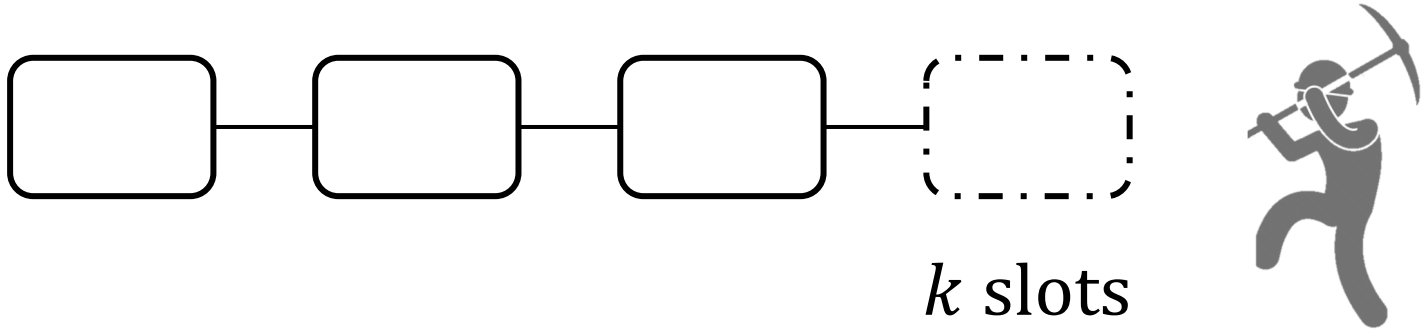
What Can Crypto do for Mechanism Design?

Elaine Shi, Hao Chung and **Ke Wu**

Carnegie Mellon University

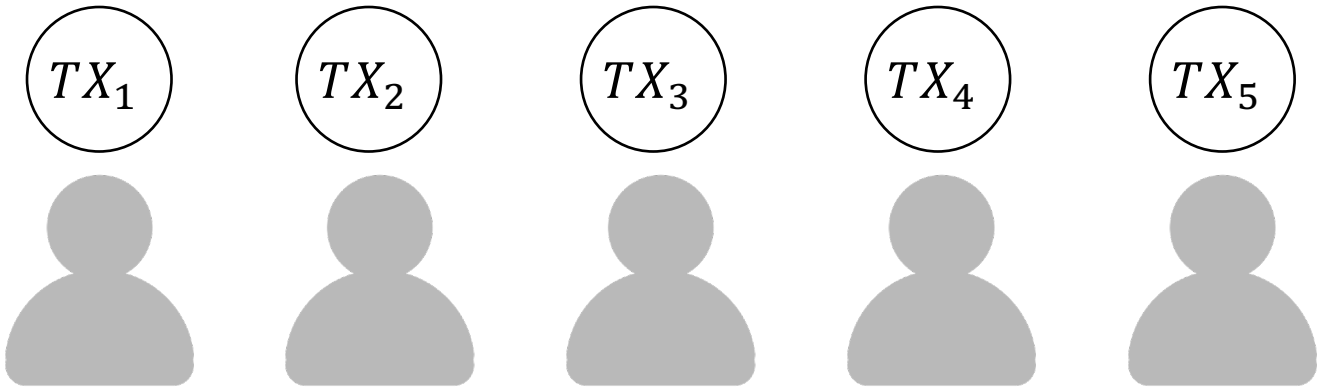
Transaction Fee Mechanism (TFM)



Which transactions to confirm?

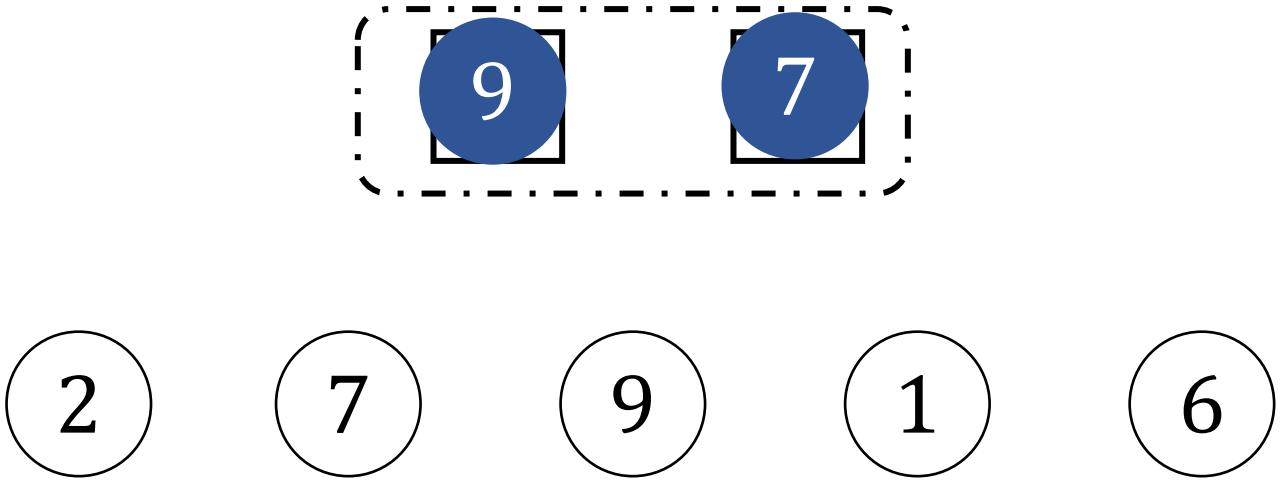
How much they pay?

How much miner gets?



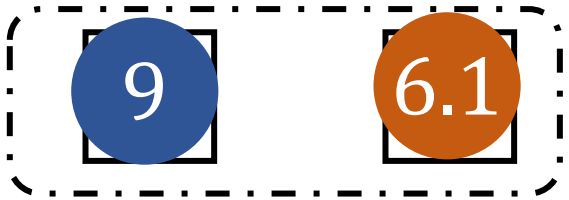
Bitcoin: first-price auction

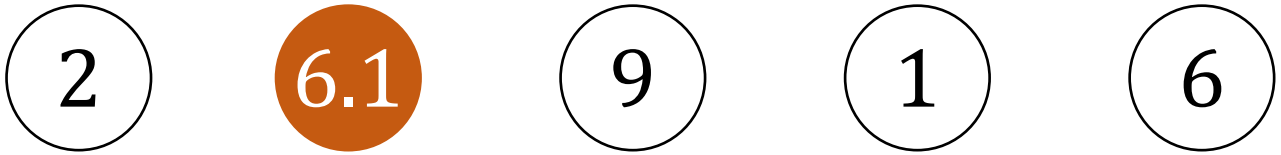
- Top k bids confirmed.
- Pay your own bid.
- All payments go to the miner.



Bitcoin: first-price auction

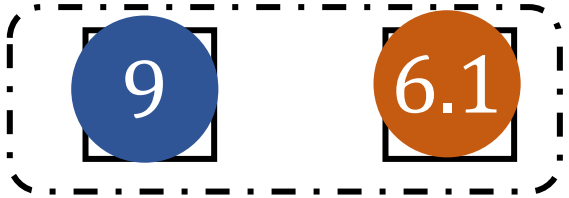
- Top k bids confirmed.
- Pay your own bid.
- All payments go to the miner.





Bitcoin: first-price auction

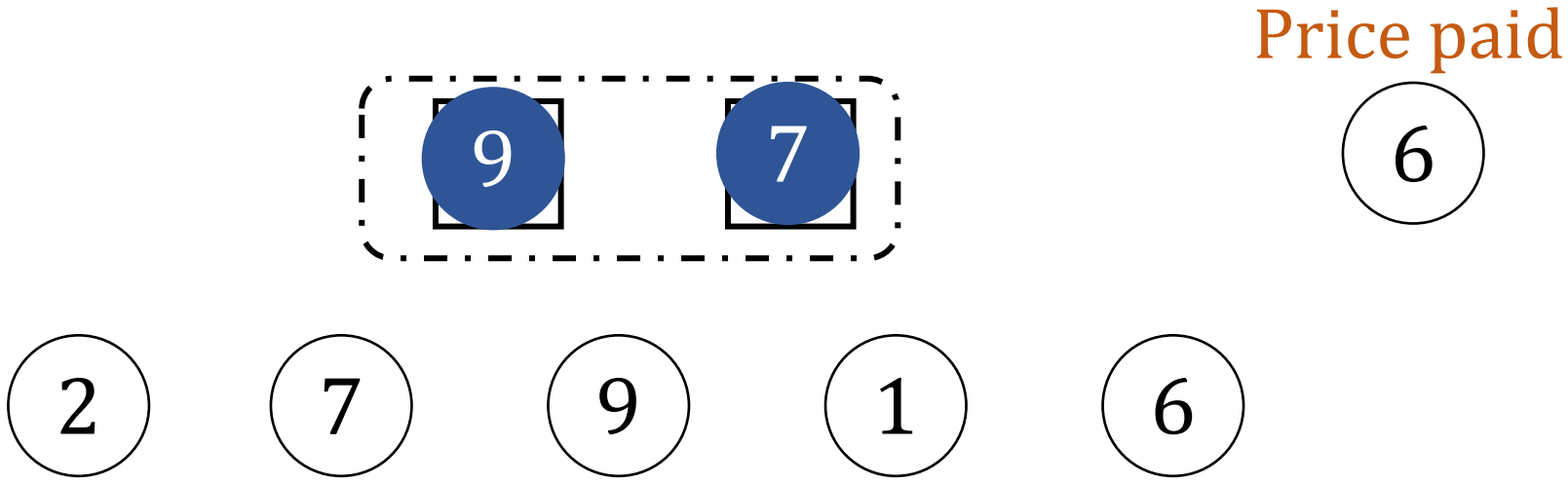
- Top k bids confirmed.
- Pay your own bid.
- All payments go to the miner.



☹ Encourage untruthful bidding

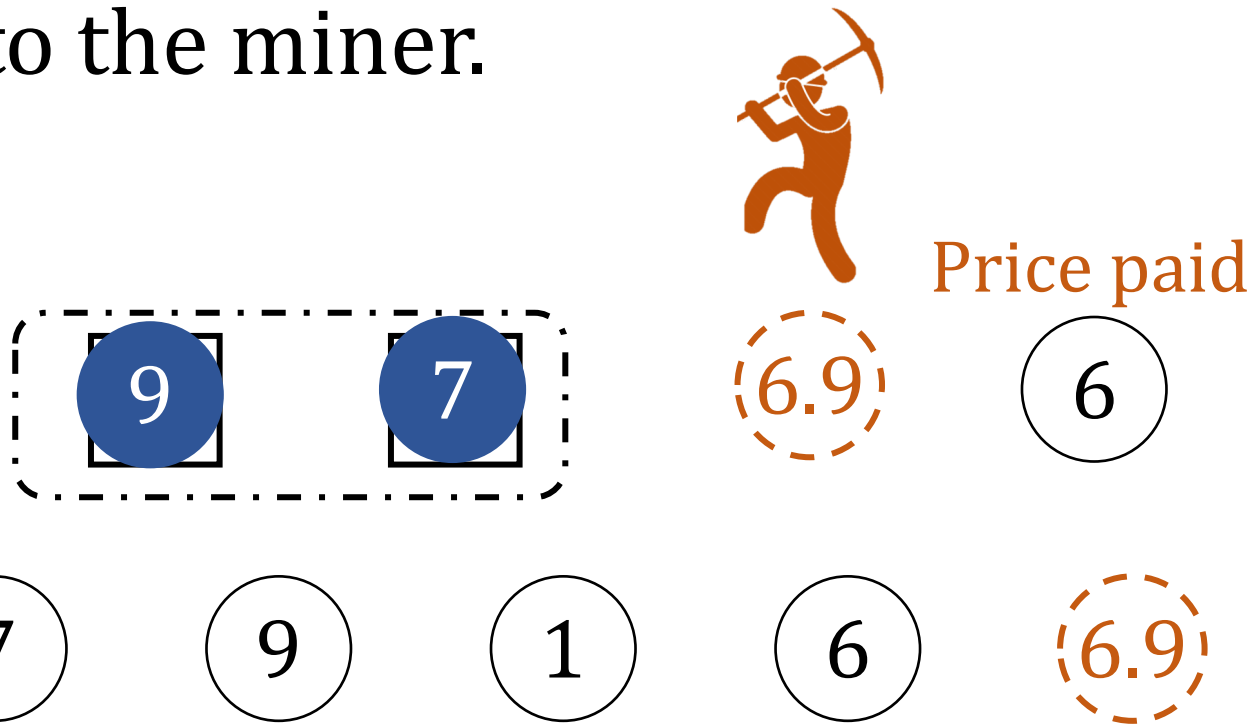
Classical mechanism: second-price auction

- Top k bids confirmed.
- Pay $(k+1)$-th bid.
- All payments go to the miner.



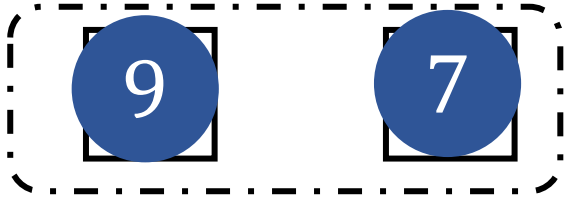
Classical mechanism: second-price auction

- Top k bids confirmed.
- Pay $(k+1)$-th bid.
- All payments go to the miner.



Classical mechanism: second-price auction

- Top k bids confirmed.
- Pay $(k+1)$-th bid.
- All payments go to the miner.



6.9

Price paid

6

Miner can deviate

What makes a dream TFM?

Three desired properties: strict-IC

User incentive compatibility (UIC):

- A user does not want to deviate

Miner incentive compatibility (MIC):

- The miner want to implement the mechanism honestly

c-side-contract-proofness (c-SCP):

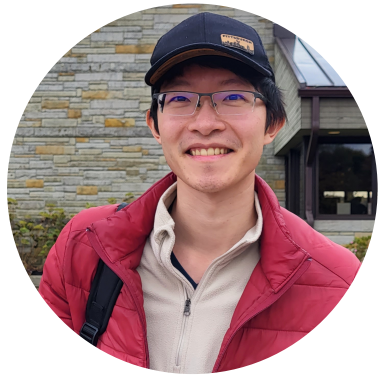
- A coalition of the miner and c user does not want to deviate

New in blockchain!

Can we have a dream mechanism?

EIP-1559 achieves all properties
if infinite block size

Tim Roughgarden: Transaction Fee Mechanism Design. EC'21

Finite block size:
No non-trivial TFM satisfies all three properties.

Hao Chung, Elaine Shi: Foundations of Transaction Fee Mechanism Design. SODA'23

Can crypto help circumvent the impossibility?

Our work

- MPC-assisted model: Mechanism is implemented by Multi-party computation (MPC).
- Approximate incentive compatibility: Strategic players can gain at most ϵ more utility by deviating.

Our work

- Feasibility
- Improve miner revenue.
- Improve social welfare.

Our result: finite block size

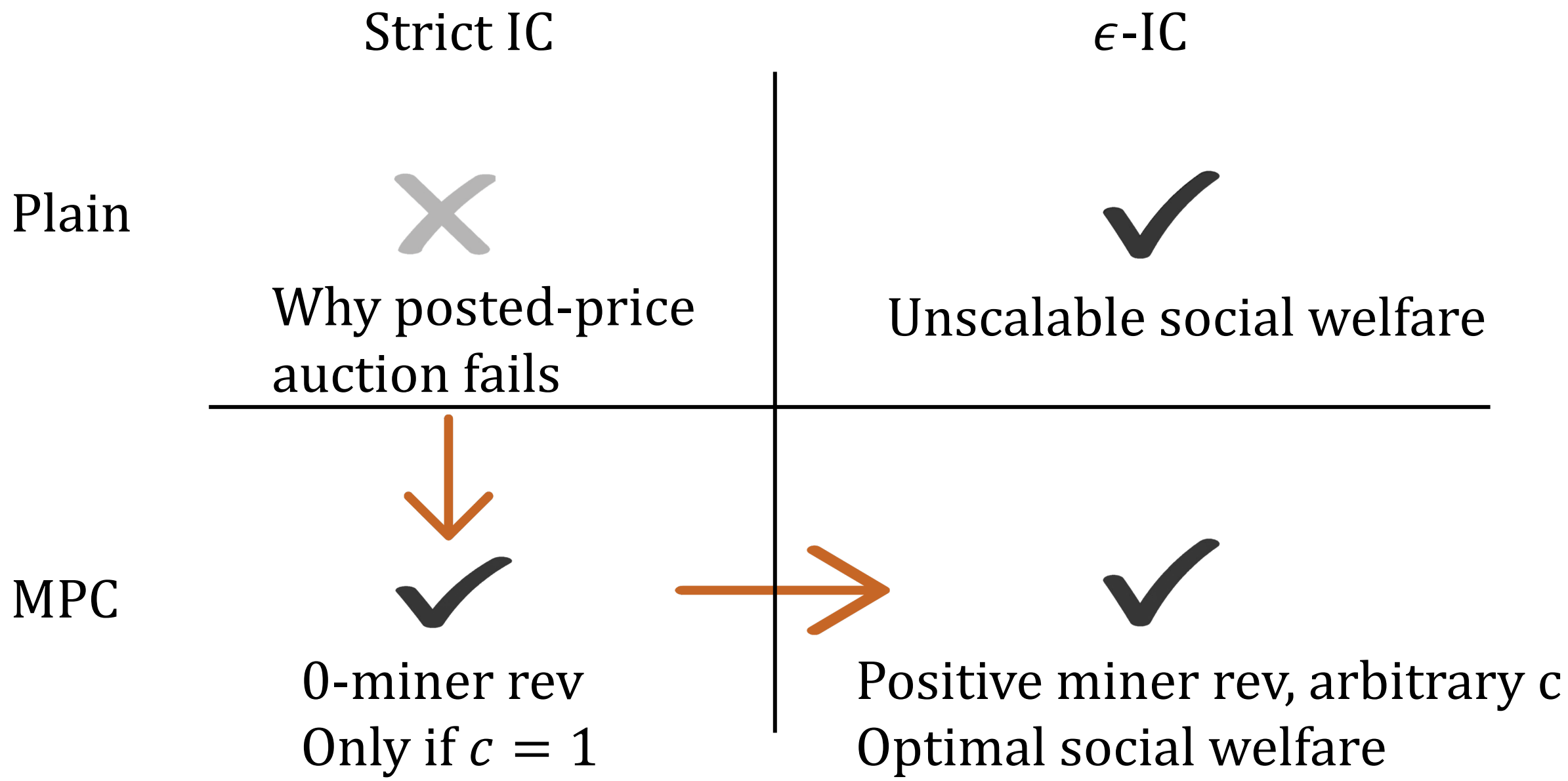
	Strict IC	ϵ-IC
Plain	✗ [CS23]	✓ Only if upper bound M Unscalable social welfare
MPC	✓ Only if $c = 1$	✓ Optimal social welfare if upper bound M

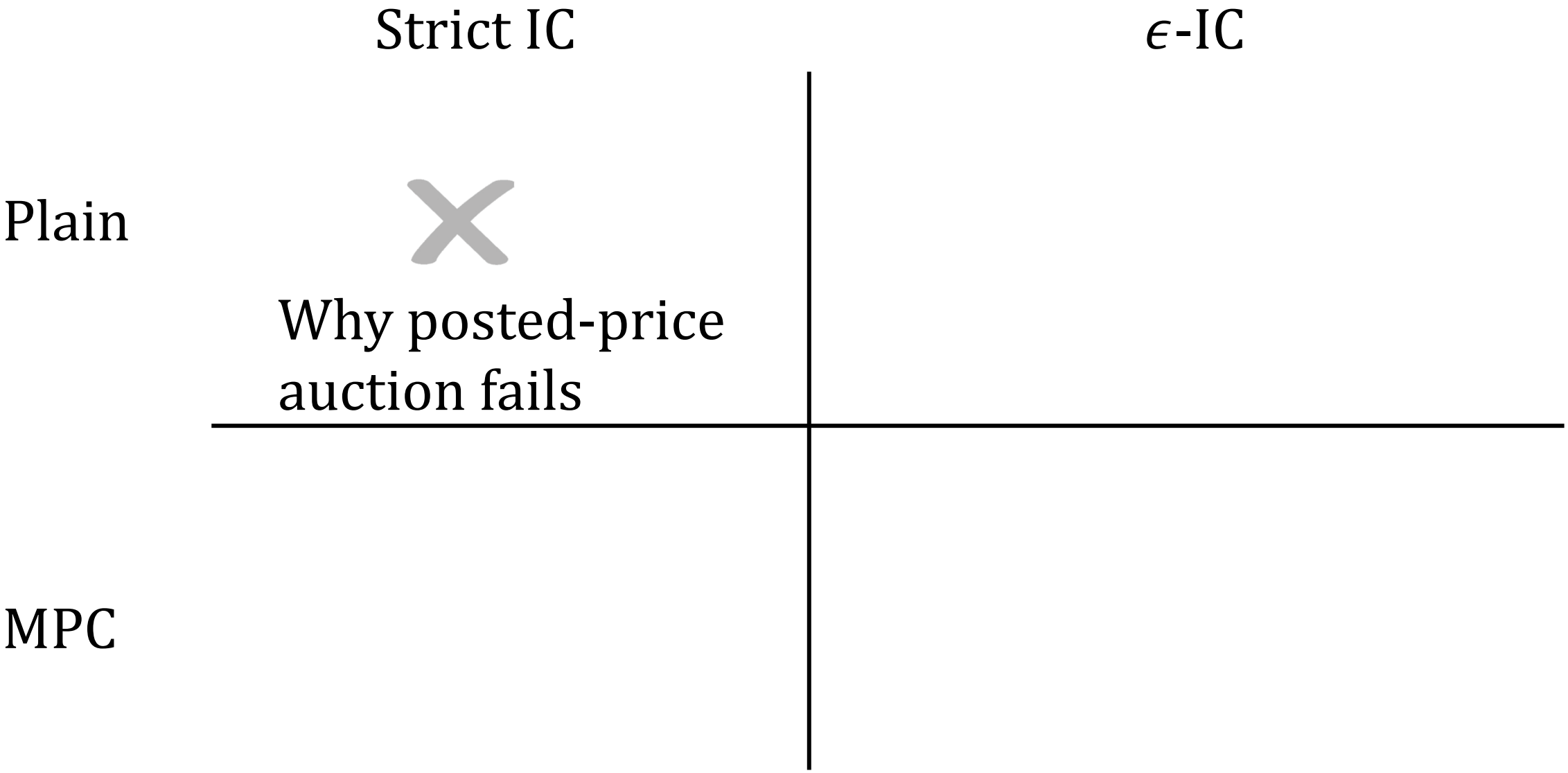
Our result: infinite block size

	Strict IC	ϵ-IC
Plain	0-miner rev	$\Theta(n \cdot (\epsilon + \sqrt{m\epsilon}))$-miner rev
MPC	0-miner rev	$\Theta(n \cdot (\epsilon + \sqrt{m\epsilon}))$-miner rev

All optimal!

Roadmap

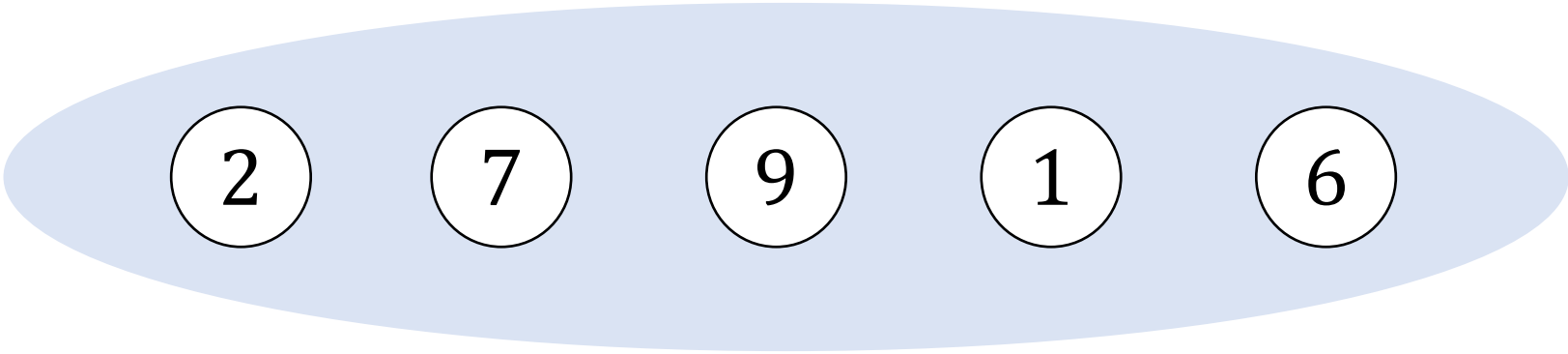

Strict IC
ϵ-IC
Plain
Why posted-price auction fails
Unscalable social welfare
MPC
0-miner rev
Only if $c = 1$
Positive miner rev, arbitrary c
Optimal social welfare

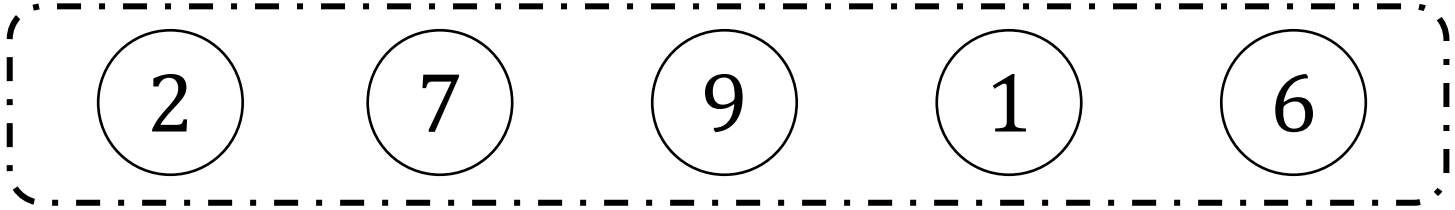

Strict IC
ϵ-IC
Plain
MPC
Why posted-price auction fails

Posted price auction: infinite block size

- Inclusion rule: all bids included.
- Confirmation rule: any bid $\geq r$ is confirmed.
- Payment rule: each confirmed bid pays r.
- Miner revenue rule: miner gets nothing.

Take $r = 4$

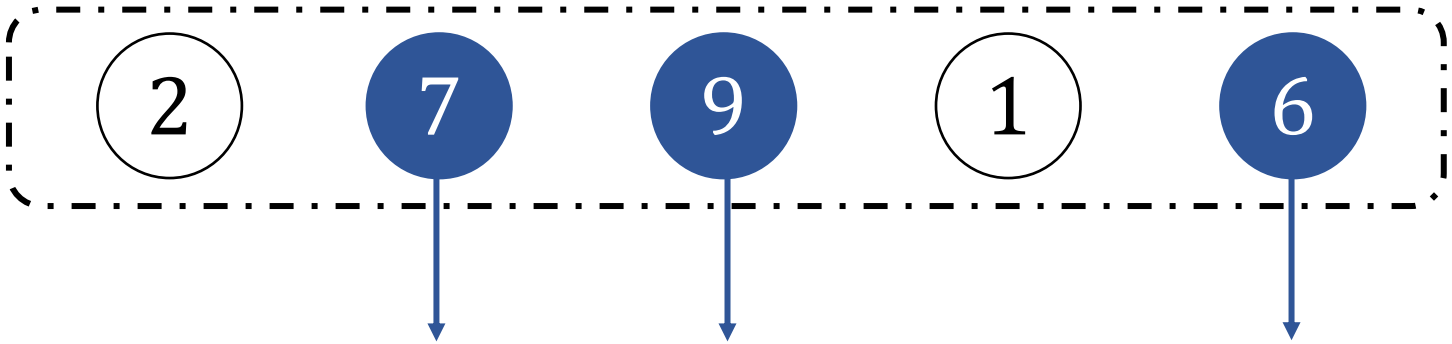




$r = 4$

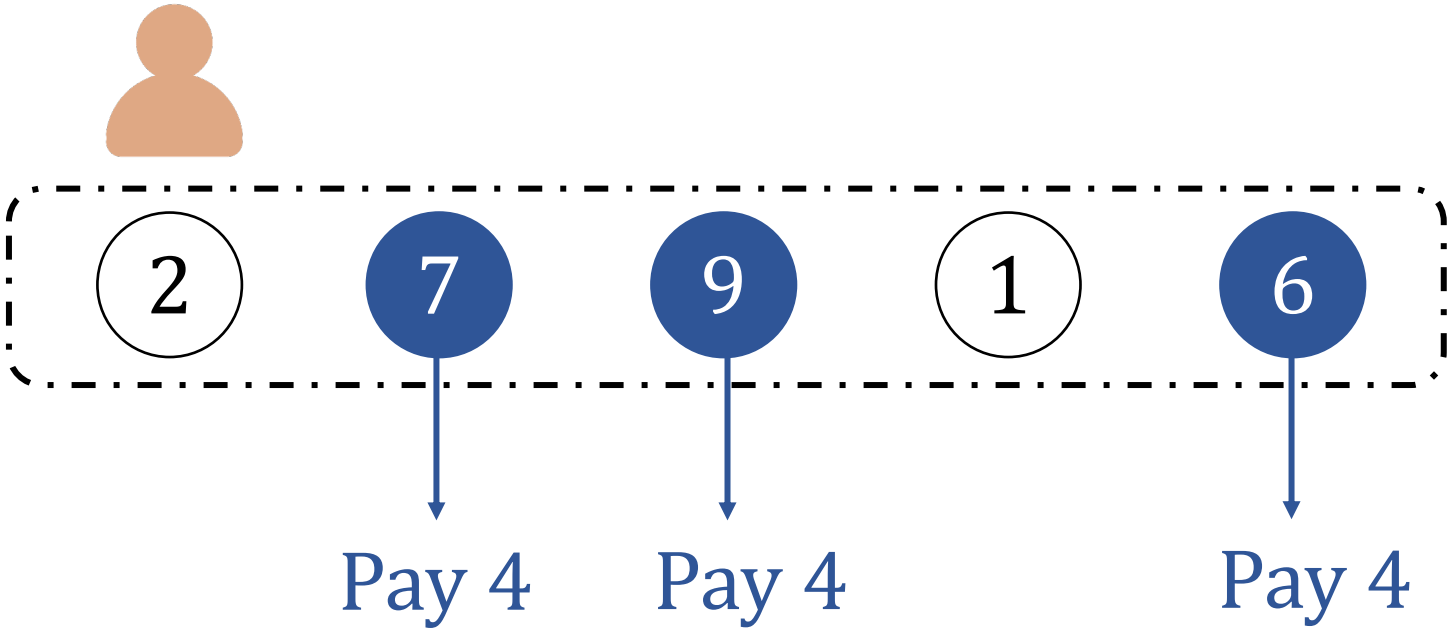
All included in the block

Implemented by



$r = 4$

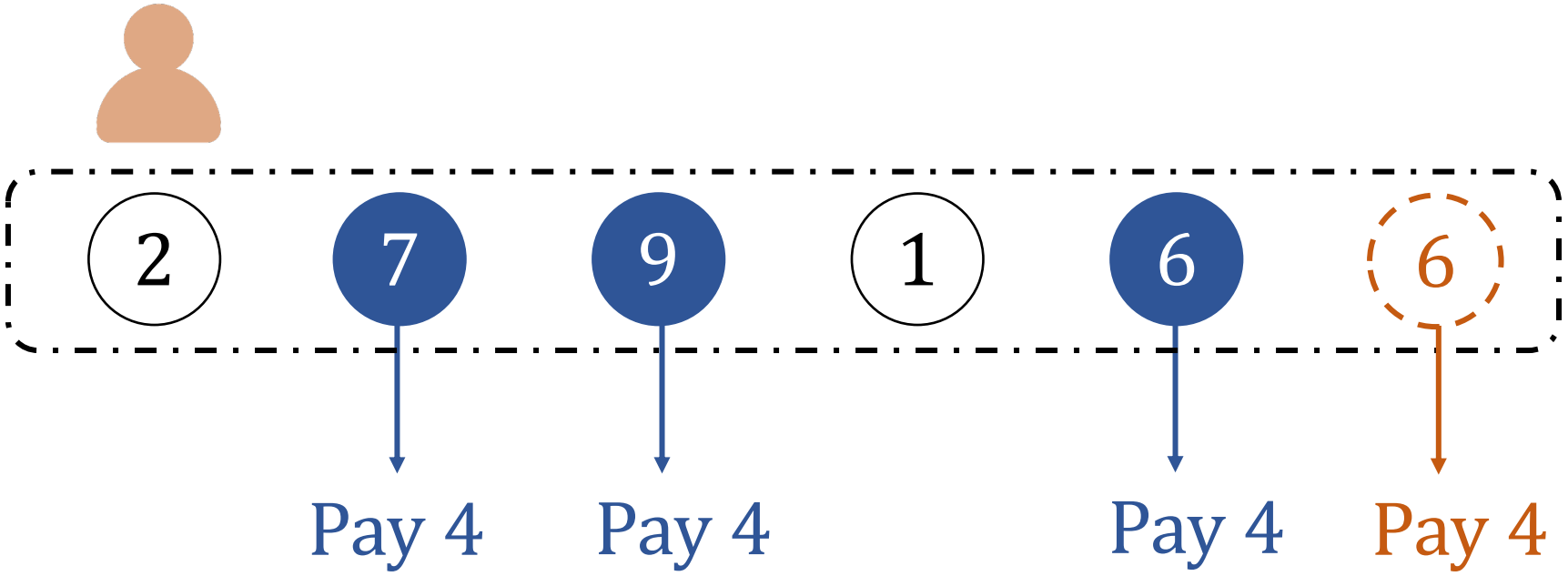
gets 0



$r = 4$

UIC

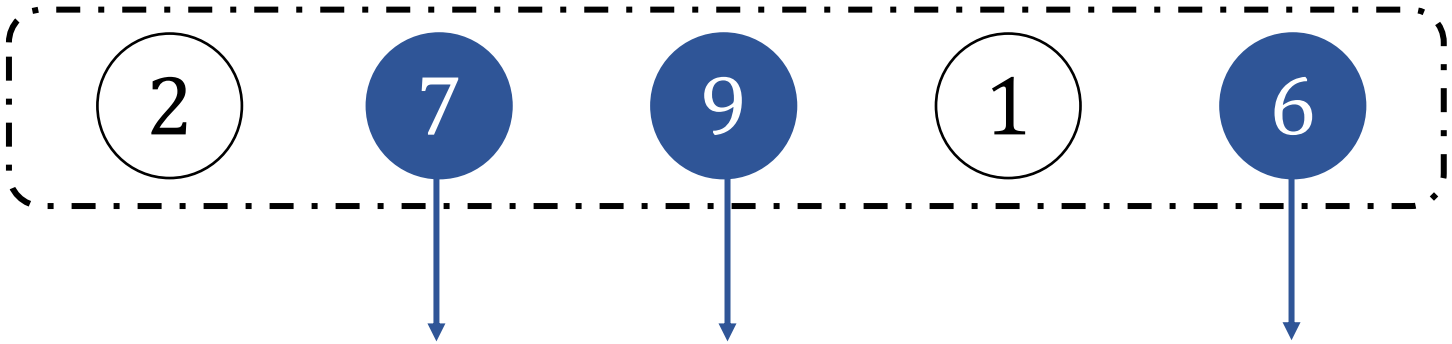
$$\text{User's util}: \begin{cases} \text{true value} - \text{payment}, & \text{if confirmed} \\ 0, & \text{if unconfirmed} \end{cases}$$



$r = 4$

UIC

Injecting doesn't help

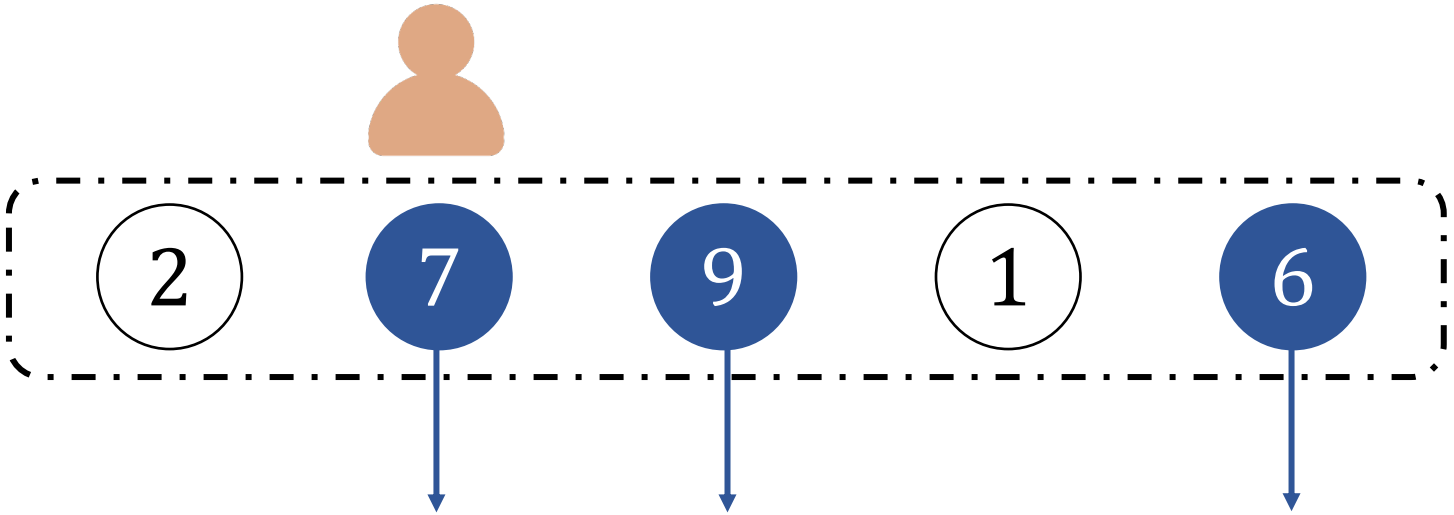


$r = 4$

gets 0

MIC

Miner's util: revenue − payment



$r = 4$

gets 0

1-SCP

Miner's utility doesn't change

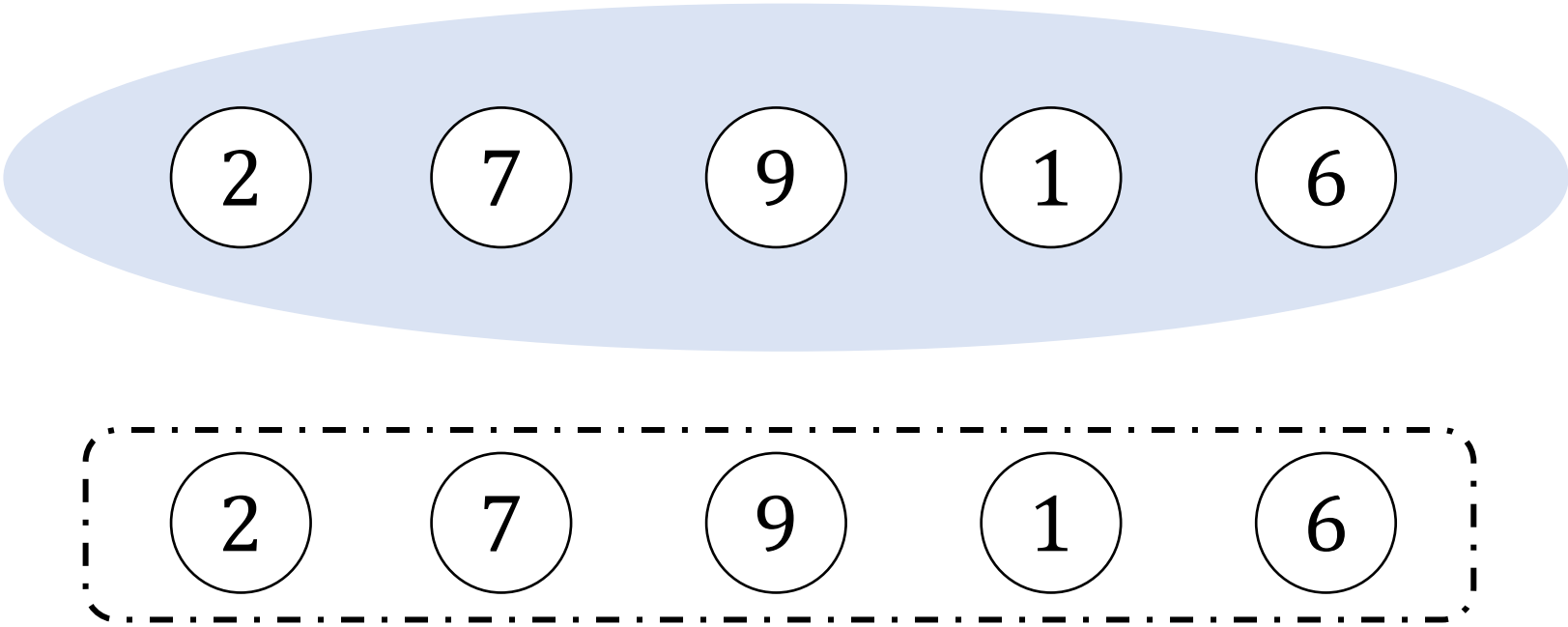
User's utility cannot increase

Posted price auction satisfies strict IC.

Assuming infinite block size

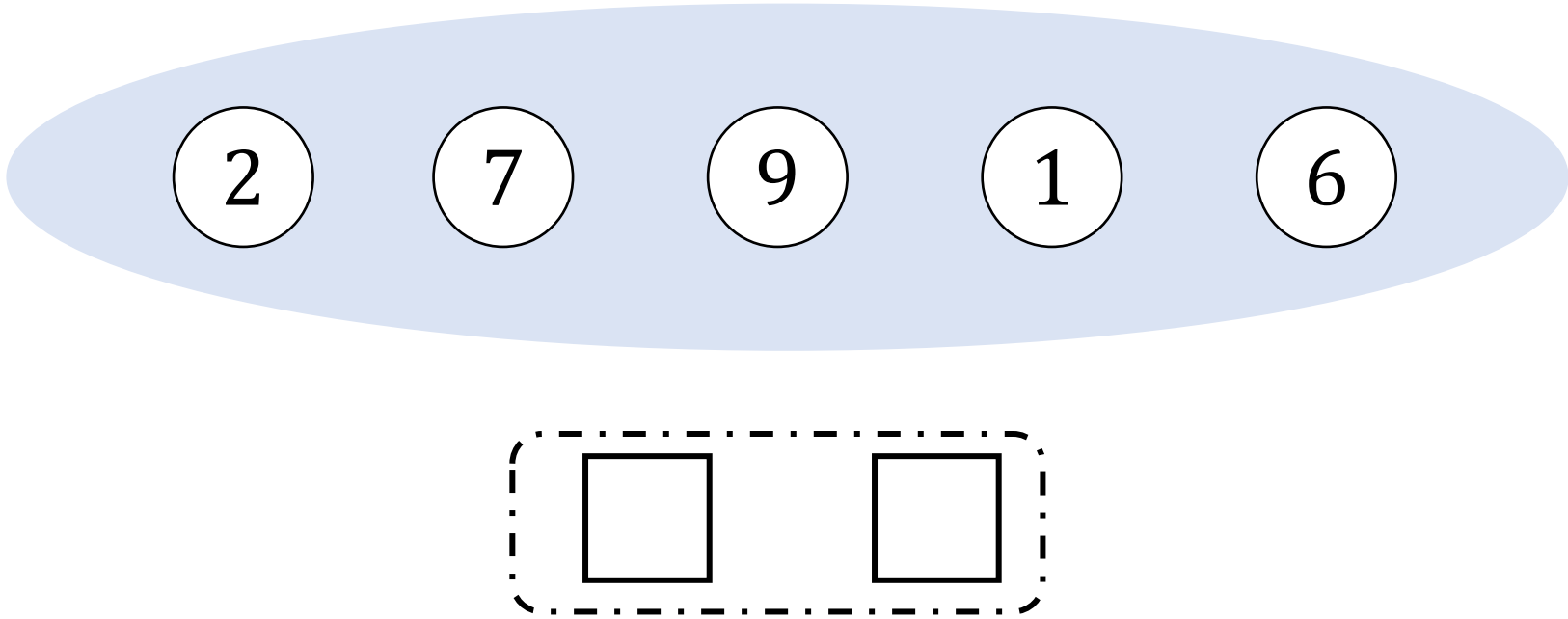
Finite block size?

Posted price auction fails for finite block size



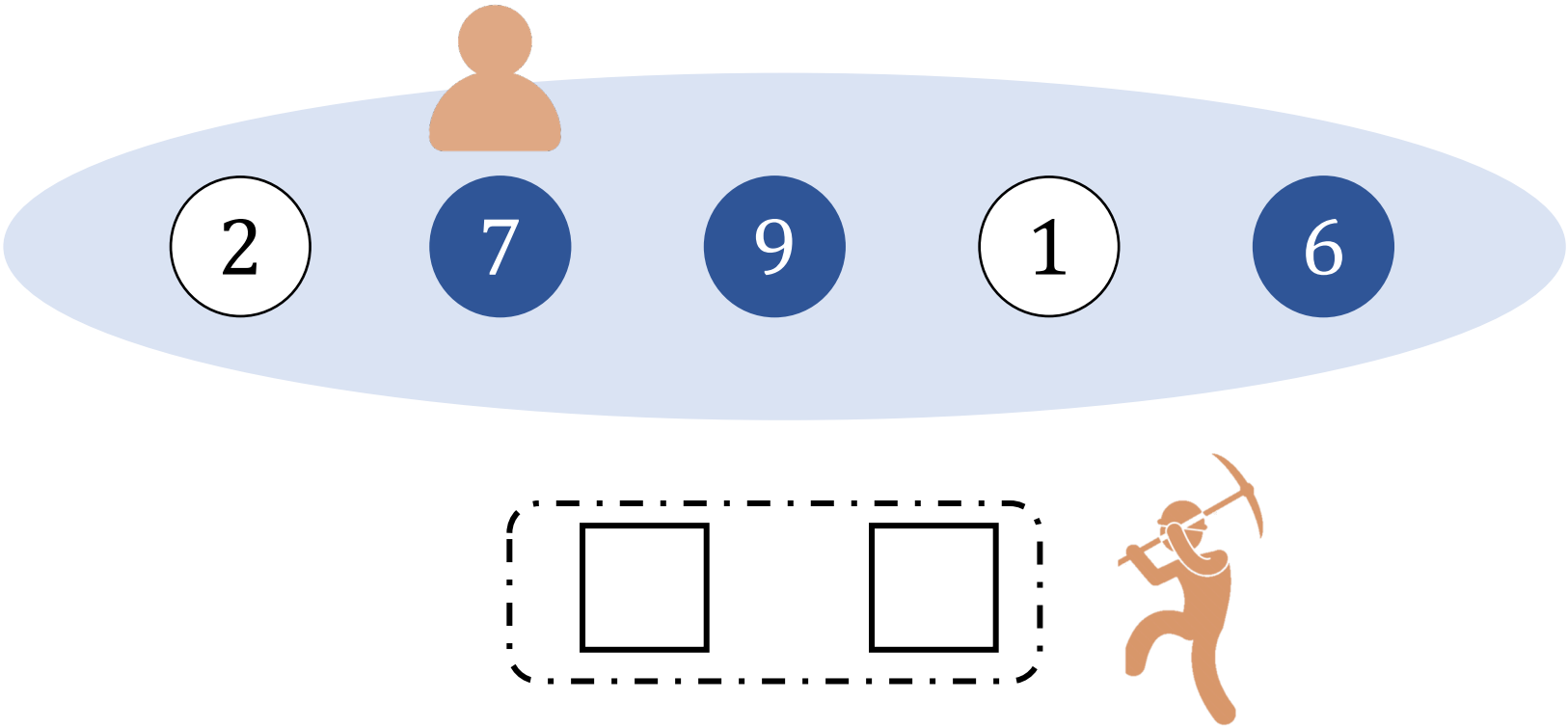
Infinite block size: all included

Posted price auction fails for finite block size



Finite block size: can only include two bids

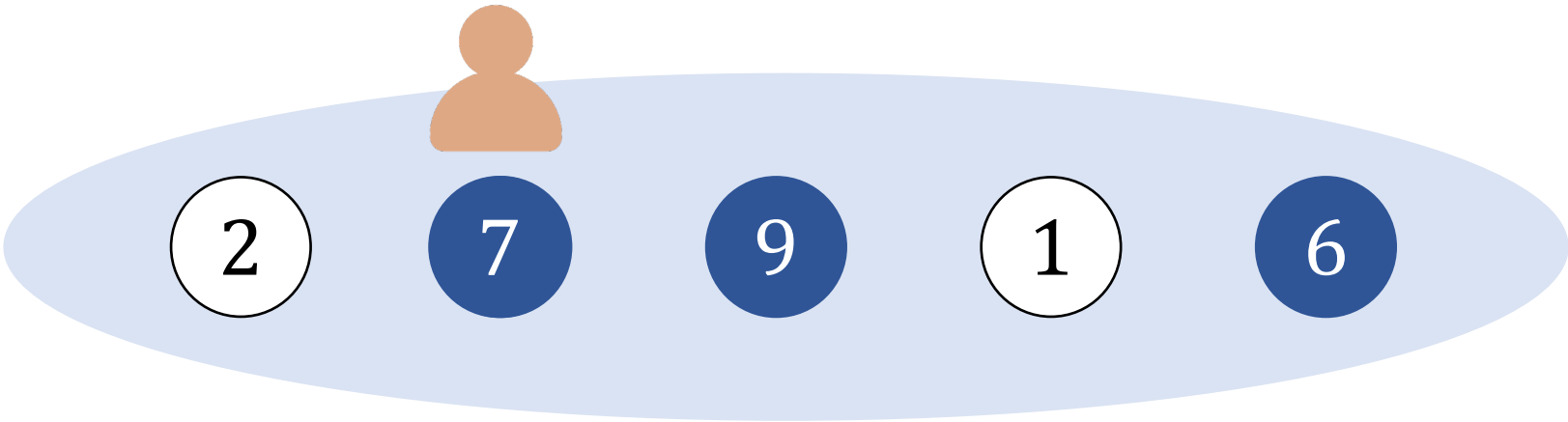
- Include random two bids ≥ 4.
- All bid included are confirmed and pay 4.
- Miner gets nothing.



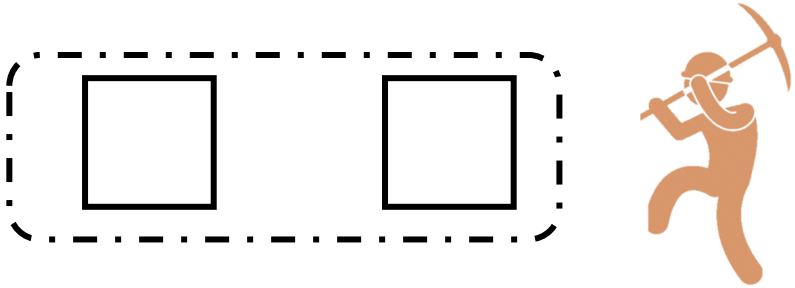
$r = 4$

1-SCP

Honest util: $\frac{2}{3} \cdot (7 - 4) = 2$



$r = 4$



always include 7

1-SCP

Stategic util: $1 \cdot (7 - 4) = 3$

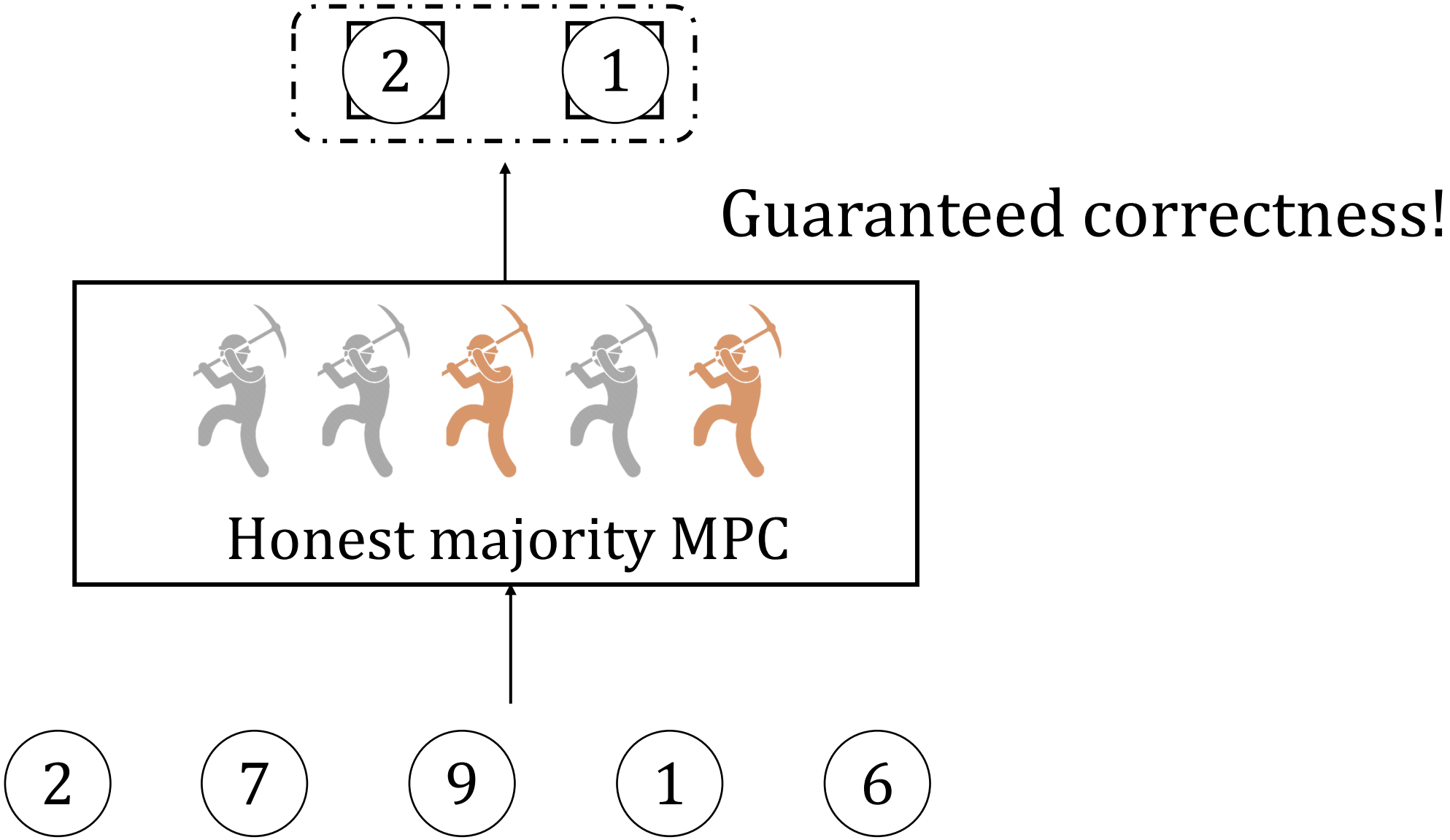
No dream mechanism for finite block size

Miner implements inclusion rule!

Force honest inclusion

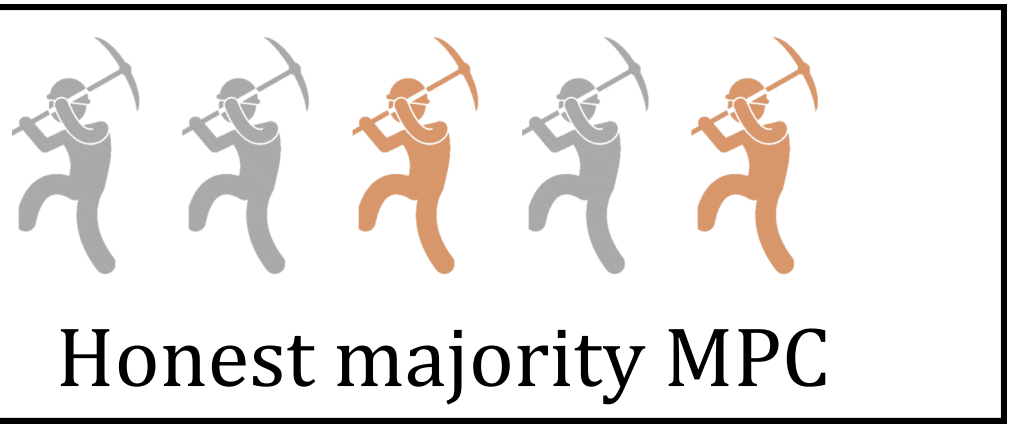
	Strict IC	ϵ-IC
Plain	 Why EIP-1559 fails	
MPC		

MPC-assisted model



MPC-assisted posted-price auction

- Include random two bids ≥ 4.
- All bid included are confirmed and pay 4.
- Miner gets nothing.



1-SCP Honest implementation + UIC

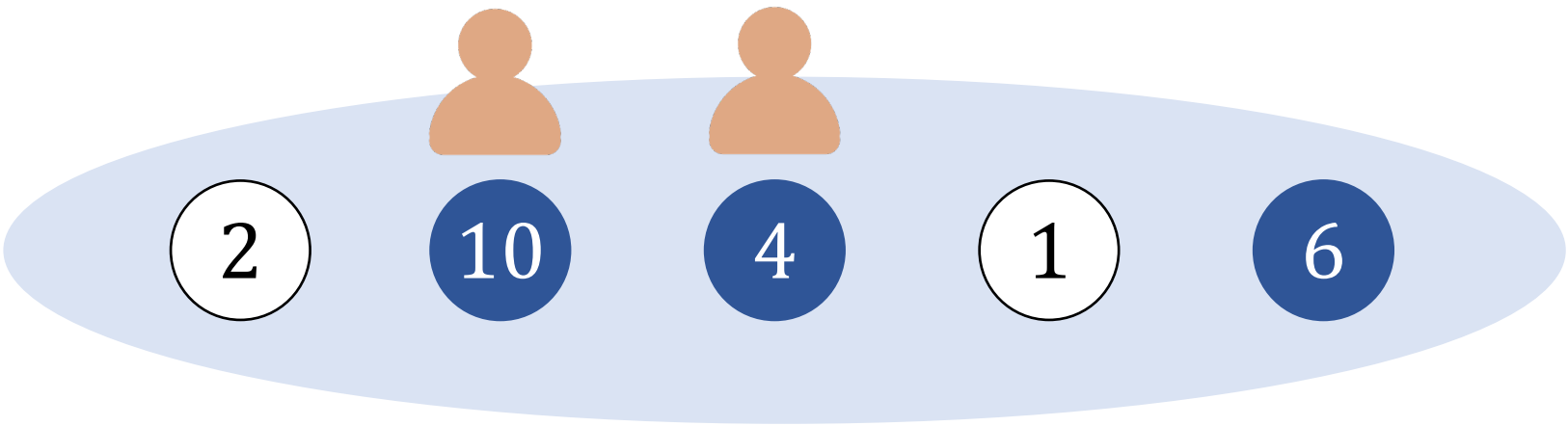
✓

Dream TFM in MPC-assisted model

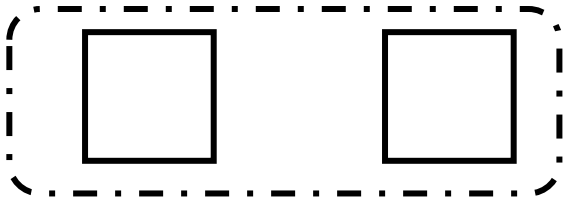
0-miner revenue

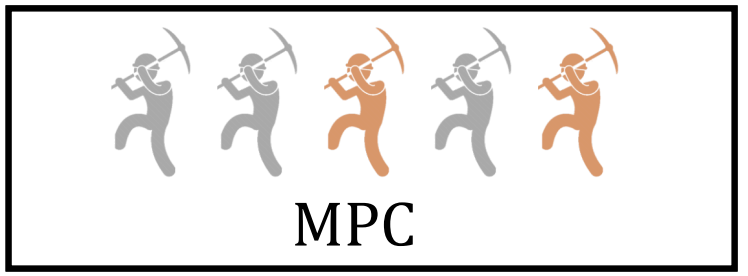
Only work for $c = 1$

MPC-assisted posted price fails for c = 2



$r = 4$

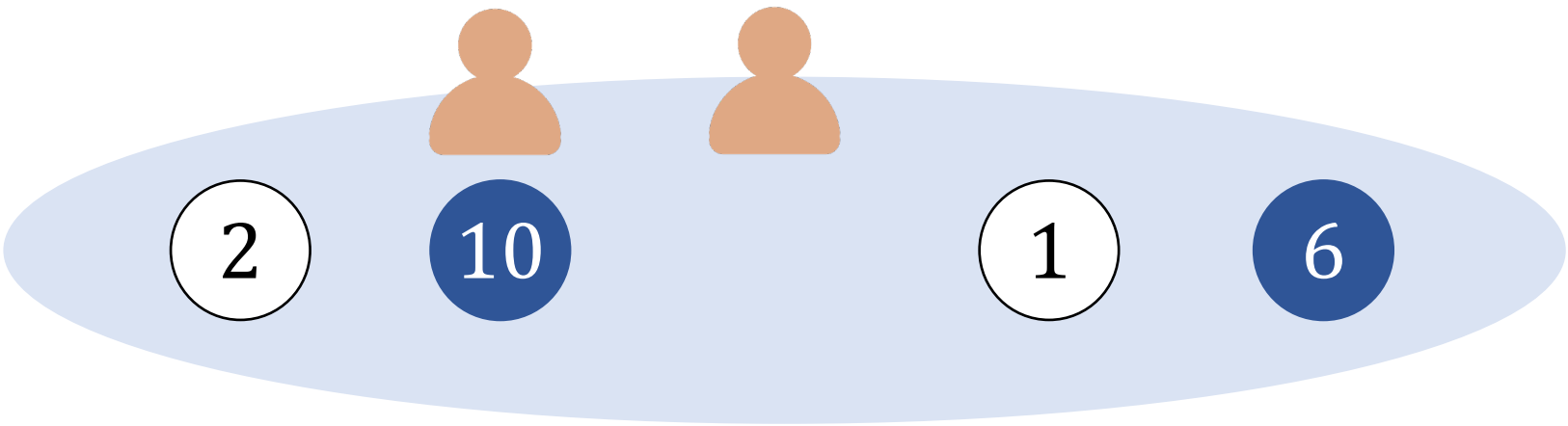




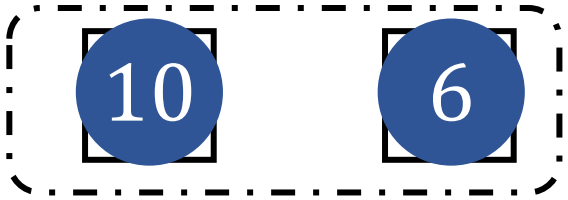
2-SCP

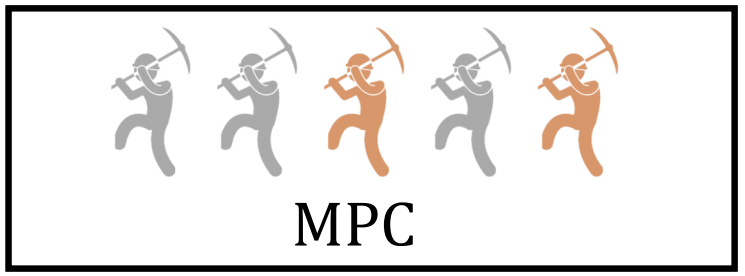
Honest joint util: $\frac{2}{3} \cdot (10 - 4) = 4$

MPC-assisted posted price fails for c = 2



$r = 4$





2-SCP

Strategic joint util: $1 \cdot (10 - 4) = 6$


0-miner revenue


c=1

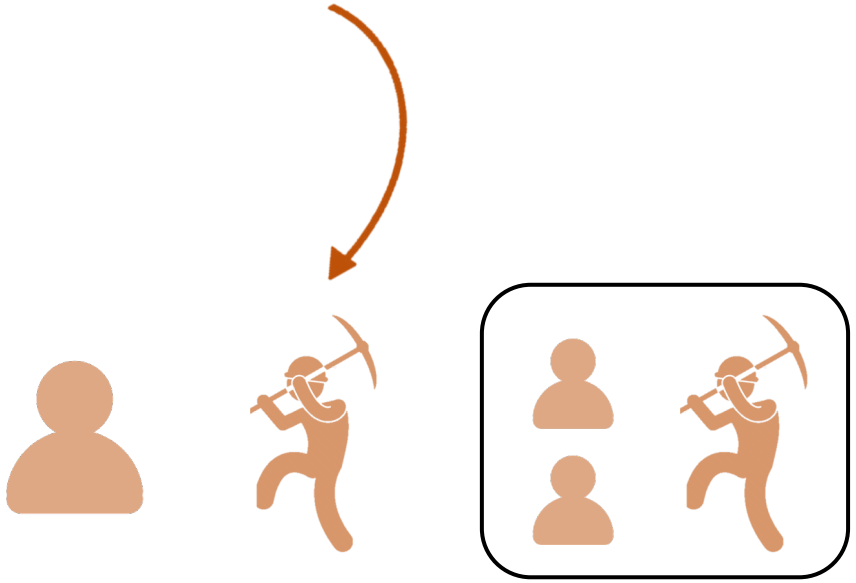
} Inherent

Can we get rid of these drawbacks?


Approximate incentive compatibility

ϵ-incentive compatibility

Strategic players can gain at most ϵ more utility by deviating.



	Strict IC	ϵ-IC
Plain	✗ Why EIP-1559 fails	
MPC	✓ 0-miner rev Only for $c = 1$	✓ Optimal social welfare

MPC-assisted diluted posted price auction

- All bids $\geq r$ as candidates.
- If # candidates t $< T = \sqrt{\frac{kM}{\epsilon}}$, add $T - t$ dummy bids.

Upper bound

- Choose random k bids from T diluted bids, confirm non-dummy bids. Each confirmed bid pays r.
- Miner gets $\frac{\epsilon}{2}$ from each confirmed bid.

Take $M = 10, \epsilon = 1$

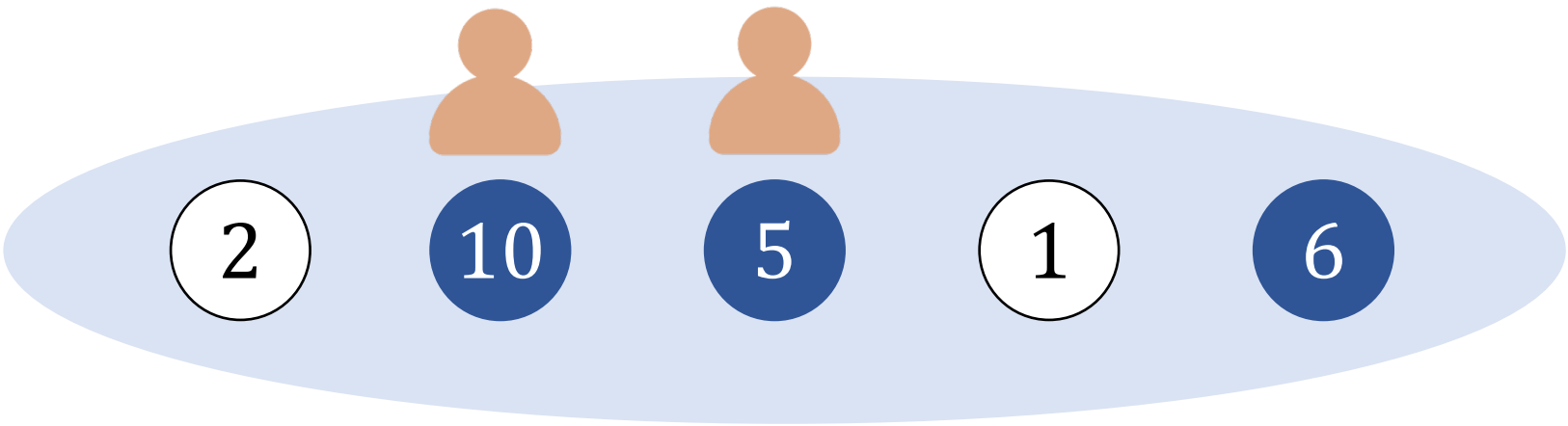
$r = 5$

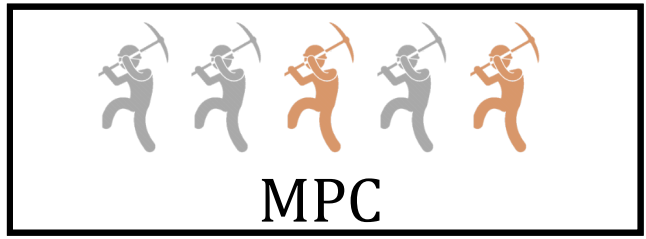
MPC-assisted diluted posted price auction

- All bids ≥ 5 as candidates.
- If # candidates t < 4, add $4 - t$ dummy bids.
- Choose random k bids from 4 diluted bids, confirm non-dummy bids. Each confirmed bids pays 5.
- Miner gets $\frac{\epsilon}{2}$ from each confirmed bid.

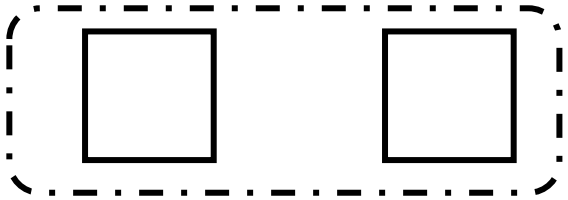
Take $M = 10, \epsilon = 1$

$r = 5$



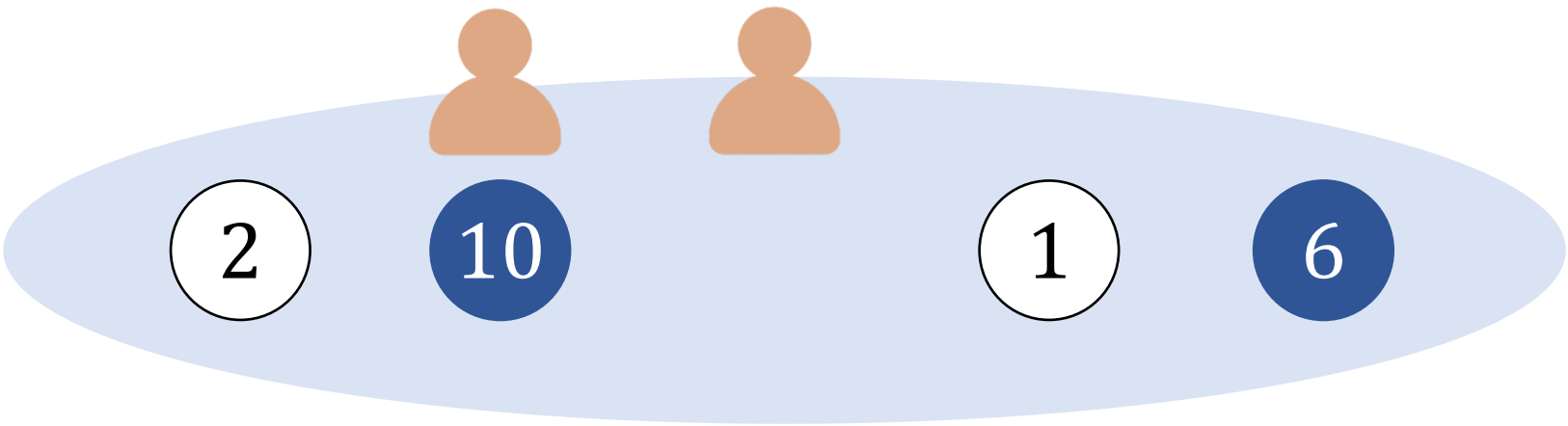


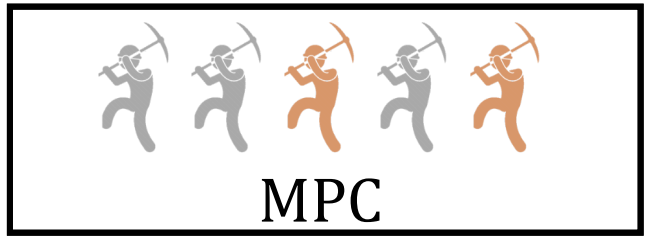
Dilution



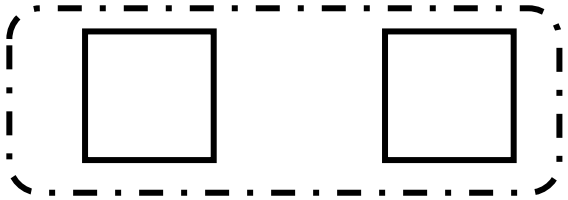
$r = 5$

Dilution to 4



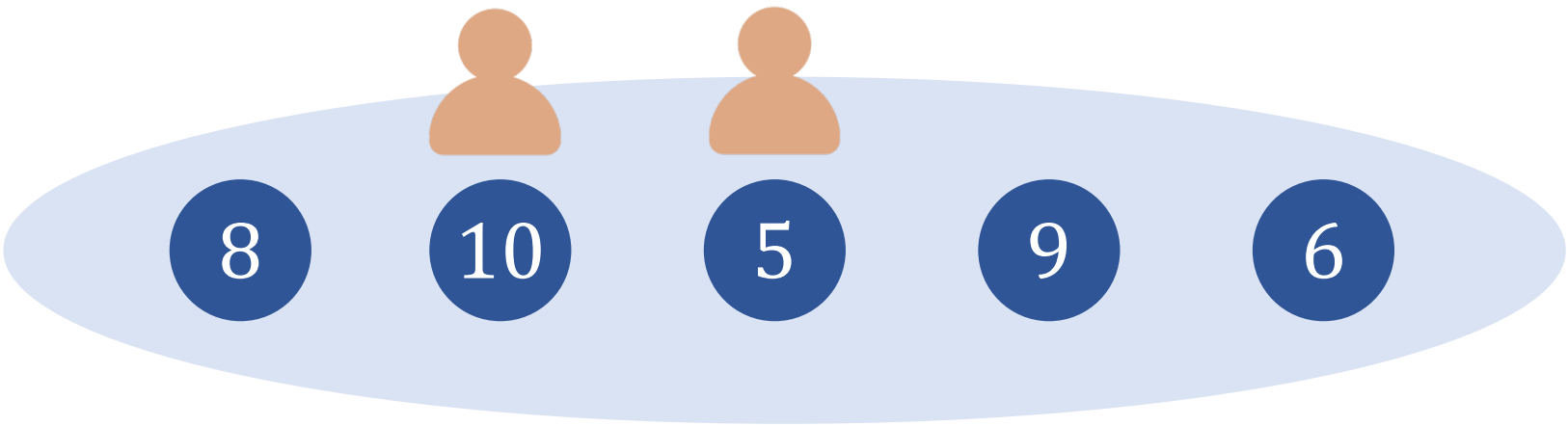


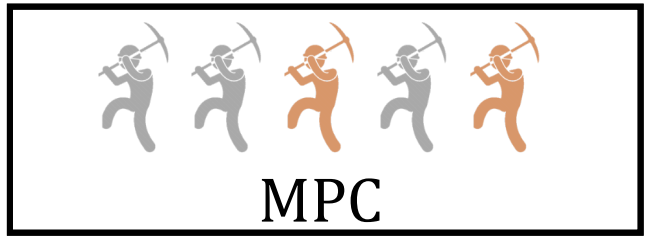
Dilution



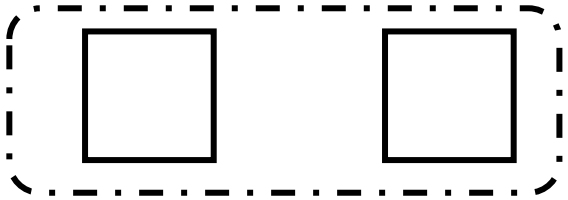
$r = 5$

Dilution to 4





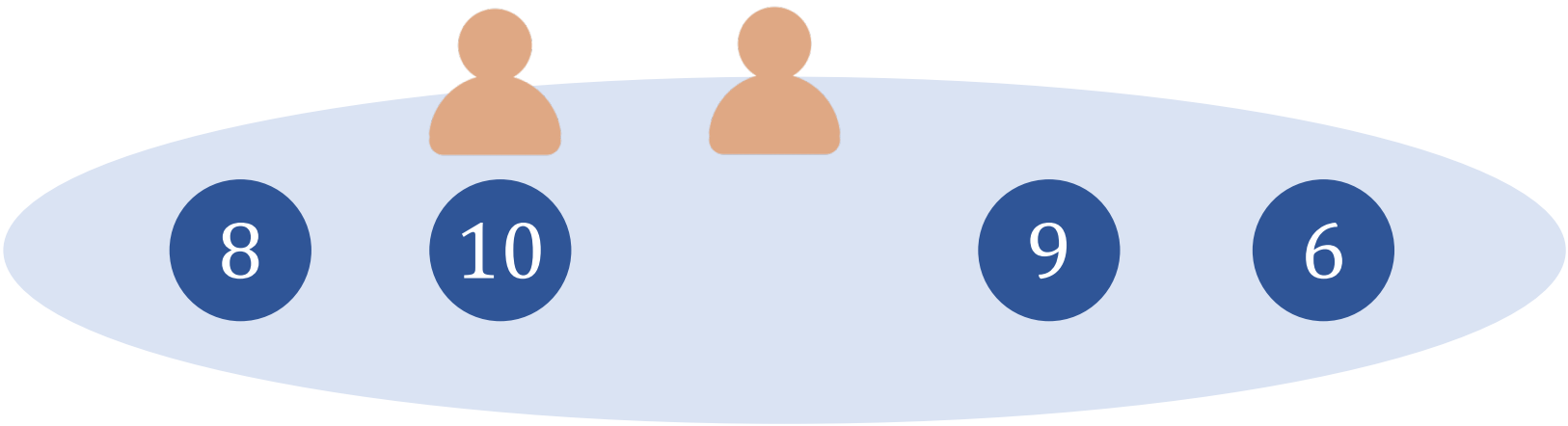
No dilution

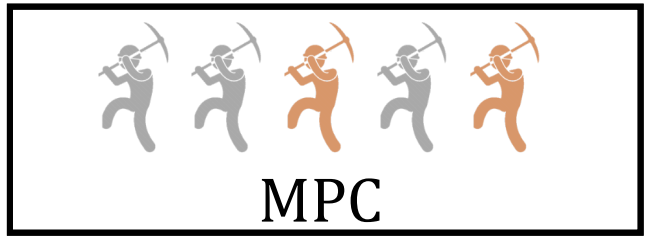


$r = 5$

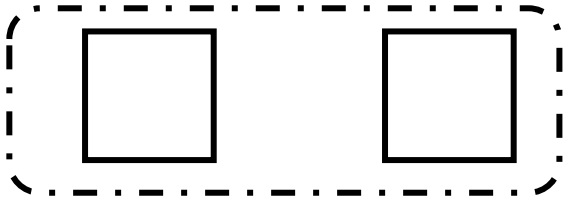
Dilution to 4

Prob of friend being confirmed: $\frac{2}{5}$





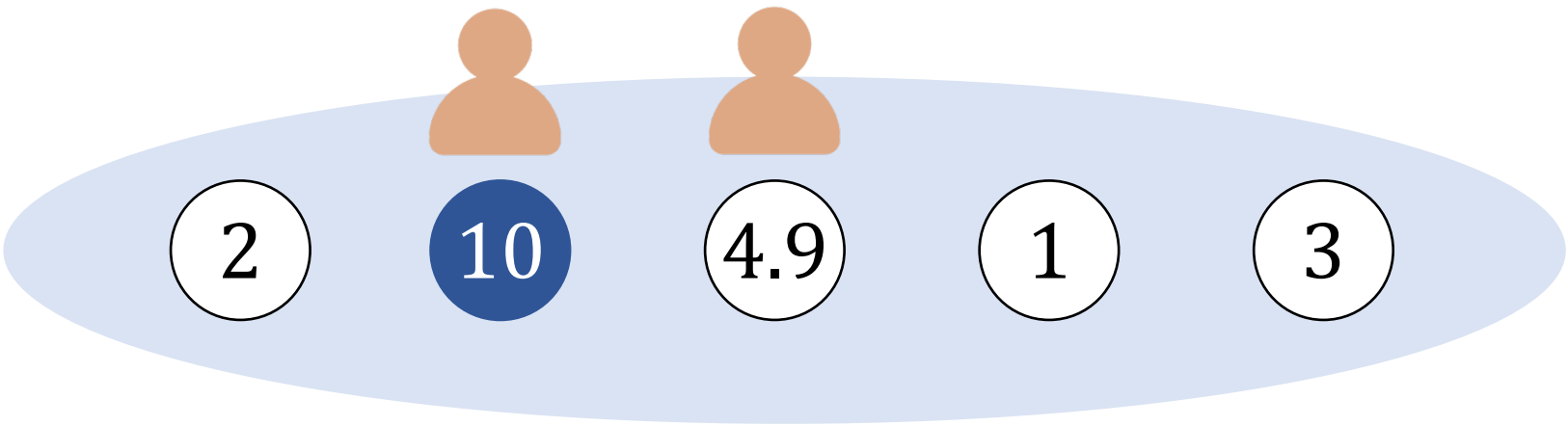
No dilution

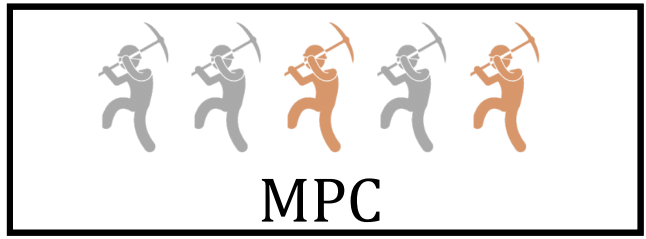


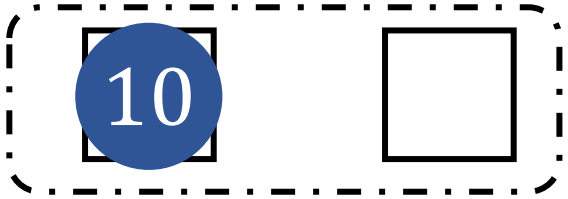
$r = 5$

Dilution to 4

Prob of friend being confirmed: $\frac{2}{5} \rightarrow \frac{1}{2}$, utility increase 1.



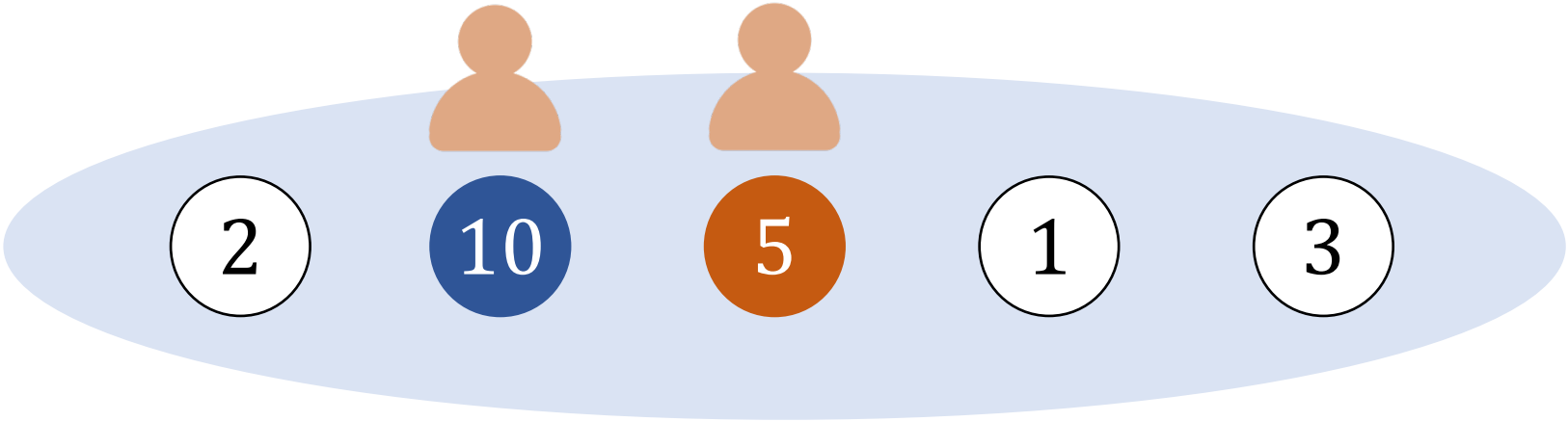


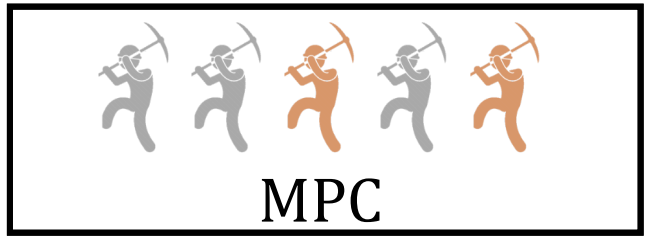


Approx 2-SCP

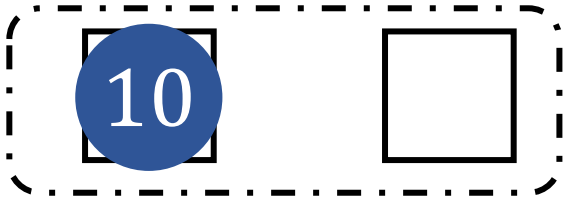
$r = 5$

Dilution to 4





Approx 2-SCP



$r = 5$

Dilution to 4

Miner gets $\frac{\epsilon}{2}$ more expected revenue.

MPC-assisted diluted posted price auction

When lots of users has true value $\geq \frac{2}{3} M$

- k users gets $\Theta(M)$ utility
- Miner gets $\Theta(k\epsilon)$ revenue

$\Theta(kM)$-social welfare
Optimal!

	Strict IC	ϵ-IC
Plain	✗ Why EIP-1559 fails	✓ Unscalable social welfare
MPC	✓ 0-miner rev Only for $c = 1$	✓ Optimal social welfare

Unscalable social welfare

If a TFM satisfies ϵ-IC in the plain model,

the social welfare is at most $\Theta_k\left(\epsilon \log\left(1+\frac{M}{\epsilon}\right)\right)$

Conclusion

MPC-assisted model

+

Approximate incentive compatibility

Feasibility + optimal social welfare

More in paper: finite block size

	Strict IC	ϵ-IC
Plain	✗	✗ If unbounded true value ✓ If bounded true value No scalability
MPC	✓ $c = 1$ ✗ $c \geq 2$	✓ If bounded true value Optimal social welfare

More in paper: infinite block size

	Strict IC	ϵ-IC
Plain	0-miner rev	$\Theta(n \cdot (\epsilon + \sqrt{m\epsilon}))$-miner rev
MPC	0-miner rev	$\Theta(n \cdot (\epsilon + \sqrt{m\epsilon}))$-miner rev

All optimal!

Open question

- Practical mechanism
- Universal mechanism

Thanks!

eprint: 2022/1294
kew2@andrew.cmu.edu