Modifying Blockchain Utility Function to Include Heterogenous Goods

David Lancashire
david.lancashire@gmail.com

January 10, 2025

1.1 The Utility Function for Users

We start with our standard equation for utility:

$$u_j^U(\theta_j, \{\theta_{j'}\}_{j' \in \mathcal{U} \setminus \{j\}}; p_j) := \begin{cases} \theta_j - p_j & \text{if } j \in S, \\ 0 & \text{otherwise.} \end{cases}$$

We have two kinds of utility:

- **public good:** the value of inclusion in the public blockchain
- **private good:** any additional benefits offered in exchange for fee flow.

We have two kinds of fees:

- **public fee:** any fee allocated to the public good
- **private fee:** any fee allocated to a private good

The price paid by user j is the sum of their public and private fees.

$$p_j = p_{pub}^j + p_{priv}^j$$

Their valuation θ_j is the sum of their public and private valuation functions:

$$\theta_j = U_{pub}^j + U_{priv}^j$$

Their public valuation function is a monotonically-increasing function of all public fees in the block.

$$U_{pub}^j = f_{pub}^j \left(\sum_{k \in S} p_{pub}^k \right)$$

Their private valuation function is a monotonically-increasing function of the users's own private fees.

$$U_{priv}^j = f_{priv}^j(p_{priv}^j)$$

The total valuation function is thus:

$$\theta_j = f_{pub}^j \left(\sum_{k \in S} p_{pub}^k \right) + f_{priv}^j(p_{priv}^j)$$

This gives us the full utility function:

$$u_j^U\,(...) := \begin{cases} \left(f_{pub}^j \left(\sum_{k \in S} p_{pub}^k \right) + f_{priv}^j(p_{priv}^j) \right) - (p_{pub} + p_{priv}) & \text{if } j \in S, \\ 0 & \text{otherwise.} \end{cases}$$

1.2 The Utility Function in the Presence of Collusion

Under collusion, users reduce their public fee by p_{fr}. Under non-atomistic market conditions (i.e. diminished competition) the producer can allocate this to the provision of a second good, which can even be a cash discount.

$$p_j = \left(p^j_{pub} - p^j_{fr}\right) + \left(p^j_{priv} + p^j_{fr}\right)$$

Therefore:

$$\theta_j = f^j_{pub}\left(\sum_{k\in S} p^k_{pub} - p^j_{fr}\right) + f^j_{priv}(p^j_{priv} + p^j_{fr})$$

Total fee is unchanged, so collusion is rational if the re-allocation increases joint utility, i.e.:

$$f^j_{pub}\left(\sum_{k\in S} p^k_{pub} - p^j_{fr}\right) + f^j_{priv}(p^j_{priv} + p^j_{fr}) > f^j_{pub}\left(\sum_{k\in S} p^k_{pub}\right) + f^j_{priv}(p^j_{priv})$$

Collusion is rational whenever the marginal utility of the second good is higher than the marginal utility of the first. Since the second good can be a cash refund, this means collusion is viable if the marginal utility of *any other good* is higher than the marginal utility of the blockchain for even a single user in the network!

1.3. Eliminating Collusion

- **private collusion:** if all goods are private goods with non-excludable benefits
- **free-riding:** if our public good is a real "public good" (has non-excludable benefits, externalities, etc.)

As per Samuelson (1954), *private collusion* is not rational at the *utility possibilities frontier*.

$$\frac{u^i_{pub}}{u^i_{priv}} = \frac{F_{pub}}{F_{priv}}$$

The problem disappears because at this point the marginal utility of all goods is in equilibrium by definition.

But free-riding remains rational at the *utility possibilities frontier*!

In any network where free-riding is rational, we will always get pulled into an equilibrium where private collusion is rational.

1.4 What Happens Without Free-Riding?

Eliminating free-riding is *necessary* but not *sufficient* for eliminating collusion. Eliminating it does not pull us into pareto optimality ("utility possibilities frontier") because eliminating cannot change the marginal utility of the second good. But it means that if we for some other reason end up with the marginal utilities of our various goods properly alligned at pareto optimal levels we will not be forcibly dragged back into an equilibrium where *private collusion* is rational.

What we are doing by eliminating free-riding is eliminating externalities.

Once that is done, you still need a mechanism to successfully implement *pareto optimality* in an informationally decentralized environment. In order to do this, per Hurwicz, we need an *indirect mechanism* that has high-dimensional and truthful preference revelation from both users and producers and contains an "incentive for truthfulness". This is not an easy problem, but it is a solvable problem.

1.5 Fundamental Analytic Errors in the Literature

The solution tells us that all of these

- assuming all blockchains give block producers "temporary monopoly" over slots
- modelling blockspace as a private good, not noticing that some forms of collusion involve free-riding
- asking for truthful preference revelation from users, not producers
- assumptions like "many honest users" rather than "atomististic competition"
- not specifying ANY social choice rule ("our goal is truthful preference revelation")
- not specifying the ONLY collusion-free social choice rule (pareto optimality -¿ utility possibilities frontier)
- low-dimensional preference revelation (the VCG "fee" rather than the marginal utilities for multiple goods at multiple price levels)

- not solving for Samuelson (collective action problems and negative externalities)
- not solving for Hurwicz (the impliediments to pareto optimality in informationally decentralized mechanisms)