Block propagation and the *Z*-parameter

June 24, 2016

Peter R. Rizun
Bitcoin Unlimited

Block propagation and the Z-parameter

Related to market price for block space & network's ability to scale

June 24, 2016

Peter R. Rizun
Bitcoin Unlimited

The Z-parameter

$$Z = \frac{\tau}{Q}$$

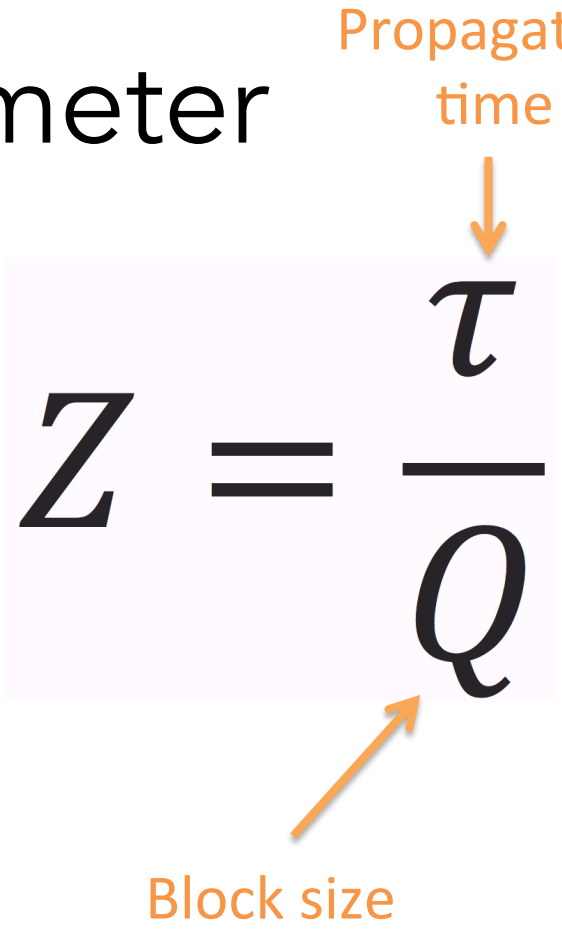
The Z-parameter

- A measure of the network's impedance to the propagation of blocks

$$Z = \frac{\tau}{Q}$$

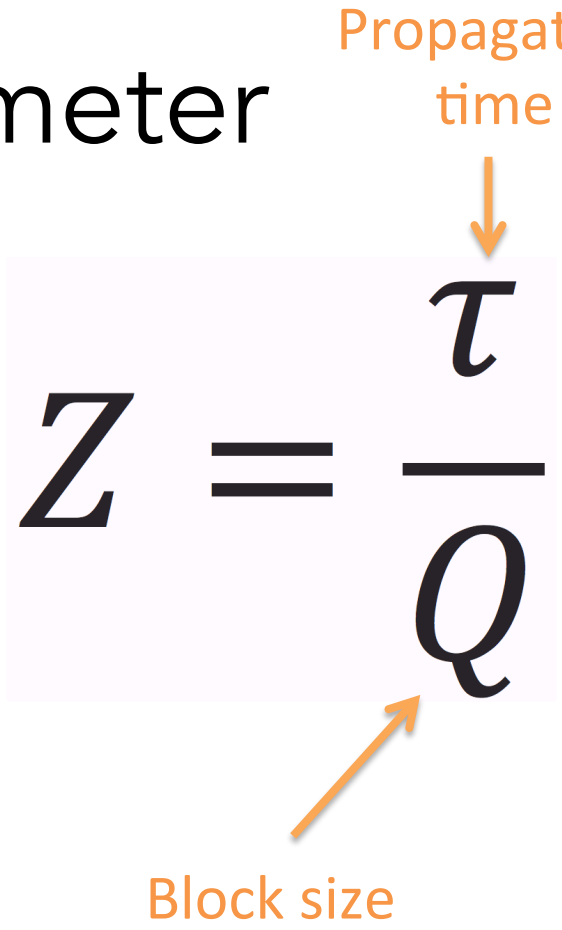
The Z-parameter

- A measure of the network's impedance to the propagation of blocks
- Units of seconds per megabyte



The Z-parameter

- A measure of the network's impedance to the propagation of blocks
- Units of seconds per megabyte
- The Z parameter is not constant over the network



Xtreme Thin Blocks (Xthin)

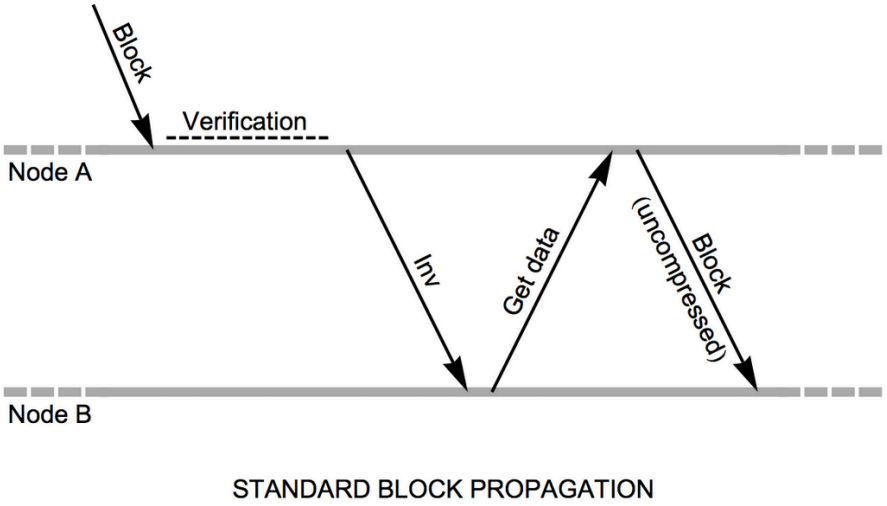
- New block propagation technology that reduces Z

Xtreme Thin Blocks (Xthin)

- New block propagation technology that reduces *Z*
- Transactions are no longer received *twice* by each node

Xtreme Thin Blocks (Xthin)

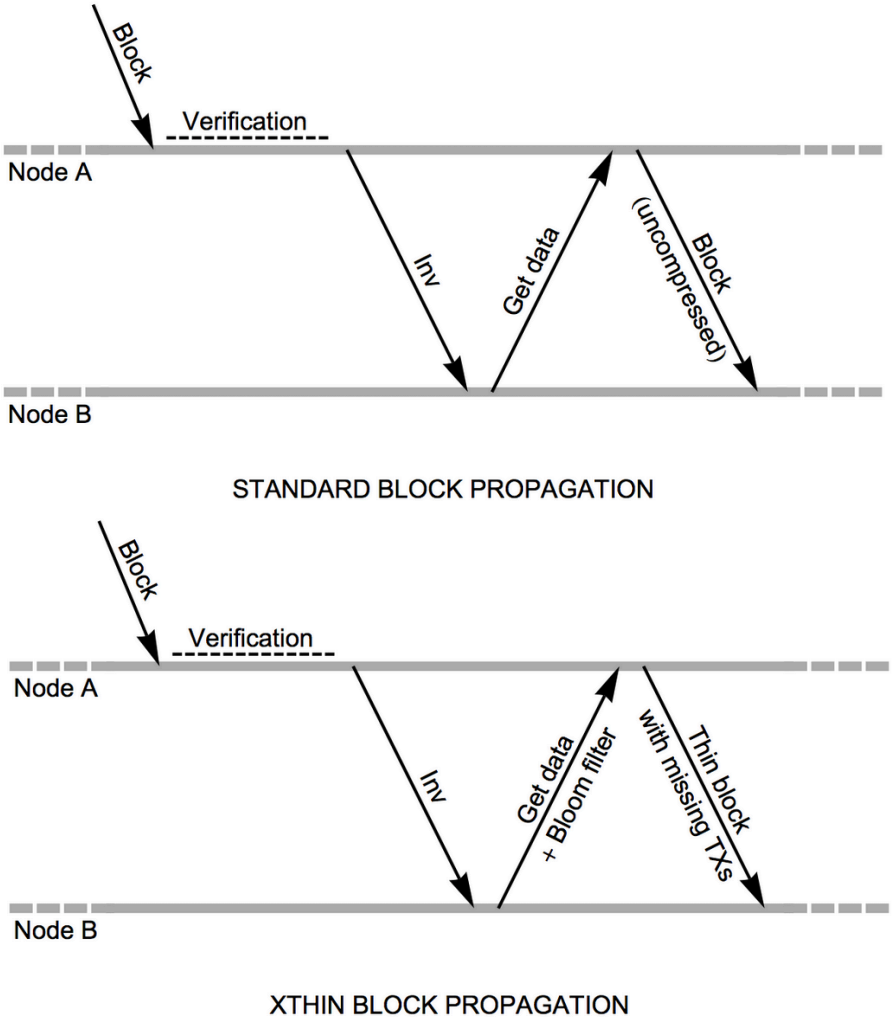
- New block propagation technology that reduces *Z*
- Transactions are no longer received *twice* by each node



STANDARD BLOCK PROPAGATION

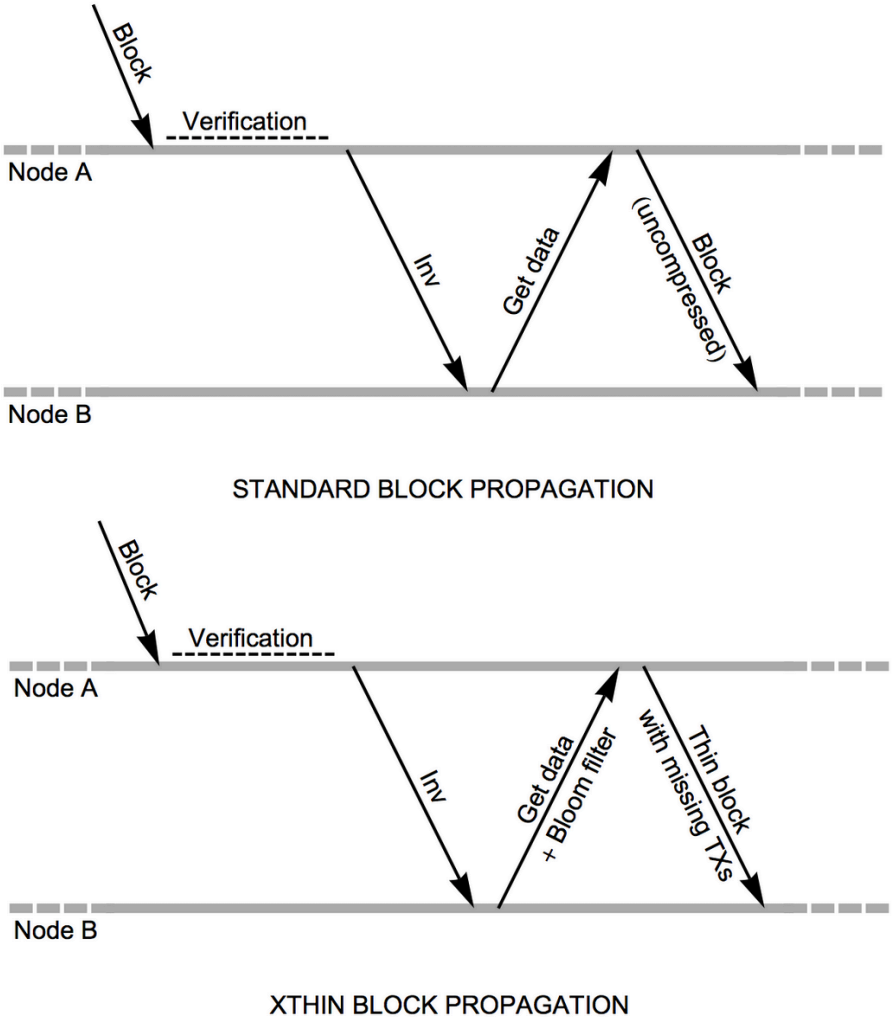
Xtreme Thin Blocks (Xthin)

- New block propagation technology that reduces *Z*
- Transactions are no longer received *twice* by each node



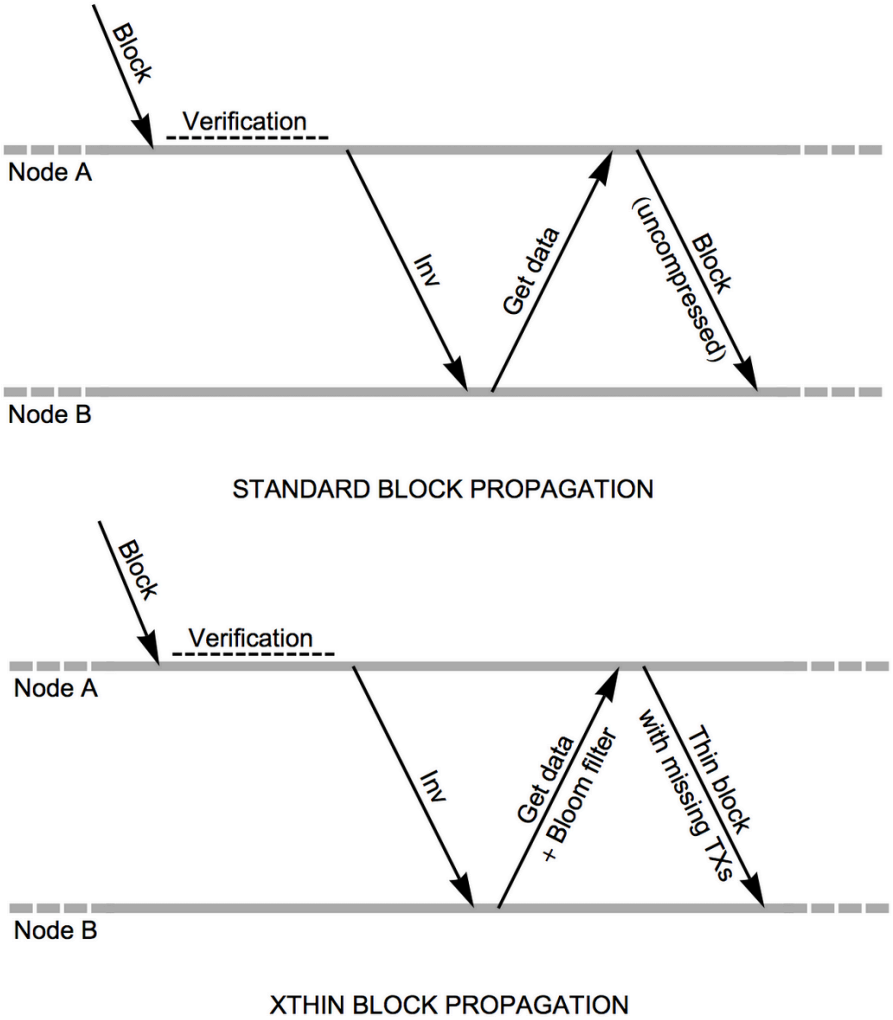
Xtreme Thin Blocks (Xthin)

- New block propagation technology that reduces *Z*
- Transactions are no longer received *twice* by each node
- Invented by Peter Tschipper (builds of work done by Mike Hearn)

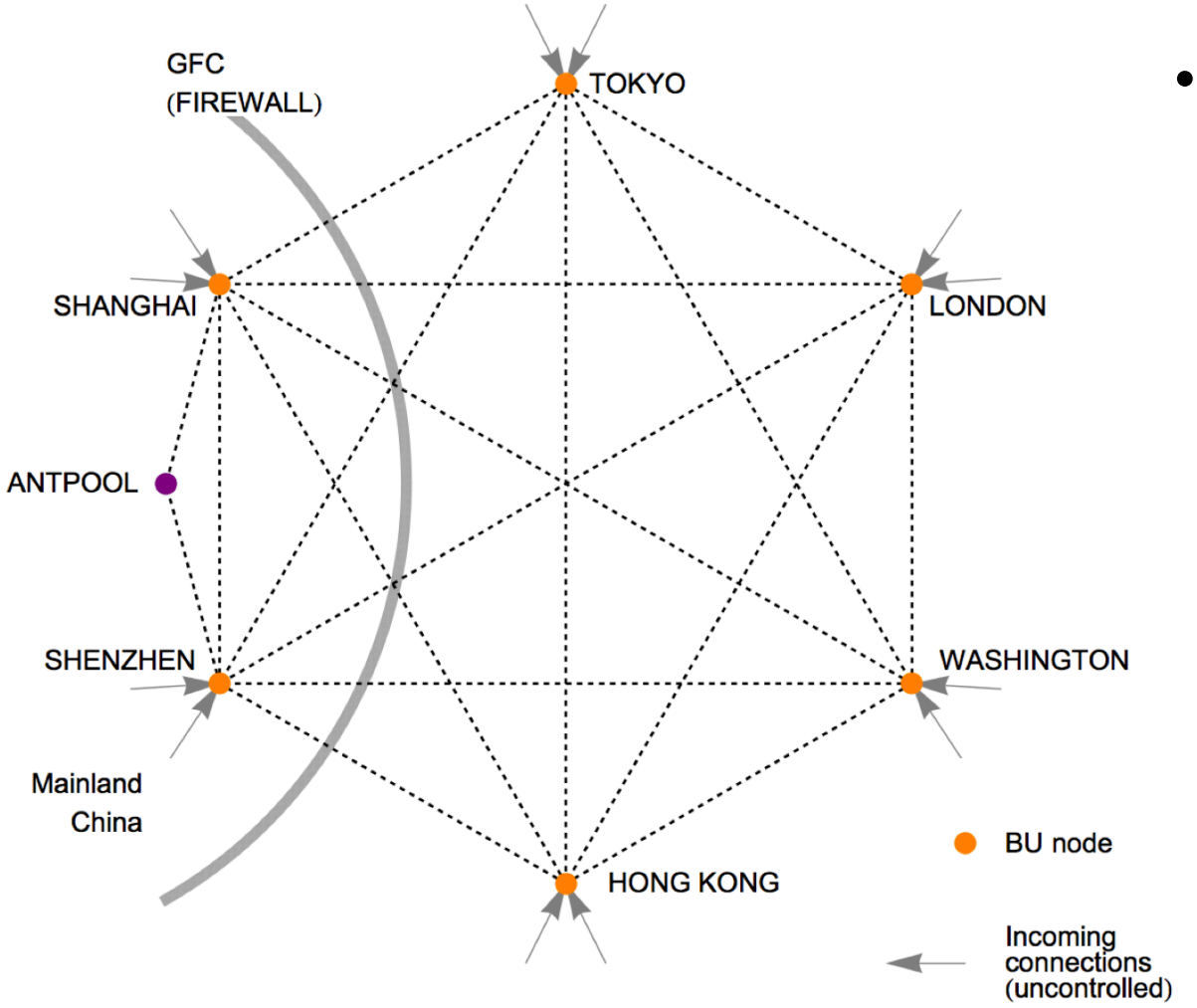


Xtreme Thin Blocks (Xthin)

- New block propagation technology that reduces *Z*
- Transactions are no longer received *twice* by each node
- Invented by Peter Tschipper (builds of work done by Mike Hearn)
- Implemented since March 2016 in Bitcoin Unlimited

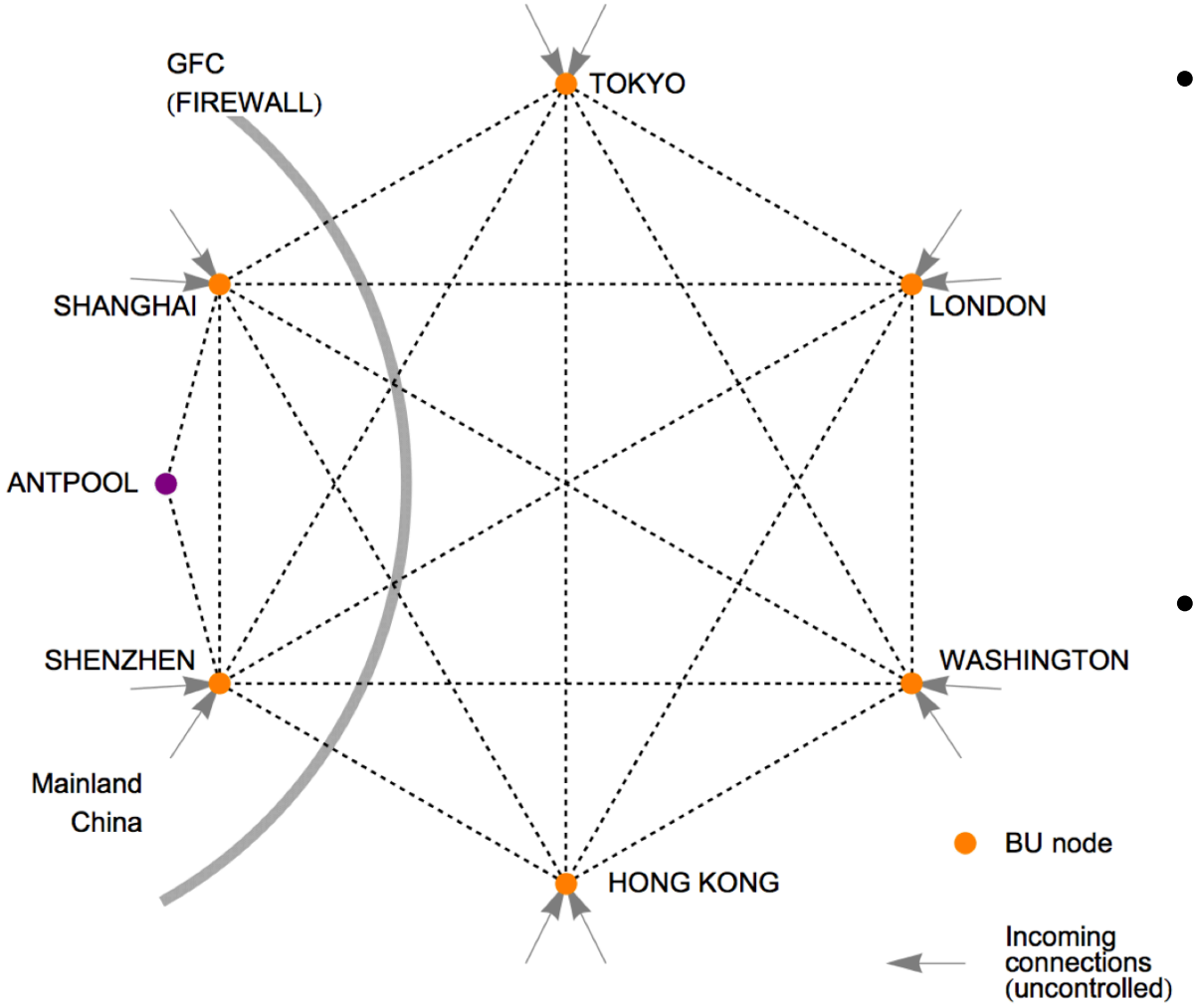


Xtreme Thin Blocks (Xthin)



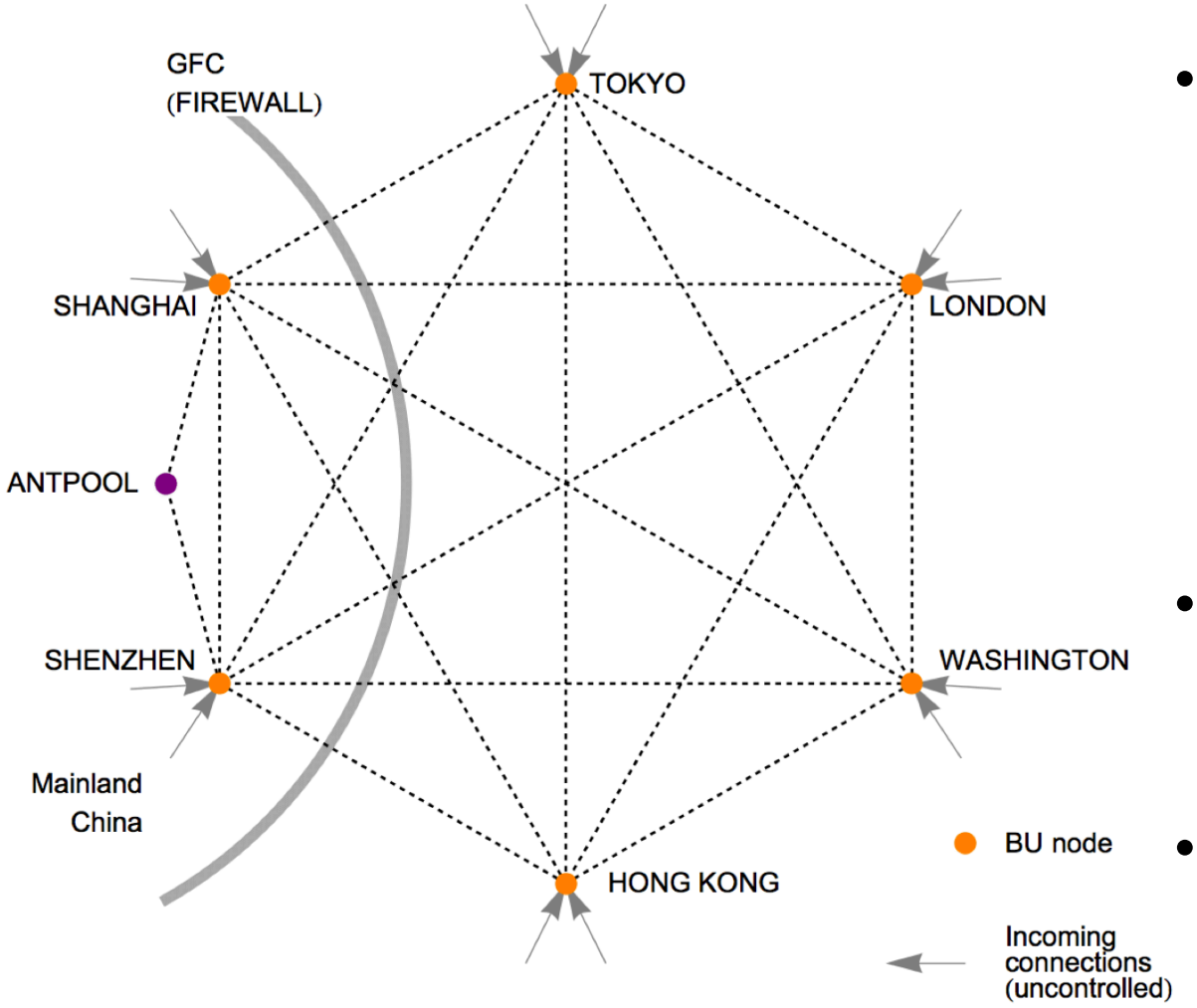
- We (BU devs) tested Xthin over 9,000 blocks
  - Across the normal P2P network
  - Through the Great Firewall of China

Xtreme Thin Blocks (Xthin)



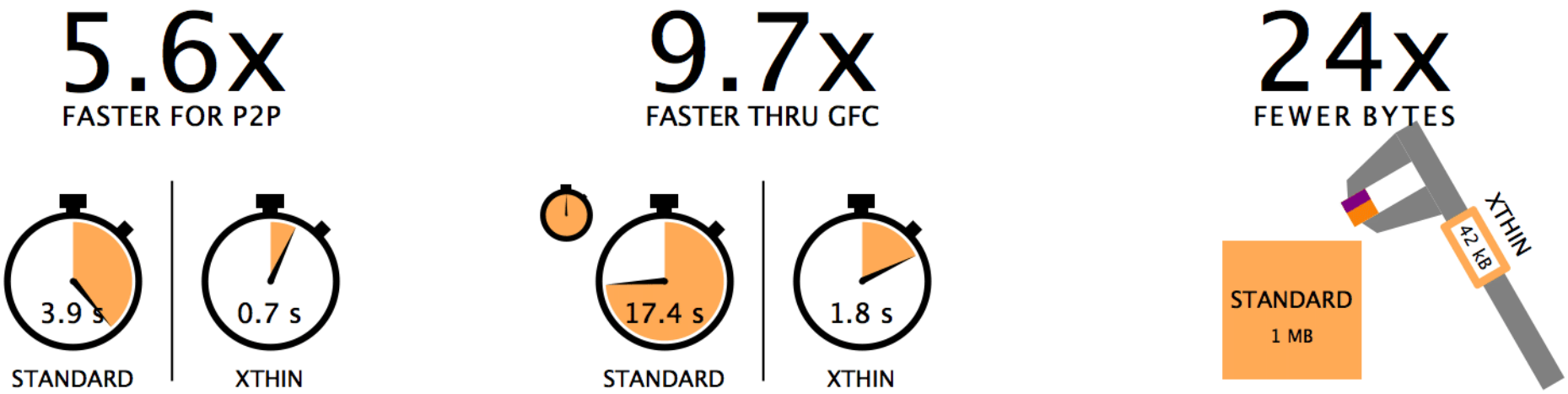
- We (BU devs) tested Xthin over 9,000 blocks
  - Across the normal P2P network
  - Through the Great Firewall of China
- Andrea Suisani will describe in more detail

Xtreme Thin Blocks (Xthin)

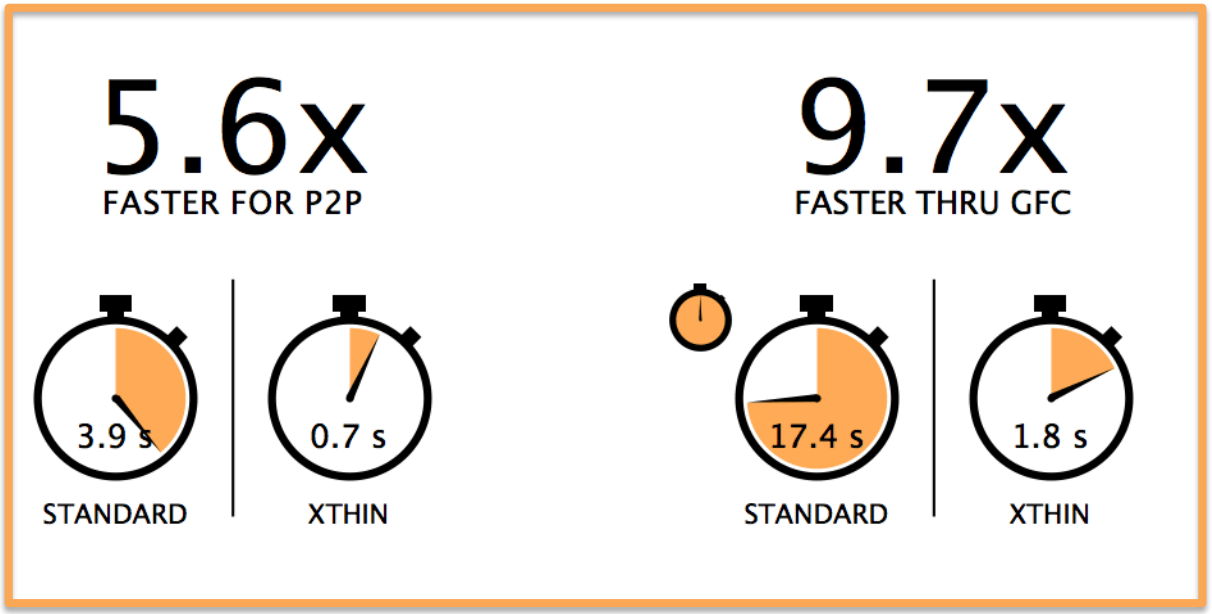


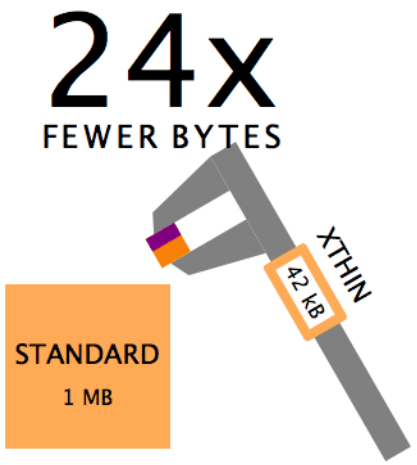
- We (BU devs) tested Xthin over 9,000 blocks
  - Across the normal P2P network
  - Through the Great Firewall of China
- Andrea Suisani will describe in more detail
- The results were impressive!

Xtreme Thin Blocks (Xthin)



Xtreme Thin Blocks (Xthin)





Xthin significantly reduces the *Z*-parameter

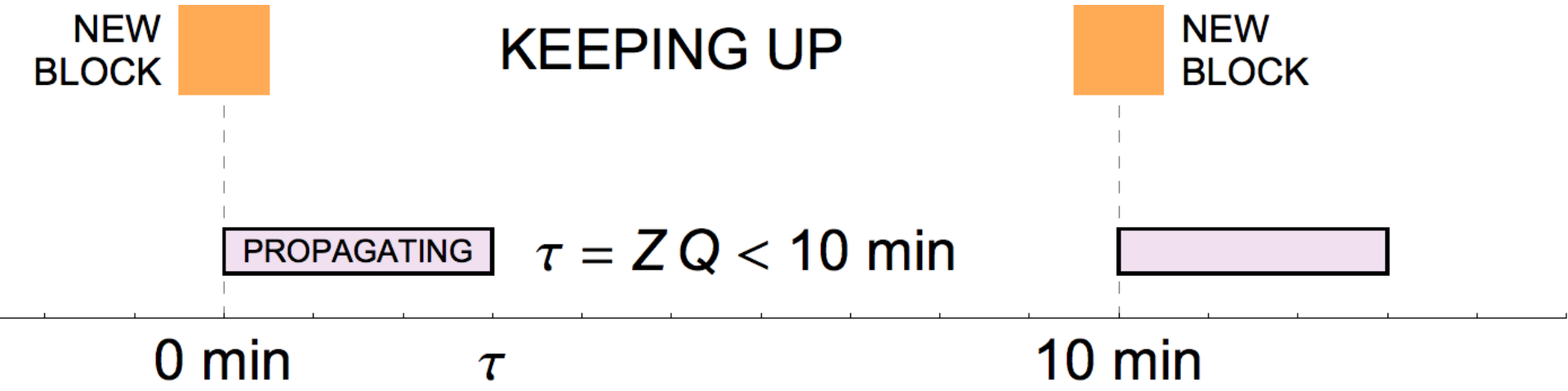
Why does the *Z*-parameter matter?

Why does the *Z*-parameter matter?

- It matters to *miners*
  - For reducing orphaning risk (we'll discuss later)

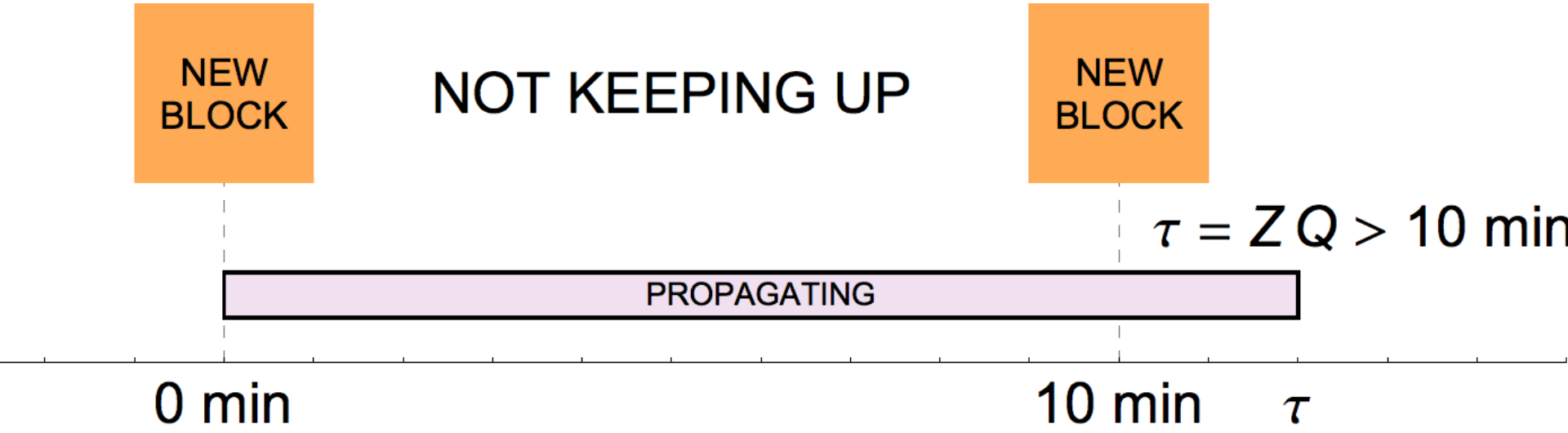
Why does the *Z*-parameter matter?

- It matters to *miners*
  - For reducing orphaning risk (we'll discuss later)
- It matters to *nodes*
  - For "keeping up" with the blockchain



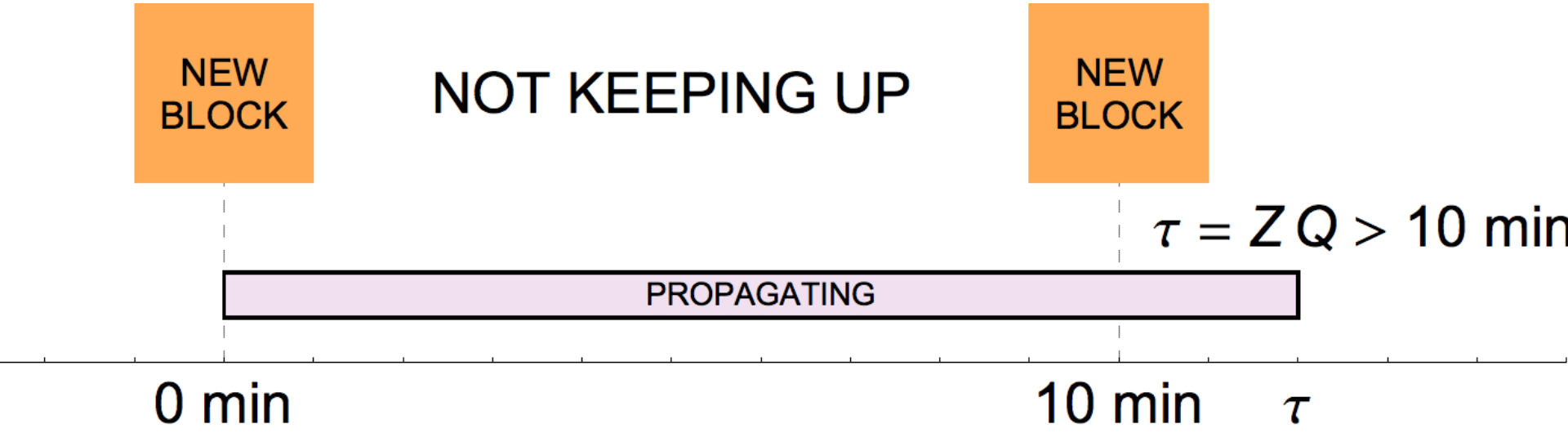
Why does the *Z*-parameter matter?

- It matters to *miners*
  - For reducing orphaning risk (we'll discuss later)
- It matters to *nodes*
  - For "keeping up" with the blockchain



Why does the *Z*-parameter matter?

- It matters to *miners*
  - For reducing orphaning risk (we'll discuss later)
- It matters to *nodes*
  - For "keeping up" with the blockchain



The smaller the *Z*-parameter, the bigger the block size a node can "keep up" with.

Block propagation to nodes is the bottleneck

Cornell Position Paper (2016)

Block propagation to nodes is the bottleneck

Cornell Position Paper (2016)

- Measured how long it took for new blocks to spread out to nodes across the network

Block propagation to nodes is the bottleneck

Cornell Position Paper (2016)

- Measured how long it took for new blocks to spread out to nodes across the network
- Found that blocks propagated at

$$Z_{50\%} = 16 \text{ sec / MB}$$

$$Z_{90\%} = 145 \text{ sec / MB}$$

Block propagation to nodes is the bottleneck

Cornell Position Paper (2016)

- Measured how long it took for new blocks to spread out to nodes across the network
- Found that blocks propagated at

$$Z_{50\%} = \quad 16 \text{ sec / MB}$$

$$Z_{90\%} = 145 \text{ sec / MB}$$

- Calculated max block size using τ =10 min

$$Z = \frac{\tau}{Q} \quad \rightarrow \quad Q_{\max} = \frac{10 \text{ min}}{Z}$$

$$= 38 \text{ MB } (50\%)$$

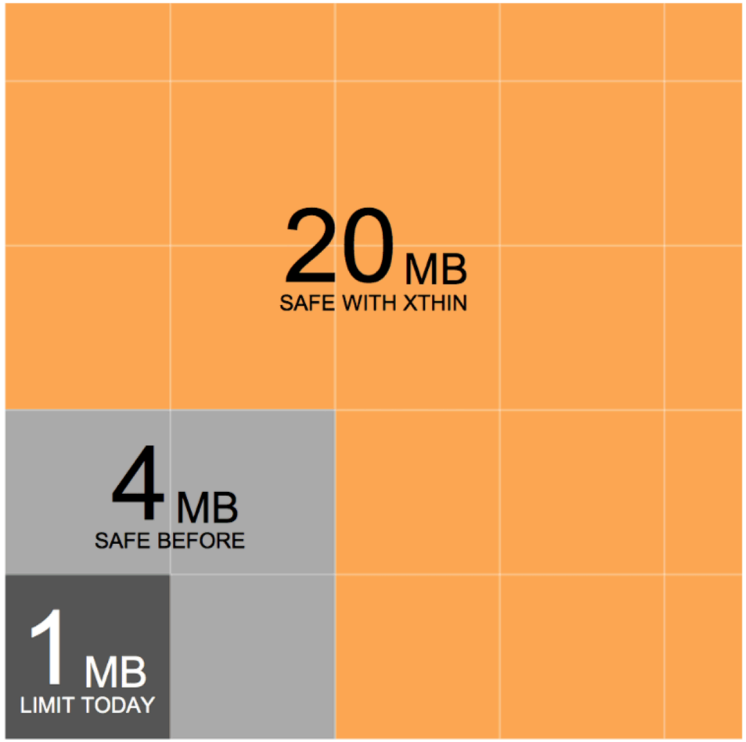
$$= \quad 4 \text{ MB } (90\%)$$

Propagation to nodes is the bottleneck
J. Toomim 'Block Size Olympics' (2015)

- Measured block propagation times
  - On TestNet, up to 10 MB
  - 20 nodes, hundreds of blocks
  - Considered effect of GFC
- Suggested 4 MB max size due largely to slow propagation through the GFC

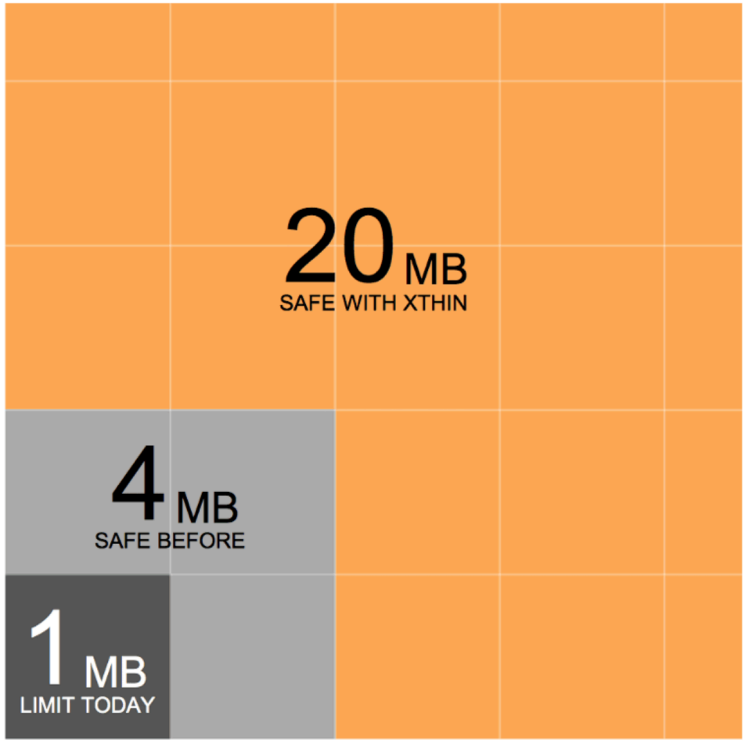
Xthin fixes the bottleneck

- Blocks now propagate faster
  - By 9.7x thru GFC
  - By 5.6x normal P2P



Xthin fixes the bottleneck

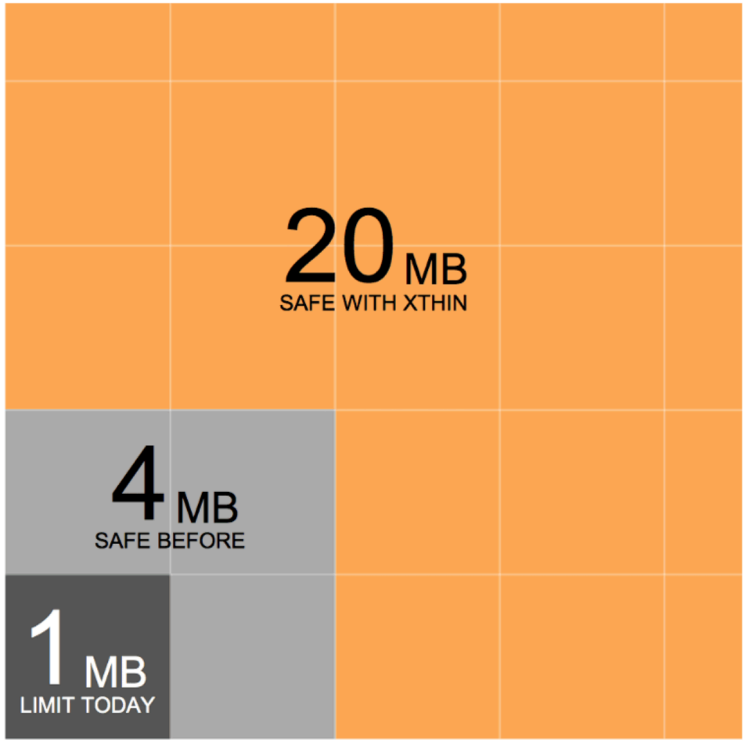
- Blocks now propagate faster
  - By 9.7x thru GFC
  - By 5.6x normal P2P
- Assume Z –> Z / 5



Xthin fixes the bottleneck

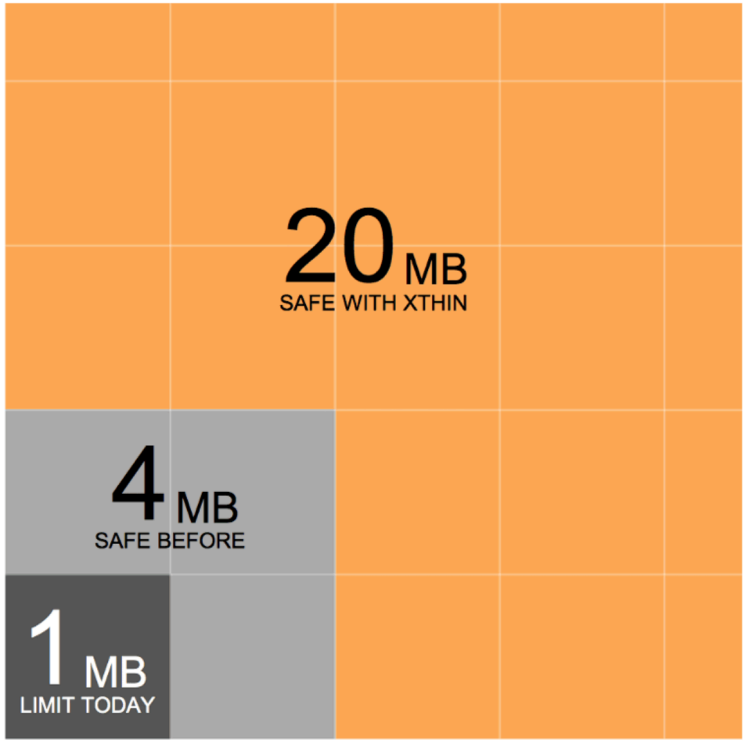
- Blocks now propagate faster
  - By 9.7x thru GFC
  - By 5.6x normal P2P
- Assume $Z \rightarrow Z / 5$
- Capacity was (90% keep up)

  $Q_{max} = \tau / Z = 4$ MB



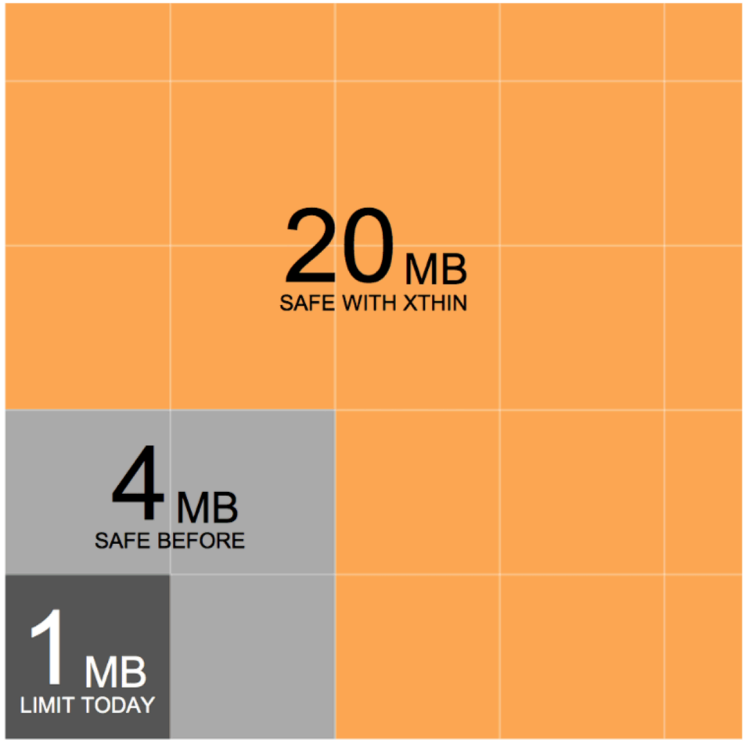
Xthin fixes the bottleneck

- Blocks now propagate faster
  - By 9.7x thru GFC
  - By 5.6x normal P2P
- Assume $Z \rightarrow Z / 5$
- Capacity was (90% keep up)
  $Q_{max} = \tau / Z = 4$ MB
- Now we have (90% keep up)
  $Q_{max} = \tau / (Z / 5) = 20$ MB



Xthin fixes the bottleneck

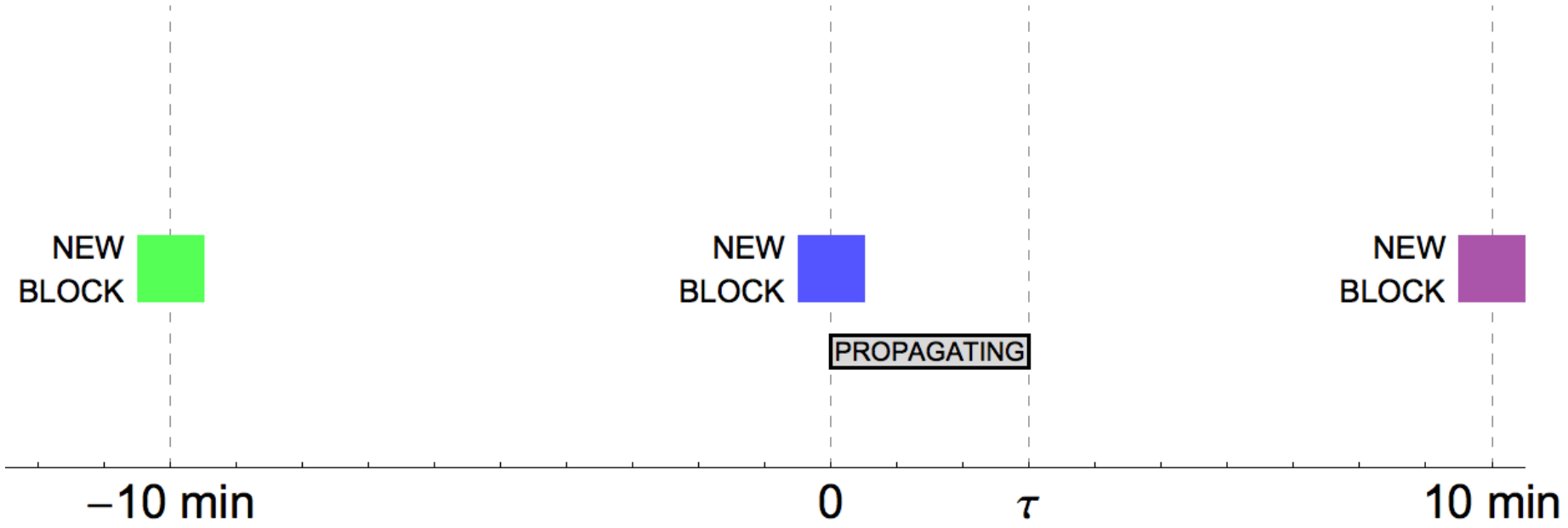
- Blocks now propagate faster
  - By 9.7x thru GFC
  - By 5.6x normal P2P
- Assume $Z \rightarrow Z / 5$
- Capacity was (90% keep up)
  $Q_{max} = \tau / Z = 4$ MB
- Now we have (90% keep up)
  $Q_{max} = \tau / (Z / 5) = 20$ MB
- This is an example of using the Z-parameter for nodes



Why do *miners* care about the Z-parameter?

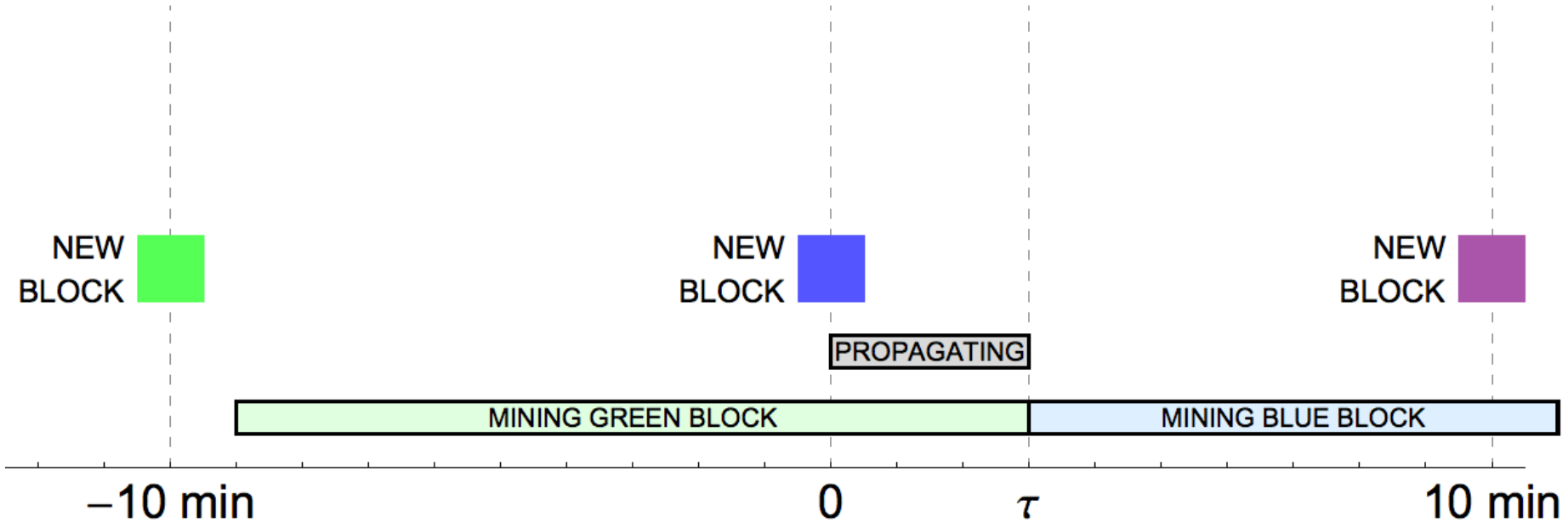
Why do *miners* care about the Z-parameter?

- To minimize orphaning risk ($$$)



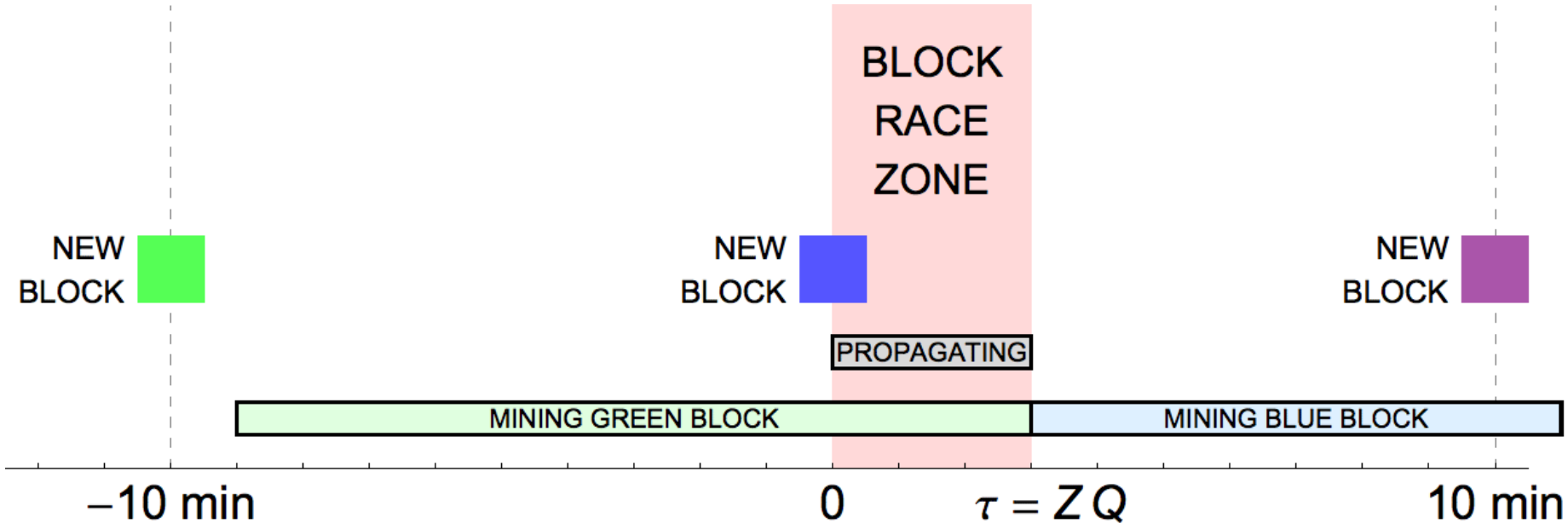
Why do *miners* care about the Z-parameter?

- To minimize orphaning risk ($$$)



Why do *miners* care about the Z-parameter?

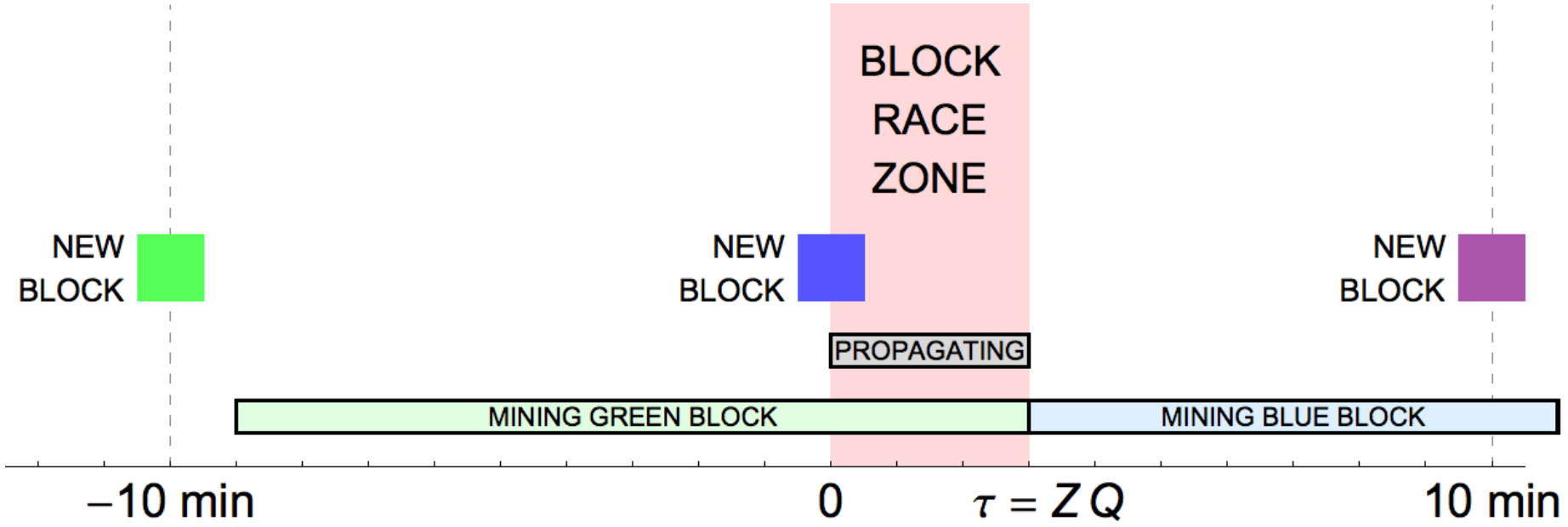
- To minimize orphaning risk ($$$)



Why do *miners* care about the Z-parameter?

- To minimize orphaning risk ($$$)

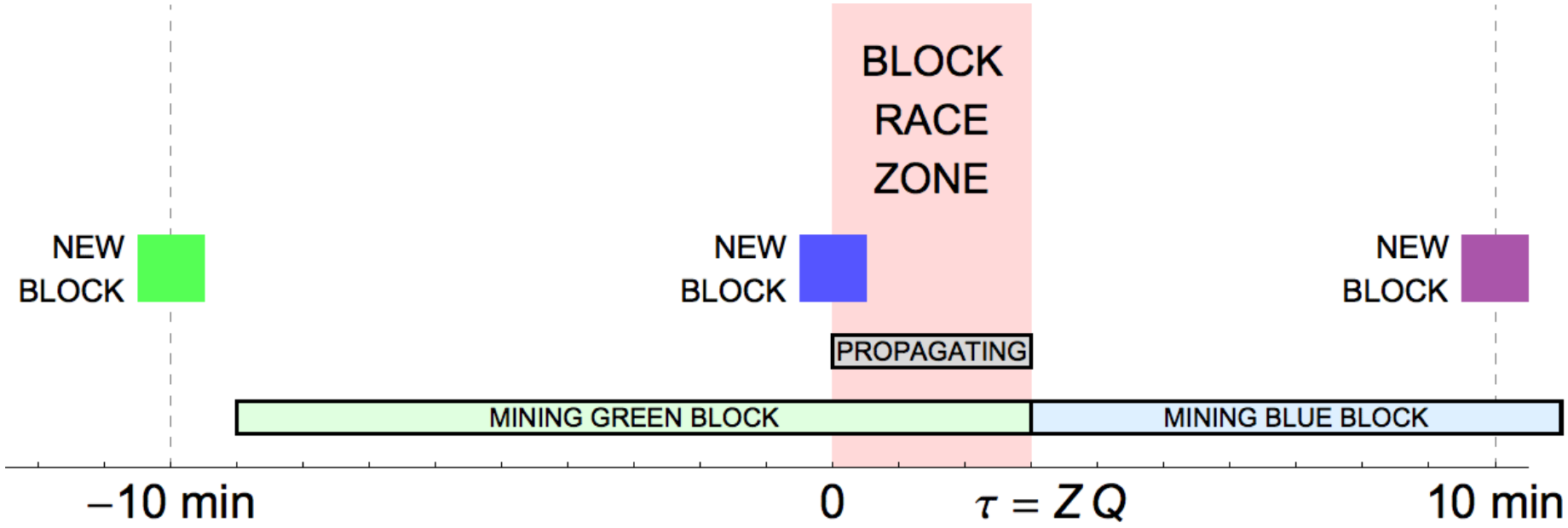
$$\frac{ZQ}{10\ \text{min}}$$



Why do *miners* care about the Z-parameter?

- To minimize orphaning risk ($$$)

$$Risk \approx \frac{ZQ}{10\ \text{min}}(block\ reward)$$

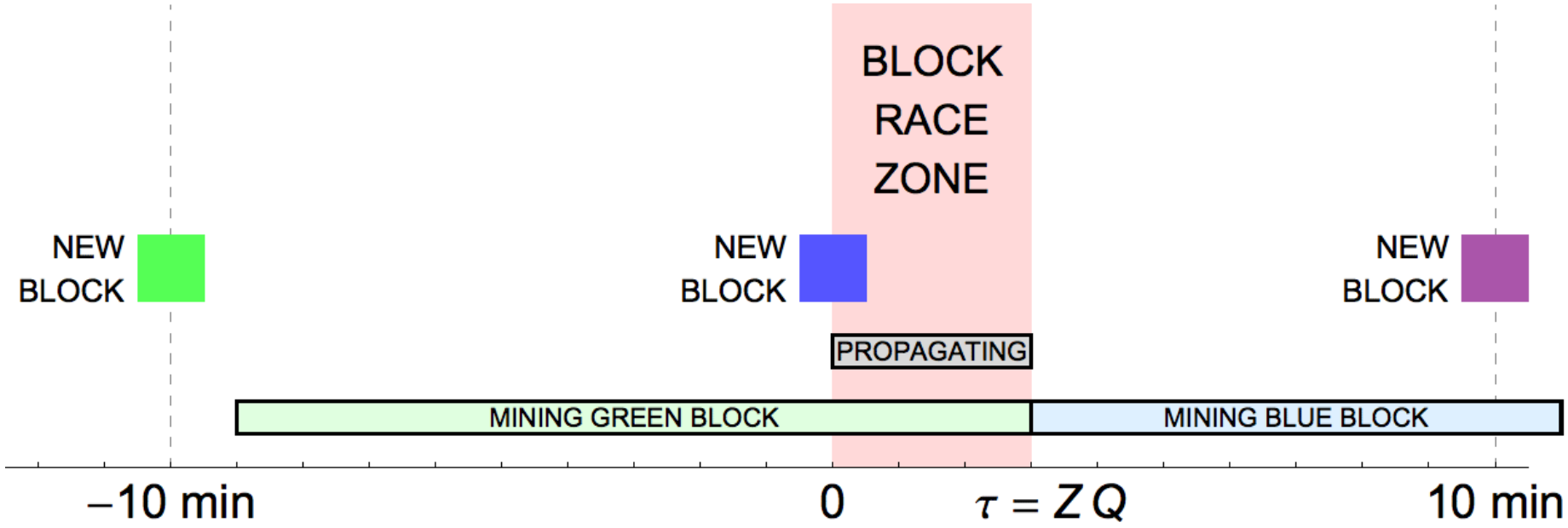


Why do *miners* care about the Z-parameter?

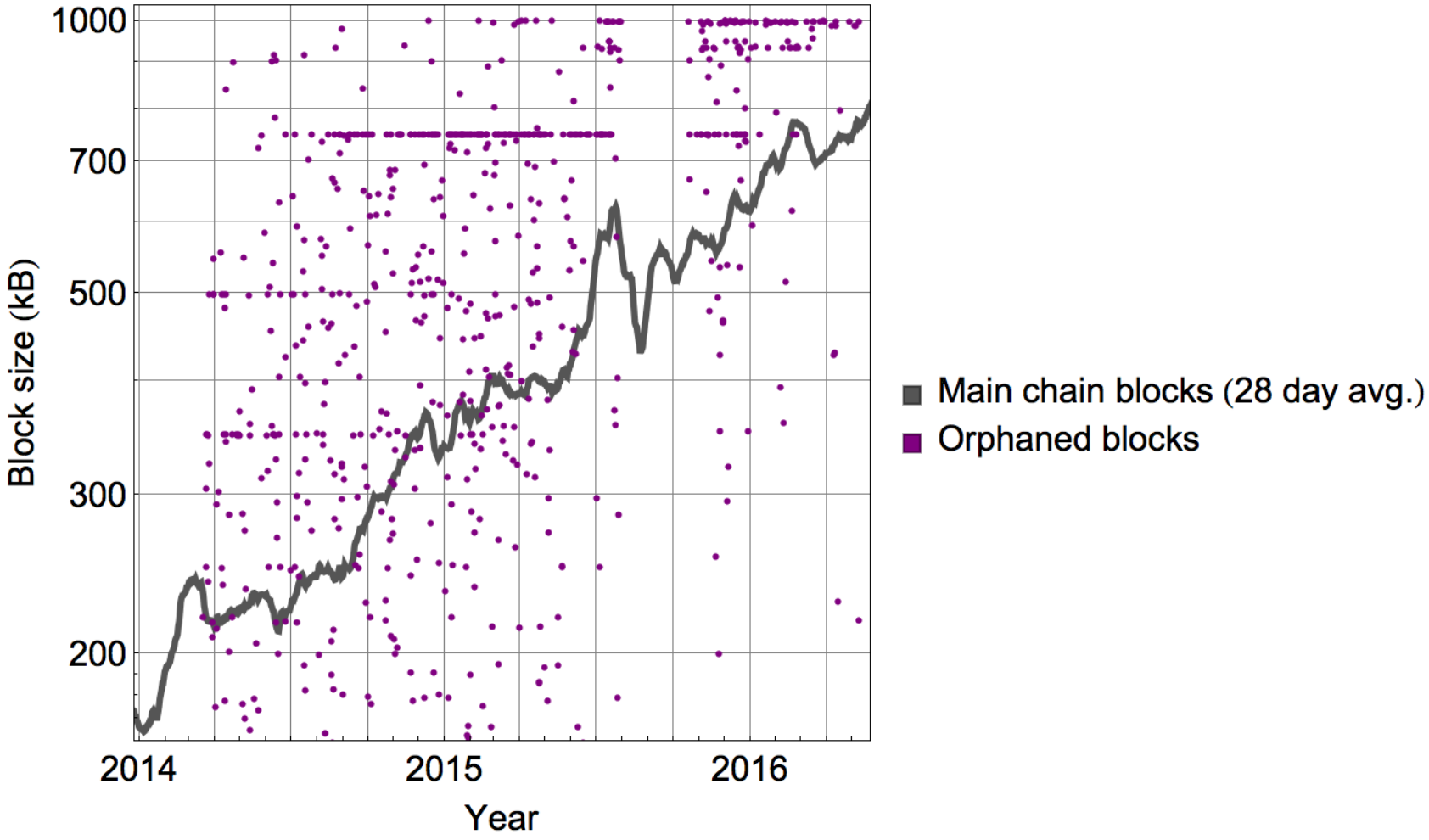
- To minimize orphaning risk ($$$)

Less risk with smaller *Z* → ← More risk with bigger blocks

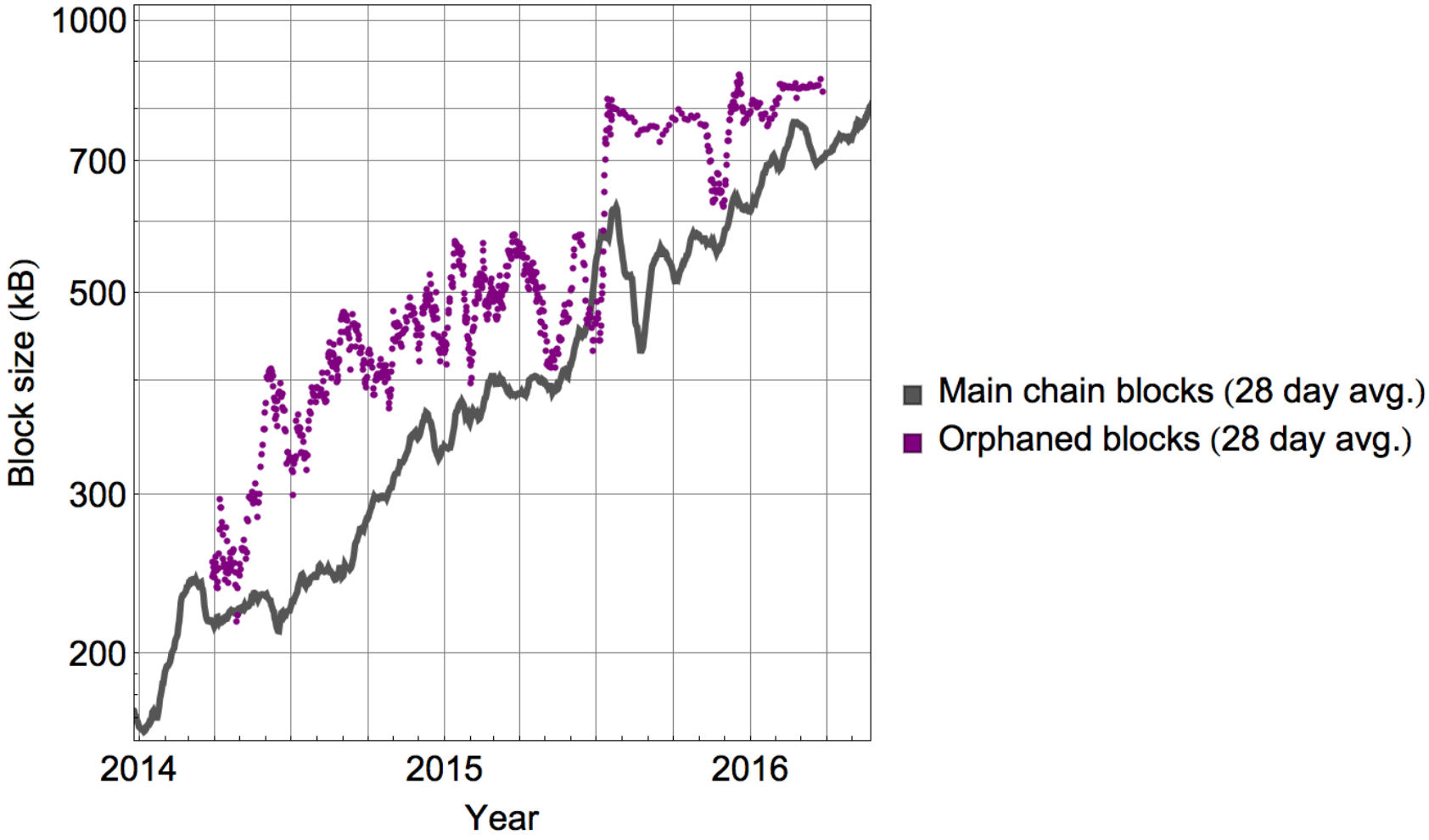
$$Risk \approx \frac{ZQ}{10\ \text{min}}(block\ reward)$$



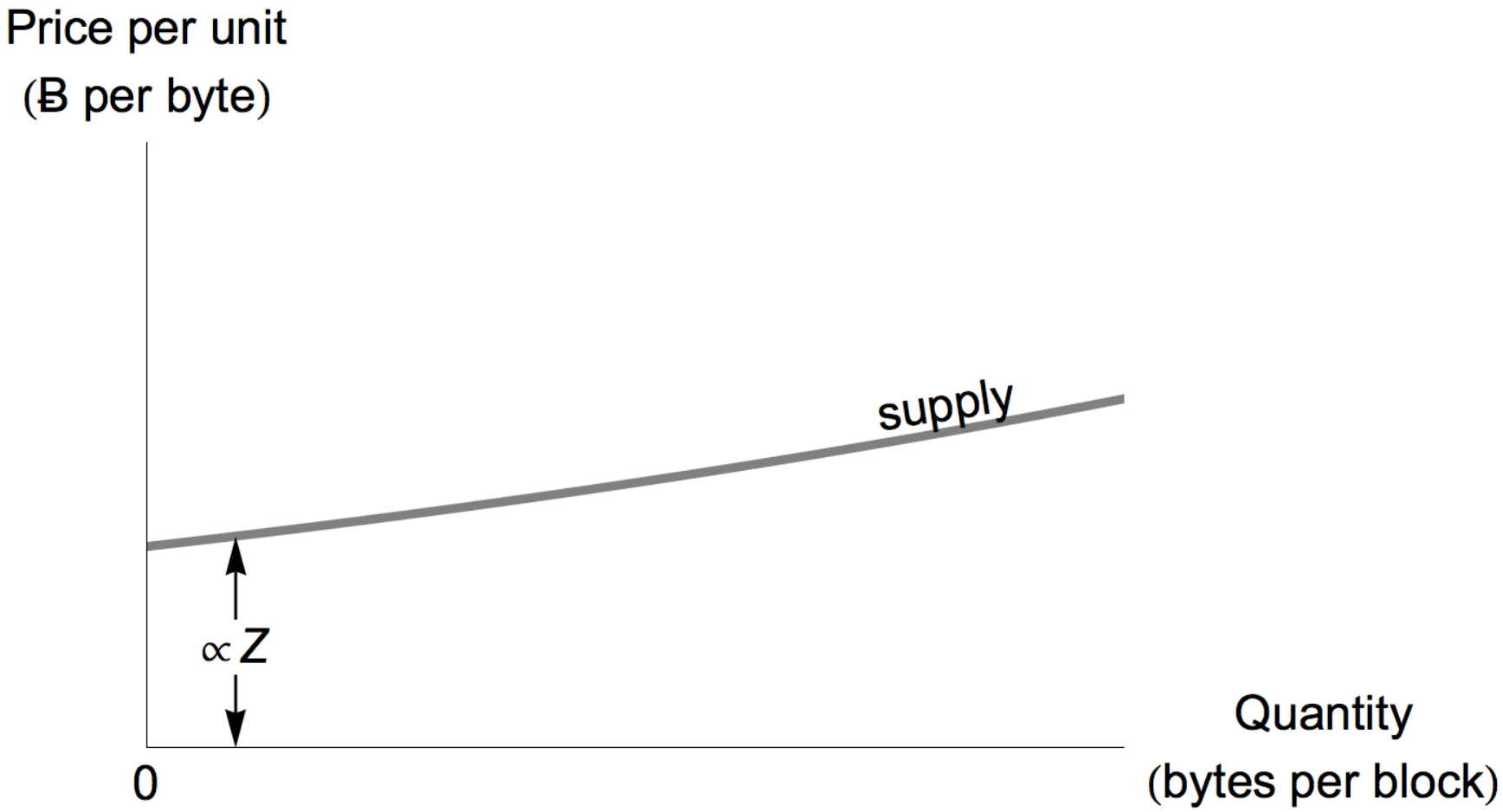
Bigger blocks are *empirically* risky



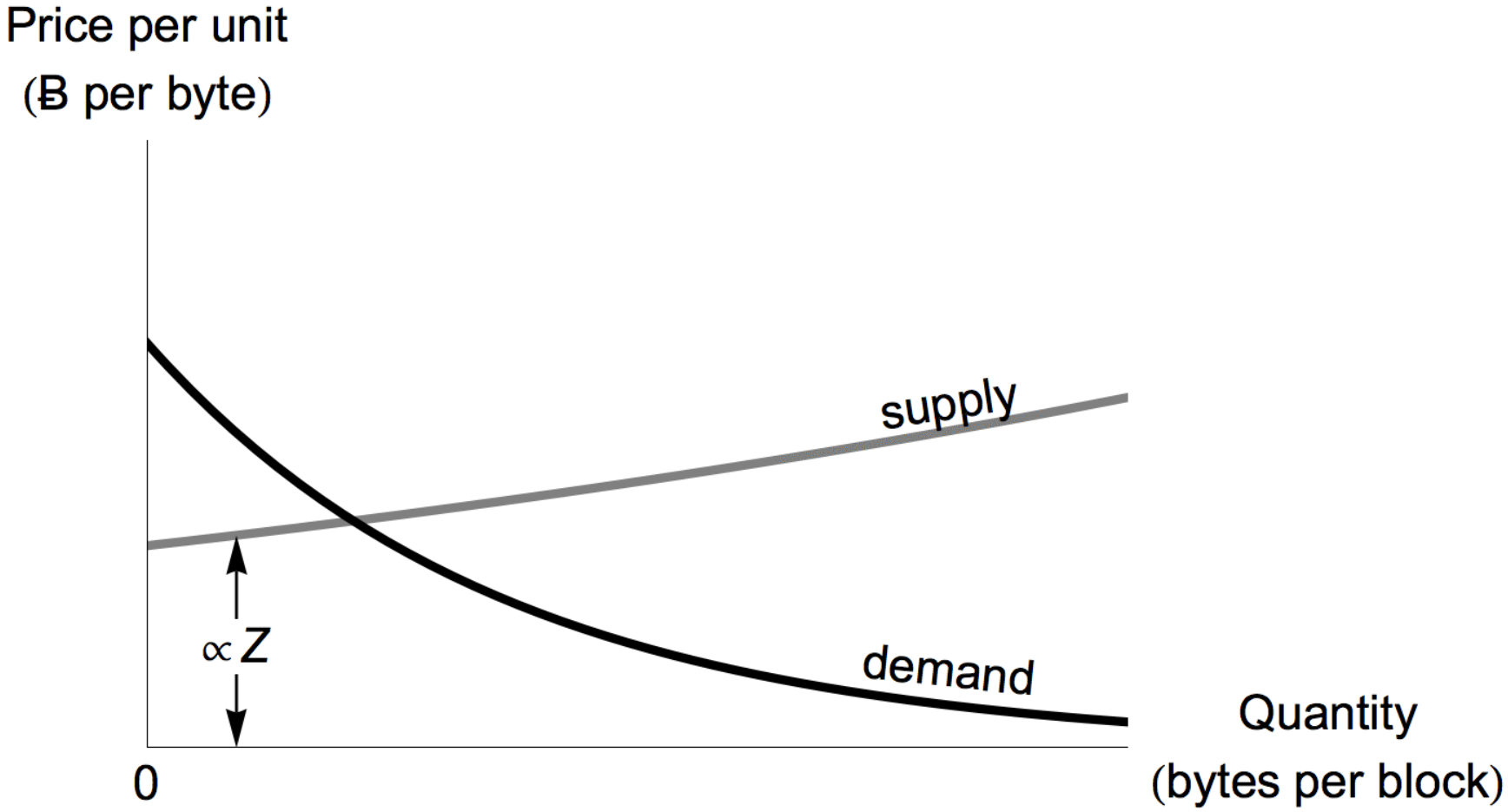
Bigger blocks are *empirically* risky



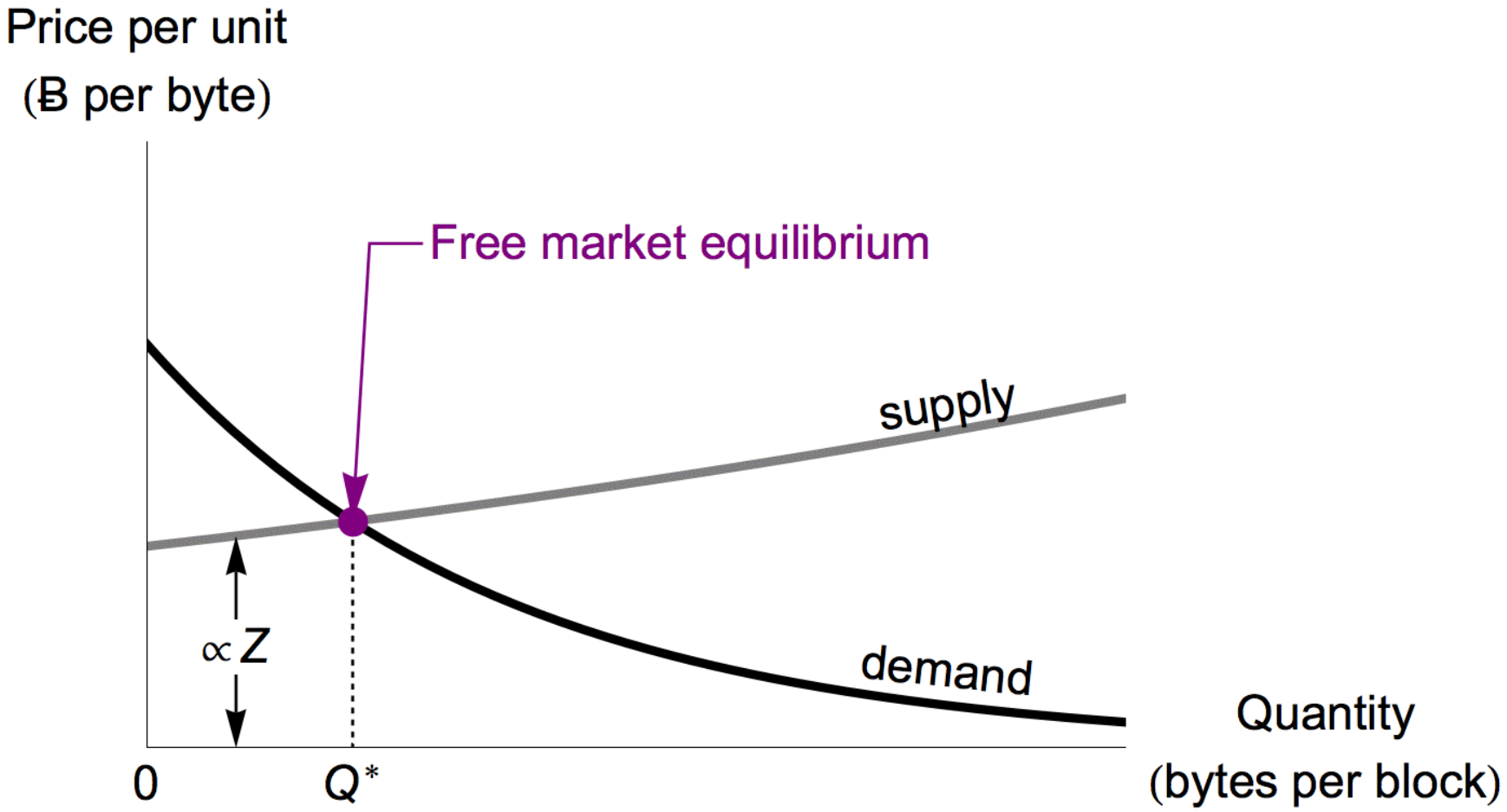
The block space supply curve



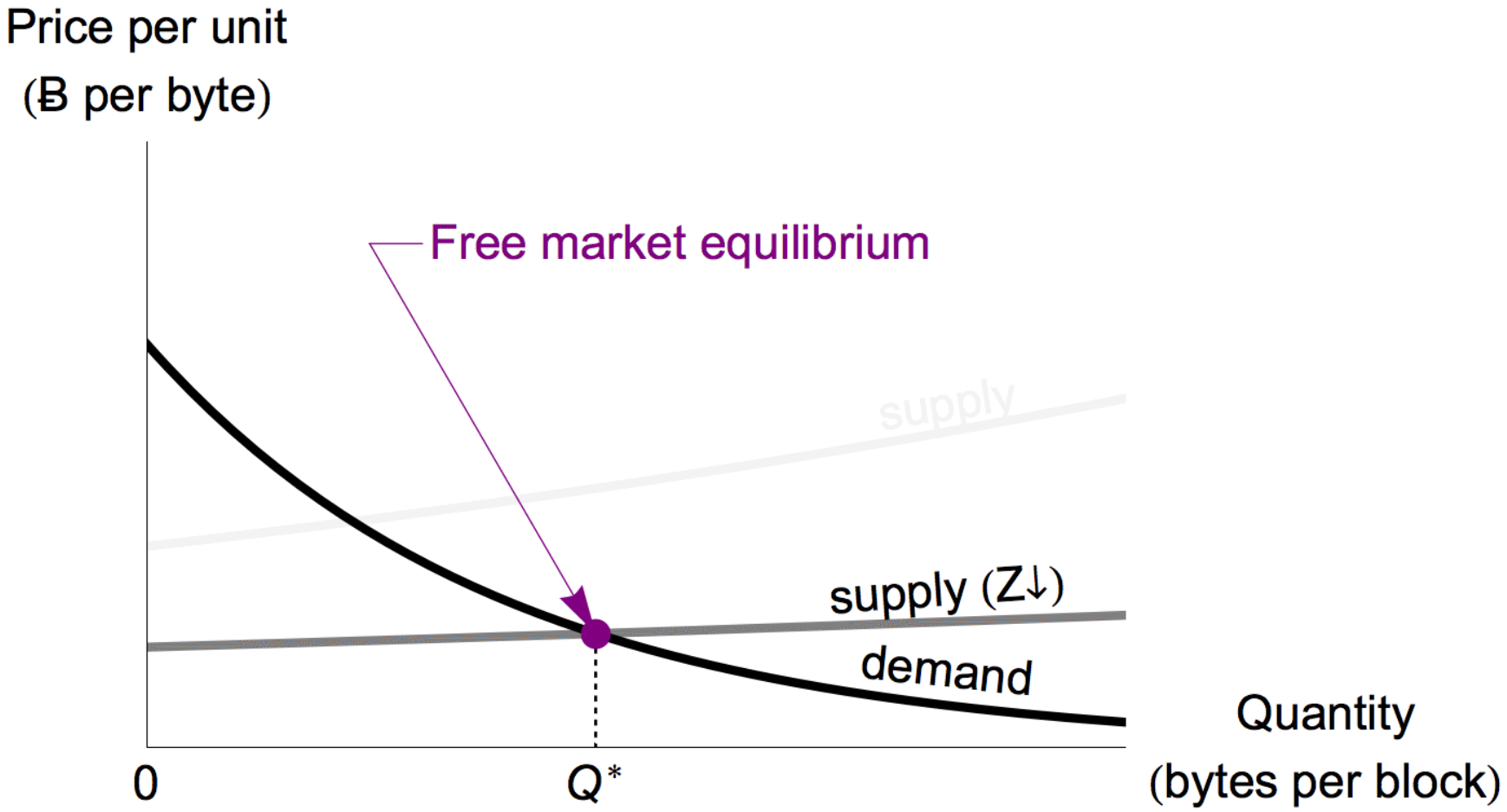
Fallacy #1:
Infinite demand = infinite blocks



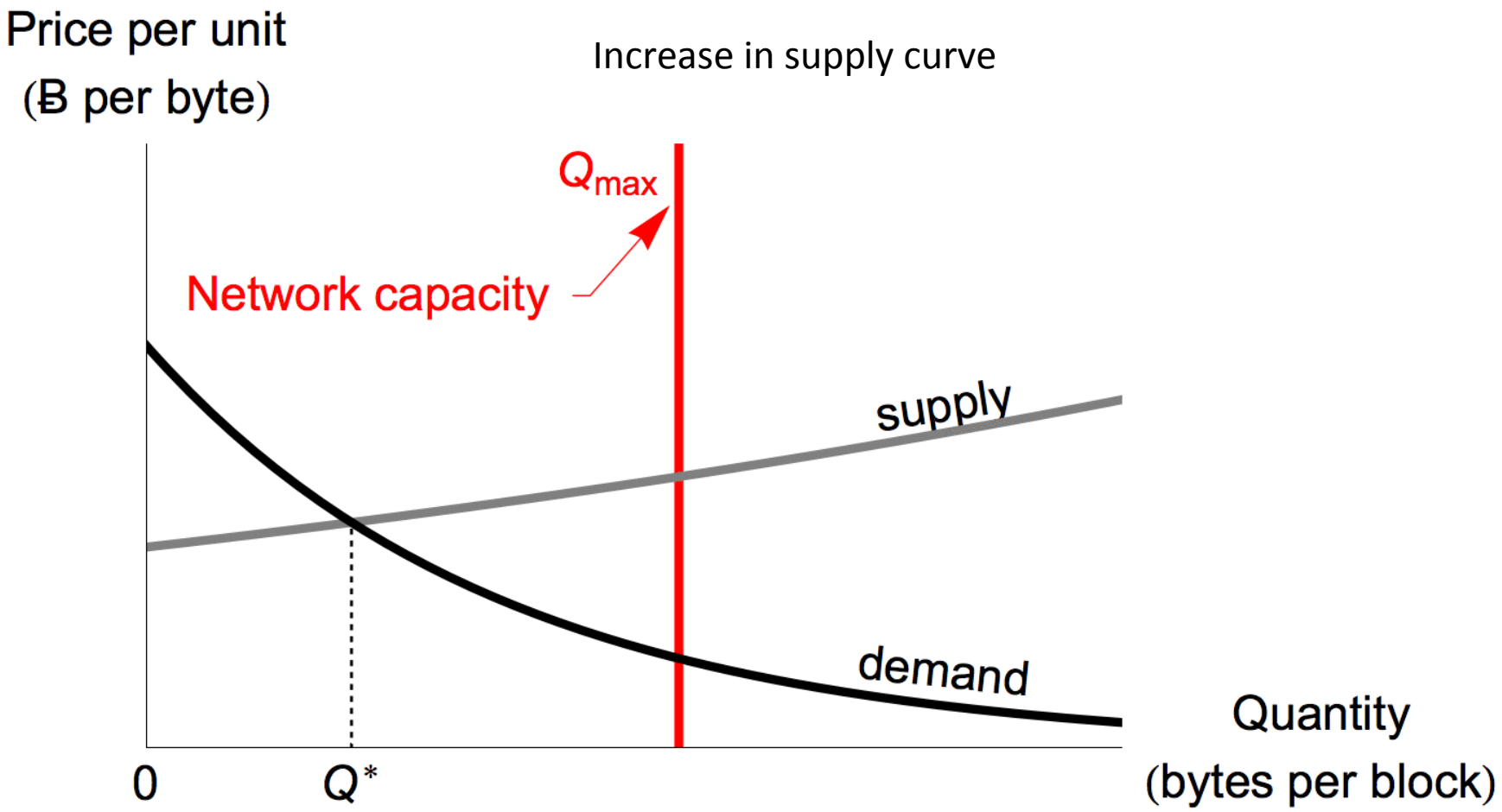
Fallacy #1:
Infinite demand = infinite blocks



Fallacy #1:
Infinite demand = infinite blocks

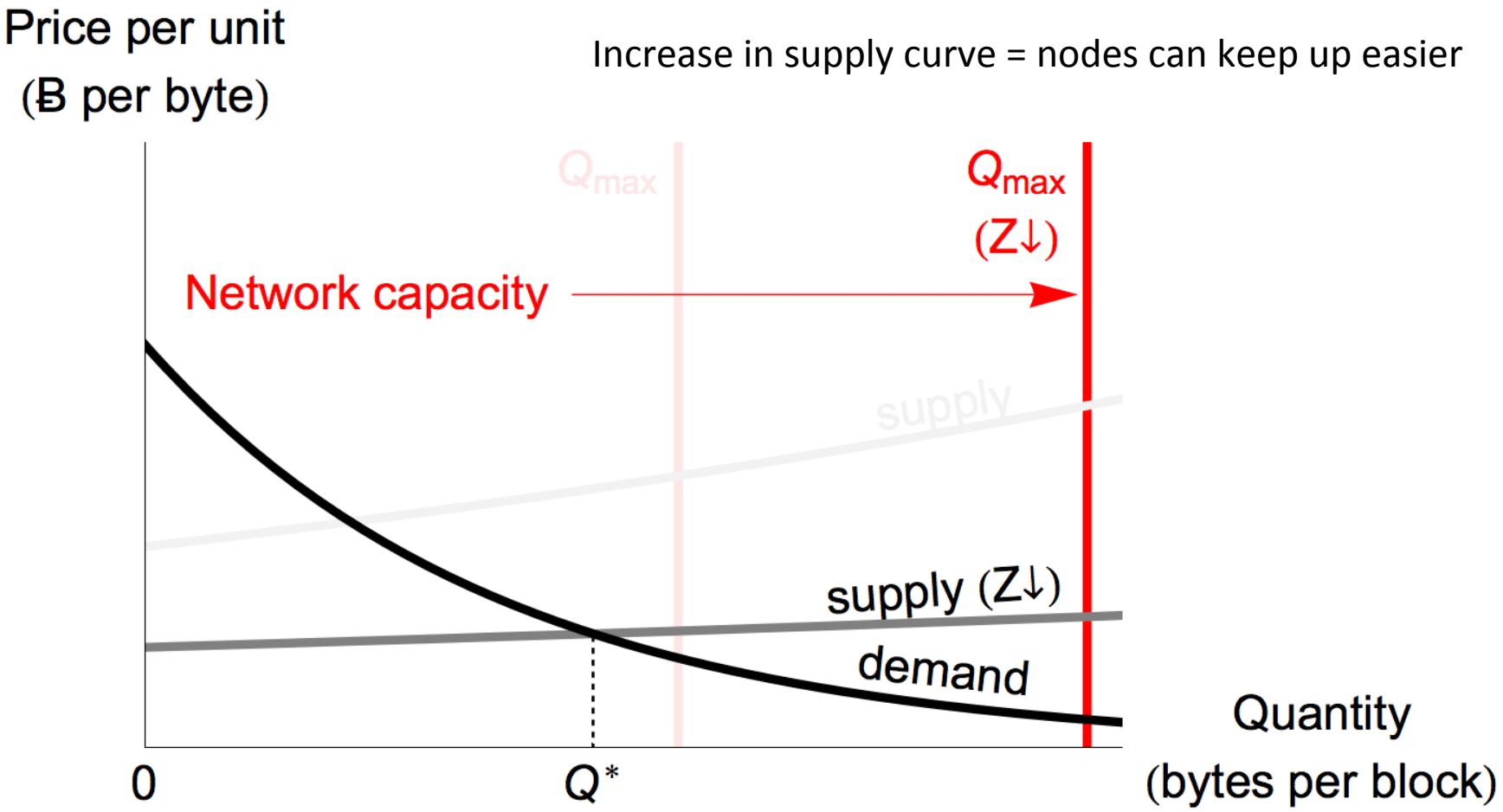


Fallacy #2:
Bigger blocks cause centralization

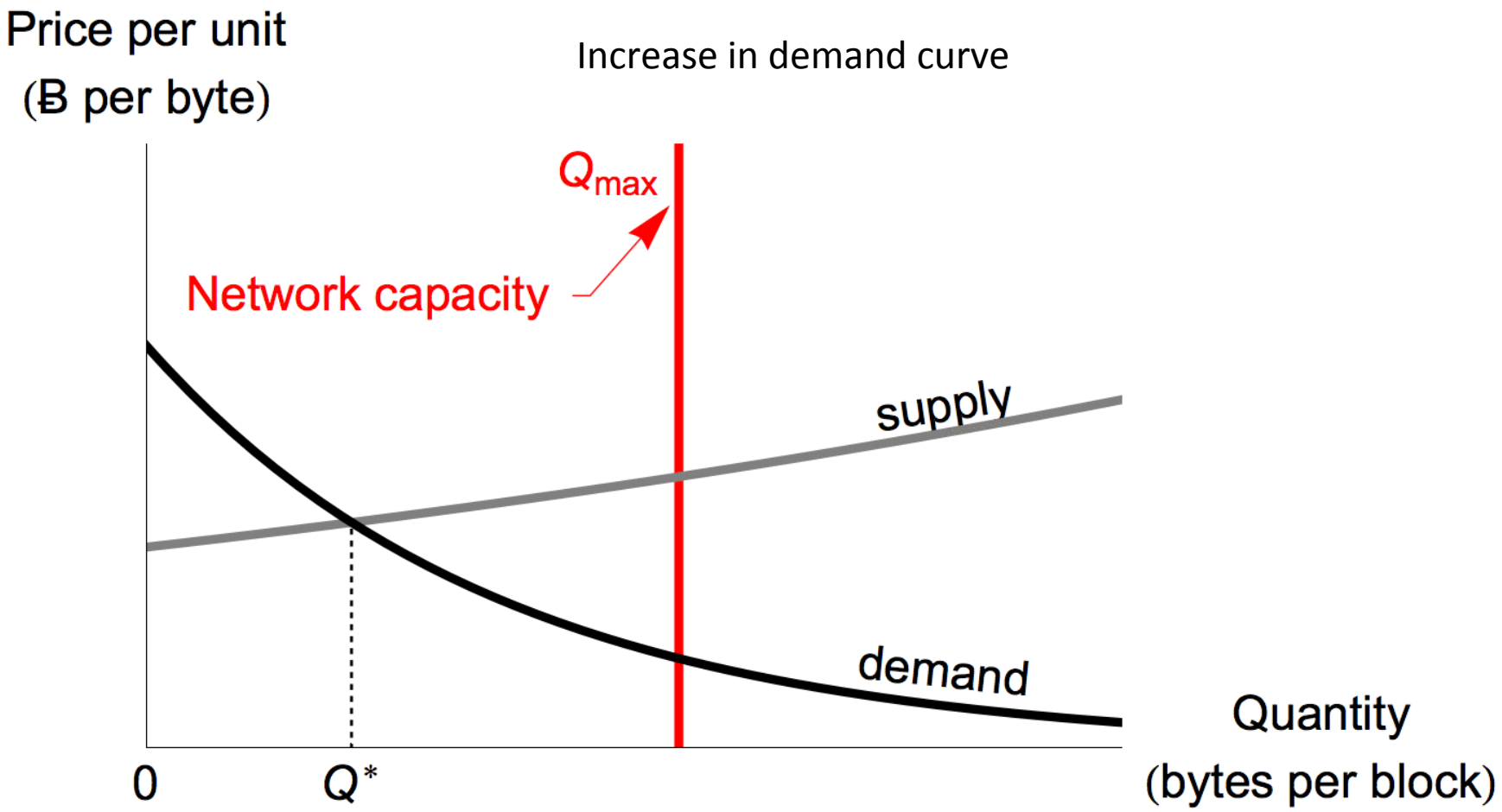


Fallacy #2:
Bigger blocks cause centralization

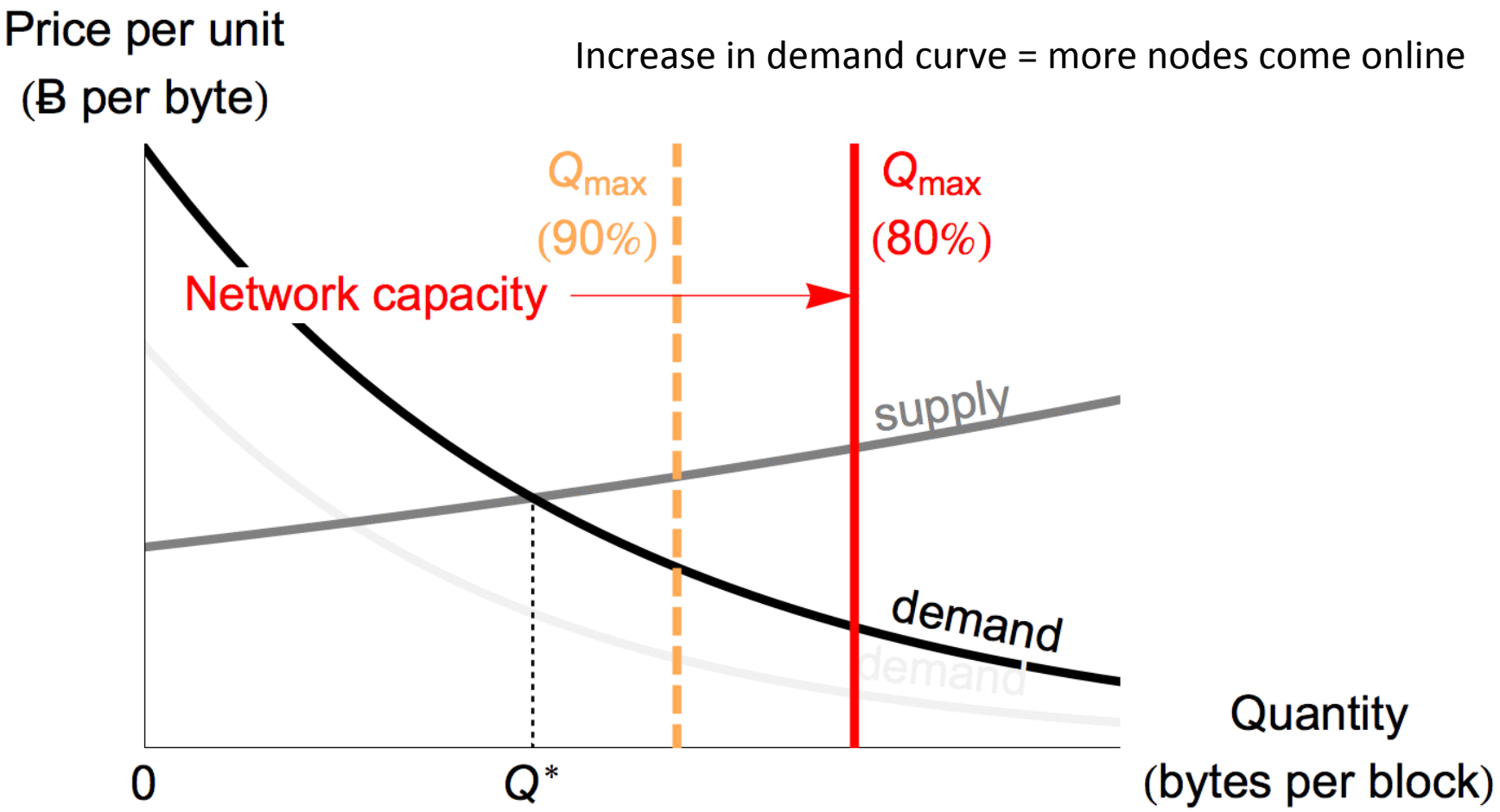
Increase in supply curve = nodes can keep up easier



Fallacy #2:
Bigger blocks cause centralization



Fallacy #2:
Bigger blocks cause centralization



Conclusion

- Unclear whether these effects will favor decentralization or centralization
- Centralizing factors are balanced by decentralizing factors
- In my opinion, the network can grow organically without the need for top-down interventions by developers.

Questions?