SoK: Preventing Transaction Reordering Manipulations in Decentralized Finance

Advances in Financial Technologies (AFT’22)
Lioba Heimbach, Roger Wattenhofer
ETH Zurich – Distributed Computing – www.disco.ethz.ch
Transaction Ordering

$T_1$
Transaction Ordering

$T_1$

$T_2$
Transaction Ordering
Transaction Ordering

\[ T_A, T_B, T_C, T_D, T_E \]
Transaction Ordering

$T_A \quad T_B \quad T_C \quad T_D \quad T_E$
Decentralized Finance (DeFi)

- Decentralized Exchanges
- Lending Protocols
Decentralized Finance (DeFi)

Decentralized Exchanges

Lending Protocols

δY/δX
Sandwich Attack
Sandwich Attack
Sandwich Attack

\[ T_V \]
Sandwich Attack

\[ T_F \xleftrightarrow{\text{ethereum}} V \xleftrightarrow{\text{ethereum}} T_B \]

\[ T_V \xleftrightarrow{\text{ethereum}} V \xleftrightarrow{\text{ethereum}} T_B \]

\[ T_F \xleftrightarrow{\text{ethereum}} V \xleftrightarrow{\text{ethereum}} T_B \]
Decentralized Finance (DeFi)

Decentralized Exchanges

Lending Protocols

δY/δX
Blockchain Extractable Value (BEV)

BEV is a measure of the profit that can be made through including, excluding, or re-ordering transactions within block.
Transaction Reordering

$T_1 \quad T_V \quad T_2 \quad T_3$

no attack
Transaction Reordering

no attack

fatal front-running
Transaction Reordering

- No attack
- Fatal front-running
- Front-running
Transaction Reordering

- **no attack**
  - $T_1$, $T_V$, $T_2$, $T_3$

- **fatal front-running**
  - $T_1$, $T_A$, $T_V$, $T_2$

- **front-running**
  - $T_1$, $T_A$, $T_V$, $T_2$

- **back-running**
  - $T_1$, $T_V$, $T_A$, $T_2$
Measures
Measures

Does the approach decrease the level of decentralization?
Measures

Is the approach susceptible to attacks?
Measures

Is the approach wide-reaching?
Does the approach create competition between traders for block inclusion?
Measures

Does the approach impact the number of genuine transactions processed?
Does the approach delay transaction execution?
Measures

Does the approach create additional costs for transaction execution?
Optimized Trade Execution

$T_V$
Optimized Trade Execution

decentralization

security

cost

delay

goodput

scope

jostling
Optimized Trade Execution
Optimized Trade Execution

decentralization

security

cost

delay

goodput

jostling

scope
Professional Market Makers

\[ T_A \]
Professional Market Makers

Diagram showing connections between nodes labeled $T_A$, $T_B$, $T_C$, $T_D$, and $T_E$. There are directed edges labeled 1 to 5 connecting these nodes.
Professional Market Makers
Professional Market Makers

decentralization

security

cost

delay

goodput

cost

delay

goodput

jostling

scope
Professional Market Makers
Professional Market Makers

cost

decentralization

delay

security

scope

jostling

goodput
Trusted Third Party Ordering
Trusted Third Party Ordering

$T_A \quad T_B \quad T_C \quad T_D \quad T_E$
Trusted Third Party Ordering

$T_A$ $T_B$ $T_C$ $T_D$ $T_E$
Trusted Third Party Ordering
Trusted Third Party Ordering
Trusted Third Party Ordering
Trusted Third Party Ordering
Trusted Third Party Ordering

decentralization

security

cost

delay

goodput

jostling

scope
eUTXO
eUTXO
eUTXO
eUTXO
eUTXO
eUTXO
eUTXO
Algorithmic Committee Ordering
Algorithmic Committee Ordering

\[ T_A \quad T_B \quad T_C \quad T_D \quad T_E \]
Algorithmic Committee Ordering

$T_A$, $T_B$, $T_C$, $T_D$, $T_E$
Algorithmic Committee Ordering
Algorithmic Committee Ordering
Algorithmic Committee Ordering
On-chain Commit & Reveal
On-chain Commit & Reveal
On-chain Commit & Reveal
On-chain Commit & Reveal

decentralization

security

cost

delay

goodput

scope

jostling
On-chain Commit & Reveal

decentralization

security

cost

delay

scope

jostling

goodput
Off-chain Commit & Reveal
Off-chain Commit & Reveal
Off-chain Commit & Reveal

\[ T_A \quad T_B \quad T_C \quad T_D \quad T_E \]
Off-chain Commit & Reveal

$\mathcal{T}_A \quad \mathcal{T}_B \quad \mathcal{T}_C \quad \mathcal{T}_D \quad \mathcal{T}_E$
Off-chain Commit & Reveal

\[ T_A \quad T_C \quad T_B \quad T_B \quad T_E \]
Off-chain Commit & Reveal
Off-chain Commit & Reveal
Off-chain Commit & Reveal
Summary

- Optimized trade execution
- Professional market makers
- Trusted third party ordering
- eUTXO model
- Algorithmic committee ordering
- On-chain commit & reveal
- Off-chain commit & reveal

Attributes:
- Scope
- Security
- Decentralization
- Cost
- Delay
- Goodput
- Jostling
## Summary

<table>
<thead>
<tr>
<th>Optimized trade execution</th>
<th>Professional market makers</th>
<th>Trusted third party ordering</th>
<th>eUTXO model</th>
<th>Algorithmic committee ordering</th>
<th>On-chain commit &amp; reveal</th>
<th>Off-chain commit &amp; reveal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>Security</td>
<td>Decentralization</td>
<td>Cost</td>
<td>Delay</td>
<td>Goodput</td>
<td>Jostling</td>
</tr>
<tr>
<td>Green</td>
<td>Red</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
</tr>
</tbody>
</table>
Summary

- Optimized trade execution
- Professional market makers
- Trusted third party ordering
- eUTXO model
- Algorithmic committee ordering
- On-chain commit & reveal
- Off-chain commit & reveal

Columns: scope, security, decentralization, cost, delay, goodput, jostling
Summary

- Optimized trade execution
- Professional market makers
- Trusted third party ordering
- eUTXO model
- Algorithmic committee ordering
- On-chain commit & reveal
- Off-chain commit & reveal

Scope, Security, Decentralization, Cost, Delay, Goodput, Jostling
Summary

- Optimized trade execution
- Professional market makers
- Trusted third party ordering
  - eUTXO model
  - Algorithmic committee ordering
  - On-chain commit & reveal
  - Off-chain commit & reveal

Attributes:
- Scope
- Security
- Decentralization
- Cost
- Delay
- Goodput
- Jostling
Summary

- optimized trade execution
- professional market makers
- trusted third party ordering
- eUTXO model
- algorithmic committee ordering
- on-chain commit & reveal
- off-chain commit & reveal

Scope, security, decentralization, cost, delay, goodput, jostling
Cyclic Arbitrage