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?

$k$ slots
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.

Price paid: 6.9
Miner's payment: 6
Top bids: 9, 7
Remaining bids: 2, 7, 9, 1, 6
Classical mechanism: second-price auction

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

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
Can we have a dream mechanism?

EIP-1559 achieves all properties if infinite block size
Finite block size:
No non-trivial TFM satisfies all three properties.
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 $\epsilon$ more utility by deviating.
Our work

- Feasibility
- Improve miner revenue.
- Improve social welfare.
Our result: finite block size

<table>
<thead>
<tr>
<th></th>
<th>Strict IC</th>
<th>ε-IC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plain</td>
<td><img src="Image" alt="X" /> [CS23] Only if upper bound M Unscalable social welfare</td>
<td><img src="Image" alt="✓" /> Only if upper bound M Unscalable social welfare</td>
</tr>
<tr>
<td>MPC</td>
<td><img src="Image" alt="✓" /> Only if $c = 1$</td>
<td><img src="Image" alt="✓" /> Optimal social welfare if upper bound M</td>
</tr>
</tbody>
</table>
Our result: infinite block size

<table>
<thead>
<tr>
<th></th>
<th>Strict IC</th>
<th>ε-IC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plain</td>
<td>0-miner rev</td>
<td>$\Theta(n \cdot (\epsilon + \sqrt{m\epsilon}))$-miner rev</td>
</tr>
<tr>
<td>MPC</td>
<td>0-miner rev</td>
<td>$\Theta(n \cdot (\epsilon + \sqrt{m\epsilon}))$-miner rev</td>
</tr>
</tbody>
</table>

All optimal!
<table>
<thead>
<tr>
<th>Method</th>
<th>Strict IC</th>
<th>(\epsilon)-IC</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Plain</strong></td>
<td>Why posted-price auction fails</td>
<td>Unscalable social welfare</td>
</tr>
<tr>
<td><strong>MPC</strong></td>
<td>0-miner rev Only if (c = 1)</td>
<td>Positive miner rev, arbitrary (c) Optimal social welfare</td>
</tr>
</tbody>
</table>

**Roadmap**
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 $r = 4$
All included in the block

Implemented by
gets $0$

$r = 4$
User’s util : \[
\begin{cases}
\text{true value} - \text{payment}, & \text{if confirmed} \\
0, & \text{if unconfirmed}
\end{cases}
\]
Injecting doesn’t help

\[ r = 4 \]
Miner's util: revenue − payment

$\text{MIC } r = 4$

gets 0

Pay 4  Pay 4  Pay 4
A miner's utility doesn't change. User's utility cannot increase.

$r = 4$
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.
1-SCP

Honest util: \( \frac{2}{3} \cdot (7 - 4) = 2 \)
$1 - SCP$

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

always include 7

$r = 4$
No dream mechanism for finite block size

Miner implements inclusion rule!

Force honest inclusion
Why EIP-1559 fails

- Strict IC
- MPC
MPC-assisted model

Guaranteed correctness!

Honest majority MPC
MPC-assisted posted-price auction

- Include random two bids \( \geq 4 \).
- All bid included are confirmed and pay 4.
- Miner gets nothing.

Honest majority MPC

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 $c = 2$

2-SCP

Honest joint util: $\frac{2}{3} \cdot (10 - 4) = 4$
MPC-assisted posted price fails for $c = 2$

\[ \begin{align*}
1 \cdot (10 - 4) &= 6
\end{align*} \]
0-miner revenue

Inherent

c=1

Can we get rid of these drawbacks?

Approximate incentive compatibility
Strategic players can gain at most $\epsilon$ more utility by deviating.
Why EIP-1559 fails

- **Plain**
  - **Strict IC**: False
  - Why EIP-1559 fails

- **MPC**
  - **Strict IC**: True
  - 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.

• 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 $\geq 5$ 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

MPC

\[ r = 5 \]
Dilution to 4
Dilution to 4

$r = 5$
No dilution

Prob of friend being confirmed: $\frac{2}{5}$
No dilution

Prob of friend being confirmed: \( \frac{2}{5} \rightarrow \frac{1}{2} \), utility increase 1.
Approx 2-SCP

\[ \frac{10}{r} = 5 \]

Dilution to 4

MPC
Approx 2-SCP

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!
Why EIP-1559 fails: Unscalable social welfare

0-miner rev
Only for $c = 1$

Optimal social welfare
Unscalable social welfare

If a TFM satisfies $\epsilon$-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

<table>
<thead>
<tr>
<th></th>
<th>Strict IC</th>
<th>$\epsilon$-IC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plain</td>
<td>$\times$</td>
<td>$\times$ If unbounded true value</td>
</tr>
<tr>
<td></td>
<td>$c = 1$</td>
<td>If bounded true value</td>
</tr>
<tr>
<td></td>
<td>$c \geq 2$</td>
<td>No scalability</td>
</tr>
<tr>
<td>MPC</td>
<td>$\checkmark$</td>
<td>$\checkmark$ If bounded true value</td>
</tr>
<tr>
<td></td>
<td>$c = 1$</td>
<td>$\checkmark$ Optimal social welfare</td>
</tr>
<tr>
<td></td>
<td>$c \geq 2$</td>
<td></td>
</tr>
</tbody>
</table>
More in paper: infinite block size

<table>
<thead>
<tr>
<th></th>
<th>Strict IC</th>
<th>$\epsilon$-IC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plain</td>
<td>$0$-miner rev</td>
<td>$\Theta(n \cdot (\epsilon + \sqrt{m\epsilon}))$-miner rev</td>
</tr>
<tr>
<td>MPC</td>
<td>$0$-miner rev</td>
<td>$\Theta(n \cdot (\epsilon + \sqrt{m\epsilon}))$-miner rev</td>
</tr>
</tbody>
</table>

All optimal!
Open question

- Practical mechanism
- Universal mechanism
Thanks!

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