Equilibria in DeFi from State Context Inspection

James Hsin-yu Chiang, Conor McMenamin, and Margherita Renieri

5th Distributed Ledger Technology Workshop (DLT23)
Bologna, May 25-26, 2023
Problem & Goal

Problem: *oracle price manipulations* occur as a result of protocol composition mal-incentives

Goal: Protocols act on “fair” states
Oracle Price Manipulation Example

Consider an AMM-based oracle at some price $P$.

If the oracle price drops 1%:

- Loss: $100 → trade with the AMM (oracle manipulation)
- Profit: $200 → buy the resultant liquidated collateral

Real scenario → Extractable Value    Ideal scenario → Remove Incentives
Solution

\[
\text{ctx} (\Gamma', \text{liquidate}) = \Gamma \xrightarrow{\text{AMM:swap}} \Gamma' \xrightarrow{\text{Coll:liquidate}}
\]

context : effect of liquidation protocol on the well-priced state
Solution

\[ \text{ctx} (\Gamma', \text{liquidate}) = \Gamma \xrightarrow{\text{AMM:swap}} \Gamma' \xrightarrow{\text{Coll:liquidate}} \]

*context* : effect of liquidation protocol on the well-priced state

*context policy*: minimize potential effects of context (maximum permitted distance on AMM price)
Solution

\[
\text{ctx} (\Gamma', \text{liquidate}) = \Gamma \xrightarrow{\text{AMM:swap}} \Gamma' \xrightarrow{\text{Coll.\ state}}
\]

*context*: effect of liquidation protocol on the well-priced state

*context policy*: minimize potential effects of context (maximum permitted distance on AMM price)

\[
\text{finalPrice}^{(\text{ctx } U \mathcal{\not Ctx})} = \text{finalPrice}^{(\text{noCtx})}
\]

**Incentive manipulation reduction**
Future directions

- Define the context(s) that generate mal-incentives.
- Create a generalized set of policies to minimize these incentives.

- Cost to manipulate oracle is typically fixed,
  - Context mal-incentives increasing in number of composed protocols.
    Can protocols communicate to notify others of their context?
    Introduce an idea of shared *manipulation budget*. 
Thank you for your attention!