frontiers

Supplementary Material

APPENDIX: CHARACTERISTICS OF USER EQUILIBRIUM STRATEGIES

In this appendix, we show the analytical framework for the analysis of user strategy in equilibrium. Let p_u denote the probability that the player joins a system. We define X and S as the amount of the player's payment to the system service and its set, respectively. Let G_u denote the distribution function of X, i.e., $G_u(x) = \Pr\{X \leq x\}$ $(x \in S)$. In the following, the decision making of a player is expressed as (p_u, G_u). Note that the player benefits from the system service in compensation with the payment X.

Let f denote the utility function of a user with decision making (p_u, G_u) and payment x. We consider the expected utility function of a user with decision making (p_u, G_u) given that other users' decision making is $(p_u^{'}, G_u^{'})$, which is defined by

$$U((p_u, G_u) \mid (p_u^{'}, G_u^{'})) = p_u \int_{x \in S} f_u(p_u^{'}, G_u^{'}, x) dG_u(x).$$

Let (p_u^*, G_u^*) denote the decision-making strategy in equilibrium. When the strategies of all other users are the same as (p_u^*, G_u^*), we have

$$U((p_u^*, G_u^*) \mid (p_u^*, G_u^*)) = \sup_{(p_u, G_u)} U((p_u, G_u) \mid (p_u^*, G_u^*)). \tag{S1}$$

Assume G_u is differentiable and a monotonically increasing function for $x \in [\underline{x}, \infty)$. Noting that $G_u(\underline{x}) = G_u^*(\underline{x}) = 0$ and $G_u(\infty) = G_u^*(\infty) = 1$, we have

$$\begin{aligned}
&U((p_u^*, G_u^*) \mid (p_u^*, G_u^*)) - U((p_u^*, G_u) \mid (p_u^*, G_u^*)) \\
&\quad = p_u^* \int_{\underline{x}}^{\infty} f_u(p_u^*, G_u^*, x) \left(\frac{d}{dx} G_u^*(x) - \frac{d}{dx} G_u(x) \right) dx \\
&\quad = p_u^* \Big[f(p_u^*, G_u^*, x)(G_u^*(x) - G_u(x)) \Big]_{\underline{x}}^{\infty} - p_u^* \int_{\underline{x}}^{\infty} dx \frac{d}{dx} f_u(p_u^*, G_u^*, x)(G_u^*(x) - G_u(x)) \\
&\quad = -p_u^* \int_{\underline{x}}^{\infty} \left(\frac{d}{dx} f_u(p_u^*, G_u^*, x) \right) \cdot (G_u^*(x) - G_u(x)) dx.
\end{aligned}$$

Suppose $\frac{df_u}{dx} > 0$ on interval $x \in [a, b]$. Since G_u is an arbitrary monotonically increasing function satisfying condition $G_u(\underline{x}) = G_u^*(\underline{x}) = 0$ and $G_u(\infty) = G_u^*(\infty) = 1$ for $x \in [\underline{x}, \infty)$, then there exists $G_u(x)$ satisfying the following equation for some interval $[a, b]$

$$\begin{cases} G_u^*(x) - G_u(x) > 0, & x \in [a, b], \\ G_u^*(x) - G_u(x) = 0, & x \notin [a, b]. \end{cases} \tag{S2}$$

Then, from (S2) and $\frac{df}{dx} > 0$ on interval $x \in [a, b]$, the following inequality holds

$$-p_u^* \int_{\underline{x}}^{\infty} \left(\frac{d}{dx} f_u(p_u^*, G_u^*, x) \right) \cdot (G_u^*(x) - G_u(x)) dx < 0. \tag{S3}$$

From (S2) and (S3), we obtain

$$U((p_u^*, G_u^*) \mid (p_u^*, G_u^*)) < U((p_u^*, G_u) \mid (p_u^*, G_u^*)),$$

which contradicts (S1). Thus, $f_u(p_u^*, G_u^*, x)$ satisfies

$$\frac{d}{dx} f(p_u^*, G_u^*, x) = 0, \quad x \in [\underline{x}, \infty]. \tag{S4}$$

When $\frac{df}{dx} < 0$, (S4) still holds by similar argument.

APPENDIX: FIGURES

5.1 Minimum entrance fee that maximizes user's total fee

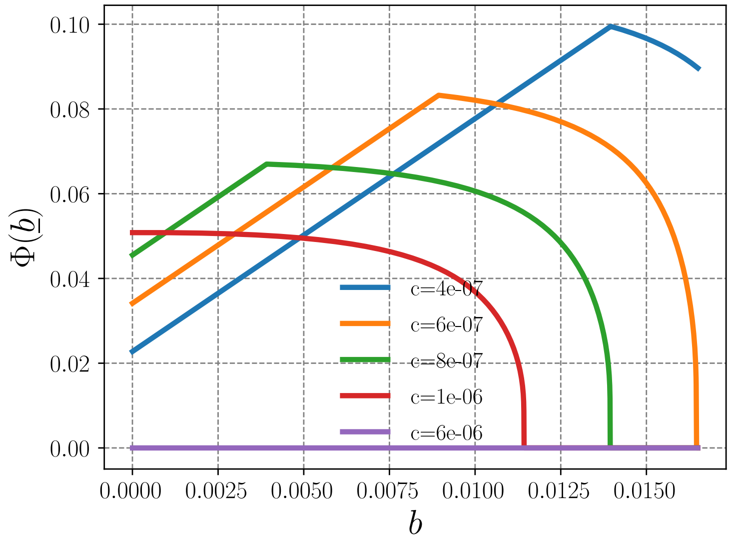

Figure 1A. Relationship between the user's total fee and the lower limit of the fee $\underline{b}$.

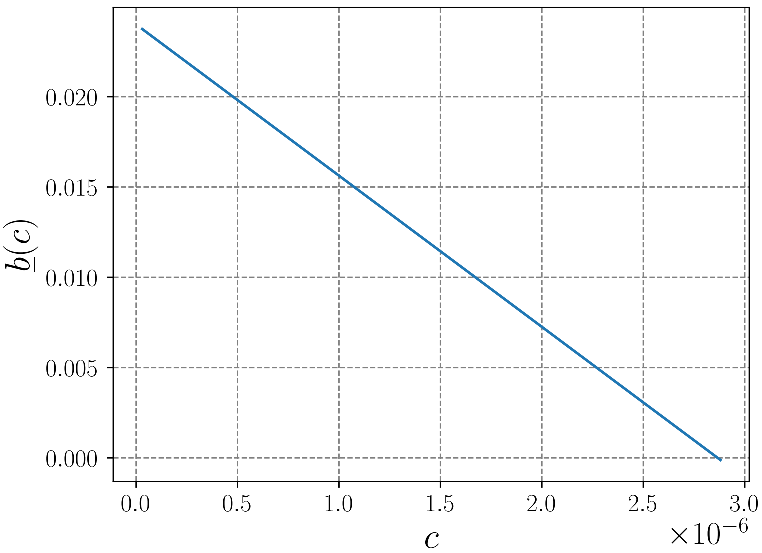

Figure 1B. The minimum transaction fee $\underline{b}$ vs. the user waiting cost c.

5.2 Equilibrium point transition for attack success probability and confirmation latency

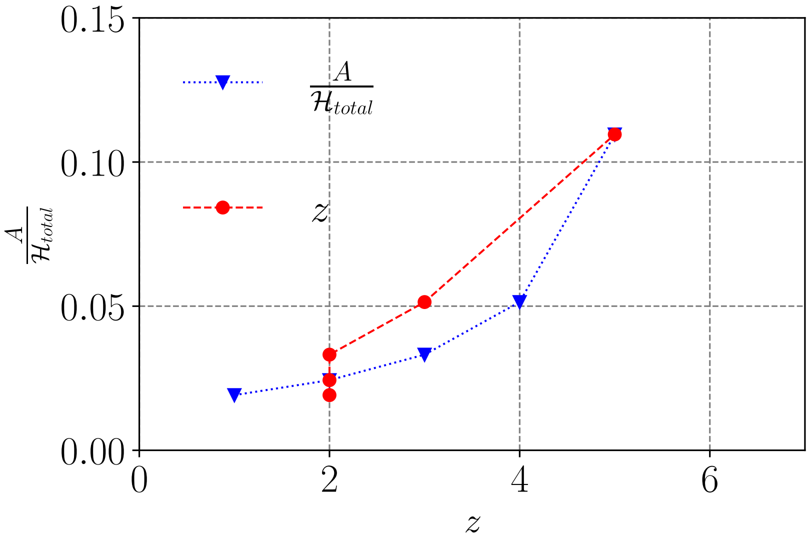

Figure 2A. The attack success probability vs. confirmation latency. ($B = 0$, $C_M = 1.5 \times 10^{-12}$)

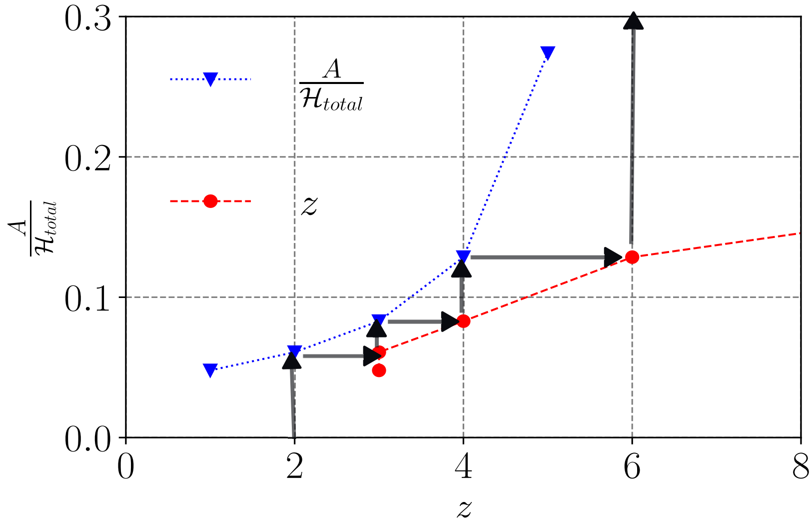

Figure 2B. The attack success probability vs. confirmation latency. ($B = 0$, $C_M = 3.8 \times 10^{-12}$)

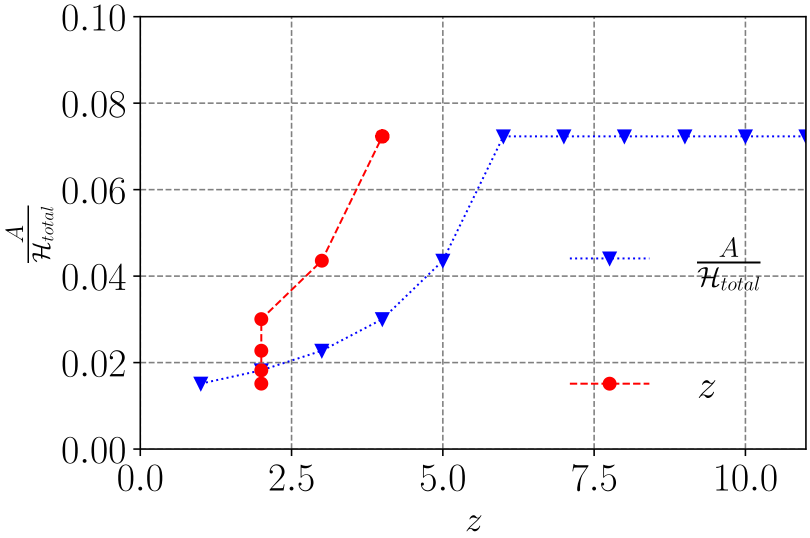

Figure 2C. The attack success probability vs. confirmation latency. ($B = 12.5$, $C_M = 1.5 \times 10^{-12}$)

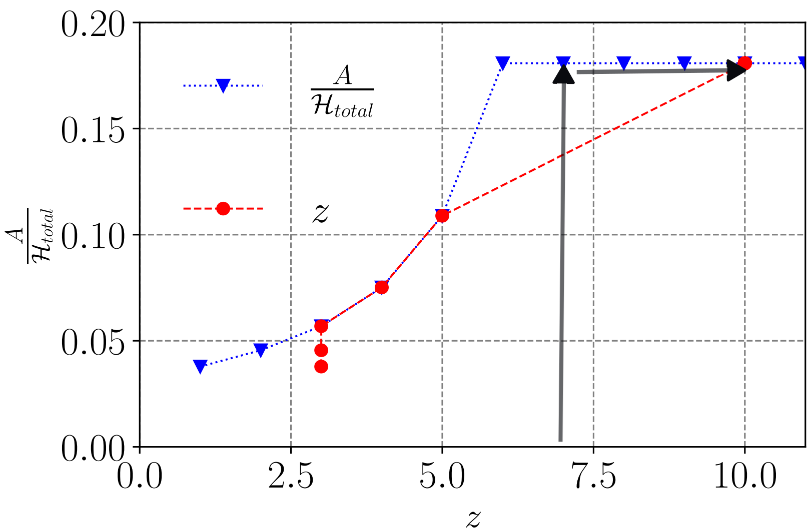

Figure 2D. The attack success probability vs. confirmation latency. ($B = 12.5$, $C_M = 3.8 \times 10^{-12}$)

APPENDIX: MINER BEHAVIOR FOR REVENUE AND HASH RATE

In order to clarify the relation between miner's revenue and the total hash rate, we obtained those data from blockchain.com. Figure 3 illustrates the miner's revenue and the total hash rate from September 10 to October 10, 31-day period data. We observe from this figure that there is a near proportional relationship between miners' revenue and the total hash rate over one month period. This fact supports the result of the analysis of our model that the total hash rate is proportional to miners revenue.

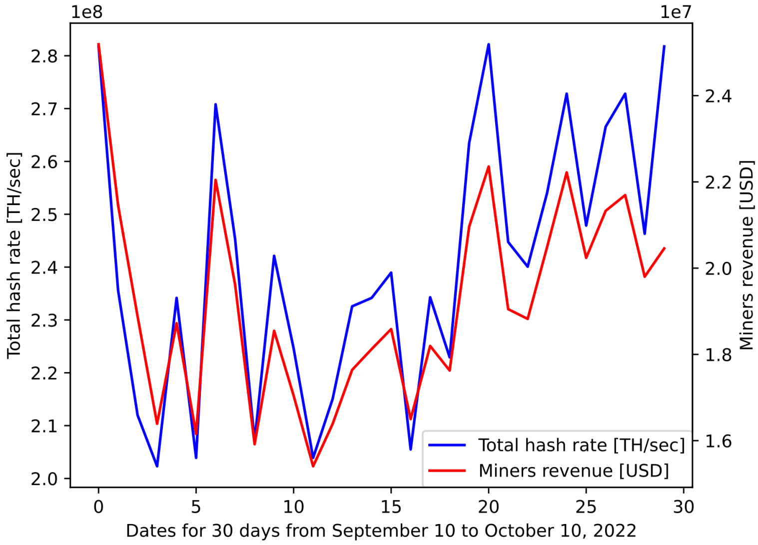

Figure 3. Miners' revenue and total hash rate.