A Dynamic Model of Bidding and Operation in the Bitcoin Market

Yuichiro Kamada (UC Berkeley + The University of Tokyo)

Shunya Noda (The University of Tokyo)

Cryptocurrency x Market/mechanism Design

- Market/mechanism design is a field to design desirable system, policy, rule, etc.

- Cryptocurrency is an interesting research topic for market/mechanism designers
  1. Cryptocurrency itself is an "**institution to be designed**"
  2. Cryptocurrency is a tool for designing mechanisms (e.g. smart contract)
  3. We need regulations to effectively reduce the harm of cryptocurrencies

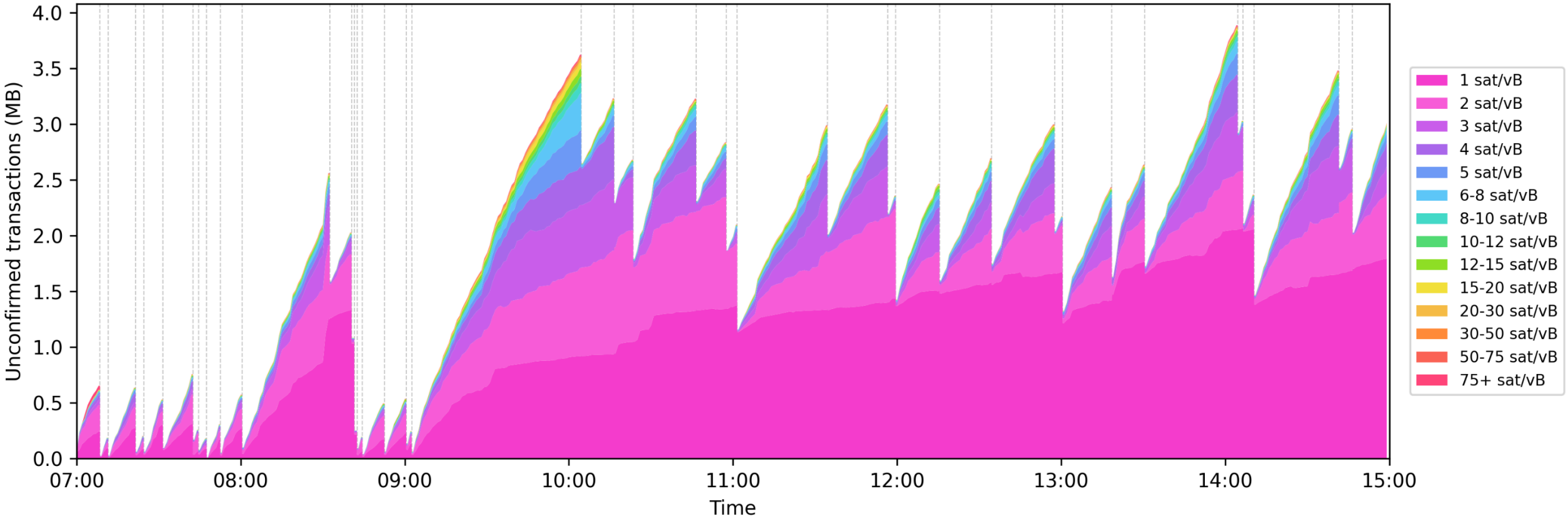
- Today's paper analyzes how Bitcoin's reward system shapes the transaction fees paid by users and miners' operation decisions.

Bitcoin Basics

- Bitcoin is an electronic payment system
- Unlike the centralized system, anyone can work as a record keeper (called **miner**)
  - A transaction is validated when it is included in a block
  - **Proof-of-Work:** Miners can probabilistically acquire the right to produce a new block by (iteratively) computing a cryptographic hash function
- Miners are rewarded with seigniorage + user-paid transaction fees
  - So far, seigniorage is dominant
  - Bitcoin halves the amount of seigniorage every four years
    → In the long run, miners will be incentivized purely through fees

Users set fees by themselves

- When users make transaction requests, they "**bid**" transaction fees
- Miners (basically) prioritizes transactions with higher fees (for their profitability)
- Higher transaction fee ↔ Rapid and sure validation



In this paper…

- We develop a dynamic model of **user bidding** and **miner operation**, capturing Bitcoin's market dynamics.
- In equilibrium, **users adjust their fees** in response to system throughput, current congestion, and miners' operational policies.
- When congestion is low, miners may **temporarily suspend operations** due to high operating costs relative to revenue, causing fees to spike.
- **Positive block rewards** (fixed rewards paid by newly minted coins) mitigate miner suspensions and enhance social welfare.

Model

- Continuous time $[0, +\infty)$
  - No transaction request at time 0
- Users arrive continuously at a rate 1
  - Each user has **one transaction request** earning a payoff of 1 when validated.
  - Upon arrival, each user makes a bid $b \in \mathbb{R}_+$, which cannot be changed later.
  - The user need to **pay her bid b** when her transaction is validated.
- A user's request is validated only when a block arrives.
- A user's payoff is $1 - b$ if the user's bid is included in the **first block**.
  - Minimal construction to capture the "fee vs validation" tradeoff.
- The set of pending transactions forms a **pool**.

Block Arrival

- For a while, we focus on **user competition**.
  - Miner operation will be incorporated later.
- Block arrival follows a homogeneous Poisson process with intensity $\lambda > 0$.
- When a block arrives, up to mass $K < +\infty$ transactions are validated.
  - λ: block arrival rate K: block capacity
  - λK represents the system's throughput.
- When a block arrives, a transaction request with bid b is validated if and only if, the mass of transaction requests that have higher bids than b is smaller than K.
- (Such a greedy choice rule is optimal for miners as long as they are infinitesimal.)

Bid Function

- Users are heterogeneous only in their arrival time $t \in \mathbb{R}_+$
  → Each user's (on-path) bid can be specified as $\beta(t)$
- $\beta: \mathbb{R}_+ \to \mathbb{R}_+$ is called a bid function.
- Users are **infinitesimal.**
  → We consider an equilibrium in which users ignore a user's unilateral deviation.
  → From a time-t user, for all $t' > t$, "A time-t' user will bid $\beta(t')$" is exogeneous.
- Once we specify β, we can identify the bid distribution at any time t.
  → We can also identify the threshold time $\bar{t}(b;\beta)$ until when a transaction request with bid b is validated.
- The probability that time-t user's bid is validated when she bids b is

$$\pi(t, b, \beta) = 1 - e^{-\lambda[\bar{t}(b;\beta)-t]^+}.$$

User's Objective and Equilibrium Definition

- A time-t user's expected payoff from bidding b is

$$\pi(t, b, \beta)(1 - b)$$

- A bid function β is an **equilibrium** if for all $t \in \mathbb{R}_+$ and $b \in \mathbb{R}_+$,

$$\pi(t, \beta(t), \beta)\big(1 - \beta(t)\big) \geq \pi(t, b, \beta)(1 - b).$$

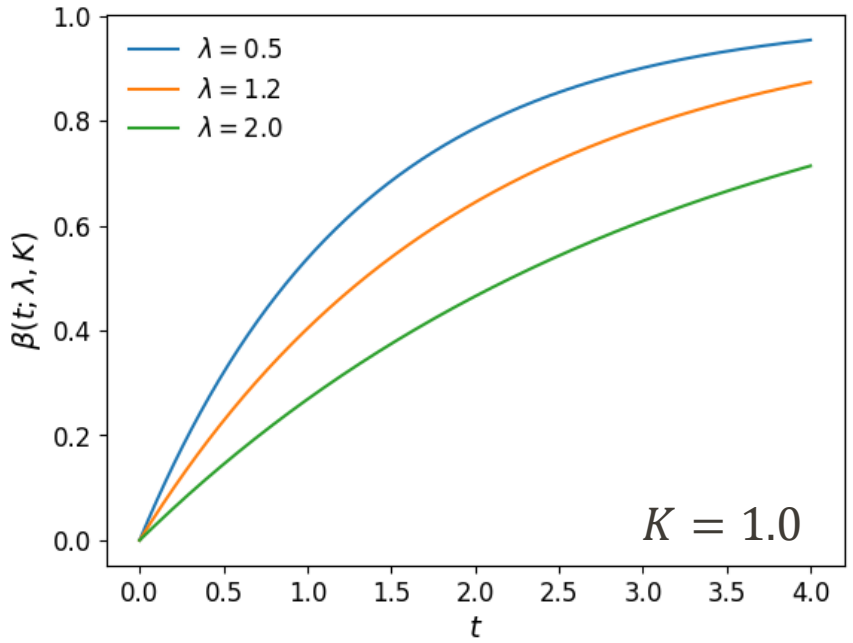
  - "When other bidders follow β, a time-t user can maximize her payoff by bidding $\beta(t)$."

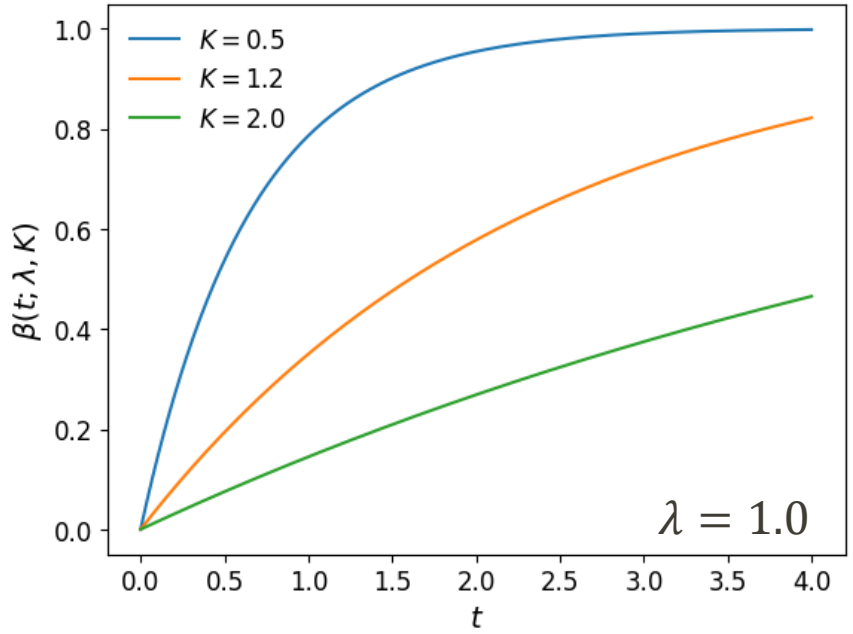
Characterization

Theorem 2: In the UC model, there is a unique equilibrium. In this equilibrium, the bid function is specified by

$$\beta(t) = \beta^E(t;\lambda,K) := 1 - e^{\frac{W'(0;\lambda,K)}{W(0;\lambda,K)}t} = 1 - e^{-\frac{\lambda e^{-\lambda K}}{1-e^{\lambda K}}t}.$$

- Proof: Take FOC and solve it as a differential equation.
- $\beta^E(t;\lambda,K)$ is decreasing in λ and K.



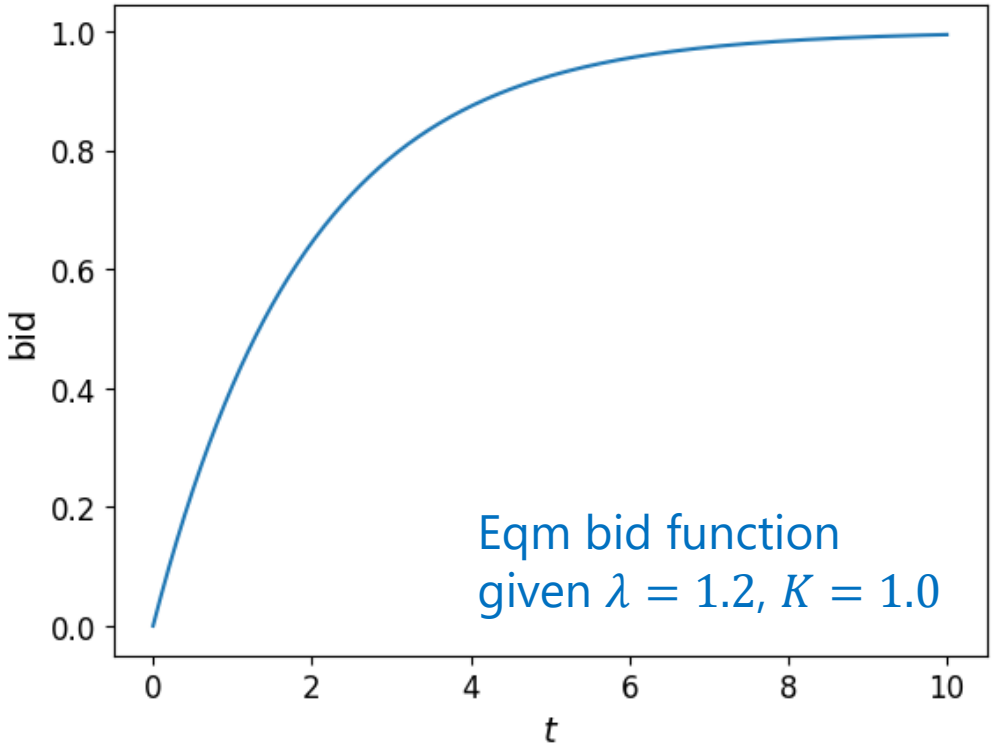


Miner Operation

- So far, we have assumed that block arrivals follow the Poisson process with a fixed arrival rate λ.
- Blocks arrive only when miners operate.
- If the reward paid for miners is too low, miners may not operate.
- This indeed happens for small t.
  - Low bid + fewer transactions

Question:

- What is miners' eqm operation policy?
- How does it influence the eqm bid function?



Endogeneous Operation Model

- Endogenize miner operation → block arrivals
- Two types of miners: **committed miners** (frac η) and **switching miners** $(1-\eta)$
  - Committed miners always operate.
  - Switching miners decide whether to operate their machines for each t to maximize their own profit (with no switching cost).
  - To eliminate uninteresting equilibria. We later focus on the limit $\eta \to 0$.
- When mass Δ of miners operate, they produce a block with a Poisson arrival rate of $\lambda\Delta$ in total, while they pay a flow cost of $c\Delta$ (with $c \geq 0$) in total.
- When they suspend, no chance to produce a block but no cost is incurred.

Switching Miners' Problem

- All switching miners have an identical cost structure
  → Their aggregate behavior solves the "**representative miner's problem**."
- "**The miner**" has a mass $1-\eta$.
  - Arrival rate $\lambda(1-\eta)$ and flow cost $c(1-\eta)$ if she operates.
  - When a block arrives, she obtains **block reward y** + **transaction fees $\int \beta$**
  - Zero flow payoff if she suspends.
  - She chooses the more profitable option.
- The miner's **operation function σ**: $\mathbb{R}_+ \to \{0,1\}$ specifies the miner's decision.
  - The total block arrival rate: $\lambda(t) = \lambda \cdot \big(\eta + (1-\eta)\sigma(t)\big)$
  - Nonhomogeneous Poisson process

Equilibrium

- $\pi(t, b, \beta, \sigma)$ is the probability that a time-t user's transaction is validated when she bids b, the other users follow a bid function β, and the miner follows an operation function σ.
- $M(t; \beta)$ is the total amount of transaction fees paid to the miner when a block arrives at time t.
  - **Spoiler:** Later we show that in the unique eqm, $M(t; \beta) = \int_{[t-K]^+}^{t} \beta(t')dt'$.
- (β, σ) is an equilibrium if the following two conditions hold:

User's Optimality: For all $t \in \mathbb{R}_+$ and $b \in \mathbb{R}_+$,

$$\pi(t, \beta(t); \beta, \sigma)\big(1 - \beta(t)\big) \geq \pi(t, \beta; \beta, \sigma)(1 - b)$$

Miner's Optimality: For all $t \in \mathbb{R}_+$,

$$\sigma(t) \in \arg\max_{x \in \{0,1\}} x \cdot (\lambda(M(t; \beta) + y) - c)$$

Optimality of the Threshold Strategy

- The sum of transaction fees collected at time t, $M(t;\beta)$ is strictly increasing.
  → The miner uses a **threshold strategy** to maximize her profit.

Lemma 1: In any equilibrium, the miner's operation function is specified by the threshold time $t^* \in \{-\infty, +\infty\} \cup \mathbb{R}_+$.

- $\sigma(t) = 0$ if $t < t^*$ and $\sigma(t) = 1$ if $t > t^*$.

- Hereafter we represent an operation function σ by its **threshold time t^***.

Characterization

Theorem 4: In the EO model, there exists an eqm. Furthermore, (β, t^*) is an eqm if it satisfies the following conditions:

1. $t^* = t^E$ is equal to (a) $-\infty$ if $\lambda y > c$, (b) $+\infty$ if $\lambda(K + y) \leq c$, and (c) otherwise, $t \in \mathbb{R}$ satisfying $\lambda(M(t; \beta) + y) = c$.
2. The bid function β is specified by $\beta(t) = \beta^E(t, t^E)$, where $\beta^E : \mathbb{R}_+^2 \to \mathbb{R}_+$ is

$$\beta^E(t, t^*) = 1 - e^{\int_0^t \frac{W_1(0, t^* - \tau)}{W(0, t^* - \tau)} d\tau},$$

and

$$W(s, l) = \begin{cases} 1 - e^{-\eta\lambda(K-s)} & \text{if } K - s \leq l, \\ 1 - e^{-\eta\lambda l - \lambda(K-s-l)} & \text{if } 0 \leq l \leq K - s, \\ 1 - e^{-\lambda(K-s)} & \text{if } l < 0. \end{cases}$$

(β^E, t^E) satisfying these conditions is unique. If $\eta > 0$, this is the unique eqm.

The case of $\eta = 0$

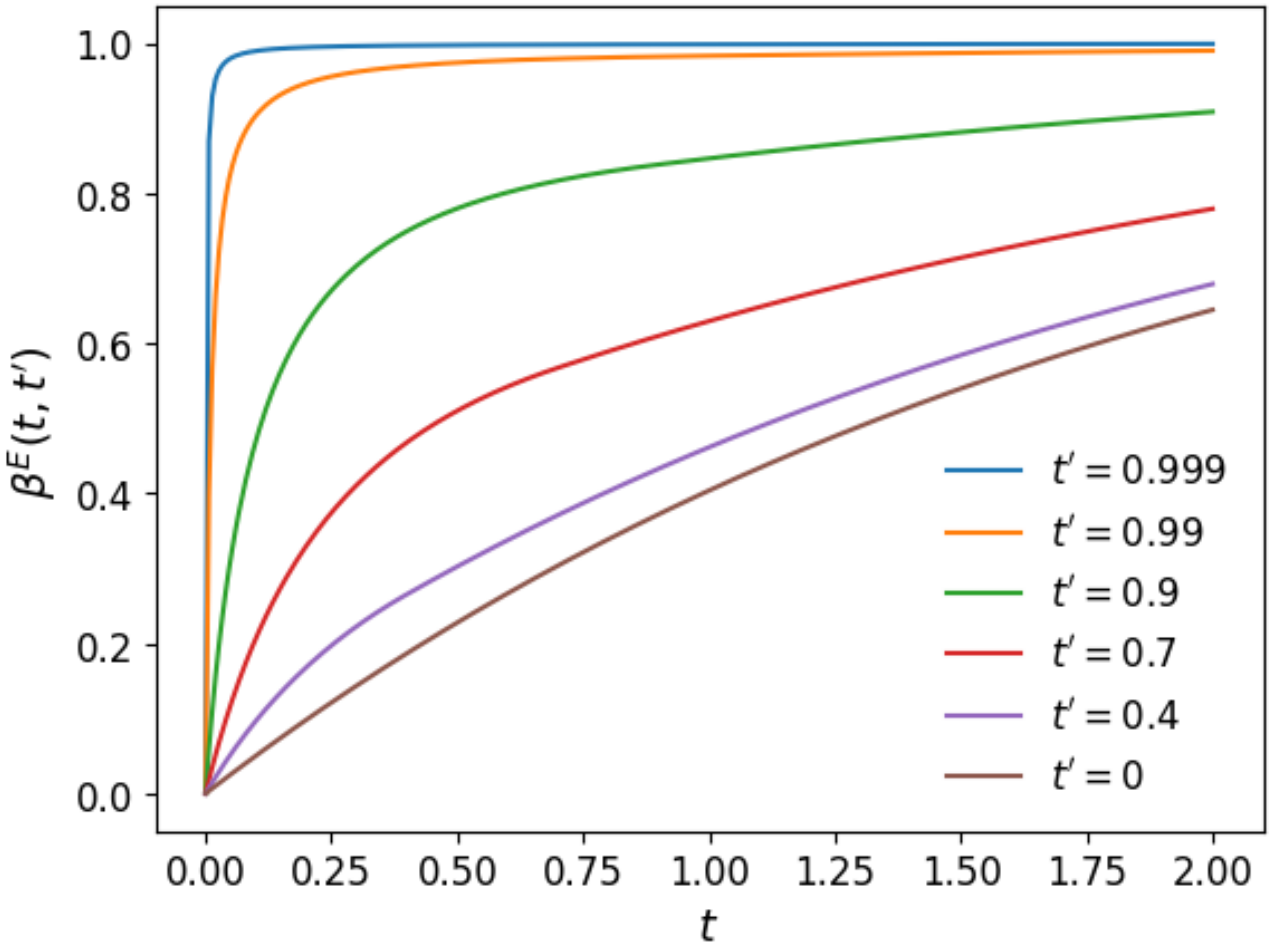
- Theorem 4 states that the eqm is unique when $\eta > 0$.
- When $\eta = 0$, there are infinitely many (uninteresting) equilibria.
  - E.g., "Every user bids zero, and the miner never operates."
  - It is easy to construct a continuum of uninteresting eqa, but we skip it.

- For $\eta = 0$, we regard (β, t^*) represented as the $\eta \to 0$ limit of the unique equilibria as the eqm of interest under $\eta = 0$.

Bid Function

Proposition 4: In the EO model, for all $\eta \in [0,1)$ and $t \in \mathbb{R}_{++}$, the equilibrium bid $\beta^E(t, t^*)$ is strictly increasing in $t^* \in [0, K)$.

- Until threshold time t^*, no block arrives.
- At time t^*, all users arrived by t^* compete against all other users.
- The competition is more severe when the miner's absence is longer.
- The eqm bid function is strictly increasing in the threshold time.



Threshold Time

- We focus on the case of interior solution: $\lambda y \leq c < \lambda(K + y)$.
  - The threshold time t^E satisfies $\lambda\left(M\left(t^E, \beta^E(\cdot; t^E)\right) + y\right) = c$.

Proposition: We have $t^E \in [0, K)$.

Proof Sketch:

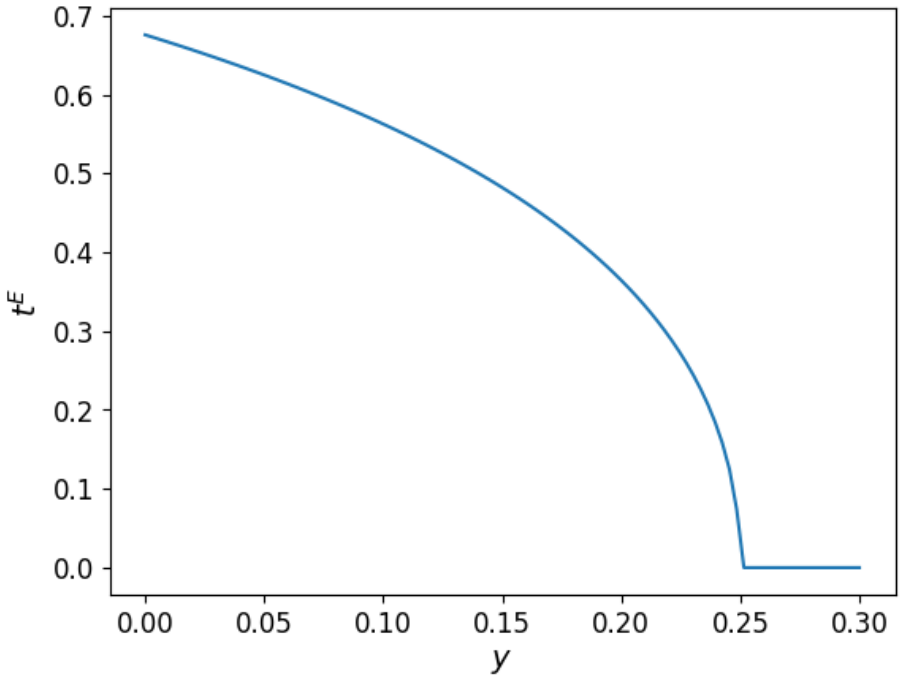
- Suppose the miner starts operation at some $t^* > K$.
- Users arriving within $[0, t^* - K)$ has no chance to win.
- Such (β, t^*) is an eqm only when $\beta(t) = 1$ for $t \in [0, t^* - K)$, implying $\beta \equiv 1$.
- Then, $M(K; \beta) = K$, and $\lambda(M(K; \beta) + y) = \lambda(K + y) \geq c$, implying that the miner starts operation before K. Thus, (β, t^*) cannot be an eqm.

Threshold Time 4

Proposition 6: In the EO model, with $\eta = 0$, the equilibrium threshold time t^E satisfies the following properties.

1. t^E is decreasing and strictly concave in y. → **Block reward changes miner operation!**
2. t^E is increasing and strictly convex in c.
3. t^E is increasing in K.
4. Given $y = 0$ and $c > 0$, t^E is not monotonic in λ.

- Recall: $M^*(t^E) = \frac{c}{\lambda} - y$
- M^* is an integration of β
  $\rightarrow M^*$ is decreasing in λ and K.



Welfare

- **Design Question:** How adjusting parameters such as block reward y can enhance **social welfare**?
- We assume that the block reward (seigniorage) dilutes the value of the currency and thus constitutes a real (zero-sum) monetary transfer from current holders of the currency to miners.
  - We only evaluate the welfare impact through miner operation.
- We consider a Markov chain in which time continuously runs forward and then resets to zero upon each block arrival, and analyze the long-run expected welfare of the economy.

Results

- Socially efficient threshold is always smaller than eqm threshold under no seigniorage reward.
  - Fee reward is zero at $t = 0 \rightarrow$ Miners always temporary suspend.
  - In eqm, miners ignore user surplus and undersupply effort.
- The optimal seigniorage aligns miner surplus with social welfare at the socially efficient threshold t^O.

Policy Implications

- Eliminating the block reward (current plan) is inefficient.
- Efficient block reward level y^O is unique, and it is positive whenever miner operation is costly.

Conclusion

- We develop a dynamic model of the Bitcoin market.

- We characterized the equilibrium **user bidding** and **miner operation**.
  - We derived the eqm bid function using an auction-theoretic approach.
  - We use it to highlight how **miner incentives** fluctuate over time.

- We characterize the amount of the **block reward to maximize social welfare**.