Allocative Inefficiencies in Public Distributed Ledgers

Agostino Capponi

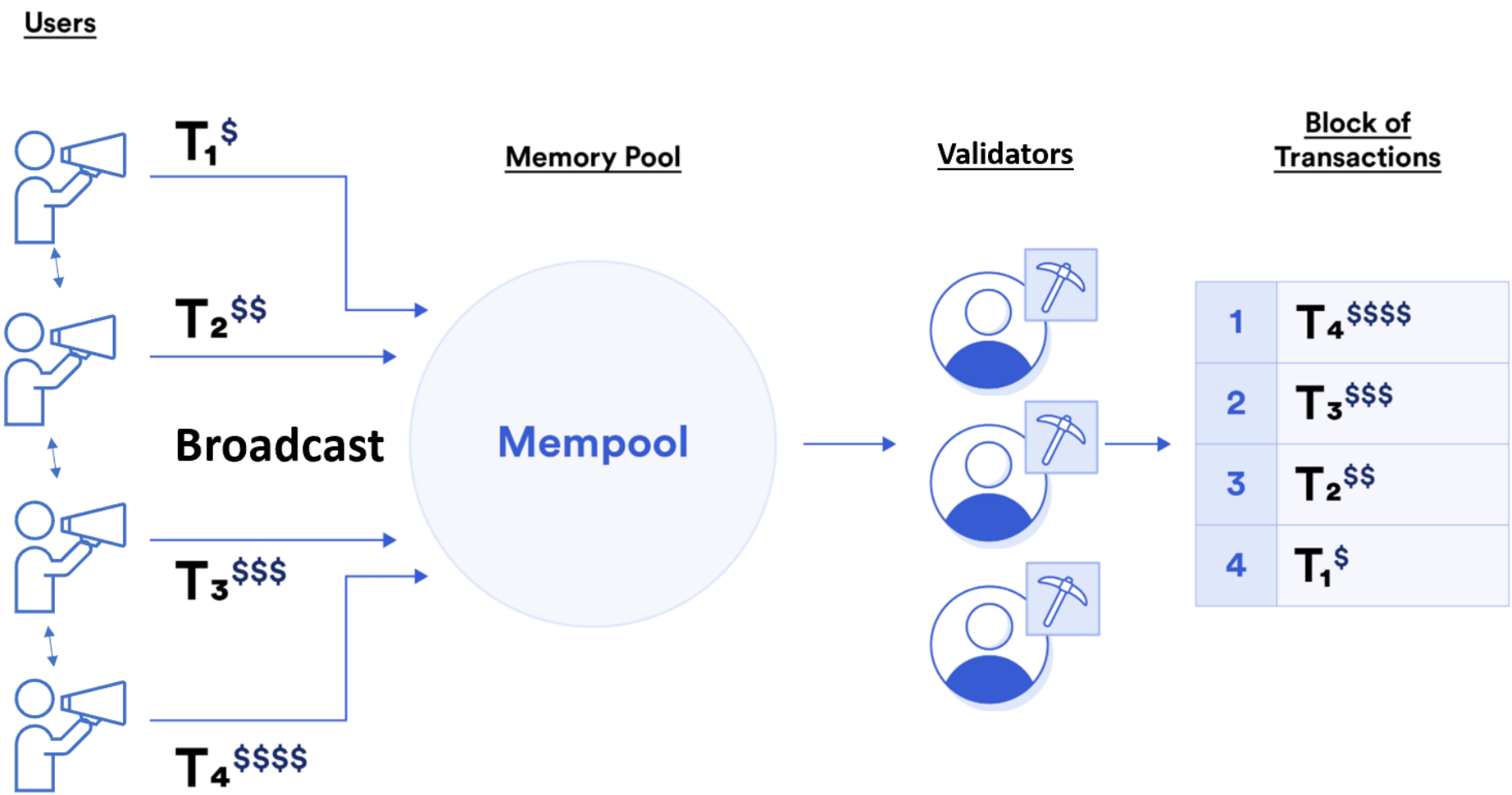
Columbia University

NYFED 2023 Fintech Research conference

joint work with Ruizhe Jia (Columbia) and Ye Wang (Macau)

Outline

Blockchain Execution Priority



Transparency of Transactions

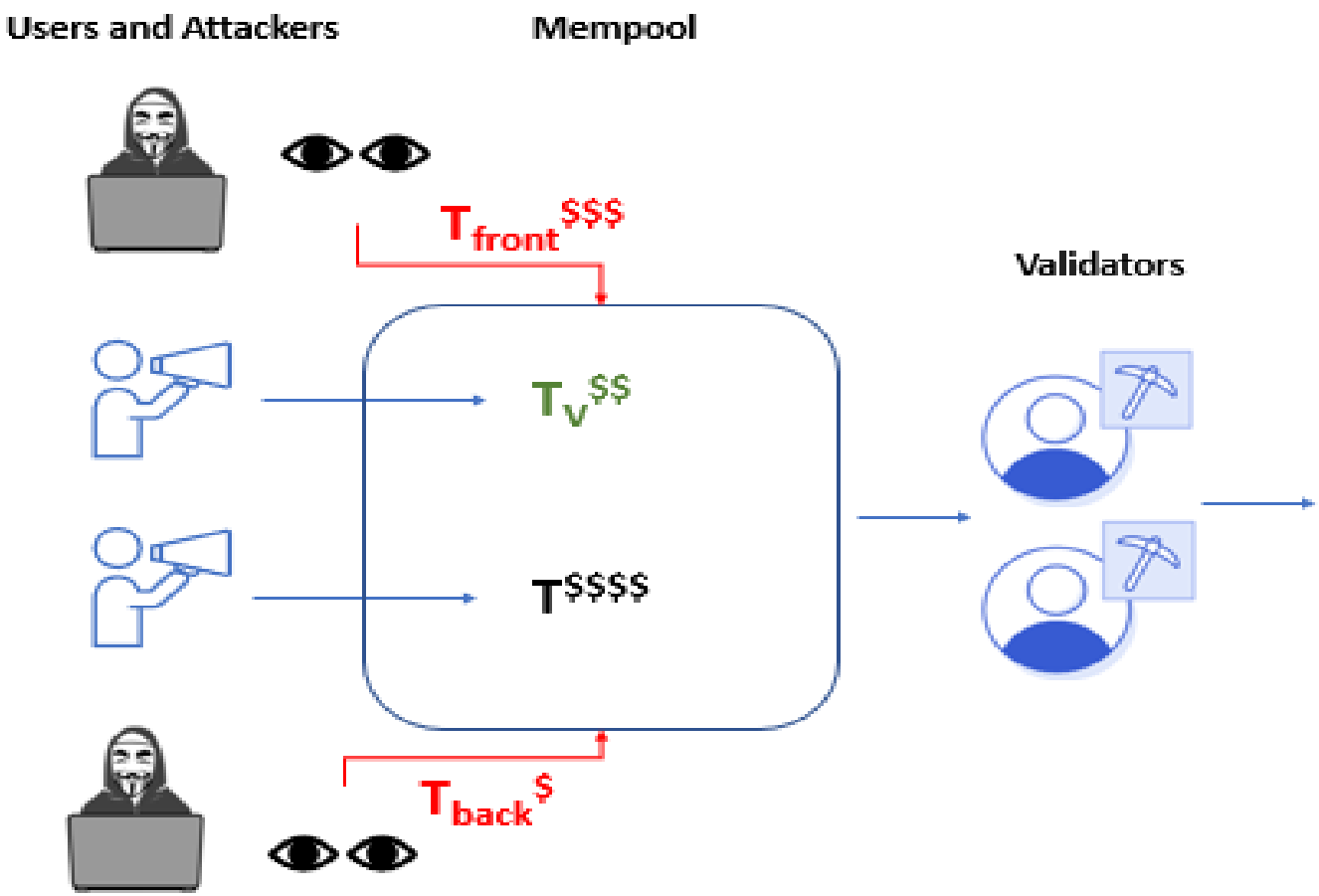
- Pending transactions are publicly observable in the mempool before settlement
- Transparency may leads to **frontrunning** attacks

A total of 235,292 pending txns found
(Showing the last 10000 records)

First ‹ Page 1 of 200 ›

Txn Hash	Nonce	Method ⓘ	Last Seen	Gas Limit	Gas Price ⓘ	From	To	Value
0x424b6f1f5098b573bf8...	31	0xc04b8d59	4 secs ago	296716	105.3884 | 1.5 Gwei	0x04729689f219cbd549...	Uniswap V3: Router	1.15 Ether
0x1f1a68ce3dd59685ed...	4164316	Transfer	4 secs ago	21000	185 | 2 Gwei	Coinbase 5	0xbcbd01a53140e26947...	0.05020473 E
0x9df4927481afc763d74...	13	Deposit	4 secs ago	45038	121.5063 | 1.5 Gwei	0x433db84f88f1944f3a5...	Wrapped Ether	0.5 Ether
0x18059111e7b412f3f55f...	475	Set Approval For...	4 secs ago	46747	110.2918 | 1.5 Gwei	0xf31fc1a5bfa83452184...	Based Fish Mafia: BFM T...	0 Ether
0xc733658c0a63c45c5f1...	73	Swap Exact Token...	4 secs ago	213798	105.3884 | 1.5 Gwei	0xc4f565416a9034ed52...	SushiSwap: Router	0 Ether

Example of Frontrunning Attack

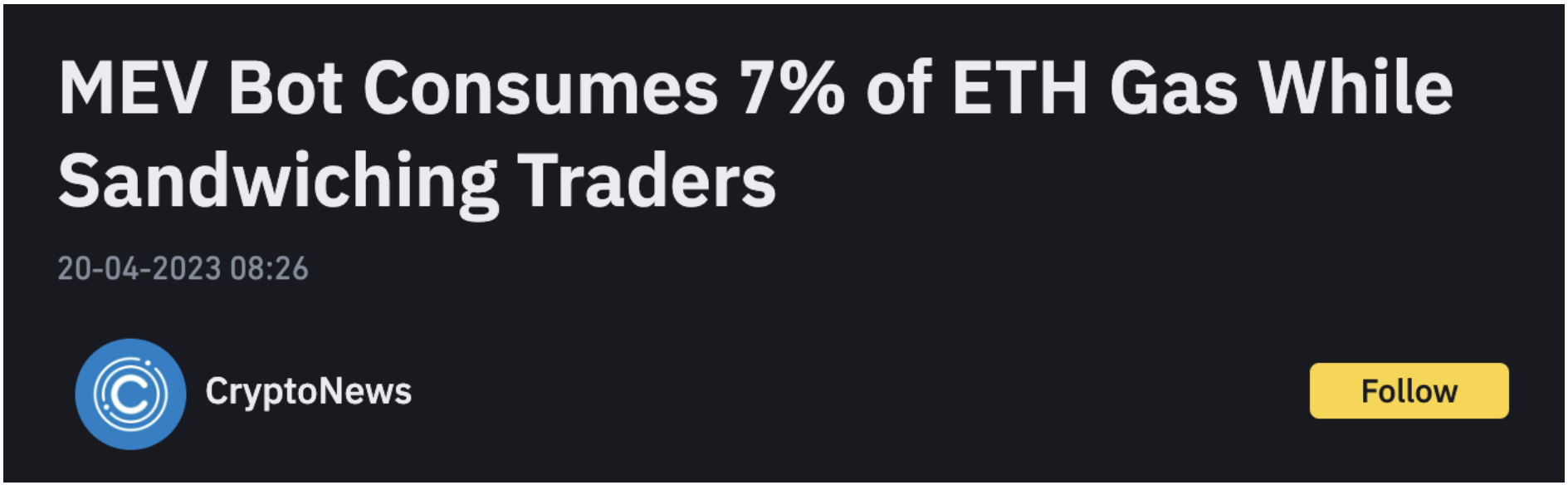


Order	Transactions
1	$T^{\$\$\$\$}$
2	$T_{front}^{\$\$\$}$
3	$T_V^{\$\$}$
4	$T_{back}^{\$}$

Is Frontrunning Material?

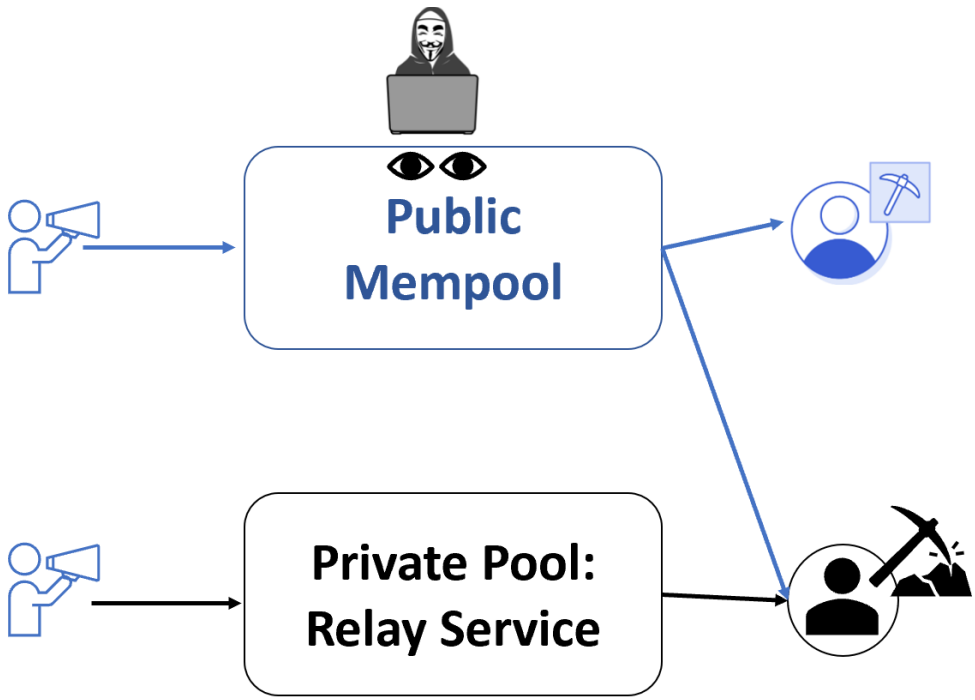
- $\geq$ **95%** of Ethereum blocks contain frontrunnable transactions
- Using data from 2018-2022, we find that each frontrun transaction costs, on average, 0.2 ETH to the victim user.
- A large amount of block space (equivalent to hundreds of full blocks) and gas fees are "wasted" on frontrunning transactions.

Blockspace Waste



Public vs Private Pools

- Relay Services (e.g. Flashbots) provide **private** parallel channels:
  - Users submit directly to validators
  - Validators admitted to the private pools can observe transactions submitted.
  - Validators must not disclose any transaction they observe.
- Goal: reduce frontrunning and transaction fee surges caused by arbitrage bots.



Research Questions

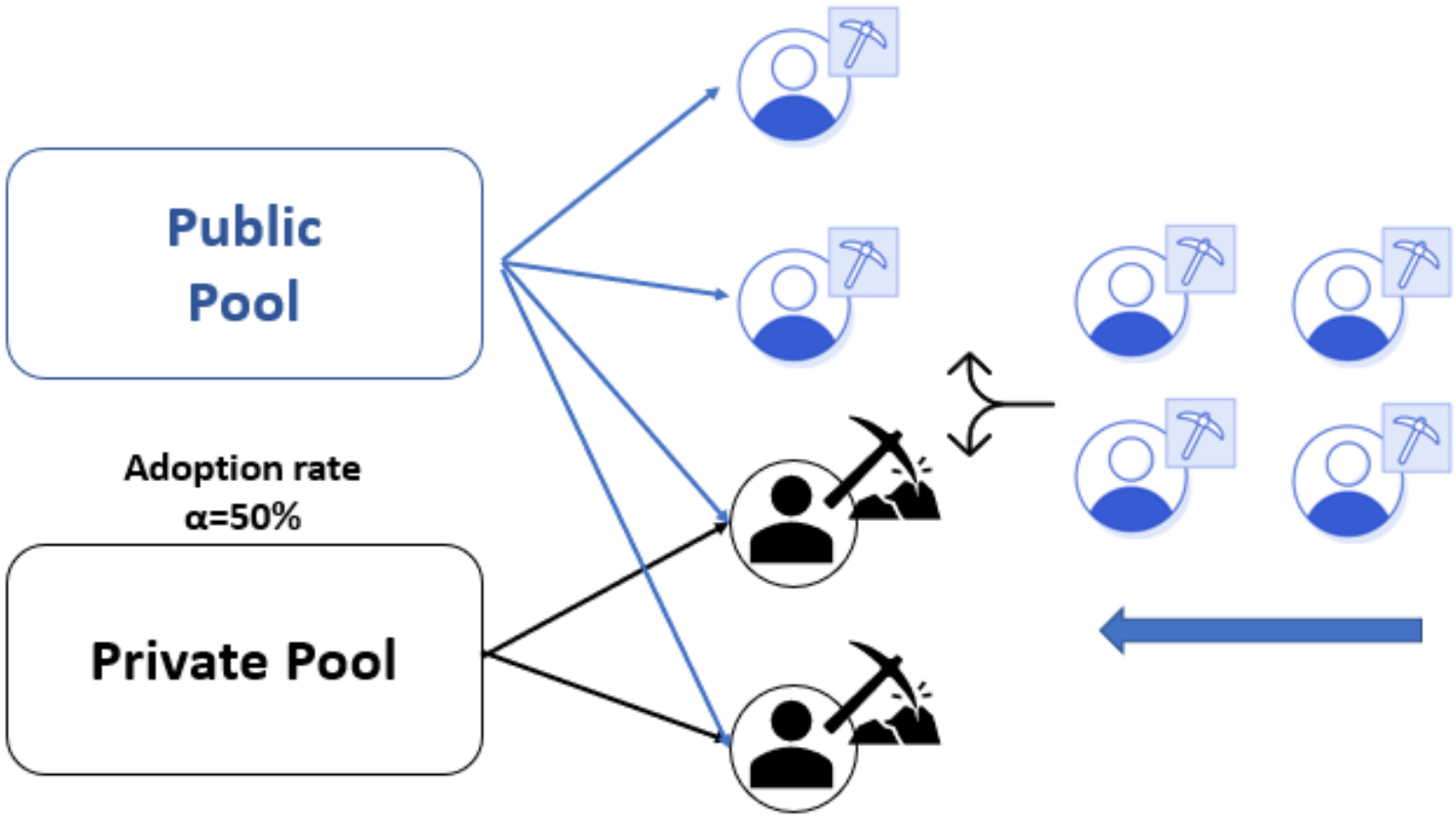
- **Adoption:** Will the private pool be adopted by participants of the blockchain ecosystem?
- **Mitigation of Frontrunning:** If adopted, will it achieve the intended purpose of improving block allocation efficiency?
- **Welfare Implications:** Is the introduction of a private pool welfare enhancing?

Model Setup

- Game theoretical model with 3 periods indexed by t, $t = 1, 2, 3$.
- 3 types of agents:
  - A continuum of homogeneous and rational validators
  - A frontrunnable user and a discrete set of non-frontrunnable users
  - Two arbitrageurs
- Two transaction submission venues: private pool and public pool

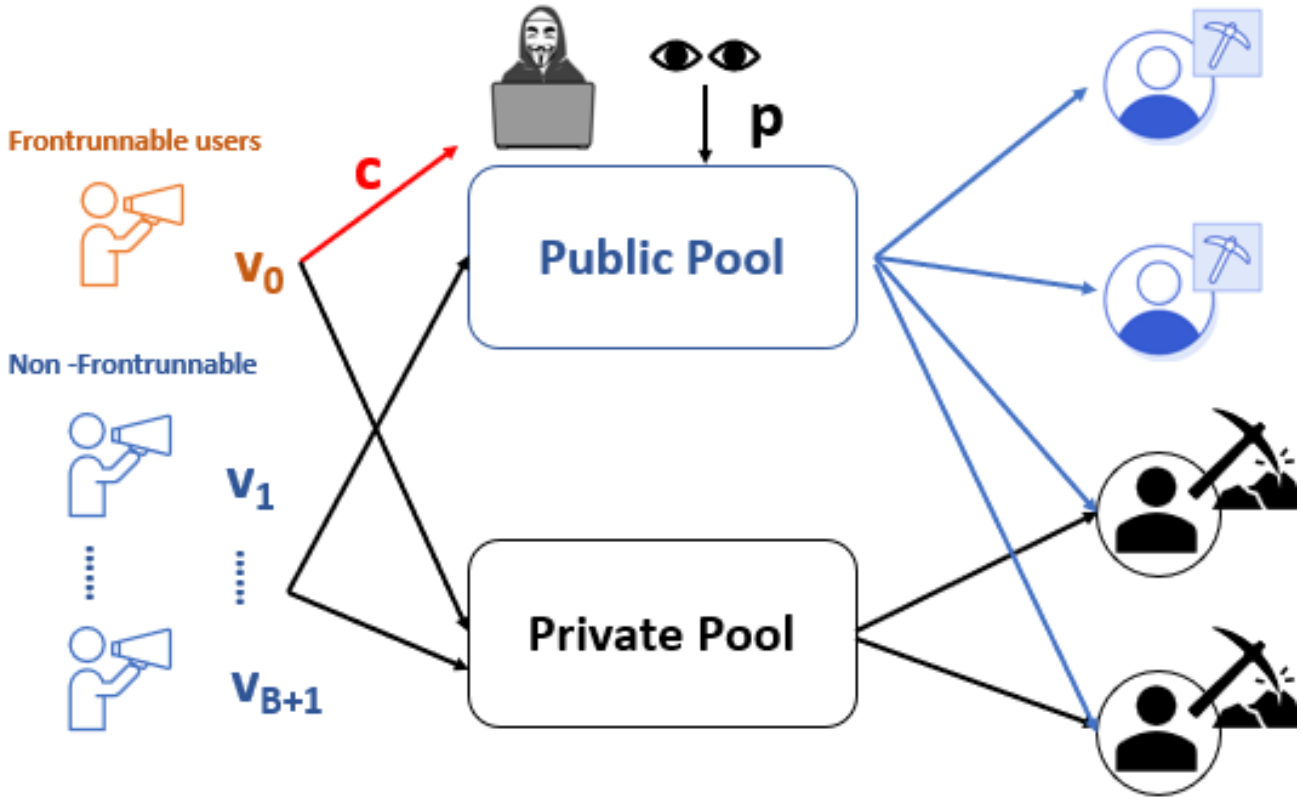
Period $t = 1$

- Validators choose whether to monitor private pool, in addition to public pool
- Transactions on the private pool are observed only by validators who join the private pool

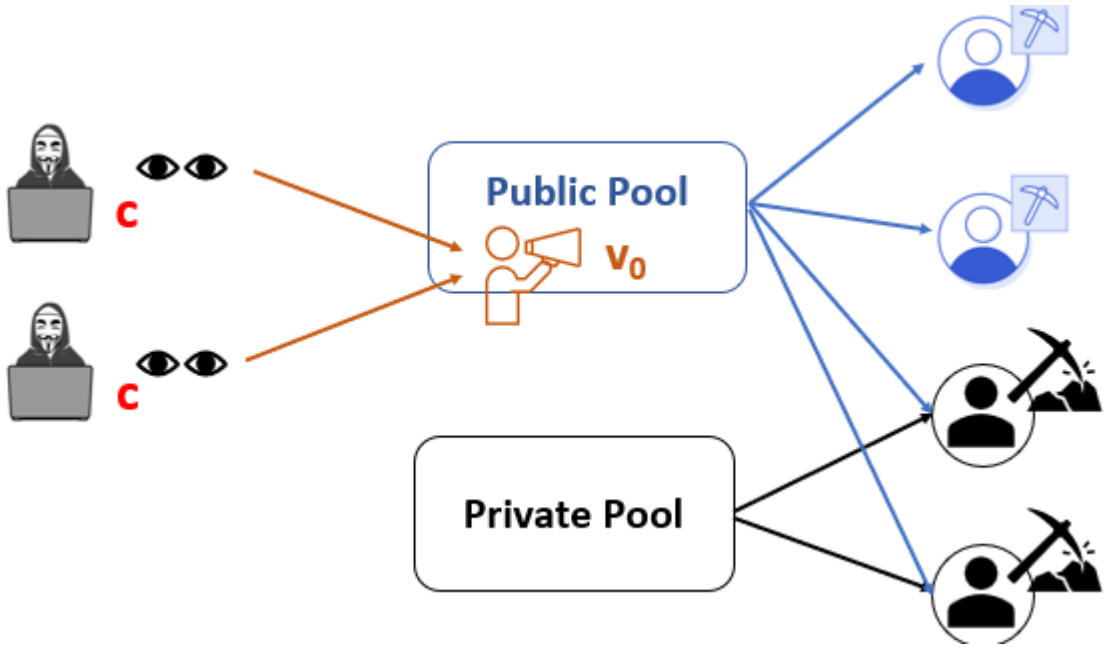


Period $t = 2$

- Users decide on bid fees and submission venue
- Users extract value from executing their transactions
- The frontrunnable user loses $c > 0$ if his transaction is frontrun by an arbitrageur

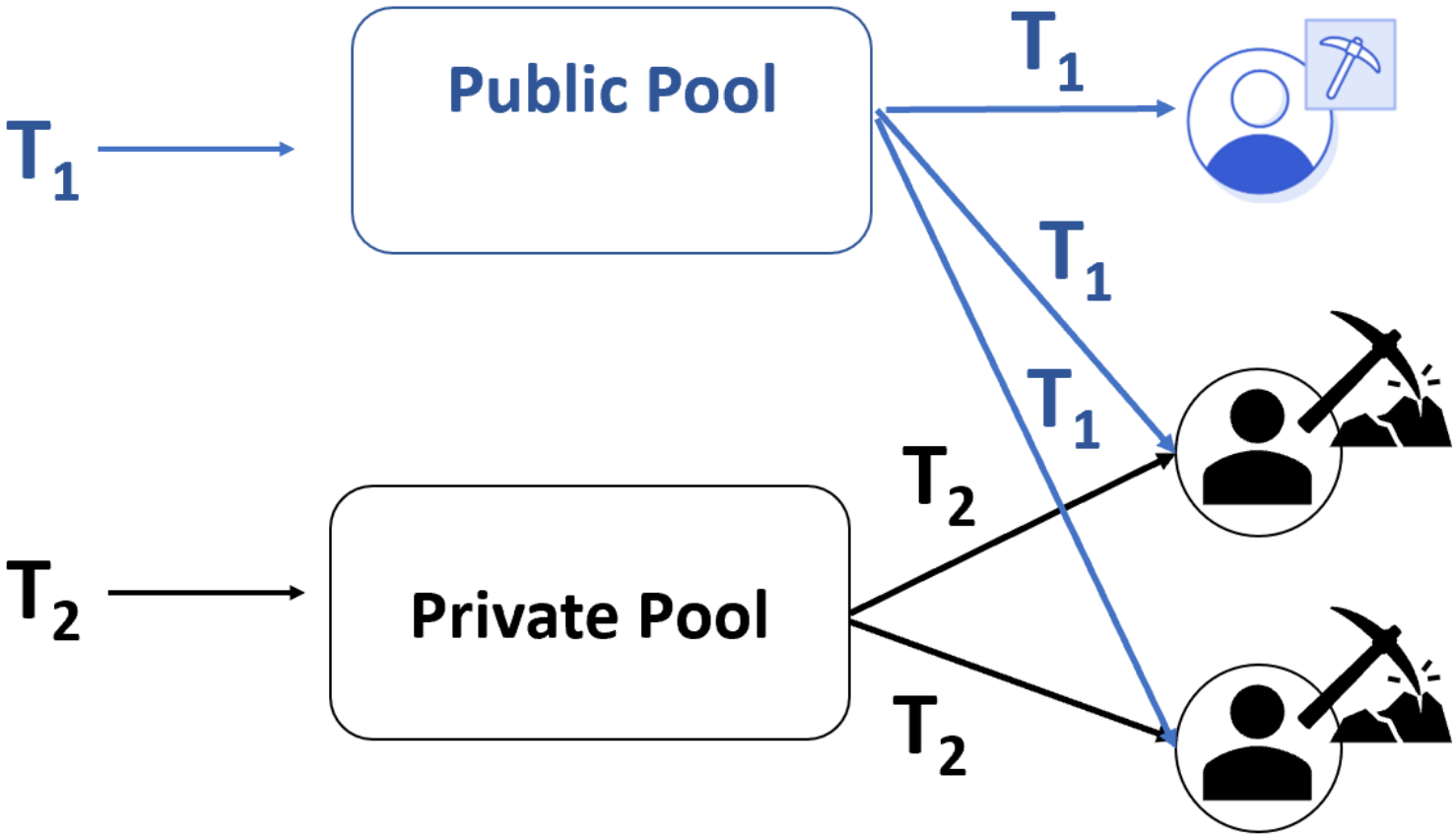


Period $t = 3$



- The arbitrageur creates an order, attaches a fee and decides which venue to use: public pool, private pool, or both.
- If the order is broadcast through the public pool, the other arbitrageur will observe it
- An arbitrageur who executes the frontrunnable transaction earns a profit $c \geq 0$.

Execution Risk in the Private Pool

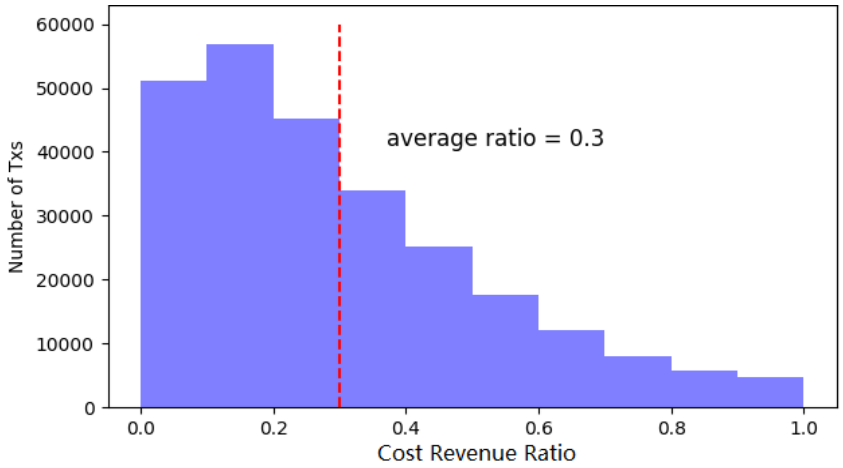


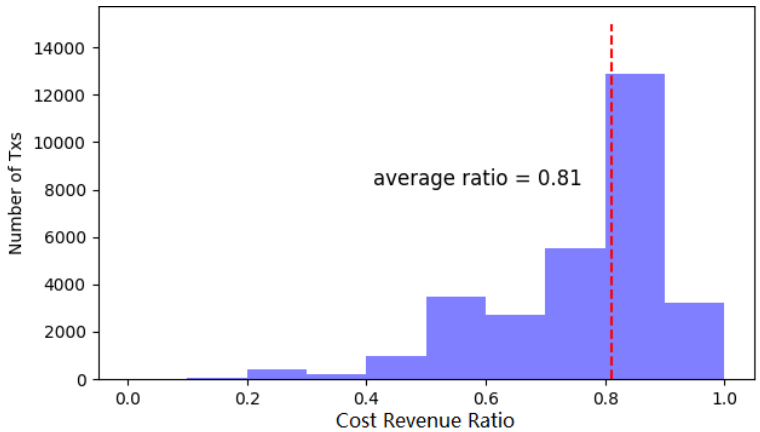
Frontrunners' Choice of Submission Venue

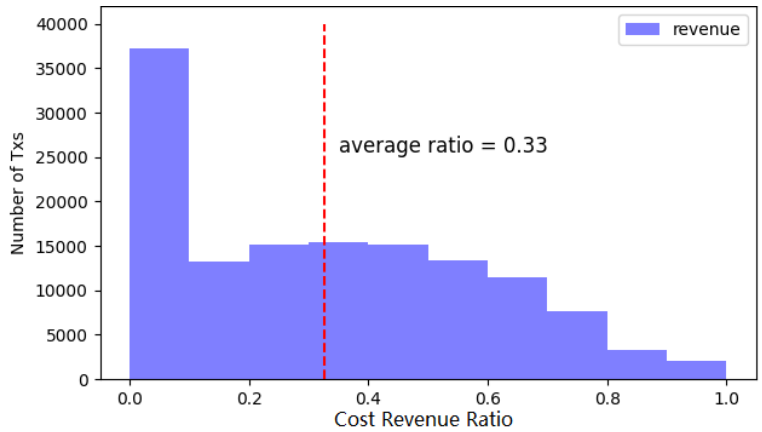
- Frontunners engage in an **"arm race"** for priority order execution
- **Prioritized execution:** transactions submitted through private pool placed at the top of the block by validators who monitor this pool.
- However, using the private pool alone presents **execution risk**
- In equilibrium, frontrunners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

Arbitrageurs' Costs

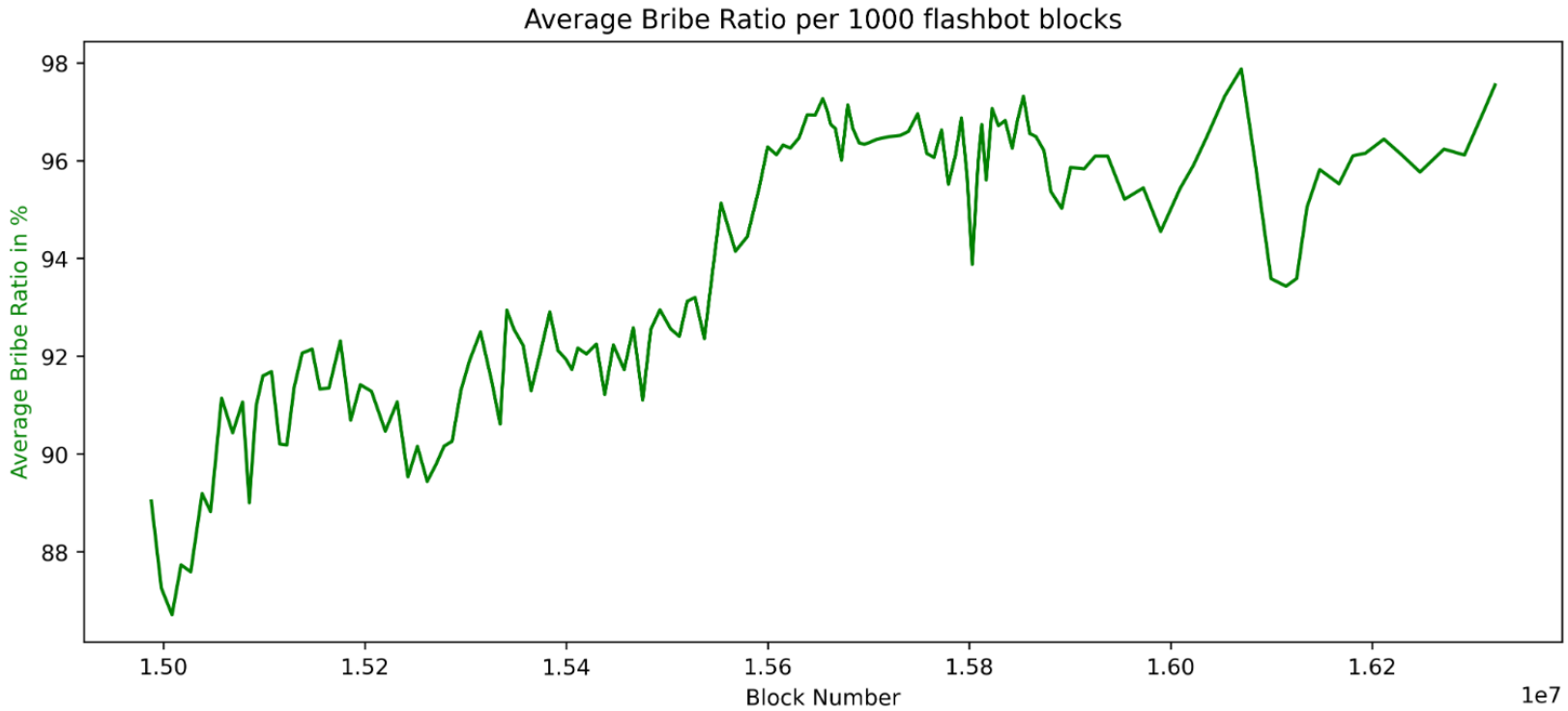
Cost-to-Revenue Ratio = Gas fees paid/ Total Revenue from frontrunning







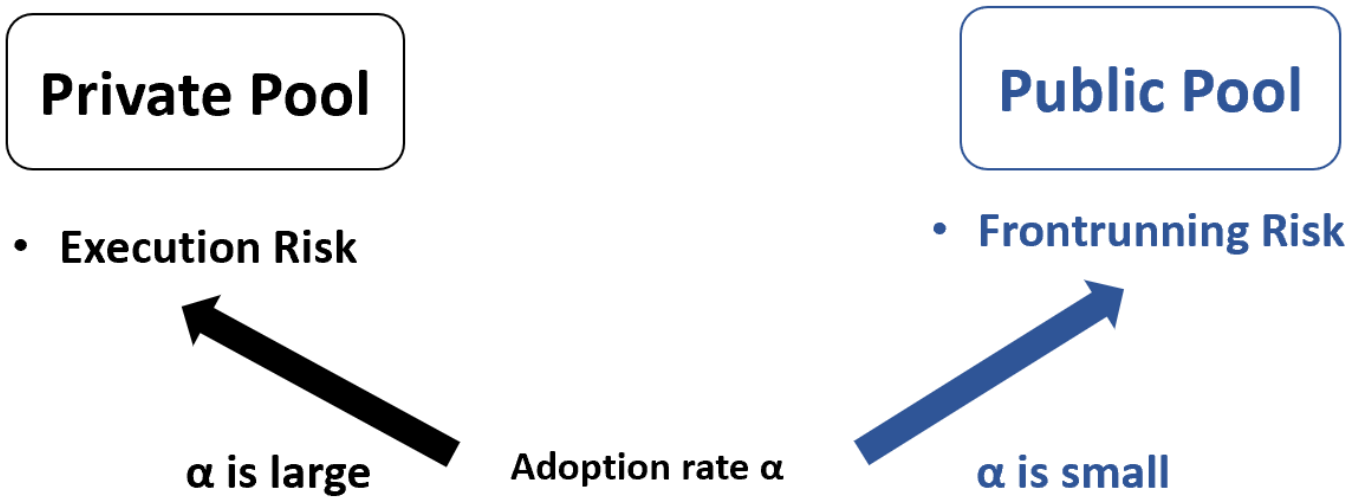
MEV Concentration



- Up to **99%** of transaction value is paid as fees by frontunners

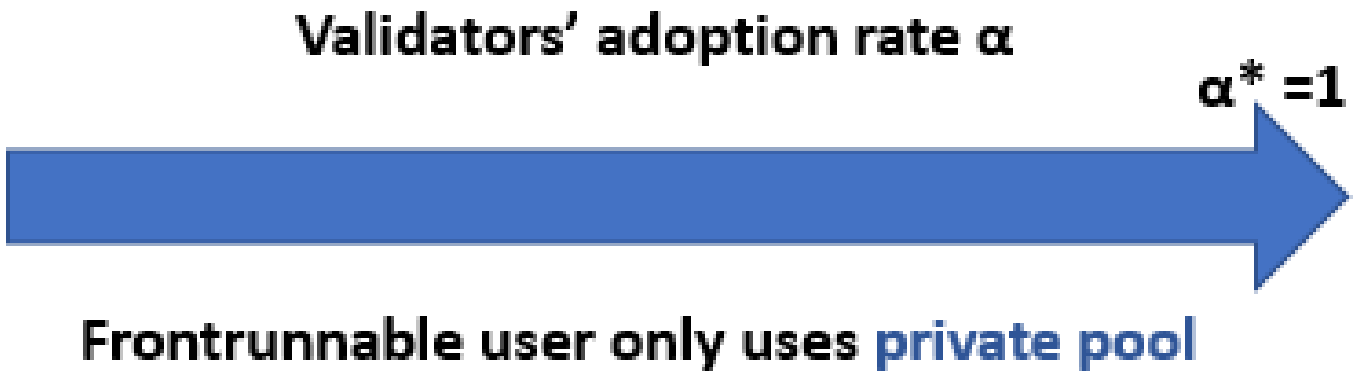
Tradeoff Faced by Frontrunnable Users

- **Execution risk:** a fraction $(1-\alpha)$ of validators may never observe transactions submitted to the private pool.



SPNE if Frontrunning Risk is High

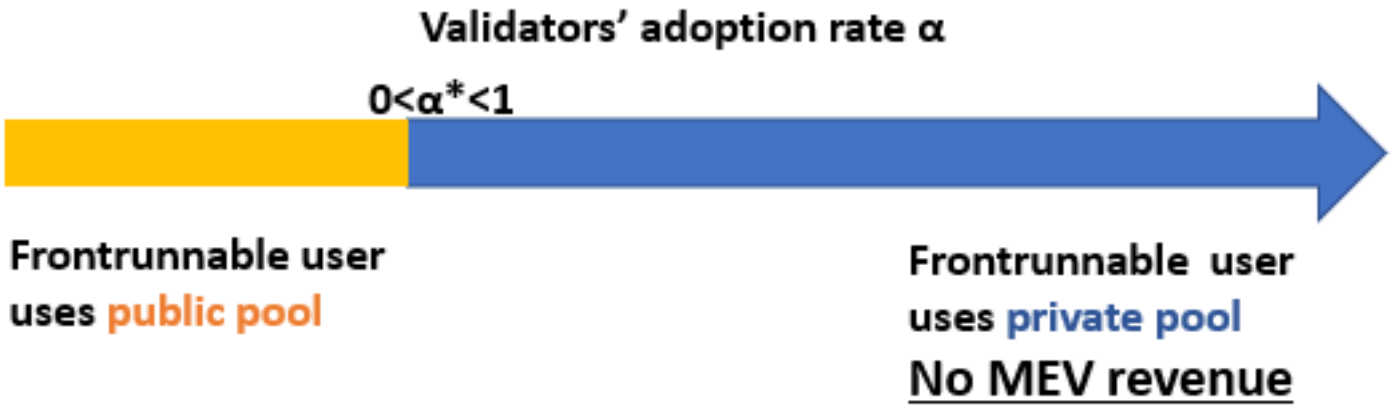
- **If c is large:**



1. The frontrunnable user only submits his transaction to the private pool.
2. In the subgame perfect Nash equilibrium, all validators join the private pool to capture the transaction submitted by the frontrunnable user.

SPNE if Frontrunning Risk is Low

- **If c is small:**



1. Without a private pool, the frontrunnable user would still submit to public pool
2. Frontrunning arbitrage generates fees (arbitrageurs bid high fees to outbid each other) for validators.
3. To maintain their revenue, only a small fraction of validators choose to adopt the private pool, which creates high execution risk.
4. In the SPNE, the frontrunnable user submits through the public pool and faces frontrunning risk.

Aggregate Welfare and Allocative Inefficiencies

- Aggregate welfare = the sum of ex-ante payoff of all agents = **the sum of private benefits of transactions on blockchain**
- Two root causes of inefficiencies in block-space allocation:
  - User does not submit transactions 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 weakly increase with a private pool:
  - The frontrunnable user gains the option to access private pool (both types of inefficiencies are reduced)
- Aggregate welfare is maximized if all validators adopt the private pool
  - Eliminates frontrunning risk and mitigates social waste due to blockspace misallocation
- **Hold up problem**: social optimum not attainable unless frontrunnable users compensate validators for the MEV loss

Conclusion

- **Adoption:** the private pool is at least partially adopted by validators and utilized by at least one arbitrageur.
- **Allocative Inefficiencies:** private pool neither eliminates frontrunning arbitrage nor reduces transaction costs.
- Welfare Implications of a private pool:
  - Welfare of Validators: $\uparrow$
  - Welfare of Arbitrageurs: $\downarrow$
  - Aggregate welfare: higher due to more efficient blockspace allocation, but not necessarily the social optimum

Thank You!

Users' Migration

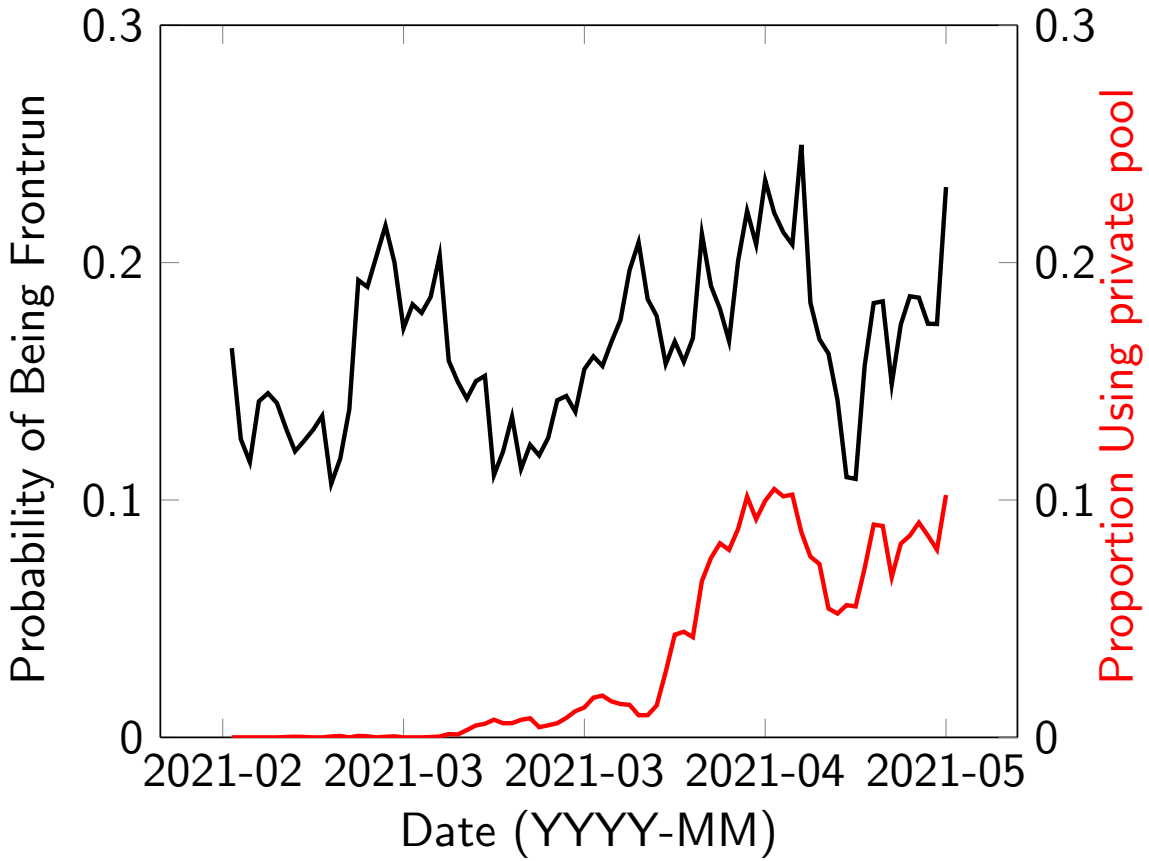
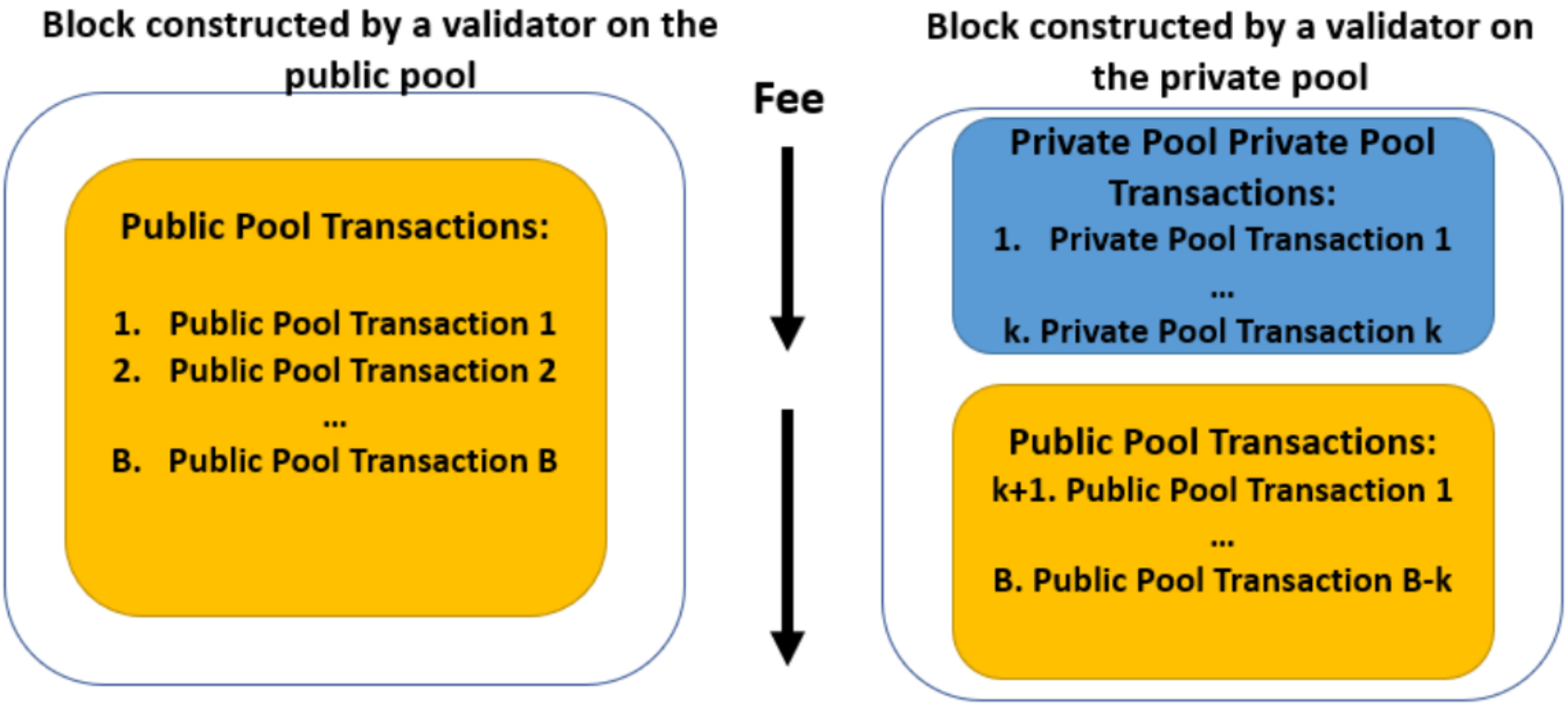


Figure: The black line represents the daily average probability of being attacked for frontrunnable users. The red line represents the daily proportion of frontrunnable transactions sent to private pool.

Transaction Execution

- Block **capacity** is B.
- The validator can only select from the transactions he observes.
- A validator who appends the block selects the B transactions with the highest fees



Adoption rate of the private pool (Flashbots).

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

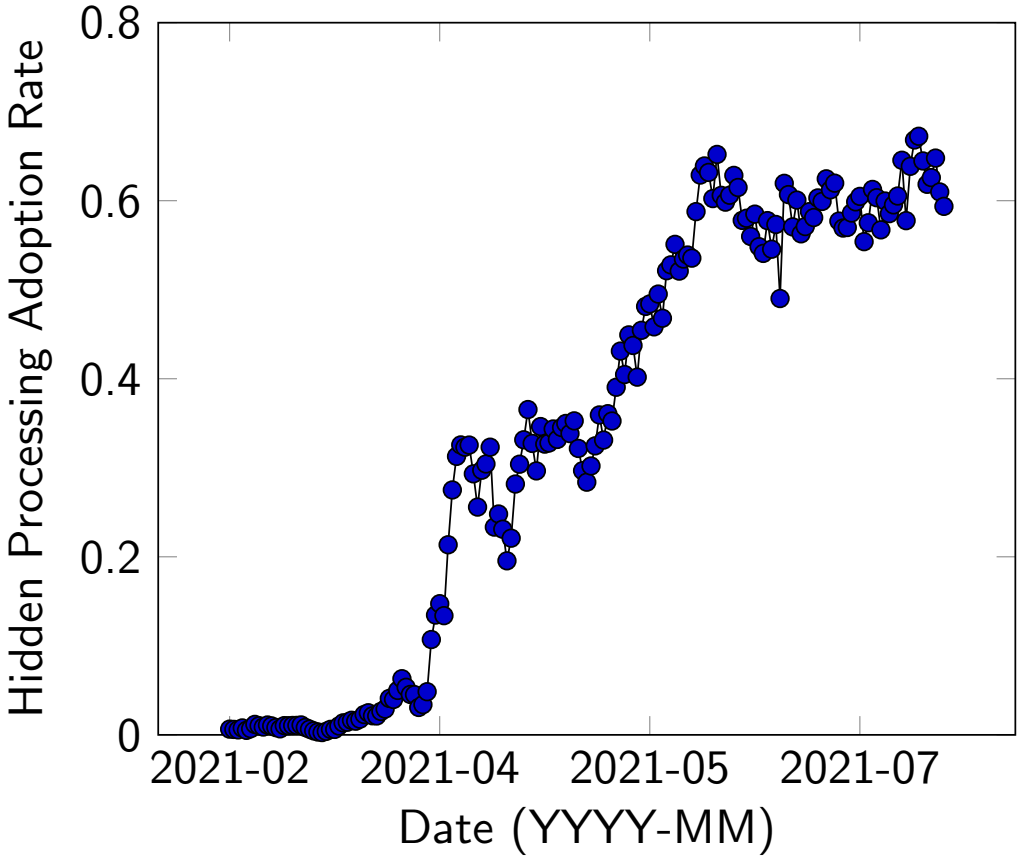
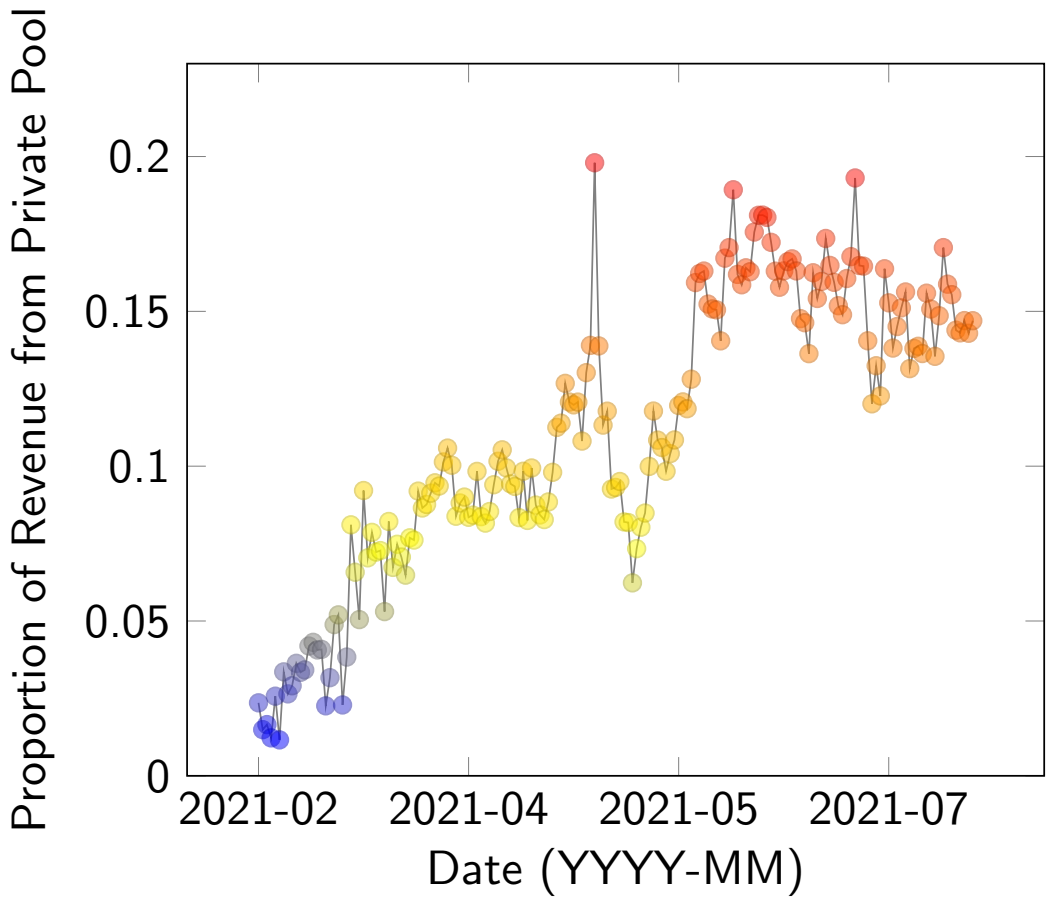


Figure: Adoption rate of Flashbots.

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

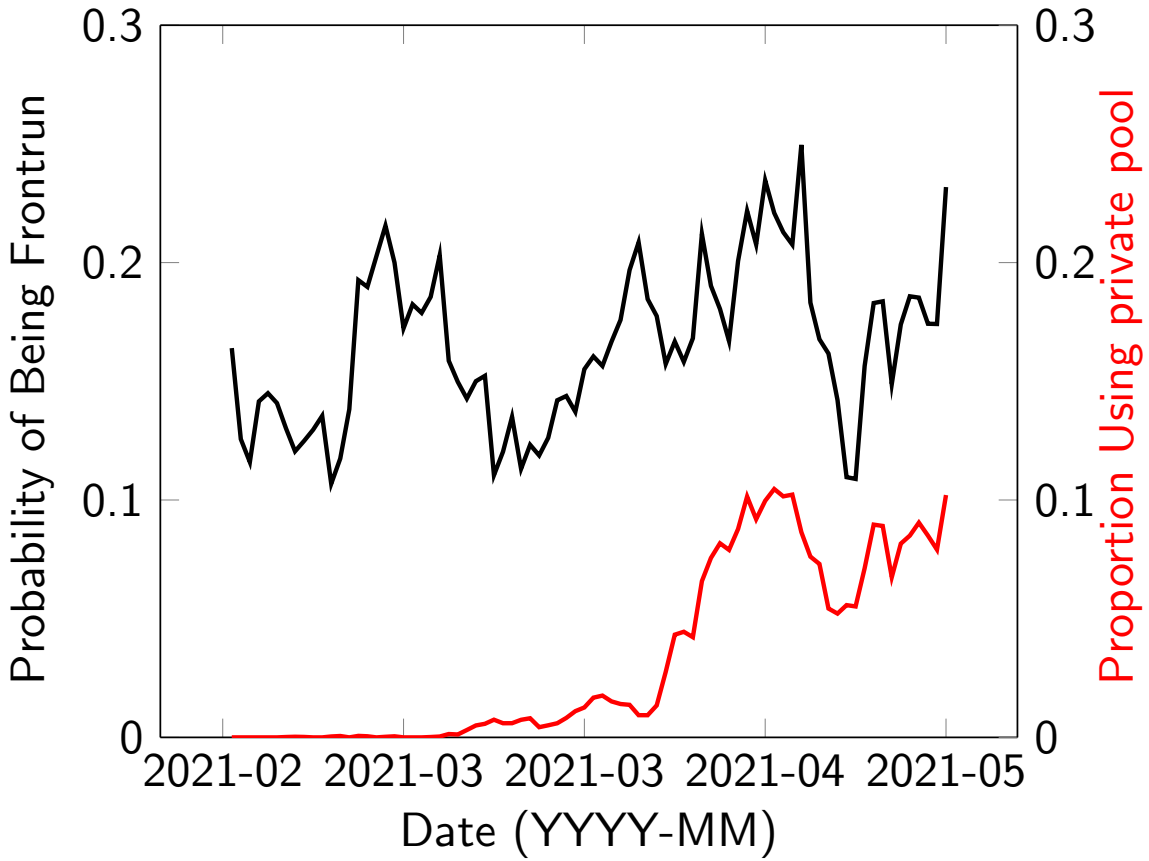


Figure: The black line represents the daily average probability of being attacked for frontrunnable users. The red line represents the daily proportion of frontrunnable transactions sent to private pool.

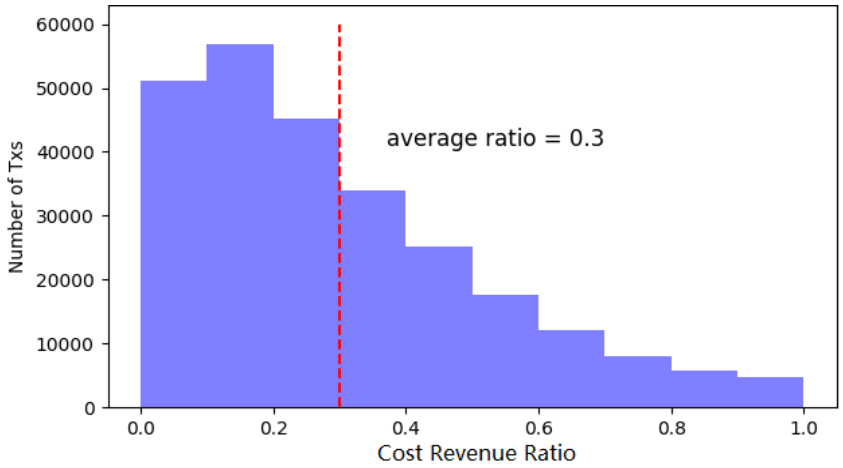
Users' Migration

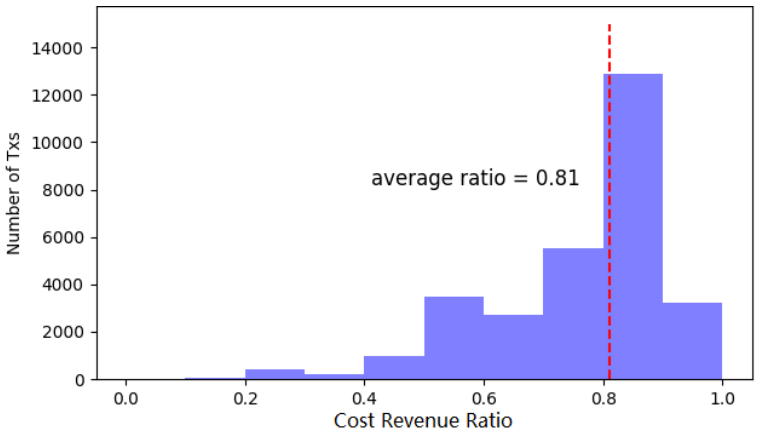
A 1% increase in probability of being frontrun is associated with a 0.6% increase in the proportion of frontrunnable transactions submitted through the private pool.

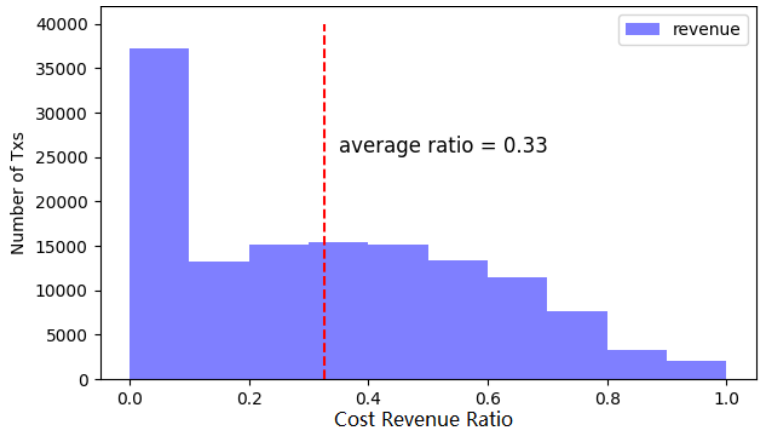
	Dependent variables:
	Proportion of Transactions Through Dark
Intercept	-0.066
	(0.18)
Probability of Being Frontrun	0.605***
	(0.010)
Observations	80
R^2	0.3
Note:	*p<0.1; **p<0.05; ***p<0.01

Arbitrageurs' Welfare

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







Arbitrageurs' Welfare

After the introduction of the private pool, arbitrageurs' 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

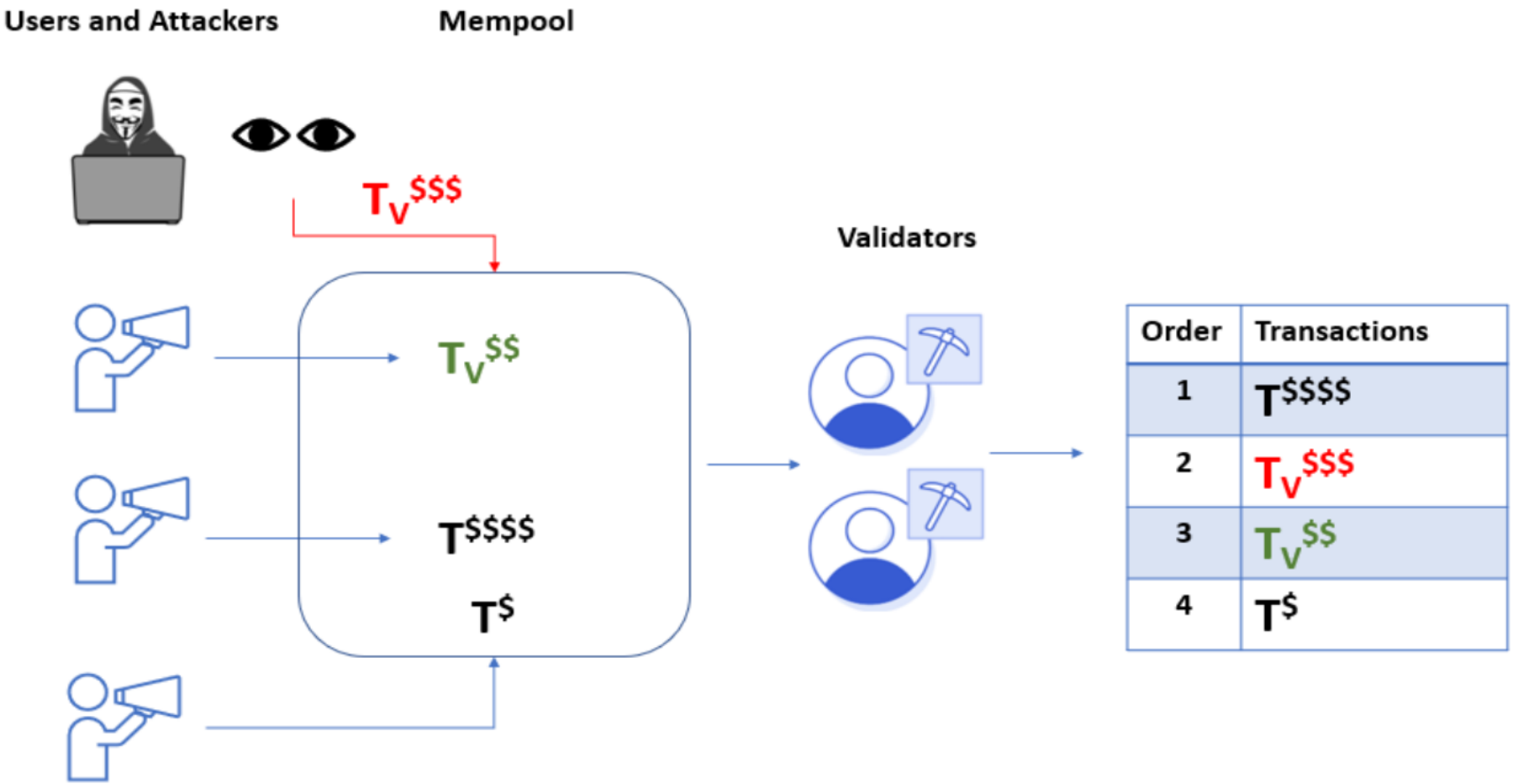
Proposition (Subgame Perfect Equilibrium (SPE))

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 arbitrageurs 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 arbitrageurs send their orders to the private pool only or to both venues.*

Transaction Fees

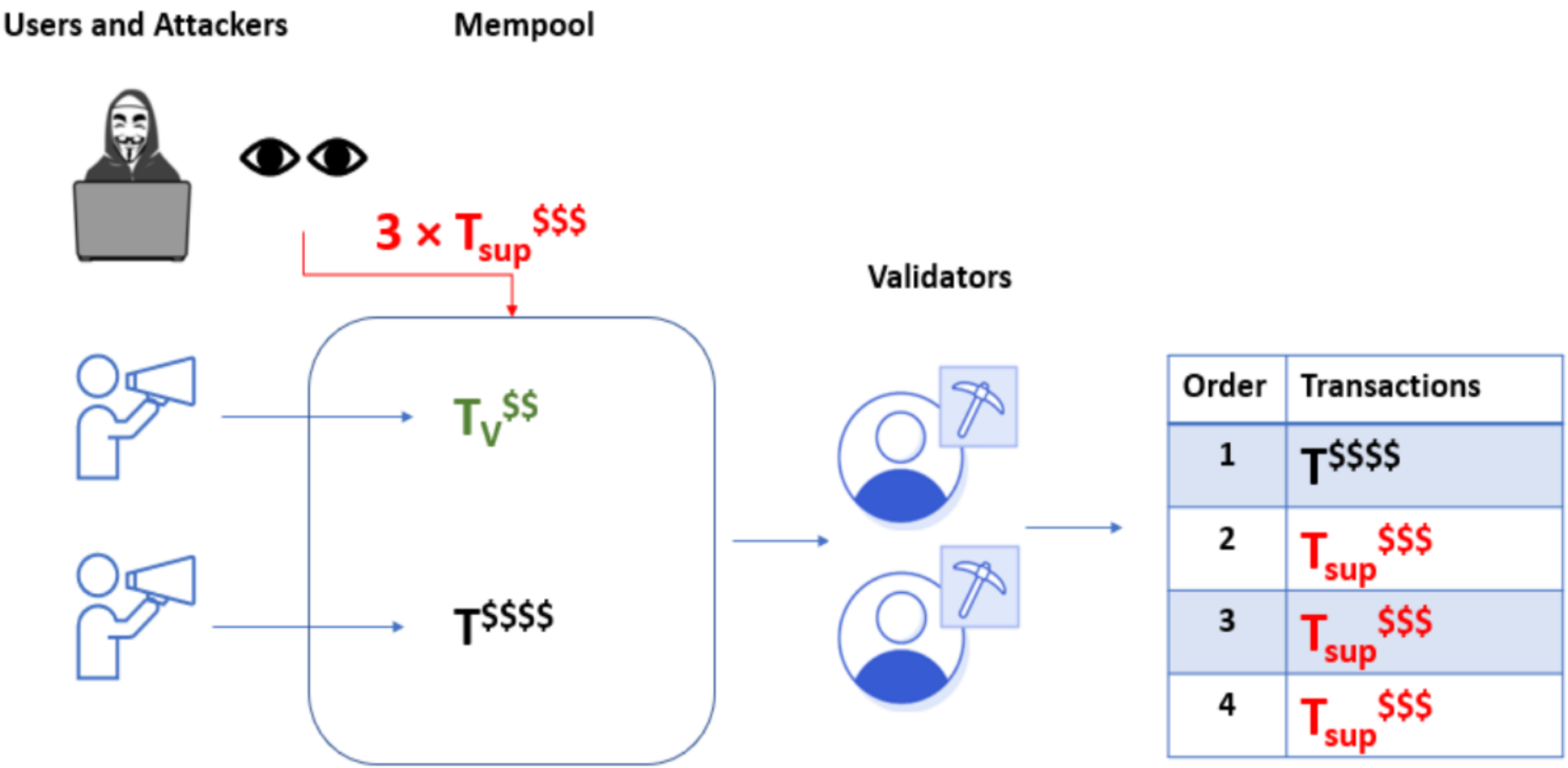
- The introduction of a private pool **increases the minimum fee** which guarantees the execution of a transaction!
  1. The introduction of the private pool may attract the frontrunnable transaction which would not have been submitted otherwise.
  2. Validators adopt the private pool only if they earn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

Frontrunning Attack: Displacement



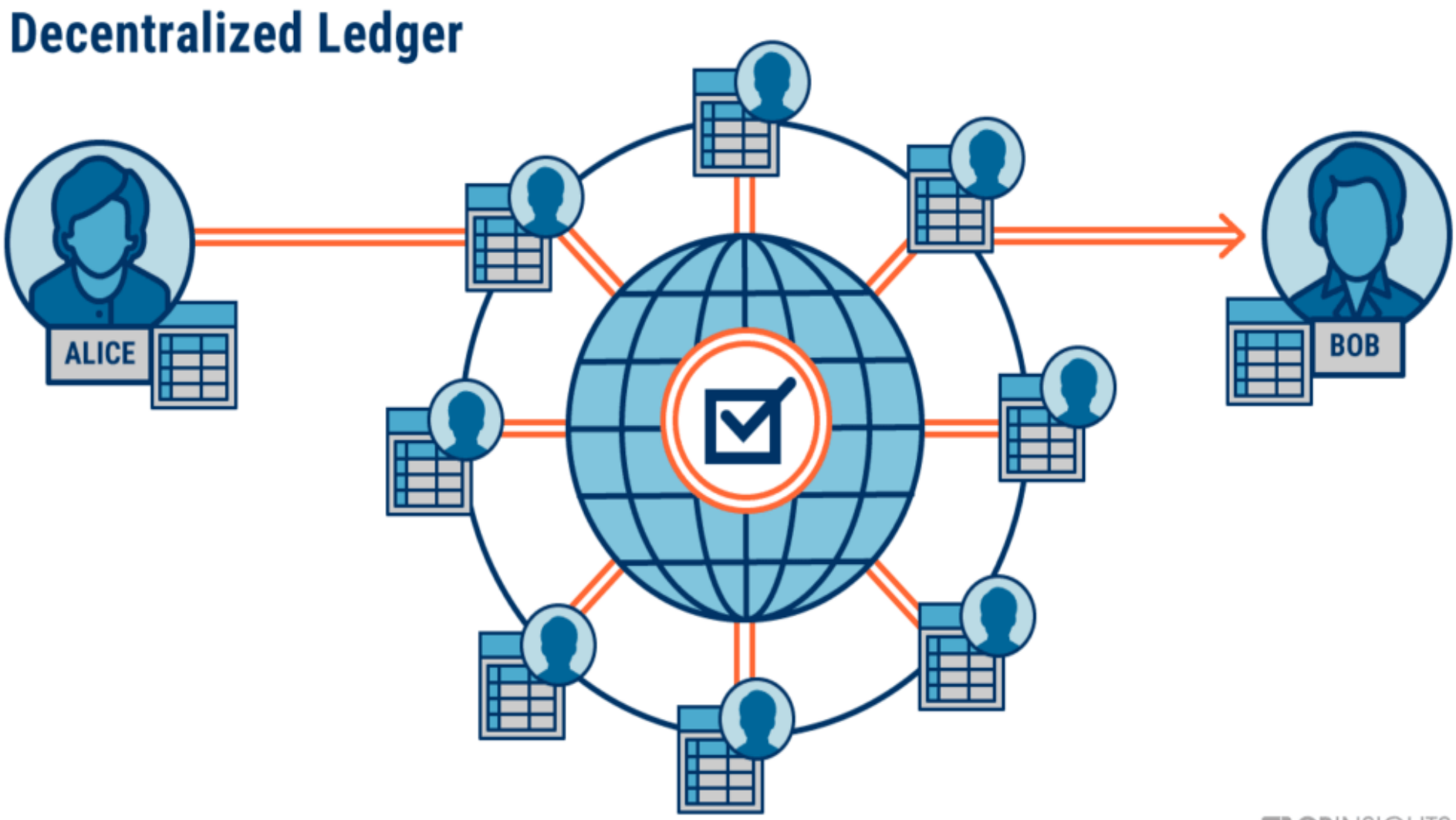
Order	Transactions
1	$T^{\$\$\$\$}$
2	$T_V^{\$\$\$}$
3	$T_V^{\$\$}$
4	$T^{\$}$

Frontrunning Attack: Suppression



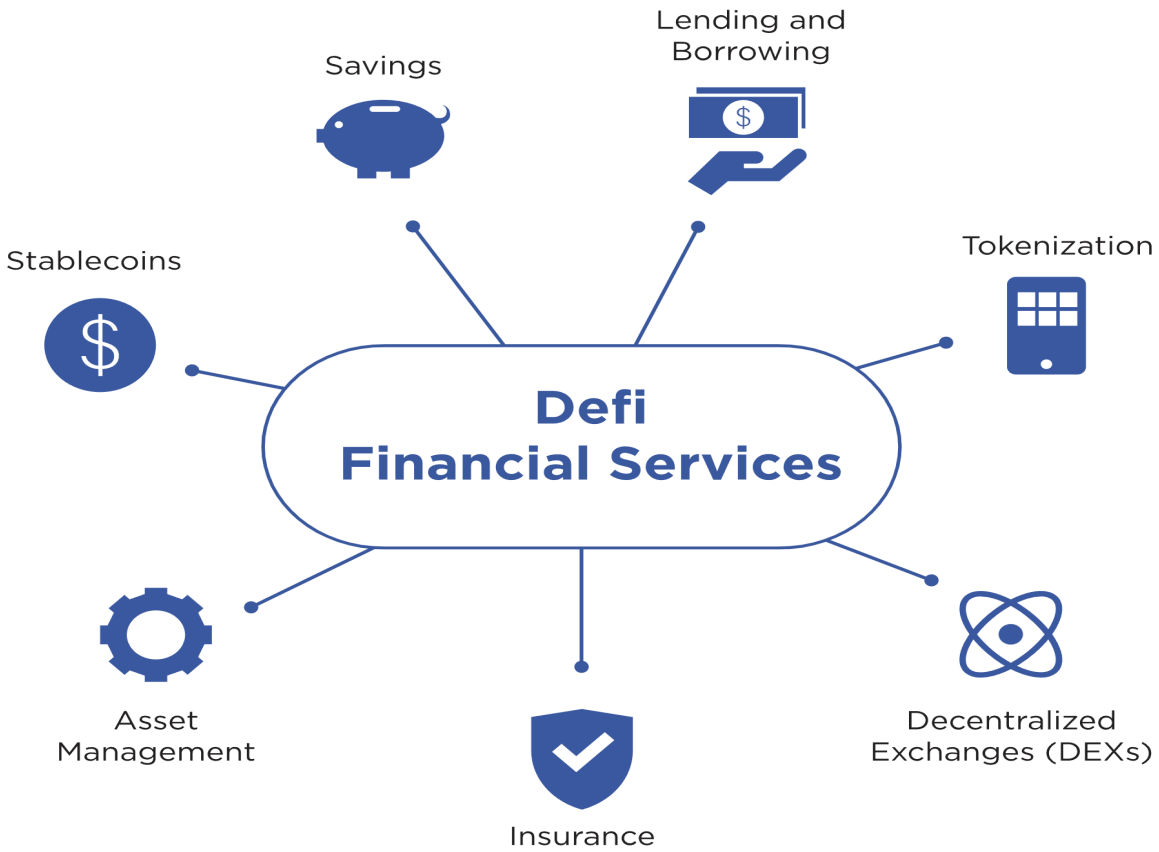
Order	Transactions
1	T $$$$
2	T_{sup} $$$
3	T_{sup} $$$
4	T_{sup} $$$

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).