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 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.

$$p_j = p^j_{pub} + p^j_{priv}$$

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

$$\theta_j = U^j_{pub} + U^j_{priv}$$

The public utility function is a monotonically-increasing function of all public fees in the block.

$$U^j_{pub} = f^j_{pub}\left(\sum_{k\in S} p^k_{pub}\right)$$

The private utility function is a monotonically-increasing function of the users's own private fees.

$$U^j_{priv} = f^j_{priv}(p^j_{priv})$$

This gives us a revised valuation equation:

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

As users do not face a variable "burn" for transaction inclusion, we remove it from our equation

$$u^U_j\,(...) := \begin{cases} \left(f^j_{pub}\left(\sum_{k\in S} p^k_{pub}\right) + f^j_{priv}(p^j_{priv})\right) - (p_{pub} + p_{priv}) & \text{if } j \in S, \\ 0 & \text{otherwise.} \end{cases}$$

1.2 The Utility Function in the Presence of Collusion

Users reduce their public fee by

$$p_{fr}$$

and replace it with an identical private payment. Under conditions where diminished competition permits the producer to effect the trade, the private payment allows the producer to provide a compensating private benefit, including a cash refund or discount. This can be modelled as the redirection of the fee into a second utility function.

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

We modify our valuation function:

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

Collusion is utility-increasing if the re-allocation increases joint utility, i.e.:

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

Eliminating Collusion Completely

- **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*.

$$\frac{u_p ub^i}{u_p riv^i} = \frac{F_p ub}{F_p riv}$$

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.

How to Achieve a Collusion-Free Equilibrium

The first step is eliminating free-riding. This is *necessary* but not *sufficient* for eliminating collusion - getting rid of free-riding does not pull us into the state of pareto optimality ("utility possibilities frontier") where *private collusion* is irrational, but it means that if we have a mechanism that induces participants to pay fees at levels that put us on the utility frontier, we will not be forcibly dragged out of it into an equilibrium where *private collusion* is rational.

The second step is to design a mechanism that successfully implements *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.

The Connection with Temporary Monopoly

All models that give block producers *temporary monopoly* over block production have free-riding. Threshold users can always lower their fee.

Ample impossibility results demonstrate this, but do not understand the underlying cause, thus identify exceptions without understanding why they become possible. To give an example of this the "many honest users" exception Shi and Chung identify eliminates collusion because atomistic competition eliminates the "diminished competition" necessary for producers to redirect a portion of the user fee into a second utility function: if they lower their spending on the security function they produce fewer blocks and collect less income.

Fundamental Analytic Errors in the Literature

* 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 * not specifying ANY social choice rule ("our goal is truthful preference revelation") * not specifying the ONLY VIABLE social choice rule (pareto optimality -¿ utility possibilities frontier) * low-dimensional preference revelation (the VCG "fee" is enough, when we need marginal utilities for multiple goods at multiple price levels) * not applying Samuelson (collective action problems and negative externalities) * not applying Hurwicz (the impledíments to pareto optimality in informationally decentralized mechanisms)

Some of the more viable approaches ("posted prices") are indirect attempts to solve problems Hurwicz considered impossible.