Beyond the doomsday economics of "Proof-of-work" in cryptocurrencies

By Raphael Auer, Bank for International Settlements

The views presented in this document are those of the author and not those of the Bank for International Settlements

What outlook for cryptocurrencies modelled on POW?

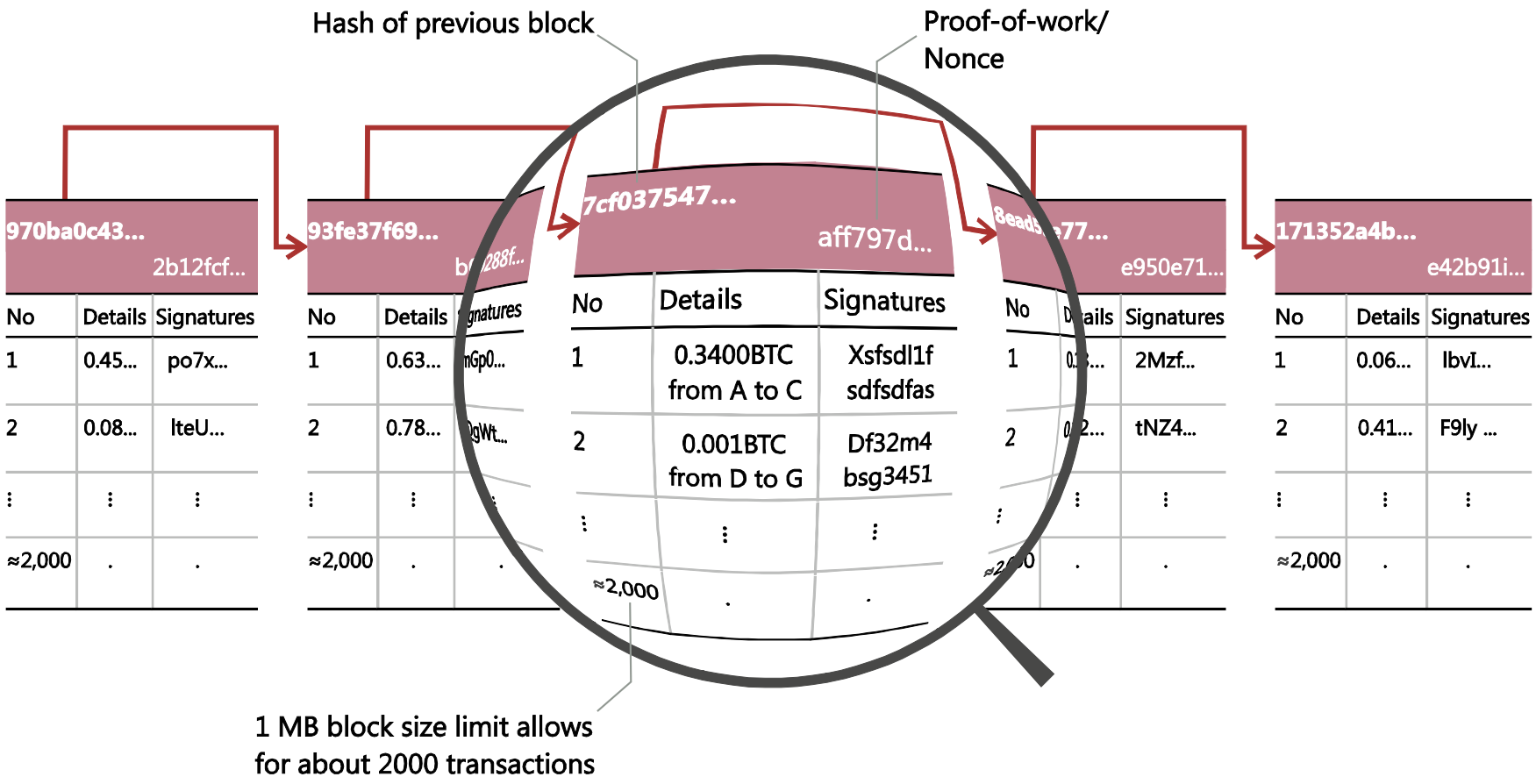
- Known technical issues: volatility, limited speed & scalability, etc. (BIS (2018))
  - But: Bitcoin has not been successfully attacked
- What about the outlook? Two limitations interact:
  - POW security is costly (Chiu and Koeppl (17/19), Budish (18))
  - Transaction market does not generate income in line with security (Easely et al. (18) and Huberman et al. (17))

➢ **As the security provided by seignorage/block rewards is phased out, Bitcoin will become vulnerable (finality will take <u>months</u>)**

Outline & sketch of the argument

1. What is proof-of-work security/finality and how costly is it?
   - Nakamoto (2008)'s probabilistic formulation is inadequate - incentives matter
2. How is the necessary mining income generated?
   - Currently, via block rewards/seignorage
   - In the future, transaction fees will have to take over
3. How are fees generated by the transaction market?
   - Without congestion: contribute to security
   - With congestion: faster queuing
4. What is the likely scenario under endogenous entry of users?

Correct ledger deters double spending, POW aims to guarantee integrity of the ledger



Equilibrium difficulty

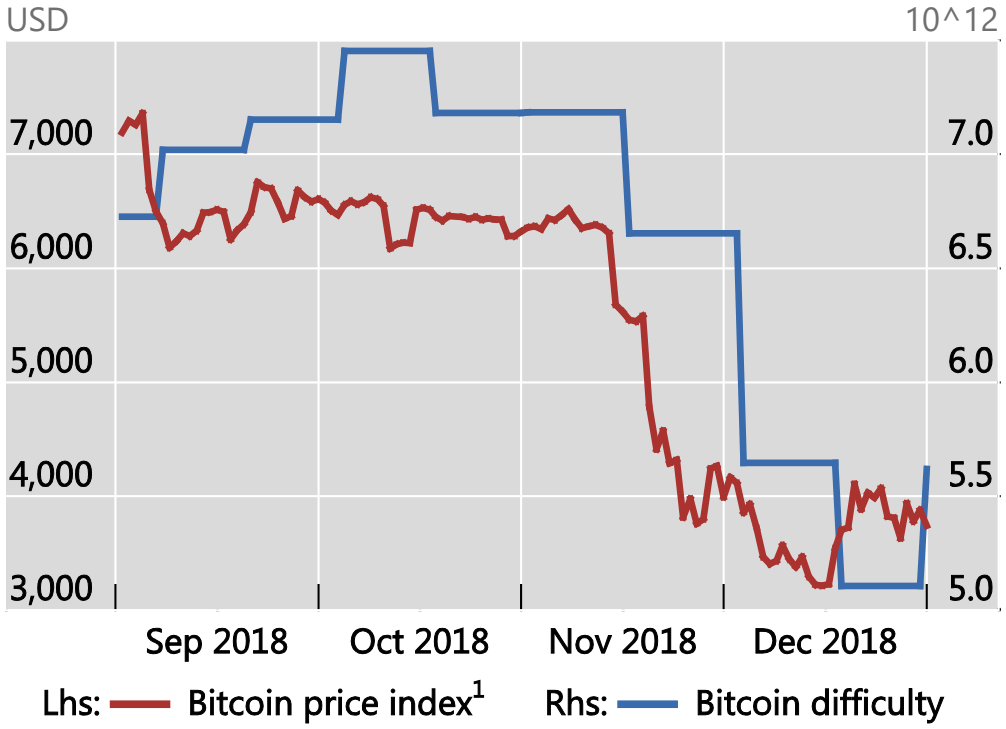
- POW: proof that a certain number of costly «hash» computations have been done, and «difficulty» is the required number of hashes for a valid POW
- Anybody can mine – **free entry condition balanced by difficulty**:

$$\underbrace{P_{USD} * (Block\ reward + \sum Fees)}_{\text{Mining Revenue in USD}} = \underbrace{Difficulty * Cost\ per\ Hash\ in\ USD}_{\text{(expected) Cost of a Proof of Work}}$$

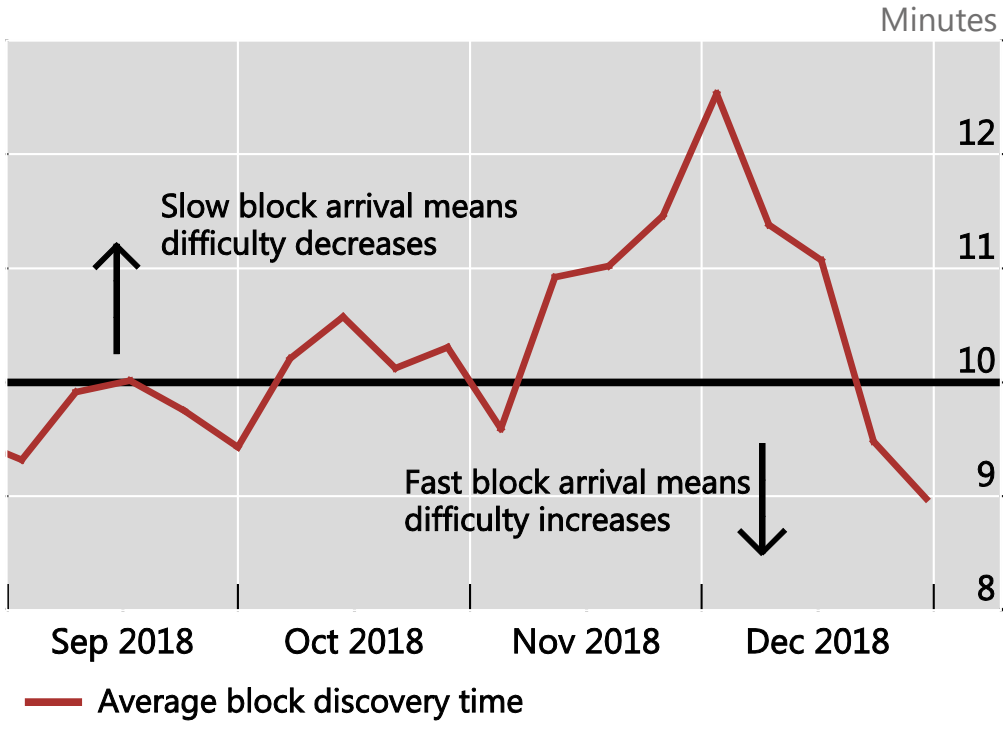
- **Block rewards & fees generate income, which miners burn away by driving up the difficulty.**
  - See Prat and Walter (2018) for richer dynamics

This is economics in action!

Proof-of-work difficulty follows the USD price of bitcoin as…



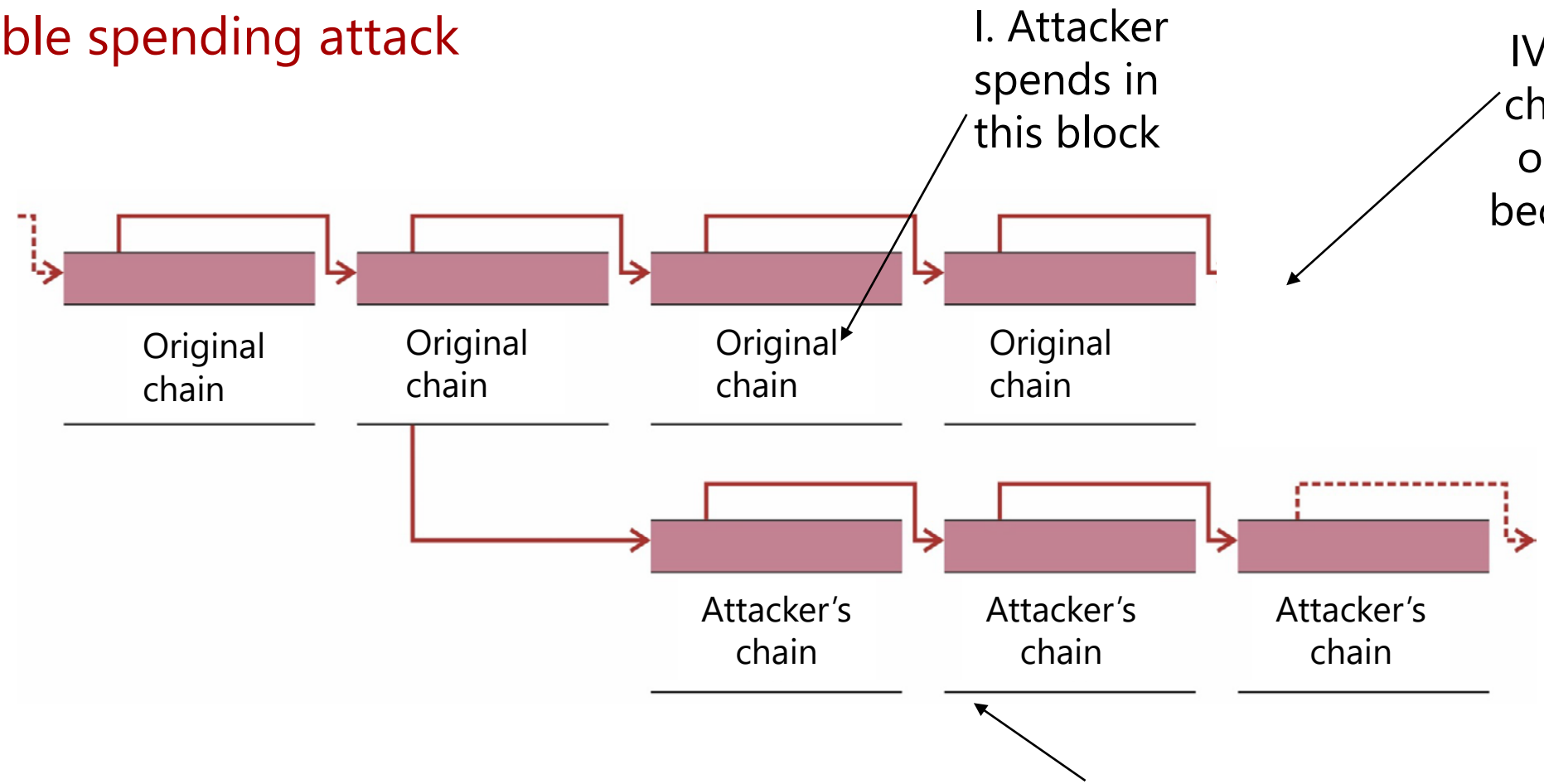
… falling bitcoin prices cause miners to shut down equipment, resulting in fewer block discoveries, and thus a downward re-calibration of difficulty[2]



Proof-of-work-based exchange

- ***How efficient is POW protection? Need to think about incentives at work.***
- Consensus is “longest chain”, ie accept the one transaction history that is most costly to forge
- Imagine an attack:
  - A pays to B
  - B observers blockchain for some time and after a wait time releases merchandise
  - A reverses blockchain
- What is the cost of an attack, what is the benefit?

A double spending attack



Income from a double spending attack

- Need to reverse logic: what is the **waittime** (in blocks) required for finality?
  - Attacker income is $\mathbf{waittime} * (\boldsymbol{Block\ reward} + \boldsymbol{Fees}) + \boldsymbol{spent\ amount}$
  - *"Honest"* mining: $\mathbf{waittime} * (\boldsymbol{Block\ reward} + \boldsymbol{Fees})$**!**
  - **Attacker advantage: strictly higher BTC income!**
- Counterforces:
  - Price of bitcoin collapses following an attack
  - Short-term equipment rental is costly
  - There could be social coordination to undo attack

Introducing "**Economic Payment Finality**"

- **Economic payment finality means $Cost\ Attack > Gain\ Attack$**

$$\underbrace{Waittime}_{\substack{Each\ block \\ adds\ security}} \quad \underbrace{\frac{Mining\ revenue_b^{BTC}}{\sum_{t\ in\ b}\ Amount_t}}_{Transaction\ cost\ in\ \%} > \underbrace{\left(\frac{Cost\ per\ rented\ hash}{Cost\ per\ hash}\frac{P_{USD}}{(1-\Pi^{HF})P_{USD}^{Attack}} - 1\right)^{-1}}_{Attacker\ disadvantage} \qquad \textbf{(1)}$$

- Economic finality in radically different from operational finality in Nakamoto (2008)!
  - Byzantine Fault Tolerance deals with network outages. Here *incentives* matter.

- If price collapse is 1/3 (Bitcoin Gold) and rented hash is twice normal price: **with 1-hour waittime, 8.3% transaction cost**!

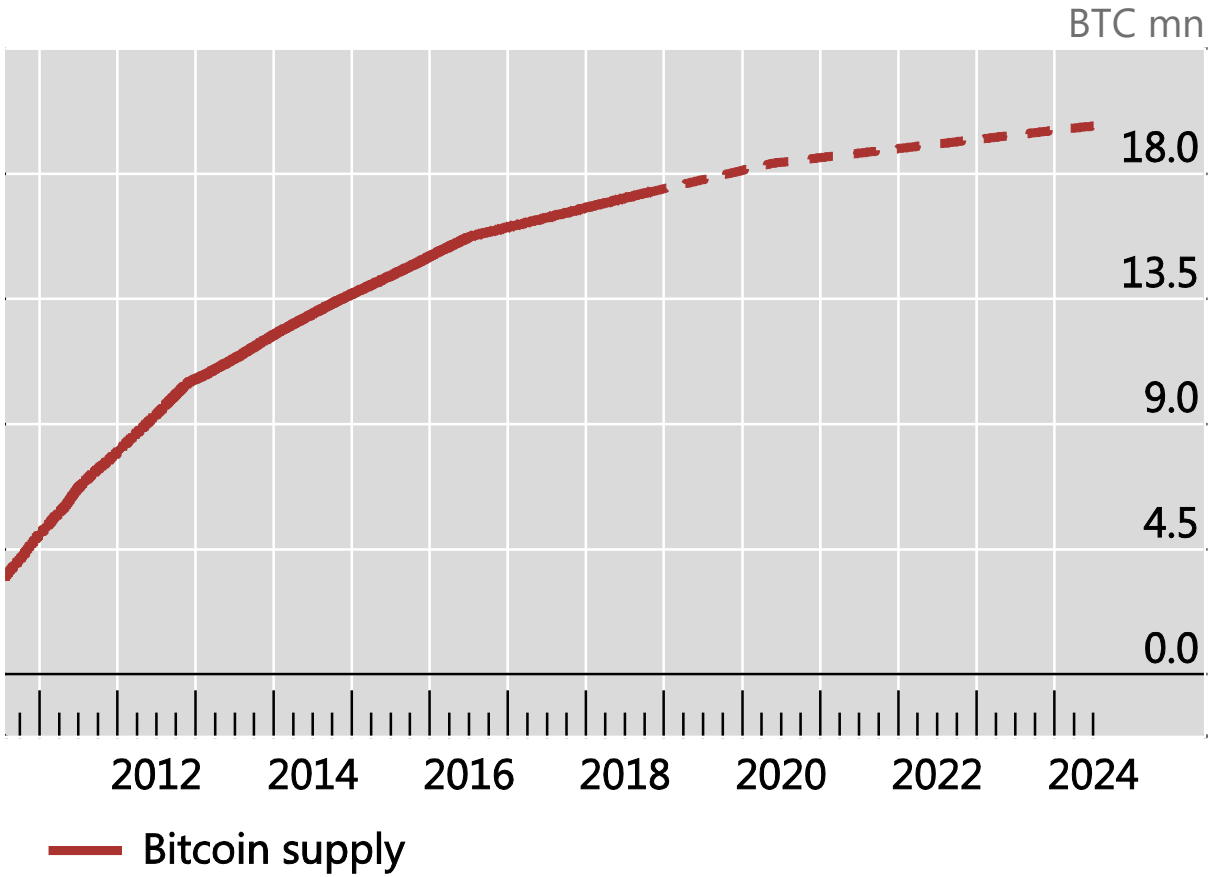
(1) in model notation and for heterogeneous blocks:

- Time is indexed by block number b
- Denote wait time w_b,
- Attacker disadvantage A
- Each transaction i has fee f_i and amount S

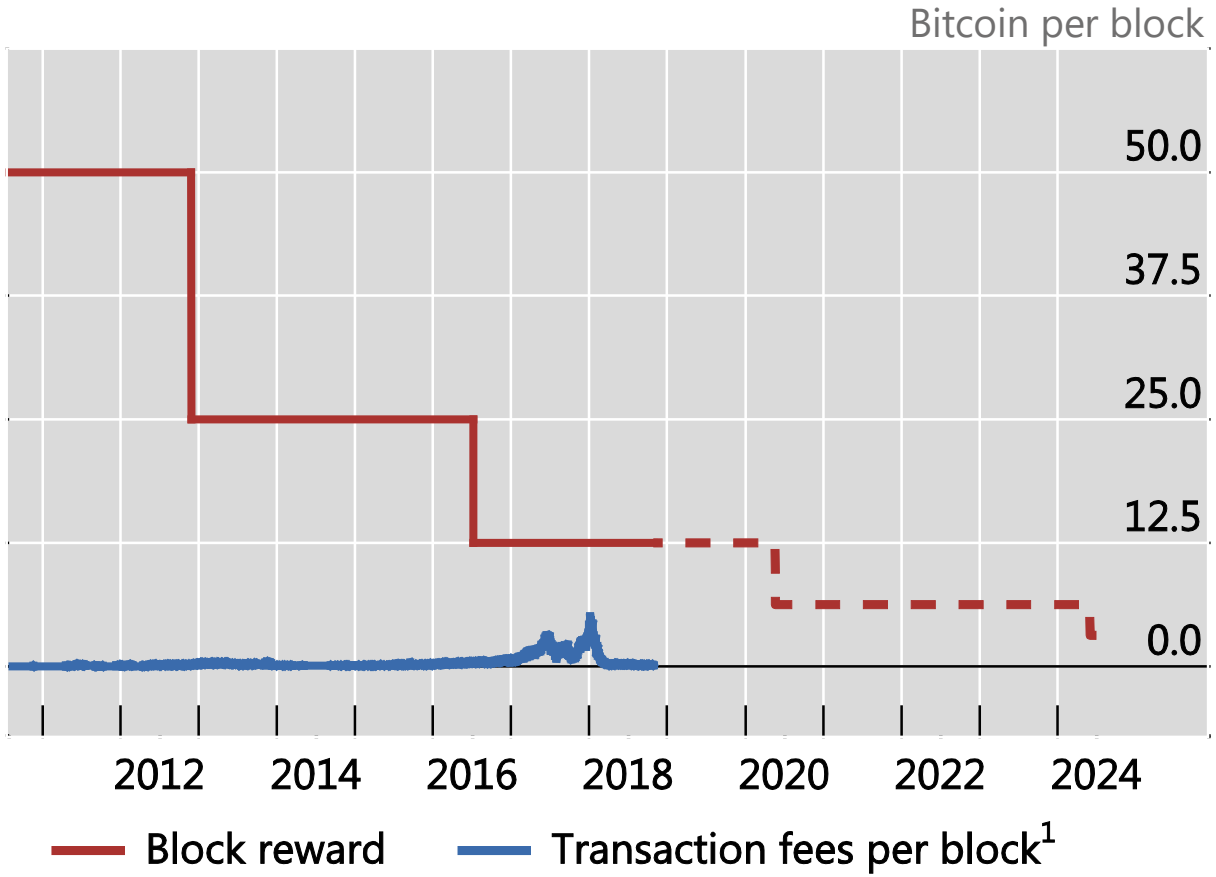
$$\frac{\sum_{t=b}^{t=b+w_b}\left(BR_t + \sum_{j\ in\ t} f_{j,t}\right)}{\sum_{j\ in\ b} S_{j,b}} > A \qquad \textbf{(1)}$$

II. Current security is provided by block rewards

Bitcoins are brought into circulation via "Block rewards"



To date, block rewards are miners' main income source

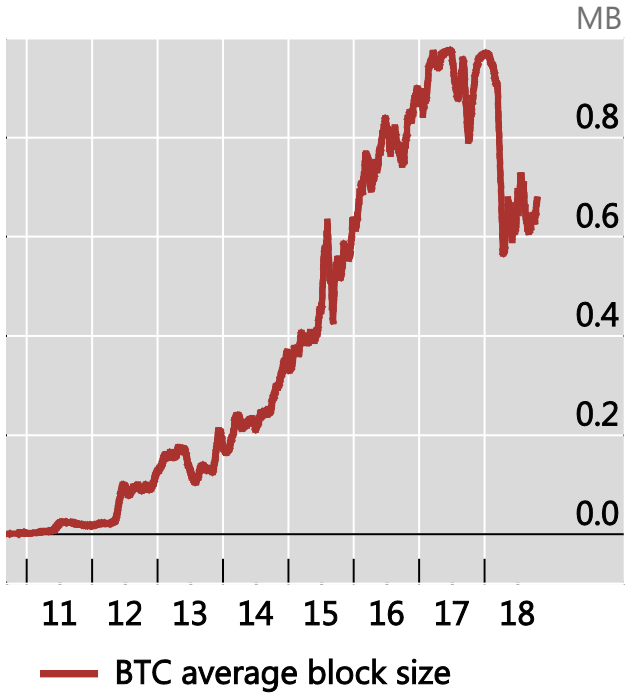


III. Can the transaction market provide high enough fees?

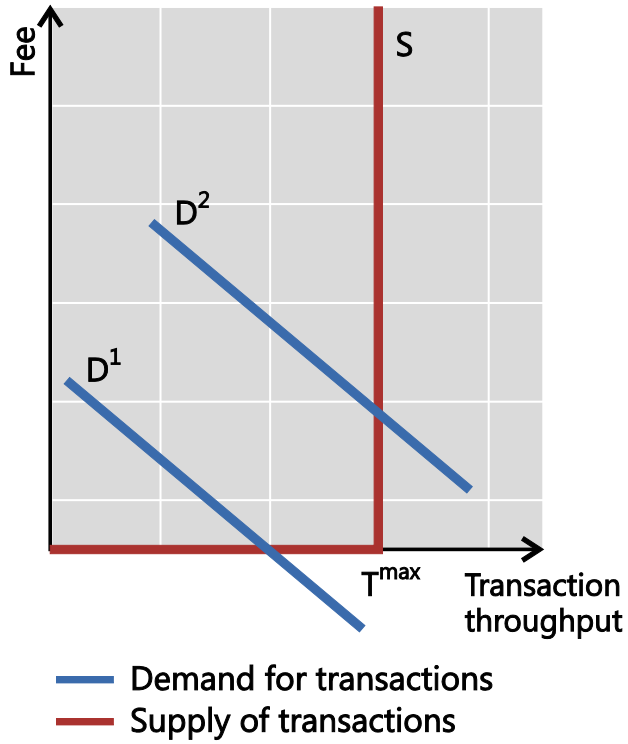
- Transaction market:
  - Users post fees when specifying transaction markets
  - Miners select which transactions to include in their block
  - Blocks have a maximum capacity (1 MB/2000-4000 transactions) and come roughly every 10 minutes
- Easley et al. (forthcoming) and Huberman et al. (2017) examine congestion motive but assume payments are final immediately
  - Instead, I next will examine transaction market in context of payment finality/irreversibility
- **Focus on tragedy of the common chain**
  - POW security determined at the level of the block (& chain), fees set by each users privately. Congestion may help in this respect

The two phases of the transaction market

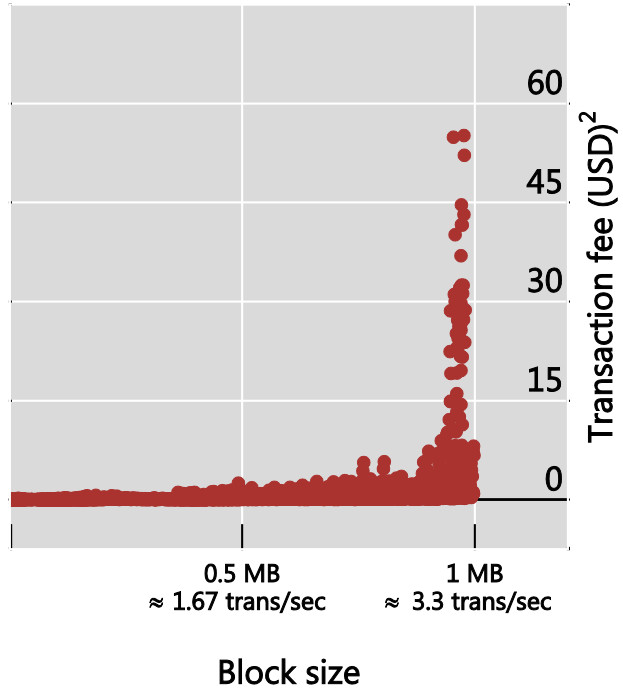
Transaction demand fluctuates widely[1]



With capped supply, demand fluctuations shift fees only when blocks are full…



…which explains the kinked relationship between block size and fees



Model

- Utility from being in the next block b is

$$u_{i,b}^{incl} = v_{i,b} - \mu w_b - f_{i,b} \qquad \textbf{(2)}$$

  - i.i.d. short-lived consumption opportunities $v_{i,b}$ (need to pay amount S)
  - $g(v) \sim \gamma v_{min}^{\gamma} v^{-\gamma-1}$ and public knowledge
  - w_b costly waiting for finality (AFTER inclusion in chain, ie two impatience motives)
  - fee $f_{i,b}$ set by users
  - Congestion if $N_b > B$

Case of non-congestion

- If number of users N_b is lower than block size limit B, no congestion motive
  - Miner includes all transaction with nonzero fees
- Individuals can however influence w_b by offering higher fee
- Rewriting **Equation (1)** from above, w_b has to satisfy:

$$\frac{\sum_{t=b}^{t=b+w_b} BR_t + \sum_{j\ in\ t} f_{j,t}}{SN_b} > A$$

Case of non-congestion

- Assume BR constant (changes only every 4 years in Bitcoin)
- Consider deviation of $f_{i,b}$ from equilibrium where others set $\mathrm{f} = f(v)$:

$$w_b \geq \frac{N_b S A}{BR_b + F_b + \left(f_{i,b} - f\left(v_{i,b}\right)\right)}$$

where $F_b = N_b \int_{v_{min}}^{\infty} f(v) g(v)\, dv$

Fees under non-congestion

- Individuals maximize:

$$u_{i,b}^{incl} = v_{i,b} - \frac{\mu N_b SA}{BR_b + F_b + \left(f_{i,b} - f\left(v_{i,b}\right)\right)} - f_{i,b}$$

- FOC (forgetting integer constraint)

$$f_{i,b} = max\left[0, (\mu N_b SA)^{1/2} - \left(BR_b + F_b - f\left(v_{i,b}\right)\right)\right]$$

- In symmetric equilibrium with positive f:

$$f_b = \left(\frac{\mu SA}{N_b}\right)^{1/2} - \frac{BR_b}{N_b}$$

The tragedy of the common chain under non-congestion

- Presence of N in $\frac{\mu SA}{N}$ term demonstrates free rider problem:

$$f^* = \left(\frac{\mu SA}{N_b}\right)^{1/2} - \frac{BR_b}{N_b}$$

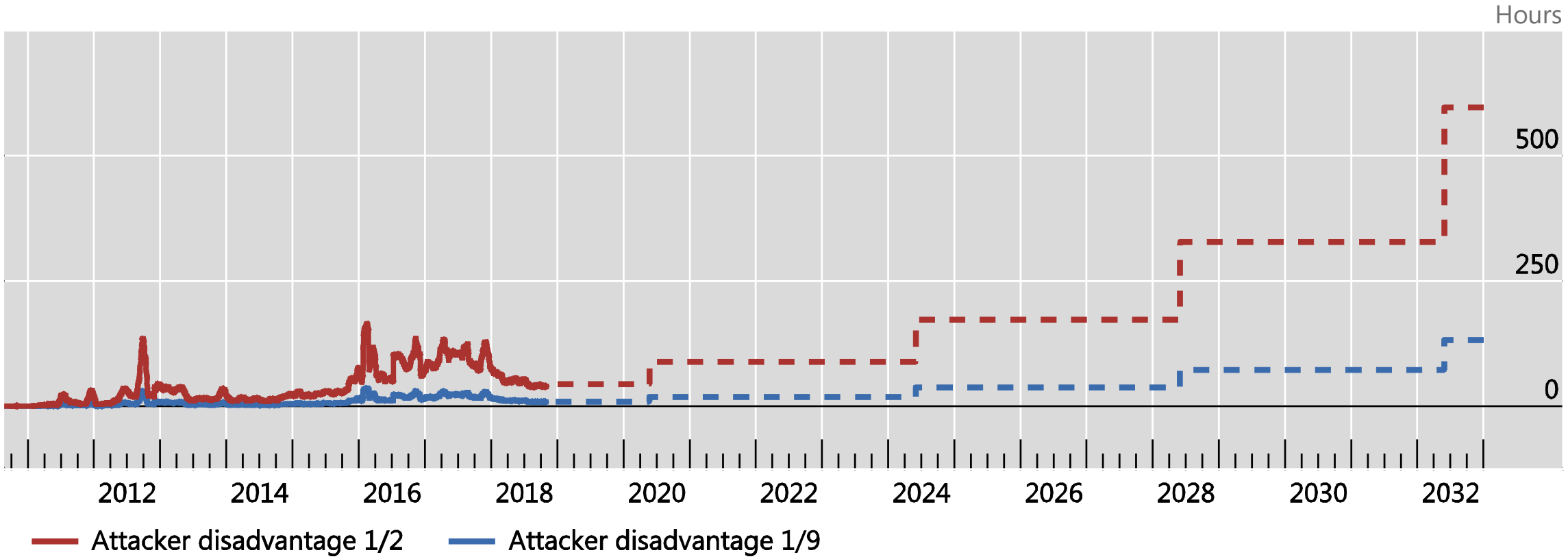
- Compares to optimal fee from point of users (assume they could agree on common $\bar{f}$):

$$\bar{f}^* = (\mu SA)^{1/2} - \frac{BR_b}{N_b}$$

The doomsday economics of POW under noncongestion

Substantially longer wait times are required once block rewards decline

Graph 12



Fees under congestion

- Miners select highest fees into block:

$$N_b \int_{\bar{v}_b}^{\infty} f(v)\, dv = B$$

- B is max transaction number (Block size)
- Competitive bidding (just congestion motive):

$$\bar{v}_b = v_{min}\left({}^{N_b}/_{B}\right)^{1/\gamma} \text{ and } \bar{f}_b = v_{min}\left({}^{N_b}/_{B}\right)^{1/\gamma} - \mu w_b$$

Comparison – fees with/without congestion

- For BR=0, congestion pricing is

$$\bar{f}_b = \frac{1}{2} v_{min} \left({}^{N_b}/_{B} \right)^{1/\gamma} + \frac{1}{2} \sqrt{\left(v_{min} \left({}^{N_b}/_{B} \right)^{1/\gamma} \right)^2 - 4SA\mu}$$

- Whereas for non-congestion, pricing it is:

$$f_b = \left(\frac{\mu SA}{N_b} \right)^{1/2}$$

- These two motives do not interact other than fee is max of f_b, $\bar{f}_b$;
  - N_b has opposite effects on f_b, $\bar{f}_b$: free riding versus congestion

IV. Closing the loop: endogenous entry

- Have analyzed case of congestion and non-congestion, but which one will prevail?
- Assume fixed cost operational cost F (per period)
  - F cost of updating the ledger
  - Assume $v_{min}\frac{\gamma}{\gamma-1} > F$, i.e. there is scope for this system
- Then, the long run (BR=0) outcome can be:
  - Under non-congestion, equilibrium is either no users or very low user numbers (self-stabilising the free rider problem)
  - Noncongestion is always an equilibrium
  - Congestion equilibrium can survive if $v_{min}\frac{1}{\gamma-1} > F$

Conclusion

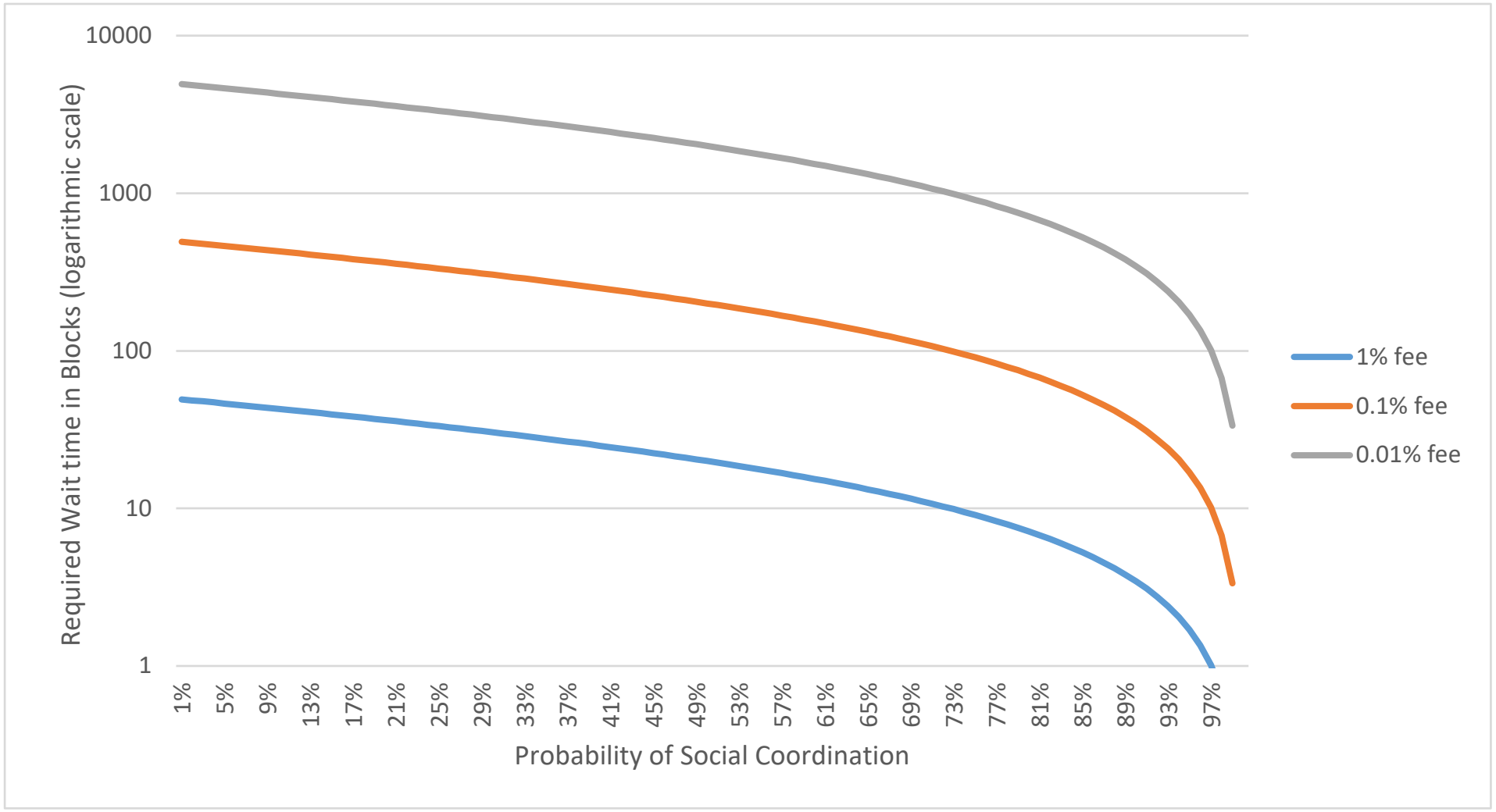
- The interaction of two economic inefficiencies casts doubt on the long-run viability of Bitcoin et al.
  - POW based exchange is either very costly or very slow
  - It is doubtful that the transaction market can generate high income
  - i.e. it could take up to months for a payment to be processed
- Paper discusses alternatives (POS, Lightning, institutionalization)

Appendix

Appendix - Beyond POW

- Second layer technologies (ie Lightning Network)
  - Peer-to-peer prefunded relations allow off-chain payments
  - Yet, technological and economic scaling limits
- Proof-of-stake (POS) (and similar) can tackle fundamental issue
  - Gambling is more efficient that burning electricity
  - Yet, POS requires some overarching coordination (nothing at stake (Saleh 18), long run attacks)
- **This, and Π^{HF}, puts institutionalization to the fore!**

Institutionalisation can greatly improve efficiency



Thinking about LR equilibria:

$$\frac{\gamma}{\gamma - 1} v_{min} >< \mathrm{F}$$

And below:

$$v_{min}(\gamma - 1) >< \mathrm{F}$$

So maybe we can nicely say:

LR is congestion if $v_{min} > (\gamma - 1)\mathrm{F}$

LR is noncongestion if $(\gamma - 1)\mathrm{F} > \frac{\gamma}{\gamma - 1} v_{min} >< \mathrm{F}$

LR is doomsday if $\frac{\gamma}{\gamma - 1} v_{min} < F$

LR equilibrium under non-congestion

$$BR_b + Nf_b = max\left[(\mu SAN_b)^{1/2}, BR_b\right]$$

Phase 2: Average utility $\bar{u}$ if BR is low:

$$\bar{u}_b = \frac{\gamma}{\gamma - 1} v_{min} - \frac{\mu N_b SA}{(\mu SAN_b)^{1/2}} - \left(\left(\frac{\mu SA}{N_b} \right)^{1/2} - \frac{BR_b}{N_b} \right) = \mathrm{F}$$

Solution to (solve for $(N_b)^{1/2}$*)*

$$\left(\frac{\gamma}{\gamma-1} v_{min} - \mathrm{F}\right) N_b - \left(N_b\right)^{3/2} \left(\mu SA\right)^{1/2} - \left(N_b \mu SA\right)^{1/2} + BR_b = 0$$

LR equilibrium under non-congestion

$$BR_b + Nf_b = max\left[(\mu SAN_b)^{1/2}, BR_b\right]$$

Phase 2: Average utility $\bar{u}$ if BR is low:

$$\bar{u}_b = \frac{\gamma}{\gamma - 1} v_{min} - \frac{\mu N_b SA}{(\mu SAN_b)^{1/2}} - \left(\left(\frac{\mu SA}{N_b} \right)^{1/2} - \frac{BR_b}{N_b} \right) = \mathrm{F}$$

Solution to (solve for $(N_b)^{1/2}$*)*

$$\left(\frac{\gamma}{\gamma-1} v_{min} - \mathrm{F}\right) N_b - \left(N_b\right)^{3/2} \left(\mu SA\right)^{1/2} - \left(N_b \mu SA\right)^{1/2} + BR_b = 0$$

LR equilibrium under non-congestion

Phase 3: Average utility $\bar{u}$ if BR=0:

$$\bar{u}_b = \frac{\gamma}{\gamma - 1} v_{min} - (\mu SA)^{1/2} \left((N_b)^{1/2} + (N_b)^{-1/2} \right) = \mathrm{F}$$

$$-N_b + \left(N_b\right)^{1/2} \left(\frac{\frac{\gamma}{\gamma - 1} v_{min} - \mathrm{F}}{(\mu SA)^{1/2}} \right) - 1 = 0$$

$$(N_b)^{1/2} = \frac{-\left(\frac{\frac{\gamma}{\gamma - 1} v_{min} - \mathrm{F}}{(\mu SA)^{1/2}} \right) \pm \sqrt{\left(\frac{\frac{\gamma}{\gamma - 1} v_{min} - \mathrm{F}}{(\mu SA)^{1/2}} \right)^2 - 4}}{-2}$$

LR equilibrium under non-congestion

Two equilibria with BR=0

$$(N_b)^{1/2} = \frac{1}{2}\left(\frac{\frac{\gamma}{\gamma-1}v_{min} - \mathrm{F}}{(\mu SA)^{1/2}}\right) \pm \sqrt{\frac{1}{4}\left(\frac{\frac{\gamma}{\gamma-1}v_{min} - \mathrm{F}}{(\mu SA)^{1/2}}\right)^2 - 1}$$

Surplus under non-congestion: high BR

- If $\left(\frac{\mu SA}{N_b}\right)^{1/2} < \frac{BR}{N_b}$ fees are 0, and average surplus is

$$\bar{u} = v_{min}\frac{\gamma}{\gamma - 1} - \frac{\mu N_b SA}{BR}$$

- More users reduces surplus due to longer wait time
- Assume fixed cost operational cost F (per period).
- Free entry:

$$N^* = \left(v_{min}\frac{\gamma}{\gamma - 1} - F\right)\frac{BR}{\mu SA}$$

Can a congestion equilibrium survive?

$$\int_{\bar{v}_b}^{\infty} f(v)\left(u_b(v)\right)dv = \frac{\bar{v}_b}{\gamma - 1}\left(\frac{v_{min}}{\bar{v}_b}\right)^{\gamma}$$

$$= \frac{v_{min}}{\gamma - 1}\left({}^{N_b}/_{B}\right)^{-(\gamma-1)/\gamma}$$

$$B\left(\frac{v_{min}}{(\gamma-1)F}\right)^{{}^{\gamma}/_{(\gamma-1)}} = N_b,$$ i.e. **yes if** $v_{min} > (\gamma - 1)F$

- «if the worst possible utility draw is still a multiple of fixed costs»
- $v_{min} > \frac{(\gamma-1)}{\gamma} F$ by assumption, but