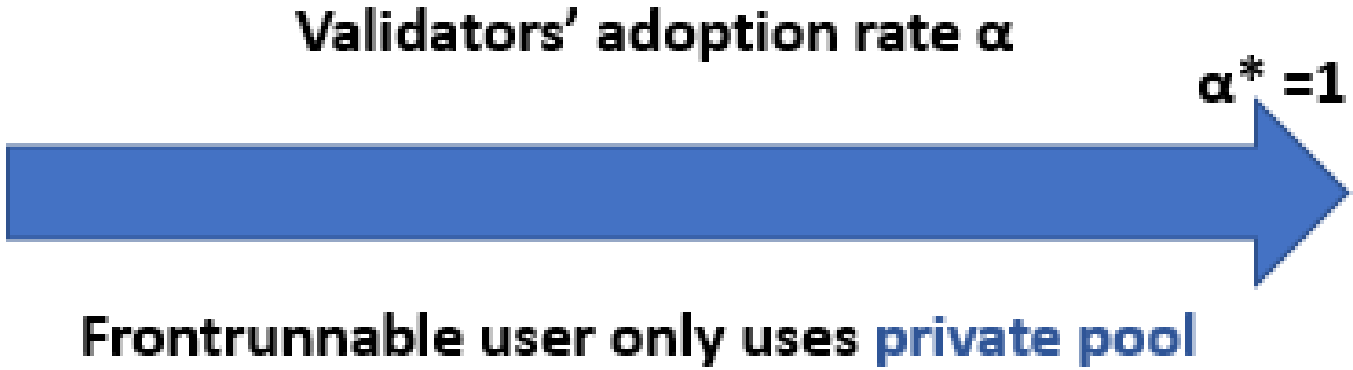
- Attackers engage in an "arm race" for priority order execution
- **Prioritized execution:** transactions submitted through private pool placed at the top of the block by validators who monitor this pool.
- However, using the private pool alone presents **execution risk**
- Attackers adopt the private pool in addition to the public pool.

# Tradeoff Faced by Frontrunnable User



# Equilibrium if Frontrunning Risk is High

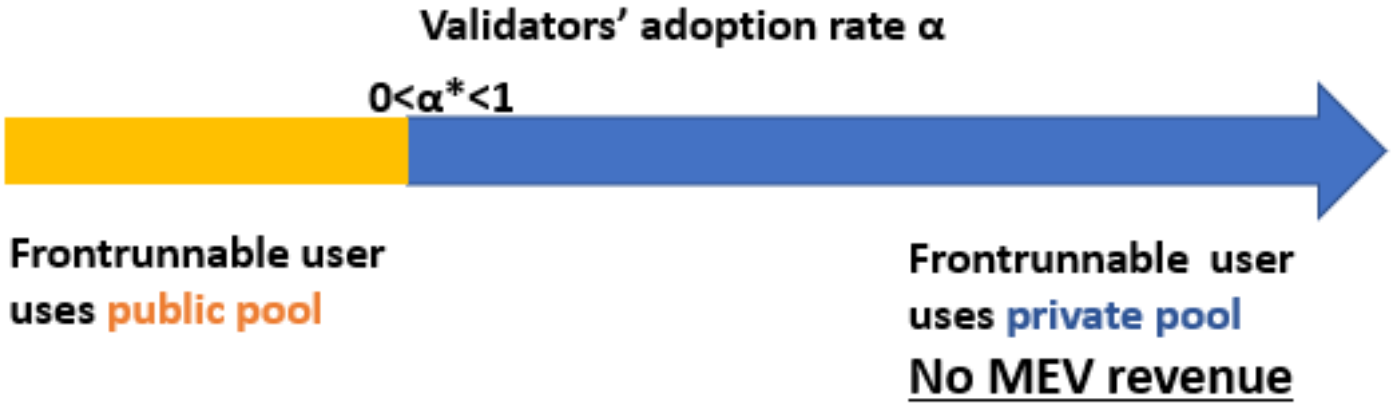
- **If $c$ is large:**




1. The frontrunnable user only submits his transaction to the private pool.
2. All validators join the private pool to observe the transaction of frontrunnable user.
3. **Frontrunning risk is eliminated**

# Equilibrium if Frontrunning Risk is Low

- **If $c$ is small:**




1. Without a private pool, the frontrunnable user submits to public pool
2. Why not $\alpha^* = 1$?
   - Frontrunning attacks generate fees for validators.
3. Why not $\alpha^* = 0$?
   - Attackers compete on fees on private pool to frontrun
4. The frontrunnable user prefers to submit through the public pool and face frontrunning risk.
5. **A private pool does not eliminate frontrunning.**

# Are Priority Fees Reduced?

- If a private pool weakly reduces the block space used by attackers, shouldn't we expect a decline in priority fees? Not quite
  1. Validators adopt the private pool only if they earn higher priority fees, and thus the equilibrium priority fees increase.
  2. With a private pool, the frontrunnable user may submit a transaction which would not have submitted otherwise.
- The private pool option leads to an **increases in the minimum fee** which guarantees execution!

# Aggregate Welfare and Blockspace Allocation

- Aggregate welfare = the sum of ex-ante payoff of all agents = **the sum of valuations of transactions on blockchain**
- Two root causes of inefficiencies in block-space allocation:
  - User does not submit because of high frontrunning risk
  - Blockspace taken up by frontrunning transactions, which are just wealth transfers

$v_0 > v_1 > \ldots > v_3$

**Efficient Allocation**

| Order | Transactions |
|---|---|
| 1 | $v_0$ |
| 2 | $v_1$ |
| 3 | $v_2$ |

$v_0 + v_1 + v_2$

**Inefficiency 1**

| Order | Transactions |
|---|---|
| 1 | $v_1$ |
| 2 | $v_2$ |
| 3 | $v_3$ |

$v_1 + v_2 + v_3$

**Inefficiency 2**

| Order | Transactions |
|---|---|
| 1 | $c$ |
| 2 | $v_0 - c$ |
| 3 | $v_1$ |

$v_0 + v_1$

# Aggregate Welfare

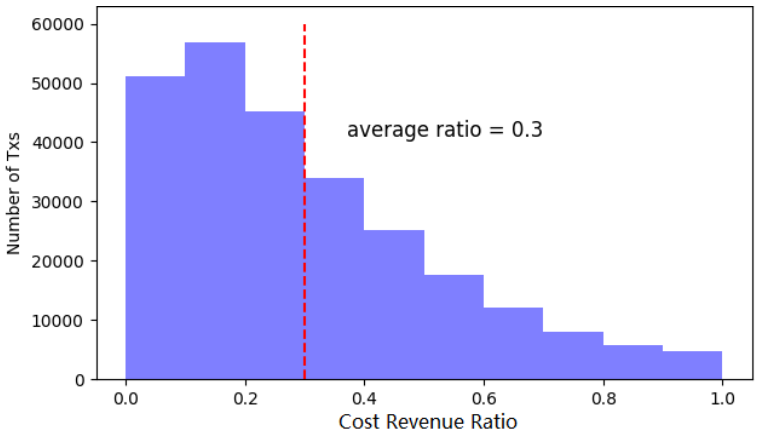
- Aggregate welfare maximized if all validators adopt the private pool $\rightarrow$ no social waste from blockspace misallocation.
- However, the social optimum is *not* always attainable
  - **Miner extractable value (MEV):** Validators want to preserve fees from arbitrageurs' competition

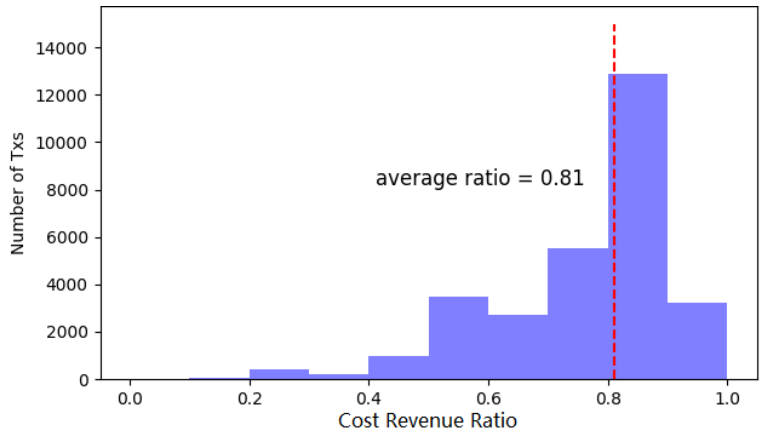
# "Hold-up" problem

- Sellers under-invest (validators do not fully adopt) in the first stage, despite it being socially optimal
- This is because the gains from the investment (adoption) are appropriated by the buyers (frontrunnable users).
- How to solve misalignment of incentives between validators and frontrunnable user:
  - Validators are willing to adopt the private pool if frontrunnable users made a credible commitment to pay

# Testable Implications

- Private pool will be at least partially adopted by validators
- Frontrunnable user chooses private pool if and only if frontrunning risk is high
- Attackers' welfare decreases with a private pool due to intensified arms race.



# Frontrunning Risk and Private Pool Usage

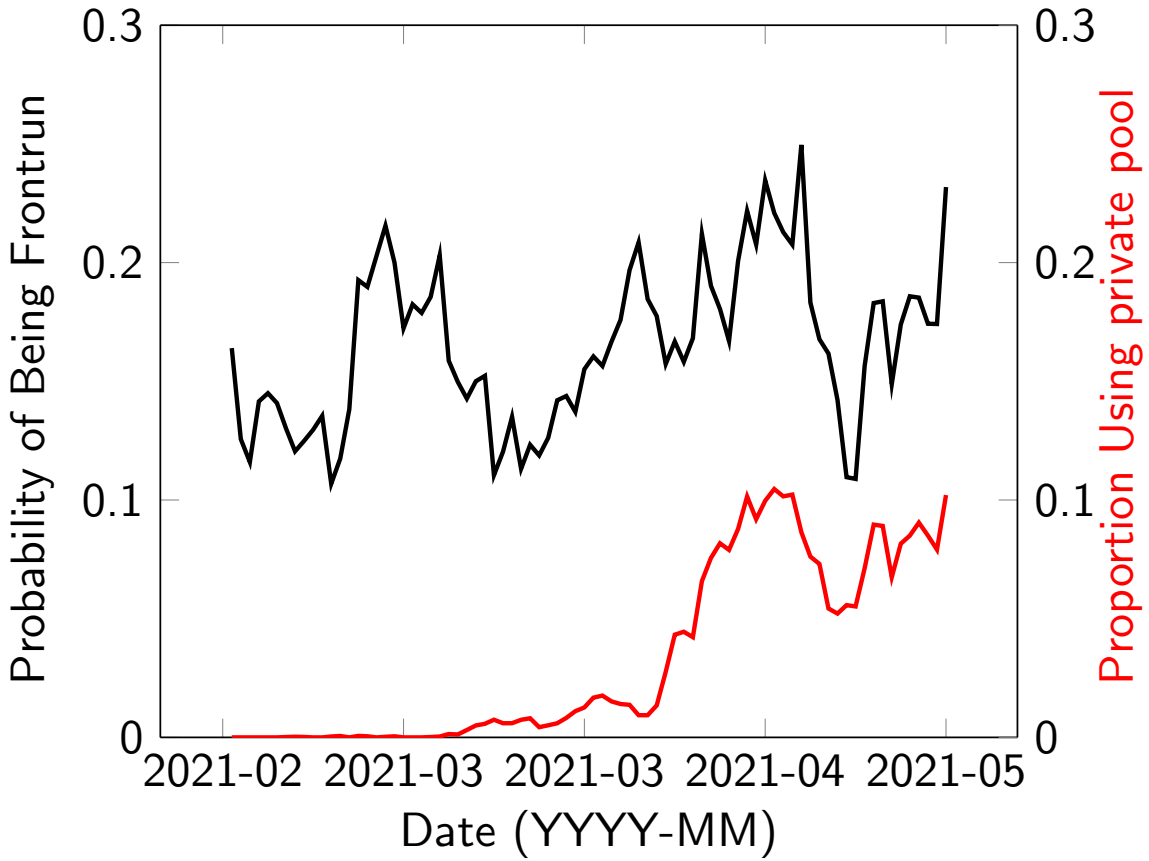



Figure: The black line represents the daily average probability of being frontrun. The red line represents the daily proportion of frontrunnable transactions submitted to private pool.

# Conclusion

- **Mitigation of Frontrunning:** private pool neither eliminates frontrunning risk nor reduces execution fees.
- Welfare Implications of a private pool:
  - Frontrunnable user : $\uparrow$
  - Welfare of Validators: $\uparrow$
  - Welfare of attackers: $\downarrow$
  - Aggregate welfare: higher due to more efficient blockspace allocation, but not necessarily the social optimum

*Thank You!*

# Individual Welfare

- The introduction of a private pool:
  - increases welfare of validators,
  - reduces welfare of attackers
  - increases expected payoff of the frontrunnable user (gains access to private pool),
  - and decreases expected payoff of non-frontrunnable users (higher transaction cost) $i, i = 1, ..., B - 2$

# Adoption rate of the private pool (Flashbots).

Estimated Adoption Rate = Blocks mined with Flashbots Relay/ Total Blocks mined

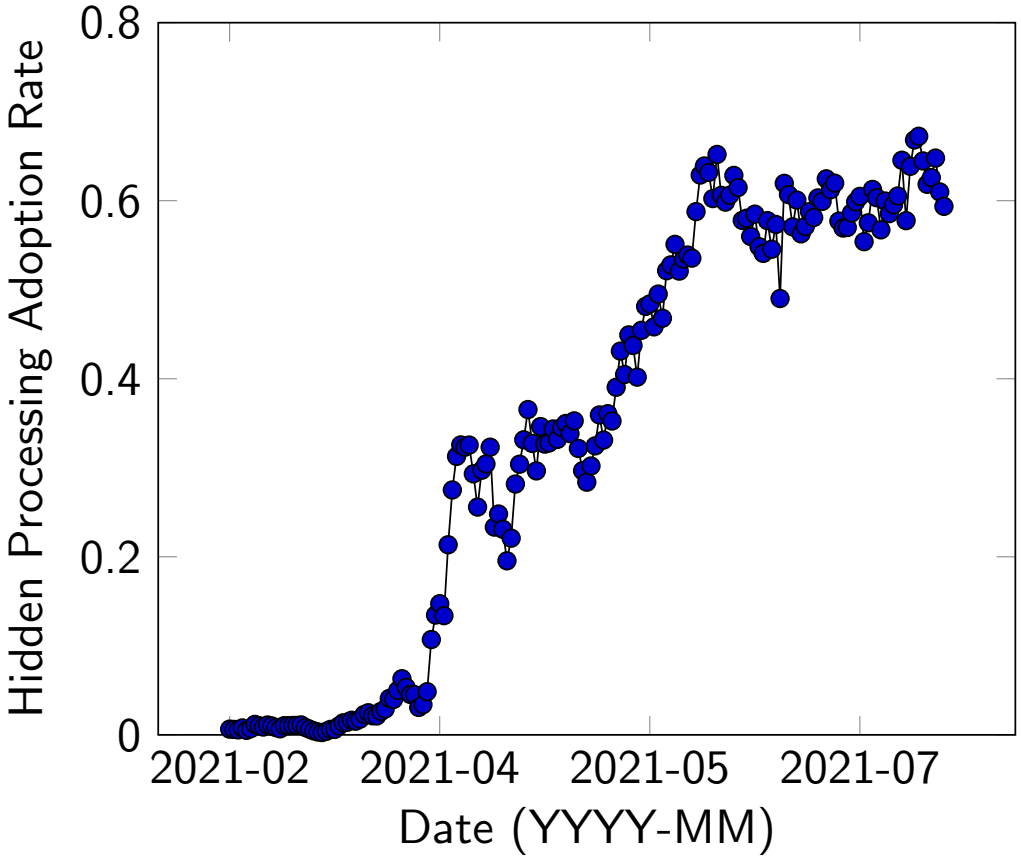
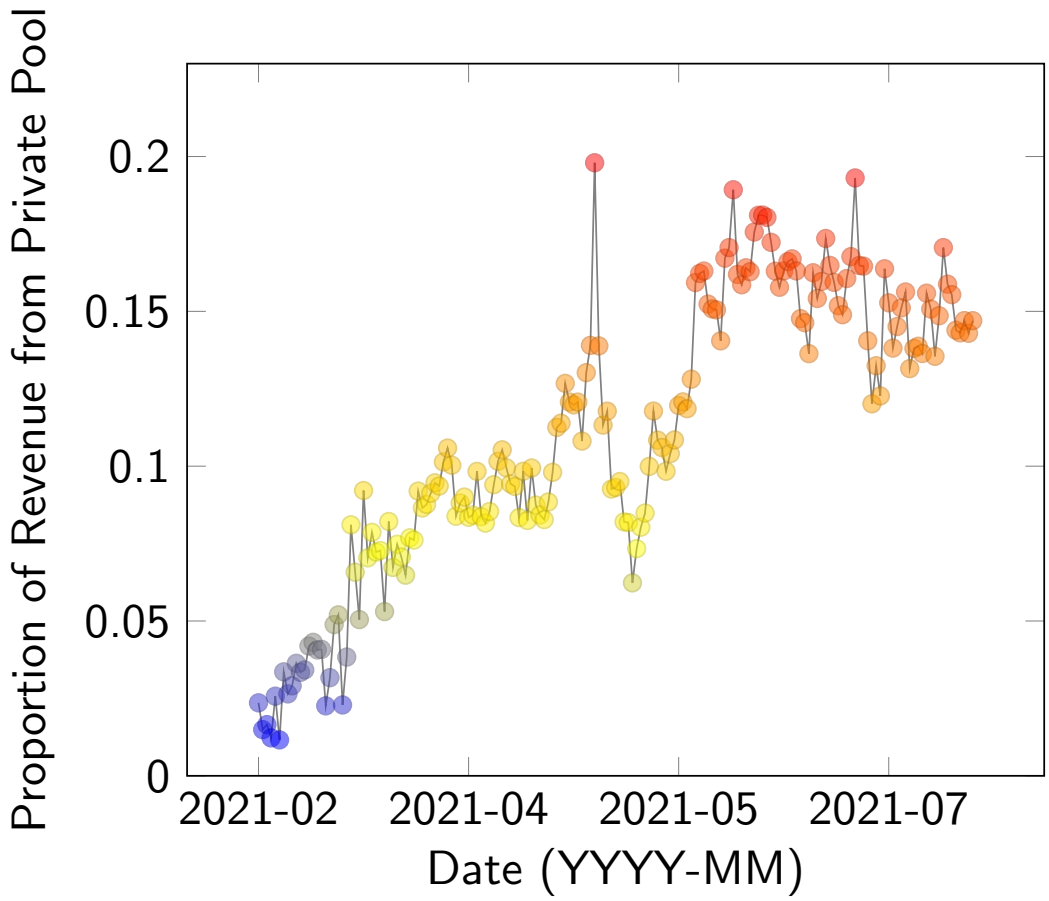



Figure: Adoption rate of Flashbots.

# Proportion of Flashbots Validators' Revenue from Private Pool.



# Validators' Revenue in Dark and public pools.

Expected payoff of validators in the private pool are higher (around 0.16 ETH per block) than the expected payoff of validators in the public pool.

| | *Dependent variables: Validators' Revenue per Block* |
|---|---|
| Intercept | $1.21^{***}$ |
| | (0.06) |
| Dark | $0.16^{***}$ |
| | (0.032) |
| Day fixed effects? | yes |
| Observations | 1,762,017 |
| $R^2$ | 0.02 |
| *Note:* | $^{*}$p<0.1; $^{**}$p<0.05; $^{***}$p<0.01 |

# Users' Migration

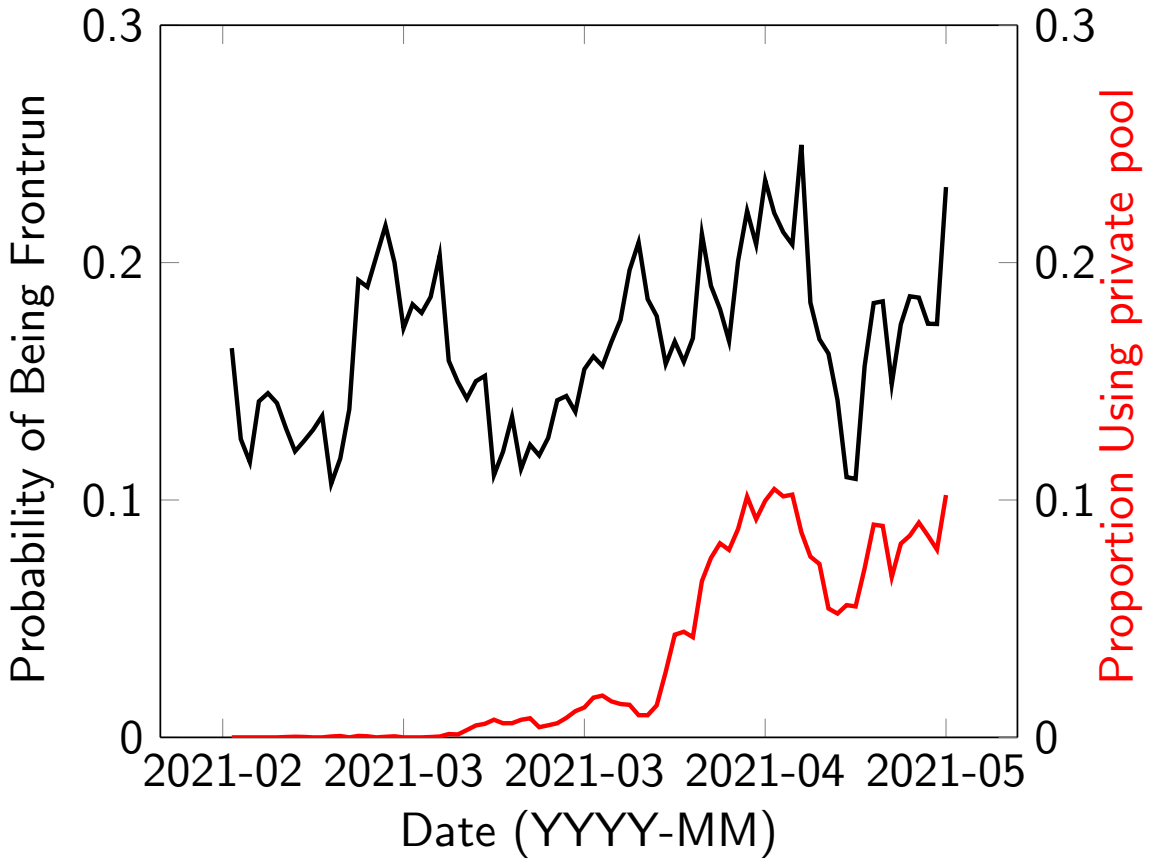



Figure: The black line represents the daily average probability of being attacked for frontrunnable users. The red line represents the daily proportion of frontrunnable transactions sent to private pool.

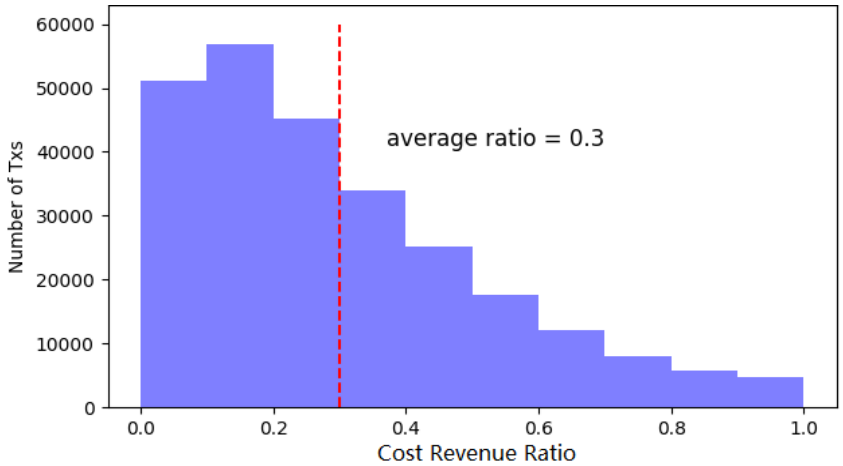
# Users' Migration

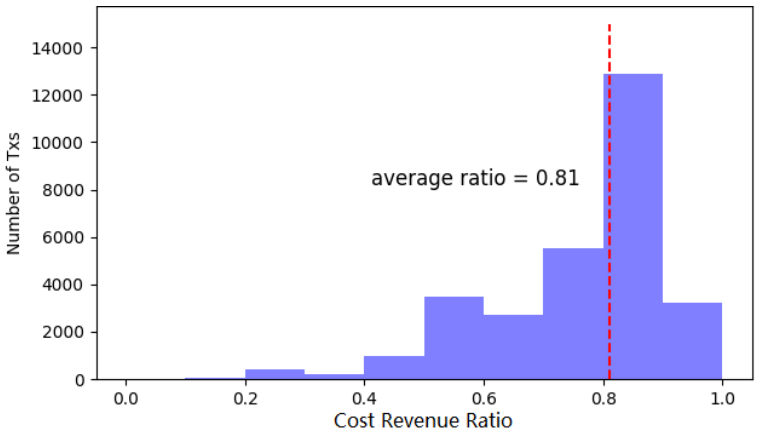
A 1% increase in probability of being frontrun is associated with a 0.6% increase in the proportion of frontrunnable transactions submitted through the private pool.

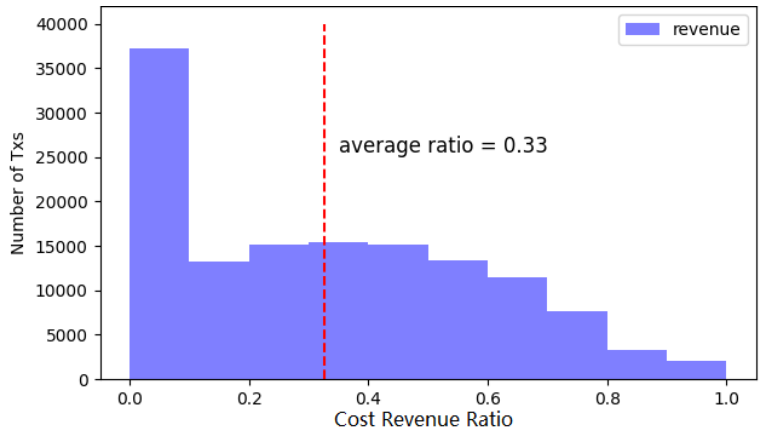
| | *Dependent variables:* *Proportion of Transactions Through Dark* |
|---|---|
| Intercept | -0.066 |
| | (0.18) |
| Probability of Being Frontrun | 0.605*** |
| | (0.010) |
| Observations | 80 |
| $R^2$ | 0.3 |
| *Note:* | *p<0.1; **p<0.05; ***p<0.01 |

# attackers' Welfare

Cost-to-Revenue Ratio = Gas fees paid/ Total Revenue from frontrunning



# attackers' Welfare

After the introduction of the private pool, attackers' cost increases by a third, mainly due to arbitrage transactions sent through private pool.

| | *Dependent variables: Cost-to-revenue Ratio* | |
|---|---|---|
| | (a) | (b) |
| Intercept | $0.300^{***}$ | $0.300^{***}$ |
| | (0.001) | (0.001) |
| After | $0.091^{***}$ | $0.013^{***}$ |
| | (0.001) | (0.001) |
| Private Pool | | $0.441^{***}$ |
| | | (0.002) |
| Observations | 428,685 | 428,685 |
| $R^2$ | 0.03 | 0.19 |
| *Note:* | | $^{*}$p<0.1; $^{**}$p<0.05; $^{***}$p<0.01 |

*Thank You!*

# Equilibrium

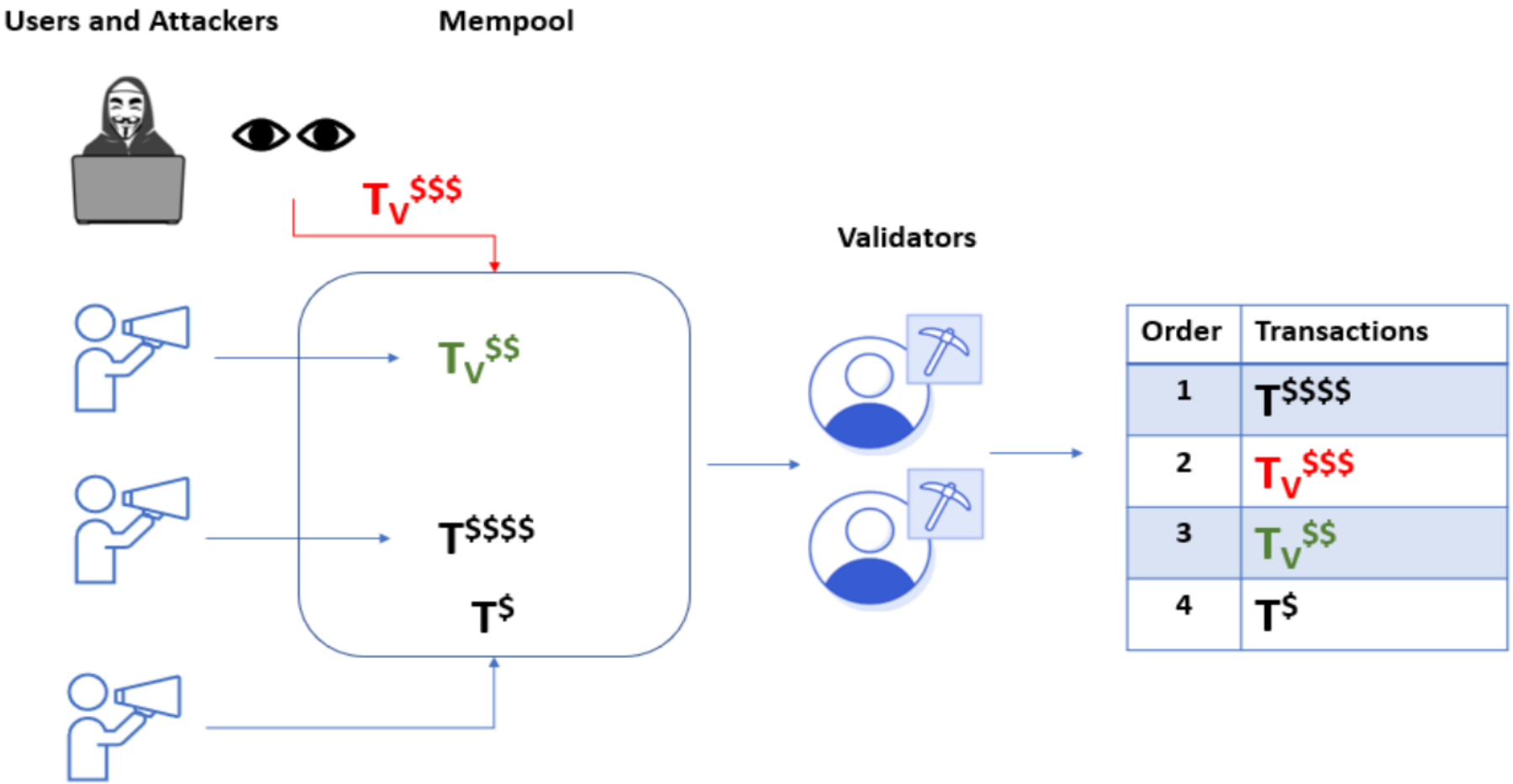
## Proposition (Subgame Perfect Equilibrium (SPE))

1. *If $c > c_1$, there exists a unique full adoption equilibrium where the adoption rate $\alpha^* = 1$, the frontrunnable user selects the private pool, and the attackers do not submit arbitrage orders.*
2. *If $c \leq c_1$, there exists a partial adoption equilibrium where the private pool's adoption rate $\alpha^* < 1$, the frontrunnable user submits her transaction through the public pool, and the attackers send their orders to the private pool only or to both venues.*

# Transaction Fees

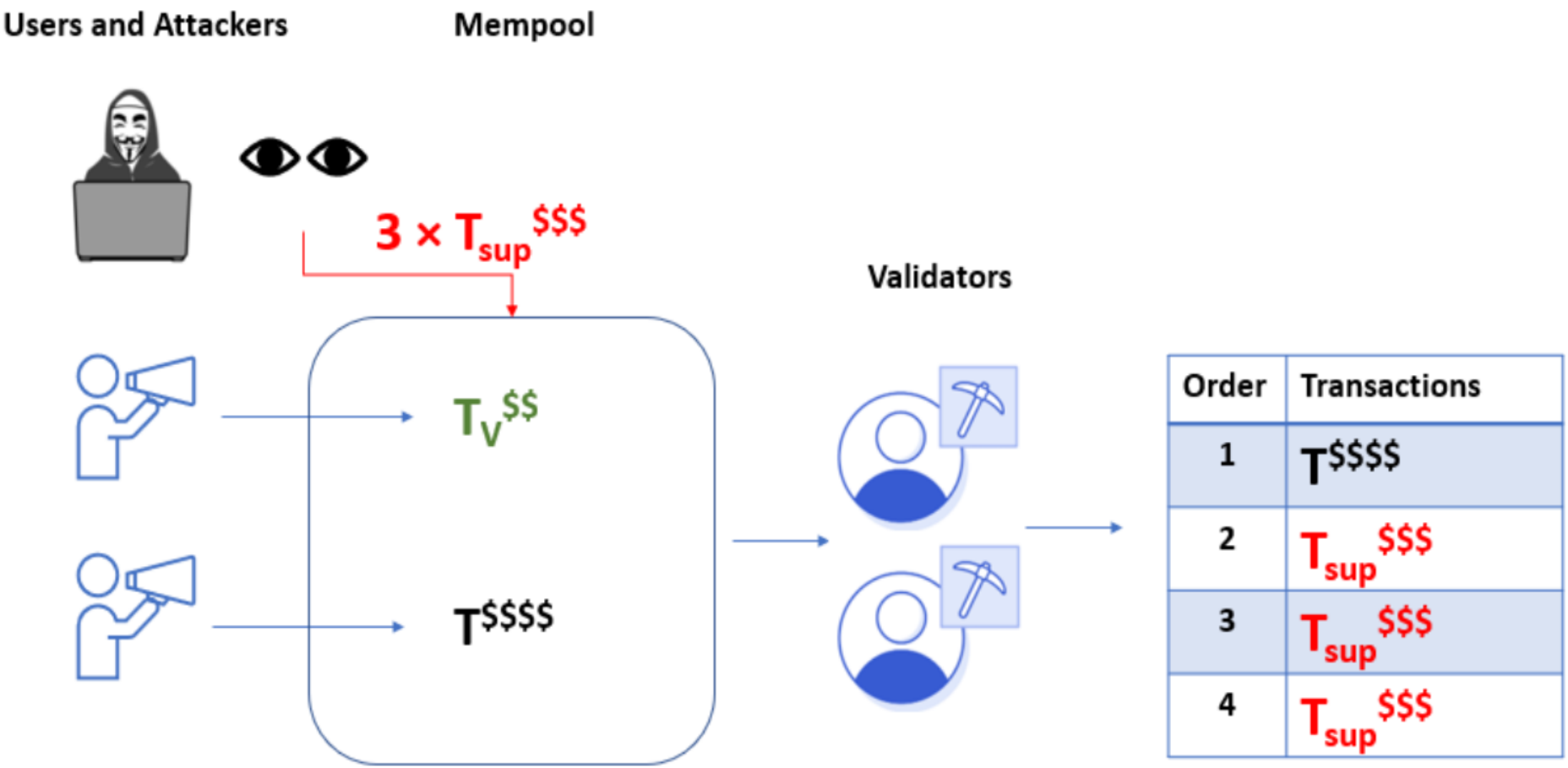
- The introduction of a private pool **increases the minimum fee** which guarantees the execution of a transaction!
  1. The introduction of the private pool may attract the frontrunnable transaction which would not have been submitted otherwise.
  2. Validators adopt the private pool if and only if they earn higher transaction fees

# Frontrunning Attack: Displacement



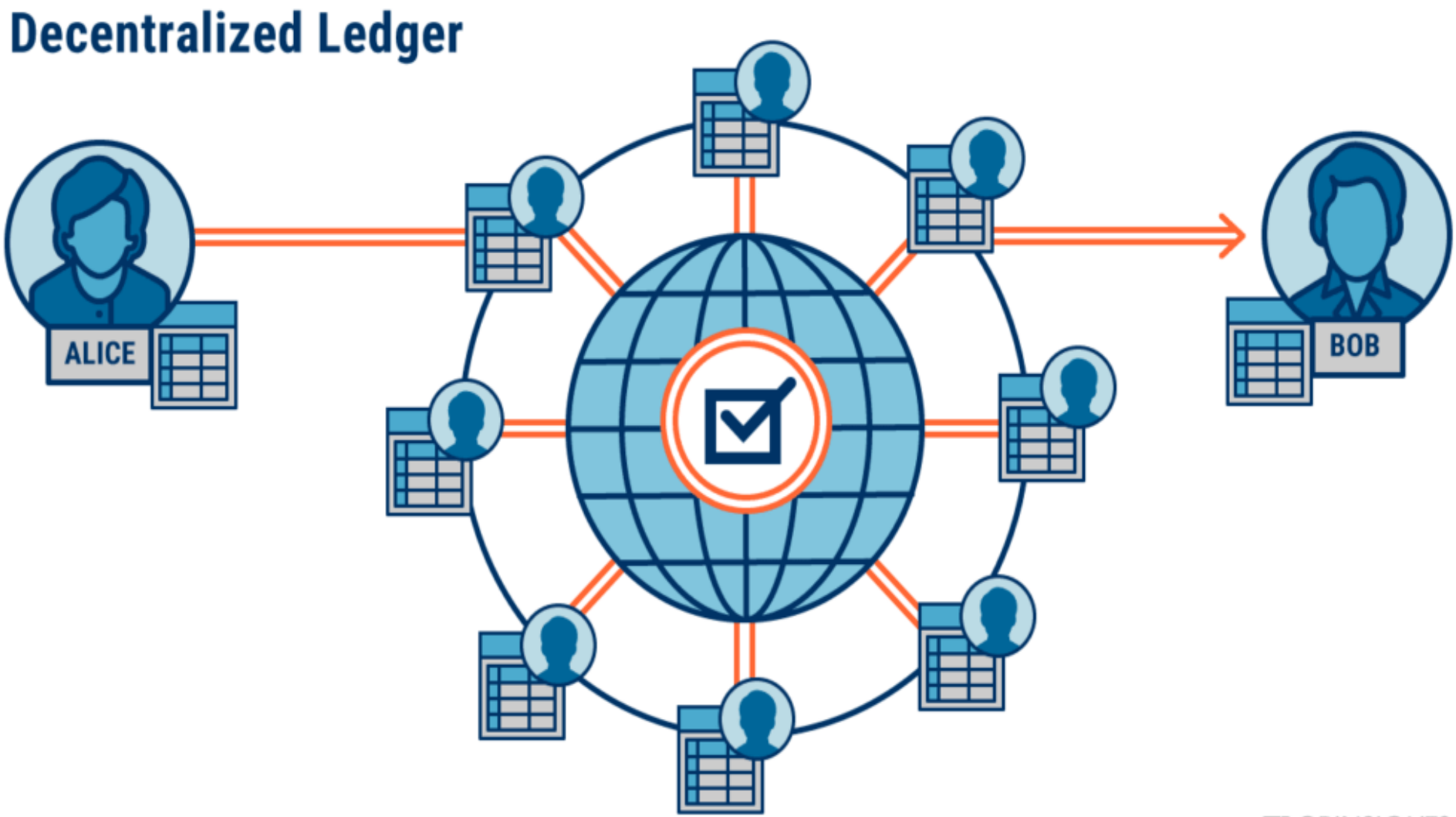

| Order | Transactions |
|---|---|
| 1 | $T^{\$\$\$\$}$ |
| 2 | $T_V^{\$\$\$}$ |
| 3 | $T_V^{\$\$}$ |
| 4 | $T^{\$}$ |

# Frontrunning Attack: Suppression



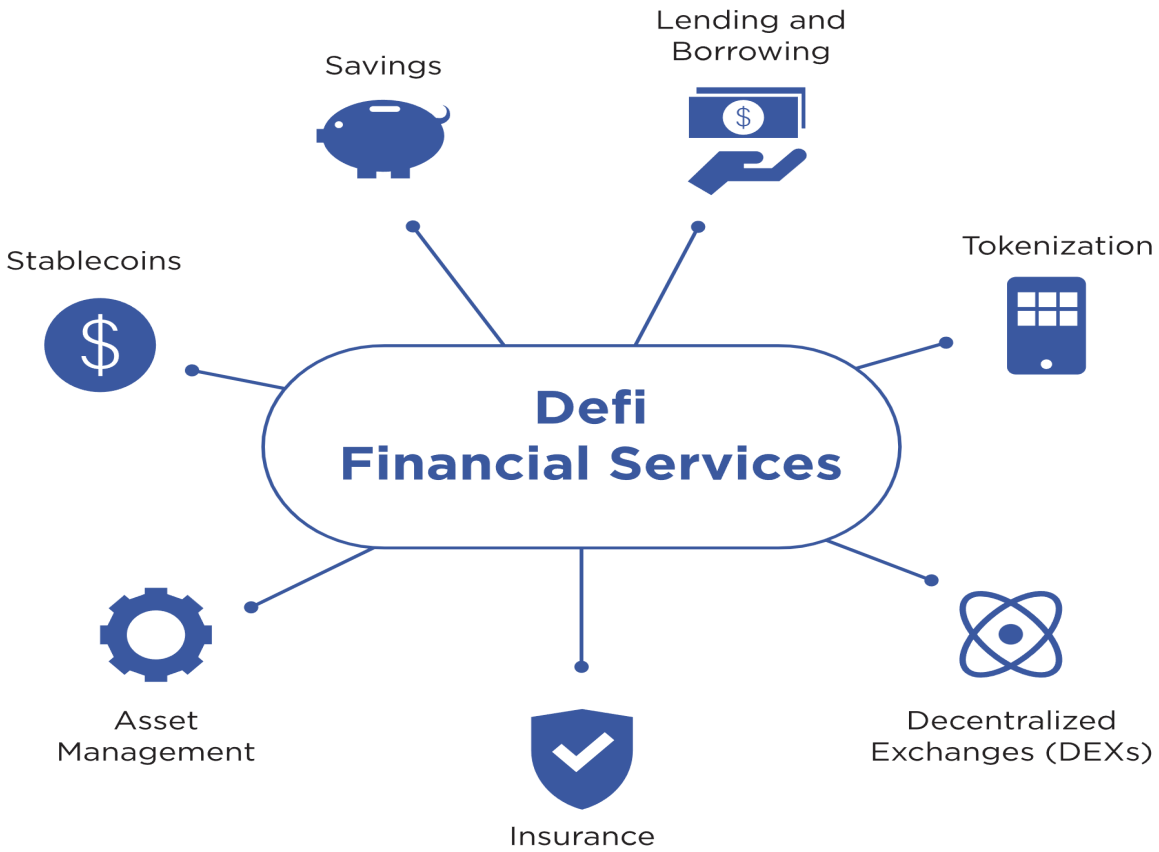

| Order | Transactions |
|---|---|
| 1 | $T^{\$\$\$\$}$ |
| 2 | $T_{sup}^{\$\$\$}$ |
| 3 | $T_{sup}^{\$\$\$}$ |
| 4 | $T_{sup}^{\$\$\$}$ |

# First Generation Blockchain: Payment Systems



# Second Generation Blockchain: Smart Contracts

- Second-generation blockchains (e.g. Etherum, Solana, ...) support smart contracts which are used to create protocols that implement financial services



# From First to Second Generation Blockchain

- The services provided by blockchain systems shifted
  - from payment system: Bitcoin, Ripple XRP
  - to broader financial services: decentralized finance (Etherum, Solana), stable coins (Tether, Dai).