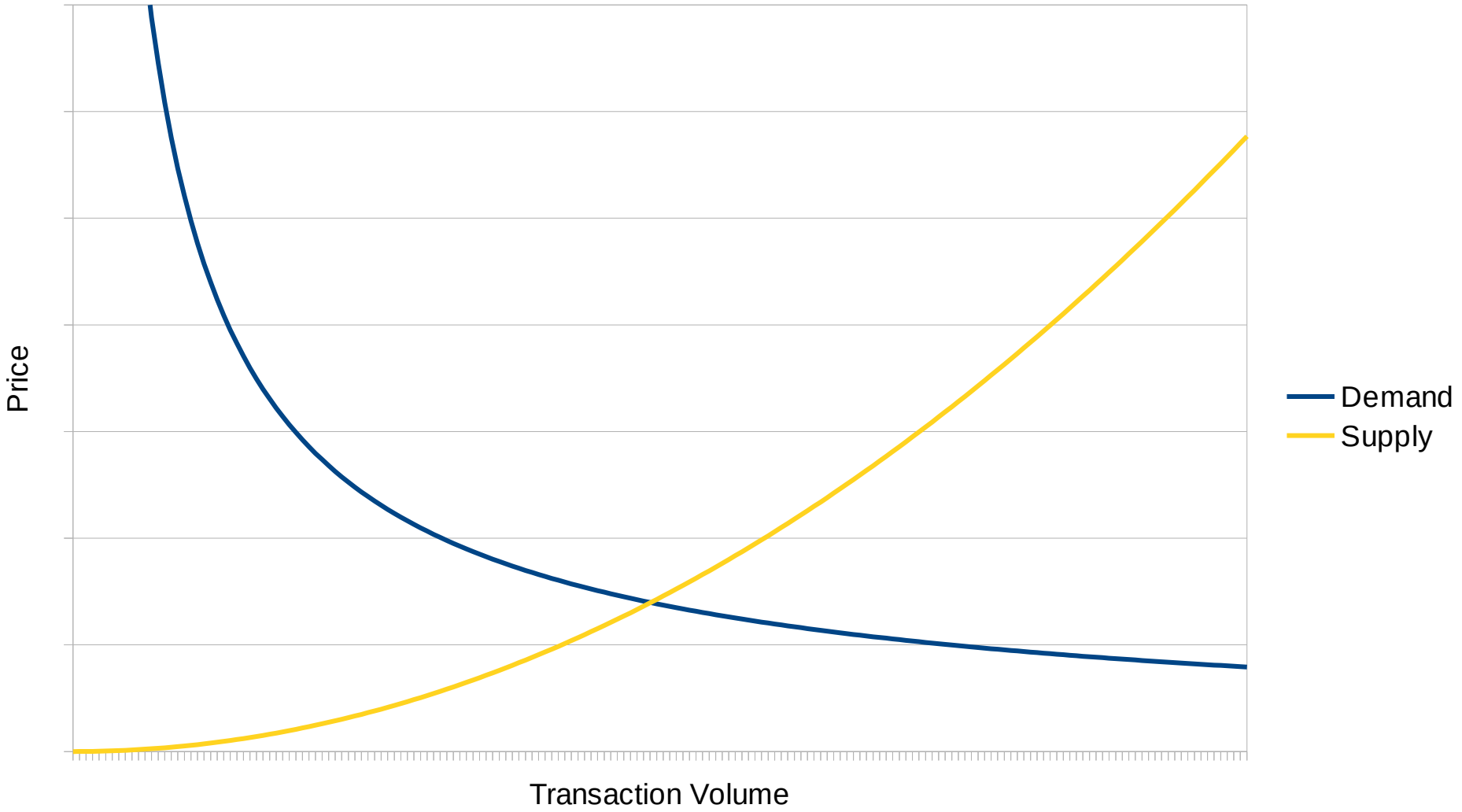
Blocksize Economics

Hong Kong - December 2015

Part 1

The marginal cost of adding a transaction to a block

Blockspace Supply & Demand Curve



What is the marginal cost?

- The marginal cost to the miner of including an extra transaction in a block, is small relative to other costs
- The marginal costs are propagation risk and a small amount of data processing costs
- **Fundamental economic problem:**
  - ***Mining is necessary for security reasons, the cost of hashing is almost totally unrelated to marginal cost of adding a transaction.***

Artificial cap to inflate fees

- Since around early 2011, there has been widespread debate about the potential requirement for an economically relevant blocksize limit, in order to artificially inflate fees, to sustain mining revenue
- A more recent response to this above argument is that “orphan risk” is a marginal cost, which can ensure high enough fees

Orphan risks

- Orphan risk could be the marginal cost which drives the fee market
- The larger the block the larger the orphan risk
- It is argued that propagation risks ensures a reasonable supply curve exists and a fee market works

Issues with “using” orphan risk

- Propagation costs could fall exponentially over time as technology improves. These technological improvements are not linked to a falling requirement for network security, therefore equilibrium difficulty could be too low
- It would require orphan risk to be a significant mining cost:
  - Orphan risk is what the entire system is designed to prevent. Miners will push orphan risk up to the limit to increase margins and security may fall
  - Miners do not need to propagate to themselves, it therefore helps larger miners at the expense of smaller miners. This incentivises mining centralisation

Defence of orphan risk idea

- Orphans are not bad and if the orphan rate increases that is not a concern
- Orphan risk is just another cost for miners. Costs already include rent, electricity, salaries, maintenance and hardware. The “Chinese” already have economise of scale in these areas, therefore adding another cost makes mining more competitive and decentralised.

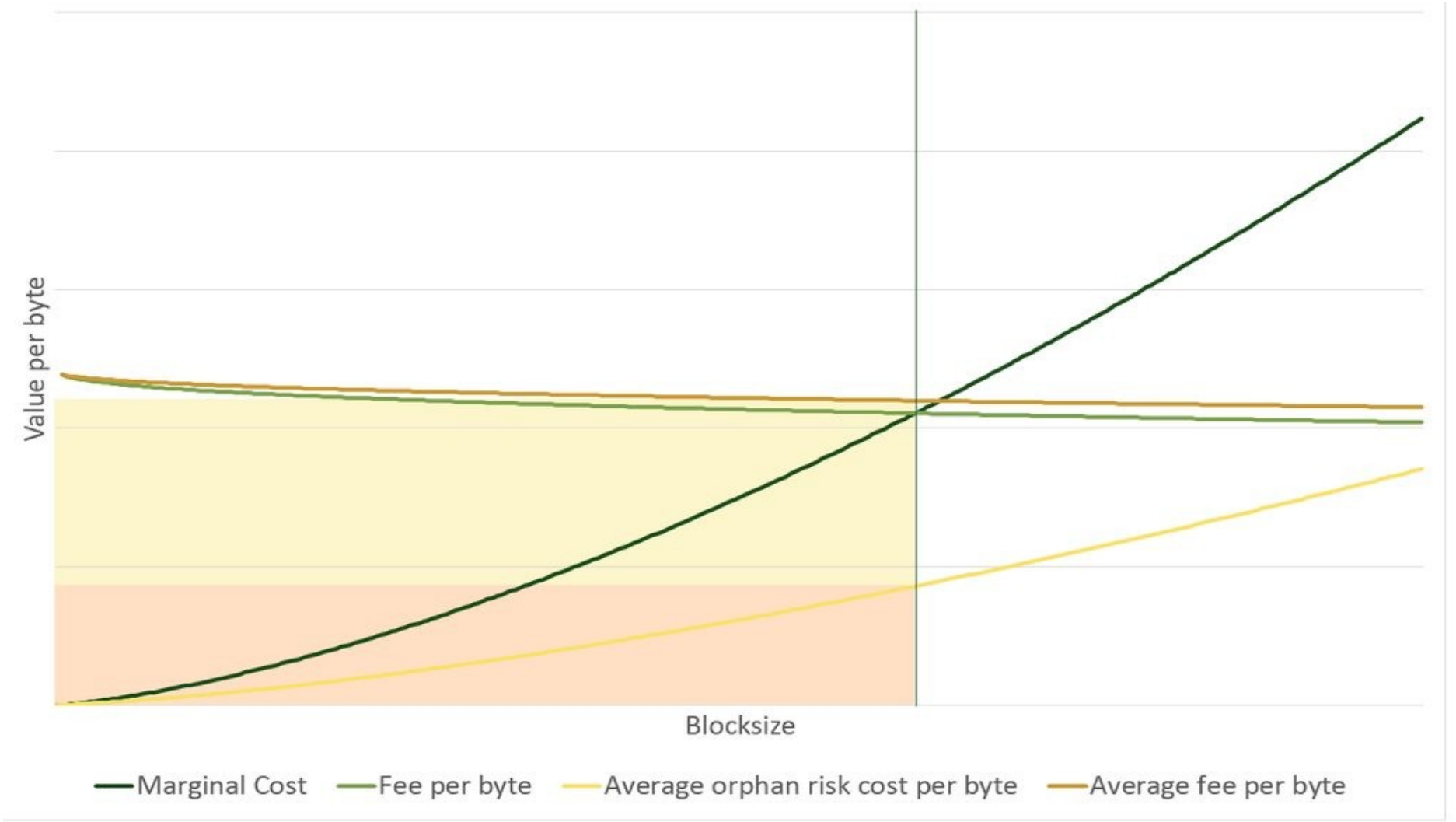
Orphan risk costs are unique

- Orphan risk costs are the only marginal cost of adding a transaction and therefore drive fees
- With respect to other costs, we can at least hope economise of scale run out
- Orphan risk is lower for larger miners and this is an inherent property of the system as miners do not need to propagate to themselves

Marginal orphan risk

- How does the marginal orphan risk change with respect to blocksize?
  - Exponential relationship?
  - Linear relationship?
  - Sublinear/Other?
- Total orphan risk cost is likely to be large relative to transaction fee revenue. The absolute orphan rate makes no difference.

Best case: Exponential relationship



Part 2

Why don't miners voluntarily produce smaller blocks on their own?

Will miners produce smaller blocks on there own?

- It benefits each individual miner to generate as much cash as possible and produce larger blocks, the classic “tragedy of the commons” situation
- Responses to the “tragedy of the commons” argument:
  - This is too theoretical and unproven
  - This argument focuses too much on “next block game theory”, one should focus more on the long term “game of life”
  - It ignores the desire for faster confirmations

This is happening now in commodity markets

- Iron ore
  - Each individual iron ore miner is increasing production, driving prices down at the expense of the industry, to benefit themselves.
- Oil
  - Oil majors are producing more oil at a loss, as oil prices fall
- Gold
  - Gold miners are producing more gold at a loss, as gold prices fall
- Miners keep producing more until they fail, they never reduce production voluntarily
- Unlike resources industries, Bitcoin always needs a healthy mining industry, for security purposes

Nobody is right

- There are two competing visions of game theory here:
  - Miners care about the long term interests of the system - “Game of life”
  - Miners maximise profit in the next block - “Nash Equilibrium”
- In reality there are a range of miners with different priorities
- These priorities could vary throughout time, in cycles and therefore we need to ensure the system is robust in a variety of different scenarios

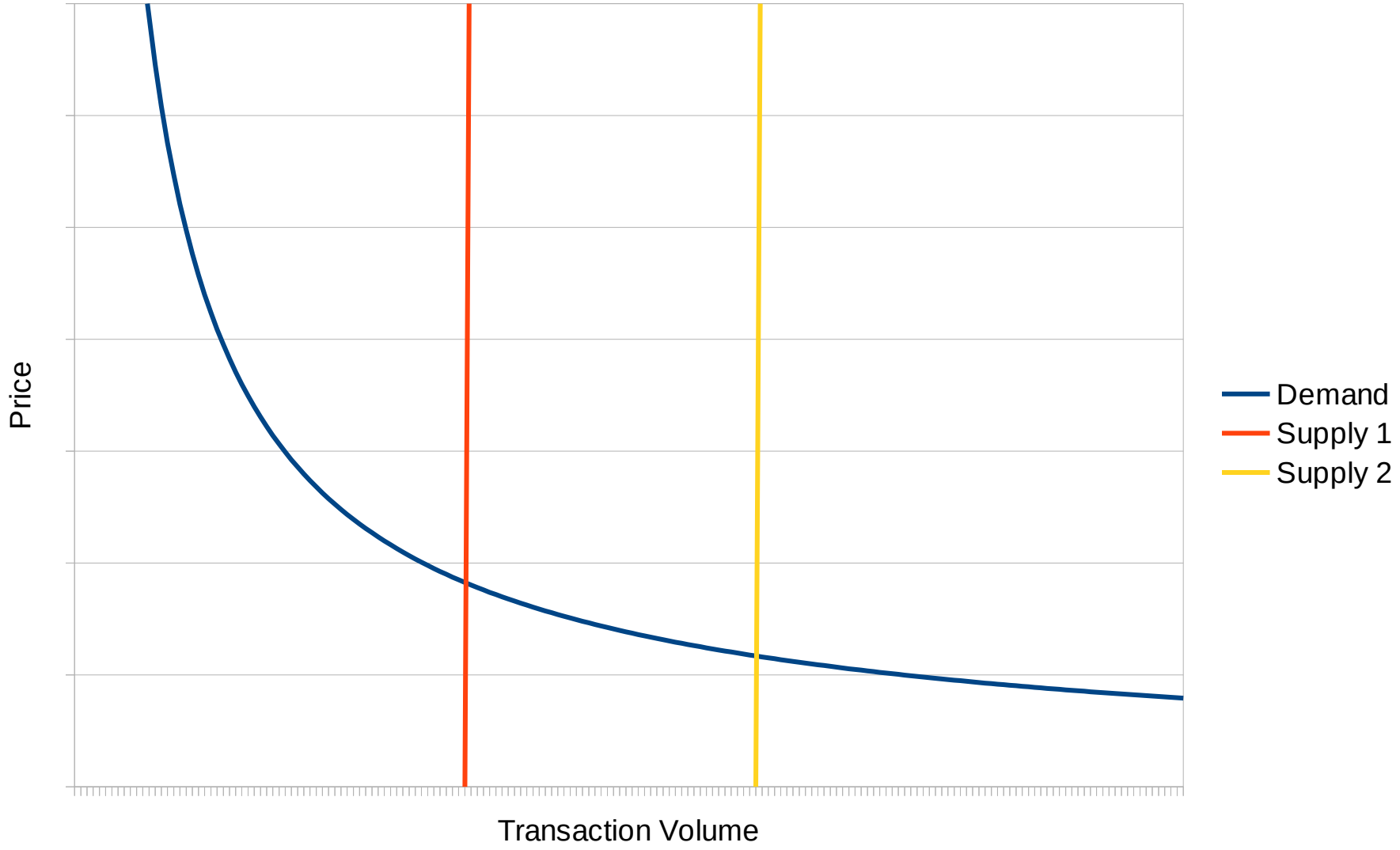
Part 3

BIP100

BIP100 Economics

- Rational miners vote to maximise revenue, similar to existing security assumptions
- Mining revenue = Block reward * Exchange rate + Transaction volume * Average Fee * Exchange rate
- Miners therefore vote to maximise the product of the exchange rate, transaction volume and the average fee
- BIP100 dynamically adjusts the limit, balancing out competing priorities within the community, in a market driven way, to reflect expected demand

Voting for larger blocks, based on expected elasticity of demand



Is BIP100 like a cartel?

- BIP100 enables cartel like pricing, whilst avoiding the difficulties of an actual cartel
- BIP100 is an open framework for miners to decide the limit in a transparent way

Shift to a simple 50th percentile voting mechanism

- Approval from all full nodes is required to increase a limit
- In contrast, a majority of miners can enforce a reduction in the limit by orphaning all blocks above a certain size
- The voting mechanism should reflect this power balance. Otherwise a 79% vote for a decrease could serve as a catalyst for the formation of a mining cartel to enforce the will of the majority and undermine the voting
- Therefore 50% of votes should be able to enforce a reduction

BIP100 is far from perfect

- The blocksize limit will be “sub optimal” as miners vote to maximise their revenue, not utility for users. However the optimal level is subjective
- In exceptional cases, miners may benefit from a lower Bitcoin price and could vote to reduce the limit and price to drive out competing miners
- The economics of BIP100 are attractive, there are other more technical reasons for the block size limit

There are no perfect solutions, therefore lets be pragmatic

BIP100, BIP102 & BIP103 seem somewhat reasonable interim proposals