incentives and game theory in blockchain systems

Péter Garamvölgyi

outline

- **incentive compatibility**
  - chain selection
  - incentives for transaction propagation
  - transaction pricing
- resource investment and transaction selection
  - miner resource investment
  - block sizing and transaction selection
- rational mining and exploitation

game theory

- what is game theory?

> *“game theory is the study of mathematical models of strategic interaction between rational decision-makers.”* *

* https://en.wikipedia.org/wiki/Game_theory

game theory

- model systems along different dimensions
  - symmetric — asymmetric
  - zero-sum — non-zero-sum
  - simultaneous move — sequential move
  - perfect information — imperfect information
  - discrete — continuous
  - deterministic — stochastic
  - one-shot — repeated
  - cooperative — non-cooperative

https://ujuzi.pressbooks.com/chapter/chapter-3-types-of-games

https://www.tutor2u.net/economics/reference/game-theory-different-types-of-games

http://www.economicsdiscussion.net/game-theory/5-types-of-games-in-game-theory-with-diagram/3827

incentive compatibility

– is the system stable if every player follows their incentive?

"a mechanism is called incentive-compatible (IC) if every participant can achieve the best outcome to themselves just by acting according to their true preferences." *

* https://en.wikipedia.org/wiki/Incentive_compatibility

outline

- incentive compatibility
  - **chain selection**
  - incentives for transaction propagation
  - transaction pricing
- resource investment and transaction selection
  - miner resource investment
  - block sizing and transaction selection
- rational mining and exploitation

chain selection

- [Kroll, 2013]
  - chain selection strategy: map current log to a chosen branch $S(L) = b^*$
  - monotonic strategy

$$\left.\begin{array}{c} L_r \xrightarrow{\text{append } b} L_{r+1} \\ S(L_r) = \text{parent}(b) \end{array}\right\} \implies S(L_{r+1}) = b$$

    - miner consistently works on the same branch
    - e.g. longest chain rule
  - **all miners play the same monotonic strategy: Nash equilibrium**

Kroll, J.A., Davey, I., & Felten, E.W. (2013). The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries

outline

- incentive compatibility
  - chain selection
  - **incentives for transaction propagation**
  - transaction pricing
- resource investment and transaction selection
  - miner resource investment
  - block sizing and transaction selection
- rational mining and exploitation

incentives for transaction propagation

- PoW is based on competition
- informed participants have an incentive not to propagate information to others
  - DARPA Red Balloon Challenge (2009)
- nodes do not pay for network infrastructure, no incentive to invest
  - tragedy of the commons
  - free-rider problem

incentives for transaction propagation

- design a mechanism that
  - incentivizes information propagation
  - counters the dis-incentive arising from competition
  - is Sybil-resistant
  - has low price overhead

incentives for transaction propagation

- keep track of propagation path
  - authorizing chain [Babaioff, 2011]
  - **signed propagation chain** [Abraham, 2016]
  - propagation path [Ersoy, 2018]
- portion of tx fee drops with each hop count [Ersoy, 2018] [Lancashire, 2019]
- nodes are incentivized to establish shortest path to miner

Babaioff, M., Dobzinski, S., Oren, S., & Zohar, A. (2011). On Bitcoin and Red Balloons

Abraham, I., et al. (2016). Solidus: An Incentive-compatible Cryptocurrency Based on Permissionless Byzantine Consensus

Ersoy, O.K., et al. (2018). Transaction Propagation on Permissionless Blockchains: Incentive and Routing Mechanisms

Lancashire, D. (2019). Saito: A Big-Data Blockchain with Proof-of-Transactions

incentives for transaction propagation

- other option: subscription-based relay networks

outline

- incentive compatibility
  - chain selection
  - incentives for transaction propagation
  - **transaction pricing**
- resource investment and transaction selection
  - miner resource investment
  - block sizing and transaction selection
- rational mining and exploitation

transaction pricing

- Bitcoin’s current fee mechanism: pay-your-bid auction
  - competition in the fee market should counter the tragedy of the commons
  - block size implicitly sets price
- bit shading, strategic bidding
  - users can check the mempool and set a lower price than their true preference
- insufficient revenue extraction in highly scalable blockchains
  - if blocks are not full, users can set arbitrarily small fees
  - mining might become less profitable, which will eventually make the system less secure

Lavi, R., Sattath, O., & Zohar, A. (2017). Redesigning Bitcoin's Fee Market

transaction pricing

- desired properties of a pricing system
  - high social welfare (utility to society)
  - revenue extraction (profitable for miners)
  - truthful bidding (users are incentivized to show their preferences)
  - adaptivity (no protocol changes needed to adjust)
  - accounting for time (users can set their urgency)
  - resistance to miner manipulation
  - resistance to manipulation via side payments

Lavi, R., Sattath, O., & Zohar, A. (2017). Redesigning Bitcoin's Fee Market

transaction pricing

- Monopolistic Price Mechanism
  - users set maximum price they are willing to pay as fee
  - miners choose the number of transactions to include in the block (k)
  - all transactions pay the smallest bid in the block

$$\boldsymbol{b} = (b_1, b_2, \ldots, b_n) \qquad b_1 > b_2 > \cdots > b_n$$

$$R(\boldsymbol{b}) = \max_{k \in \{1,\ldots,n\}} k \cdot b_k$$

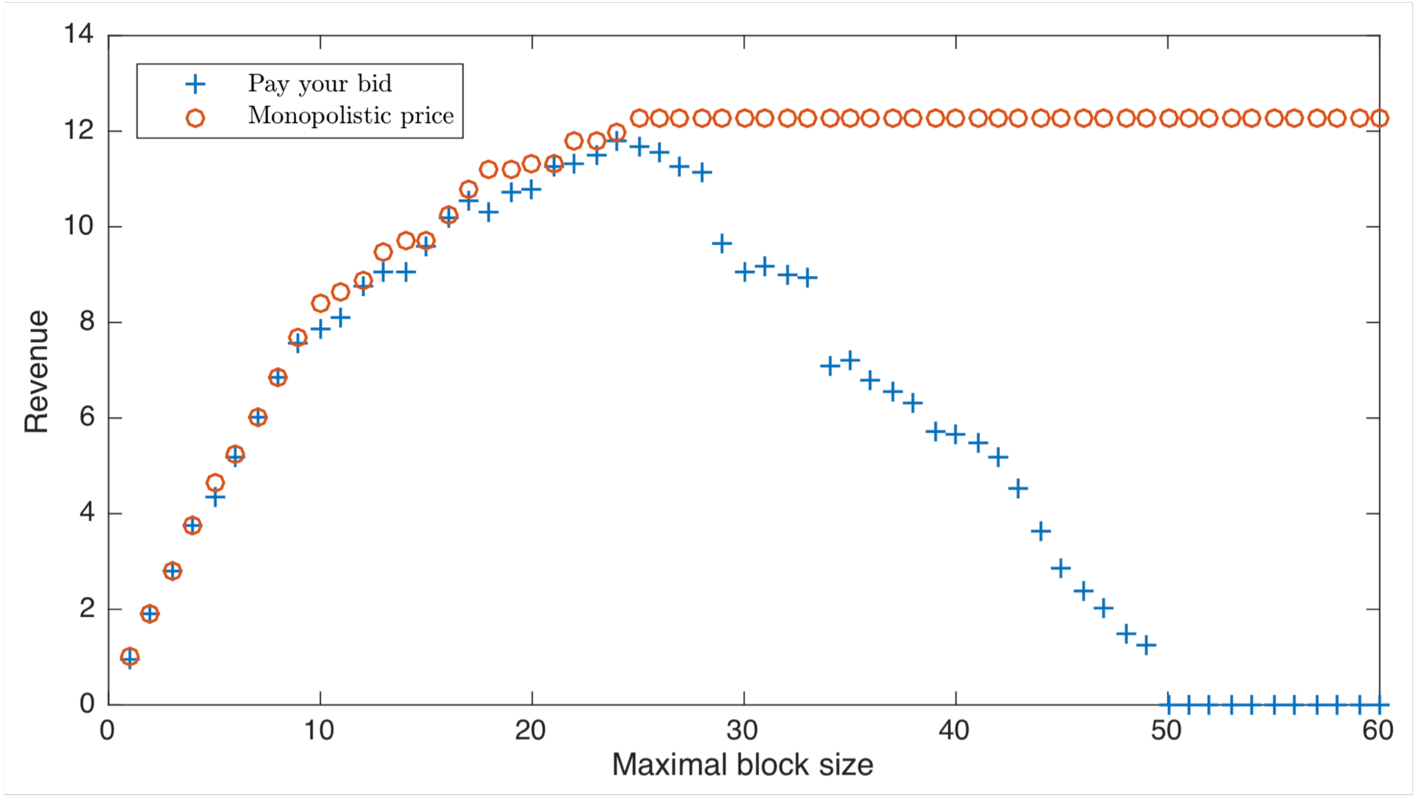
Lavi, R., Sattath, O., & Zohar, A. (2017). Redesigning Bitcoin's Fee Market

transaction pricing

- Monopolistic Price Mechanism
  - dynamic block size
  - nearly incentive compatible; honest behaviour is nearly an equilibrium (proven in [Yao, 2018])
    - analyze as a single-shot game (impatient users)
    - the relative profit of strategic bidding decreases with the number of bids
  - no need for strategic bidding, fee estimation, etc.

Yao, A.C. (2018). An Incentive Analysis of some Bitcoin Fee Designs
Lavi, R., Sattath, O., & Zohar, A. (2017). Redesigning Bitcoin's Fee Market

transaction pricing



Lavi, R., Sattath, O., & Zohar, A. (2017). Redesigning Bitcoin's Fee Market

others

- Goldfinger attack [Kroll, 2013]
  - the attacker achieves utility outside the Bitcoin economy
    - law enforcement
    - social protest
    - investment gain (shorting)

Kroll, J.A., Davey, I., & Felten, E.W. (2013). The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries

others

- death spiral [Kroll, 2013]
    1. people lose confidence in Bitcoin
    2. Bitcoin price falls
    3. miners lose revenue and some leave
    4. lower mining rate makes the system easier to attack
    5. go back to 1.

Kroll, J.A., Davey, I., & Felten, E.W. (2013). The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries

others

- consensus levels [Kroll, 2013]
  - **state** (ledger)
  - value (market)
  - rules (governance)
- governance mechanism is rarely discussed
  - social process, where a small group have large power (maintainers)
  - possibility of forks regulates the decision-makers
  - protocol changes, the DAO attack, re-align incentives in the future

Kroll, J.A., Davey, I., & Felten, E.W. (2013). The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries

outline

- incentive compatibility
  - chain selection
  - incentives for transaction propagation
  - transaction pricing
- **resource investment and transaction selection**
  - miner resource investment
  - block sizing and transaction selection
- rational mining and exploitation

outline

- incentive compatibility
  - chain selection
  - incentives for transaction propagation
  - transaction pricing
- resource investment and transaction selection
  - **miner resource investment**
  - block sizing and transaction selection
- rational mining and exploitation

miner resource investment

- how do miners decide whether to participate or not?
- model the problem as a static all-pay contest with complete information
  - computational power $h_i \geq 0$
  - mining reward $R \geq 0$
  - cost function $C_i(h_i) = c_i h_i$

Dimitri, N. (2017). Bitcoin Mining as a Contest

miner resource investment

- profit

$$\Pi_i(h_i) = \begin{cases} R - c_i h_i & & \frac{h_i}{h_{(n)}} & & h_i > 0 \\ -c_i h_i & \text{with probability} & \frac{h_{-i}}{h_{(n)}} & \text{if} & h_i > 0 \\ 0 & & 1 & & h_i = 0 \end{cases}$$

$$\langle \Pi_i(h_i) \rangle = \frac{R h_i}{h_{(n)}} - c_i h_i, \quad i = 1, \ldots, n.$$

Dimitri, N. (2017). Bitcoin Mining as a Contest

miner resource investment

- finding the equilibrium

$$\frac{\delta}{\delta h_i}\left(\frac{Rh_i}{h_{(n)}} - c_i h_i\right) = \frac{Rh_{(n)} - Rh_i}{h_{(n)}^2} - c_i = 0 \quad \rightarrow \quad \frac{R\left(h_{(n)} - h_i\right)}{h_{(n)}^2} = c_i$$

$$c_{(n)} = \sum_{i=1}^{n} c_i = \sum_{i=1}^{n} \frac{R\left(h_{(n)} - h_i\right)}{h_{(n)}^2} = \frac{Rnh_{(n)} - Rh_{(n)}}{h_{(n)}^2} = \frac{R(n-1)}{h_{(n)}} \quad \rightarrow \quad h_{(n)} = \frac{R(n-1)}{c_{(n)}}$$

$$h_i = h_{(n)}\left(1 - \frac{c_i h_{(n)}}{R}\right) = h_{(n)}\left(1 - \frac{c_i(n-1)}{c_{(n)}}\right) = h_{(n)}\left(\frac{c_{(n)} - c_i(n-1)}{c_{(n)}}\right) = \frac{R(n-1)\left[c_{(n)} - c_i(n-1)\right]}{c_{(n)}^2}$$

miner resource investment

– the unique pure strategy Nash equilibrium of the Bitcoin mining game is

$$(h_1, \dots, h_n) \quad \text{where} \quad h_i = \frac{R(n-1)\left[c_{(n)} - c_i(n-1)\right]}{c_{(n)}^2}$$

– observations

1. mining activity depends on the miner's relative cost structure only and not on R

$$h_i > 0 \quad \Longrightarrow \quad c_{(n)} - c_i(n-1) > 0$$

Dimitri, N. (2017). Bitcoin Mining as a Contest

miner resource investment

- the unique pure strategy Nash equilibrium of the Bitcoin mining game is

$$(h_1, \ldots, h_n) \quad \text{where} \quad h_i = \frac{R(n-1)\left[c_{(n)} - c_i(n-1)\right]}{c_{(n)}^2}$$

- observations

  2. the expected profit is given by

$$\langle \Pi_i(h_i) \rangle = R\left(\frac{h_i}{h_{(n)}}\right)^2$$

miner resource investment

- further observations
  3. decreasing c_i might increase profits and event exclude other miners if $n > 2$
  4. with only 2 active miners, both will have positive expected profit regardless of the other
  5. monopoly could only form if investment outside Bitcoin would be more profitable

Dimitri, N. (2017). Bitcoin Mining as a Contest

outline

- incentive compatibility
  - chain selection
  - incentives for transaction propagation
  - transaction pricing
- resource investment and transaction selection
  - miner resource investment
  - **block sizing and transaction selection**
- rational mining and exploitation

block sizing & transaction selection

- how does the block size affect miner revenue?
  - intuition: more transactions mean more revenue
  - reality: higher TPS might bring down transaction fees
- how do miners pick transactions?
  - intuition: pick many transactions of high value
  - reality: balance trade-off between reward and orphaning risk
- can mining empty blocks be an equilibrium?

block sizing & transaction selection

- [Houy, 2014]
  - fix block size + fee market is equivalent to fix transaction fee
  - free block size + fee market is unsustainable
  - model as market for a physical good with bitcoin as means of exchange
  - assumption: marginal cost for attaching is estimated to be 0

Houy, N. (2014). The Economics of Bitcoin Transaction Fees

block sizing & transaction selection

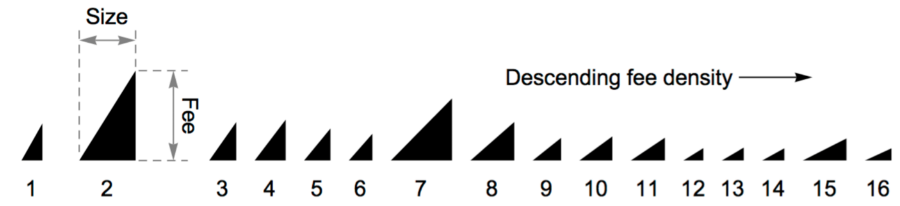
- [Rizun, 2016]
  - miners have a nonzero marginal cost for attaching more txs (orphaning risk)
  - miner's profit equation

$$\langle V \rangle = (R + M)\frac{h}{H}\left(1 - P_{orphan}\right) \qquad P_{orphan} \approx 1 - e^{-\frac{\tau}{T}}$$

$$\langle \Pi \rangle = (R + M)\frac{h}{H}e^{-\frac{\tau}{T}} - \langle C \rangle$$

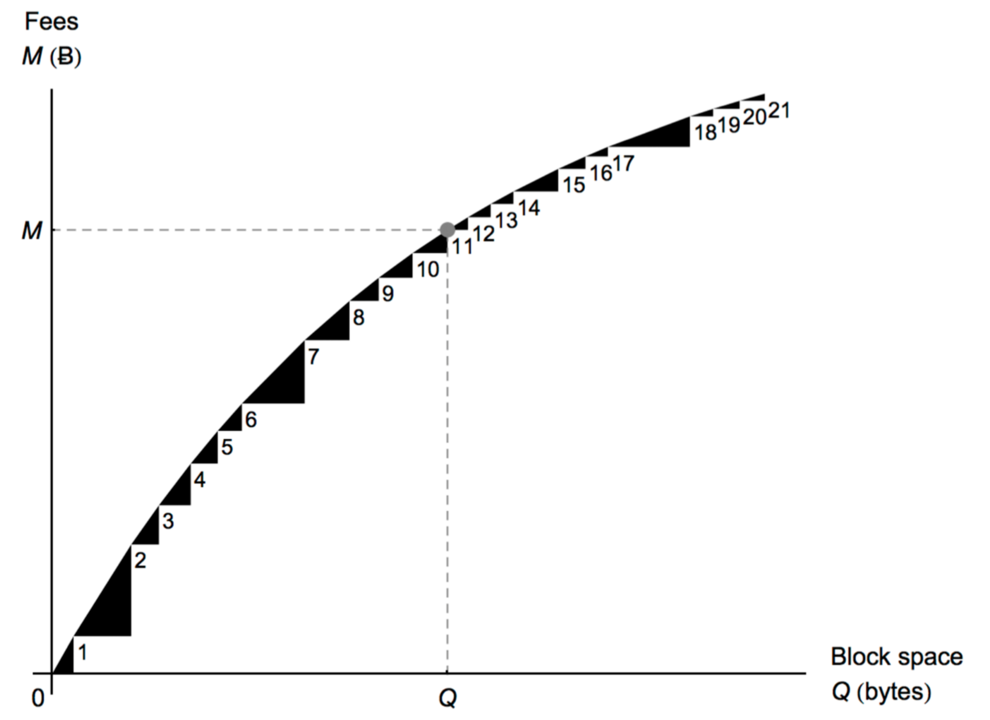
block sizing & transaction selection

- the mempool demand curve



$$M(b) = \sum_{i=1}^{b} \text{fee}_i$$

$$Q(b) = \sum_{i=1}^{b} \text{size}_i$$



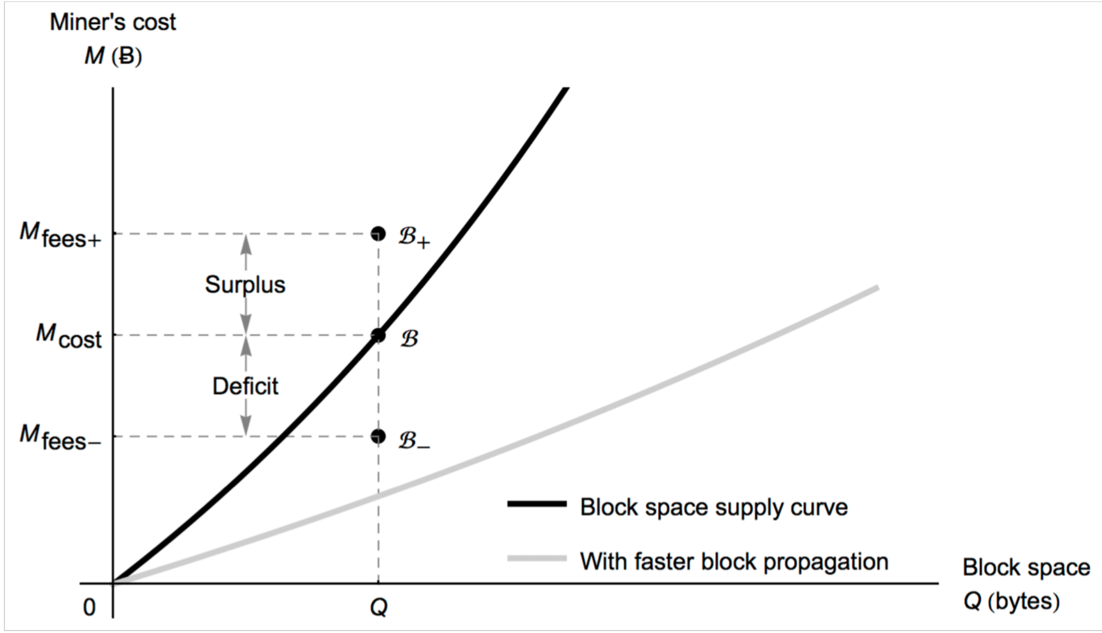
Rizun, P.R. (2016). A Transaction Fee Market Exists Without a Block Size Limit

block sizing & transaction selection

– the block space supply curve

$$\frac{d}{dQ}\langle\Pi\rangle = 0 \quad \Longrightarrow$$

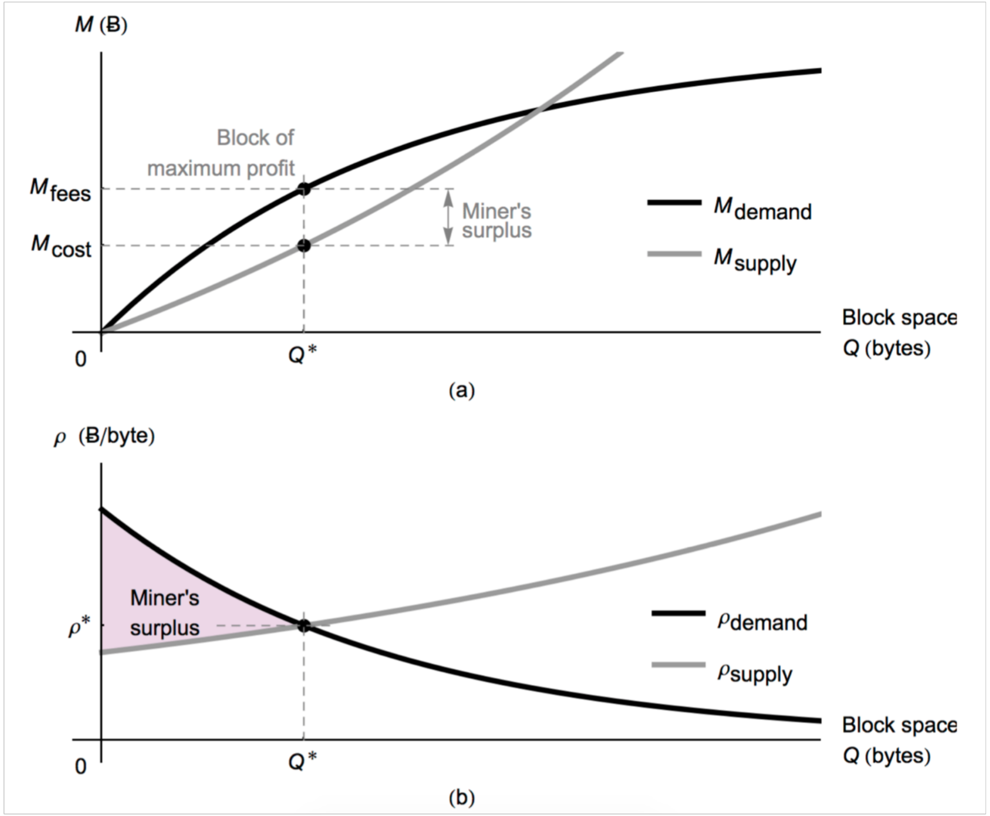
$$M_{supply}(Q) = R\left(e^{\frac{\tau(Q)-\tau(0)}{T}} - 1\right)$$



Rizun, P.R. (2016). A Transaction Fee Market Exists Without a Block Size Limit

block sizing & transaction selection

– maximum profit



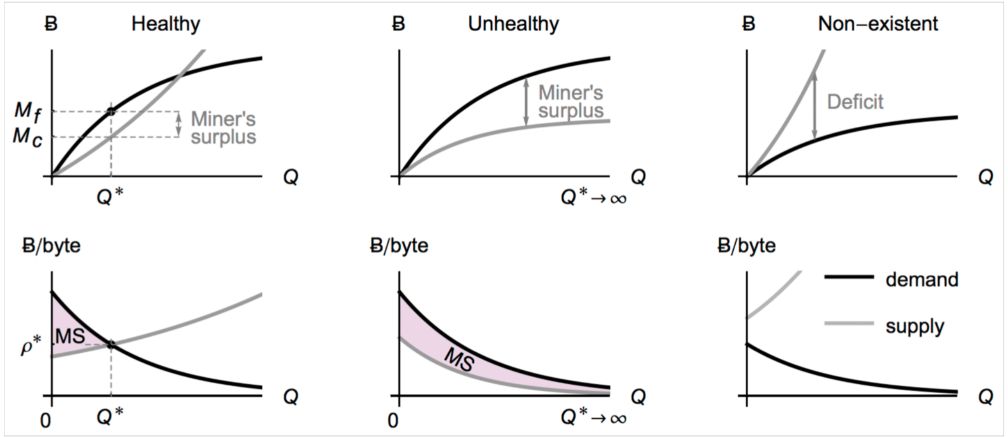
Rizun, P.R. (2016). A Transaction Fee Market Exists Without a Block Size Limit

block sizing & transaction selection

- types of fee markets
  - healthy fee market: miner’s profit is maximized at finite block size
  - unhealthy fee market: miner’s profit increases unbounded
  - non-existent market: any block size causes deficit

Rizun, P.R. (2016). A Transaction Fee Market Exists Without a Block Size Limit

block sizing & transaction selection



Market type	Block size (maximizes profit)	Demand constraint[17]	Supply constraint	Propagation time asymptote	Physically possible?
Healthy	Finite		$\frac{d\rho_{\text{supply}}}{dQ} > 0$	$\tau(Q) > O(\log Q)$	Yes
Unhealthy	Infinite	$\frac{d\bar{\rho}_{\text{demand}}}{dQ} < 0$	$\frac{d\rho_{\text{supply}}}{dQ} < 0$	$\tau(Q) < O(\log Q)$	No
Non-existent	Zero		$\rho_{\text{supply}} > \bar{\rho}_{\text{demand}}$	-	Yes

Rizun, P.R. (2016). A Transaction Fee Market Exists Without a Block Size Limit

block sizing & transaction selection

- [Houy, 2016]
  - equilibrium with current block reward and fees is mining empty blocks
  - why not then?
    - miners have revenue in Bitcoin
    - default / ideology / reputation
    - lack of awareness of such predictions

Houy, N. (2016). The Bitcoin Mining Game

outline

- incentive compatibility
  - chain selection
  - incentives for transaction propagation
  - transaction pricing
- resource investment and transaction selection
  - miner resource investment
  - block sizing and transaction selection
- **rational mining and exploitation**

selfish mining

- keep new block, continue mining on it secretly
  - violate information propagation protocol
- release attacker chain when public chain length approaches it

Eyal, I., & Sirer, E.G. (2014). Majority is Not Enough: Bitcoin Mining is Vulnerable

Nayak, K., et al. (2015). Stubborn Mining: Generalizing Selfish Mining and Combining with an Eclipse Attack

Carlsten, M. (2016). The Impact of Transaction Fees on Bitcoin Mining Strategies

Sapirshtein, A., Sompolinsky, Y., & Zohar, A. (2016). Optimal Selfish Mining Strategies in Bitcoin

Göbel, J., et al. (2016). Bitcoin Blockchain Dynamics: The Selfish-mine Strategy in the Presence of Propagation Delay

Beccuti, J., & Jaag, C. (2017). The Bitcoin Mining Game: On the Optimality of Honesty in Proof-of-work Consensus Mechanism

block withholding (BWH)

- split hash power into different pools
  - part A: mine honestly in pool A
  - part B: mine but do not reveal in pool B
- decrease overall hashrate
- decrease revenue in B, increase in A

Eyal, I. (2015). The Miner's Dilemma

Tosh, D.K., et al. (2017). Security Implications of Blockchain Cloud with Analysis of Block Withholding Attack

Luu, L., et al. (2015). On Power Splitting Games in Distributed Computation: The Case of Bitcoin Pooled Mining

Laszka, A., et al. (2015). When Bitcoin Mining Pools Run Dry - A Game-Theoretic Analysis of the Long-Term Impact of Attacks ...

Bag, S., Ruj, S., & Sakurai, K. (2017). Bitcoin Block Withholding Attack: Analysis and Mitigation

other attacks on pools

- Lie-in-Wait (LIW)
- pool hopping
- etc.

Rosenfeld, M. (2011). Analysis of Bitcoin Pooled Mining Reward Systems

final thoughts

- incentives are an integral part of blockchain system design
- it is hard to get it right and it is hard to know how the system will behave
- you can have nice results but it will be useless if your model is not relevant

references

Kroll, J.A., Davey, I., & Felten, E.W. (2013). The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries ✓
https://weis2013.econinfosec.org/papers/KrollDaveyFeltenWEIS2013.pdf

Babaioff, M., Dobzinski, S., Oren, S., & Zohar, A. (2011). On Bitcoin and Red Balloons
https://www.avivz.net/pubs/12/Bitcoin_EC0212.pdf

Abraham, I., Malkhi, D., Nayak, K., Ren, L., & Spiegelman, A. (2016). Solidus: An Incentive-compatible Cryptocurrency Based on Permissionless Byzantine Consensus
https://arxiv.org/pdf/1612.02916v1.pdf

Ersoy, O.K., Ren, Z., Erkin, Z., & Lagendijk, R.L. (2018). Transaction Propagation on Permissionless Blockchains: Incentive and Routing Mechanisms
https://arxiv.org/pdf/1712.07564.pdf

Lancashire, D. (2019). Saito: A Big-Data Blockchain with Proof-of-Transactions
https://saito.tech/saito-whitepaper.pdf

references

Lavi, R., Sattath, O., & Zohar, A. (2017). Redesigning Bitcoin's Fee Market ✓
https://arxiv.org/pdf/1709.08881.pdf

Yao, A.C. (2018). An Incentive Analysis of some Bitcoin Fee Designs
https://arxiv.org/pdf/1811.02351.pdf

Dimitri, N. (2017). Bitcoin Mining as a Contest ✓
https://ledger.pitt.edu/ojs/index.php/ledger/article/download/96/67

Houy, N. (2014). The Economics of Bitcoin Transaction Fees
https://halshs.archives-ouvertes.fr/halshs-00951358/file/1407.pdf

Rizun, P.R. (2016). A Transaction Fee Market Exists Without a Block Size Limit ✓
https://www.bitcoinunlimited.info/resources/feemarket.pdf

Houy, N. (2016). The Bitcoin Mining Game
https://www.ledgerjournal.org/ojs/index.php/ledger/article/download/13/59

references

Eyal, I., & Sirer, E.G. (2014). Majority is Not Enough: Bitcoin Mining is Vulnerable ✓
https://www.cs.cornell.edu/%7Eie53/publications/btcProcFC.pdf

Nayak, K., Kumar, S., Miller, A., & Shi, E. (2015). Stubborn Mining: Generalizing Selfish Mining and Combining with an Eclipse Attack
https://eprint.iacr.org/2015/796.pdf

Carlsten, M. (2016). The Impact of Transaction Fees on Bitcoin Mining Strategies
ftp://ftp.cs.princeton.edu/techreports/2016/983.pdf

Sapirshtein, A., Sompolinsky, Y., & Zohar, A. (2016). Optimal Selfish Mining Strategies in Bitcoin
https://arxiv.org/pdf/1507.06183.pdf

Göbel, J., Keeler, H.P., Krzesinski, A.E., & Taylor, P.G. (2016). Bitcoin Blockchain Dynamics: The Selfish-mine Strategy in the Presence of Propagation Delay
https://arxiv.org/pdf/1505.05343.pdf

references

Beccuti, J., & Jaag, C. (2017). The Bitcoin Mining Game: On the Optimality of Honesty in Proof-of-work Consensus Mechanism
http://www.swiss-economics.ch/RePEc/files/0060JaagBeccuti.pdf

Eyal, I. (2015). The Miner's Dilemma ✓
https://www.cs.cornell.edu/~ie53/publications/btcPoolsSP15.pdf

Tosh, D.K., Shetty, S., Liang, X., Kamhoua, C.A., Kwiat, K.A., & Njilla, L. (2017). Security Implications of Blockchain Cloud with Analysis of Block Withholding Attack
https://ieeexplore.ieee.org/document/7973732

Luu, L., Saha, R., Parameshwaran, I., Saxena, P., & Hobor, A. (2015). On Power Splitting Games in Distributed Computation: The Case of Bitcoin Pooled Mining
https://eprint.iacr.org/2015/155.pdf

Laszka, A., Johnson, B., & Grossklags, J. (2015). When Bitcoin Mining Pools Run Dry - A Game-Theoretic Analysis of the Long-Term Impact of Attacks Between Mining Pools
http://aronlaszka.com/papers/laszka2015when.pdf

references

Bag, S., Ruj, S., & Sakurai, K. (2017). Bitcoin Block Withholding Attack: Analysis and Mitigation
https://ieeexplore.ieee.org/document/7728010

Rosenfeld, M. (2011). Analysis of Bitcoin Pooled Mining Reward Systems
https://arxiv.org/pdf/1112.4980.pdf

Wang, W., Hoang, D.T., Xiong, Z., Niyato, D., Wang, P., Hu, P., & Wen, Y. (2019). A Survey on Consensus Mechanisms and Mining Management in Blockchain Networks ✓
https://arxiv.org/pdf/1805.02707.pdf