Mind the Gap

Security implications of the evolution of Bitcoin mining

Miles Carlsten Harry Kalodner Arvind Narayanan

Structure of this talk:

- Miners no longer be incentivized to mine all the time
- The future of the mining hardware
- Impact on the Bitcoin system
- Implications and assumptions of the model

Block Reward

Block Reward = Minting Reward +Tx fees

Block Reward = Minting Reward +Tx fees

Minting Reward 

Tx Fees 

Block Reward = Minting Reward +Tx fees

Minting Reward 

Tx Fees 

Equivalent?

Block Reward = Minting Reward +Tx fees

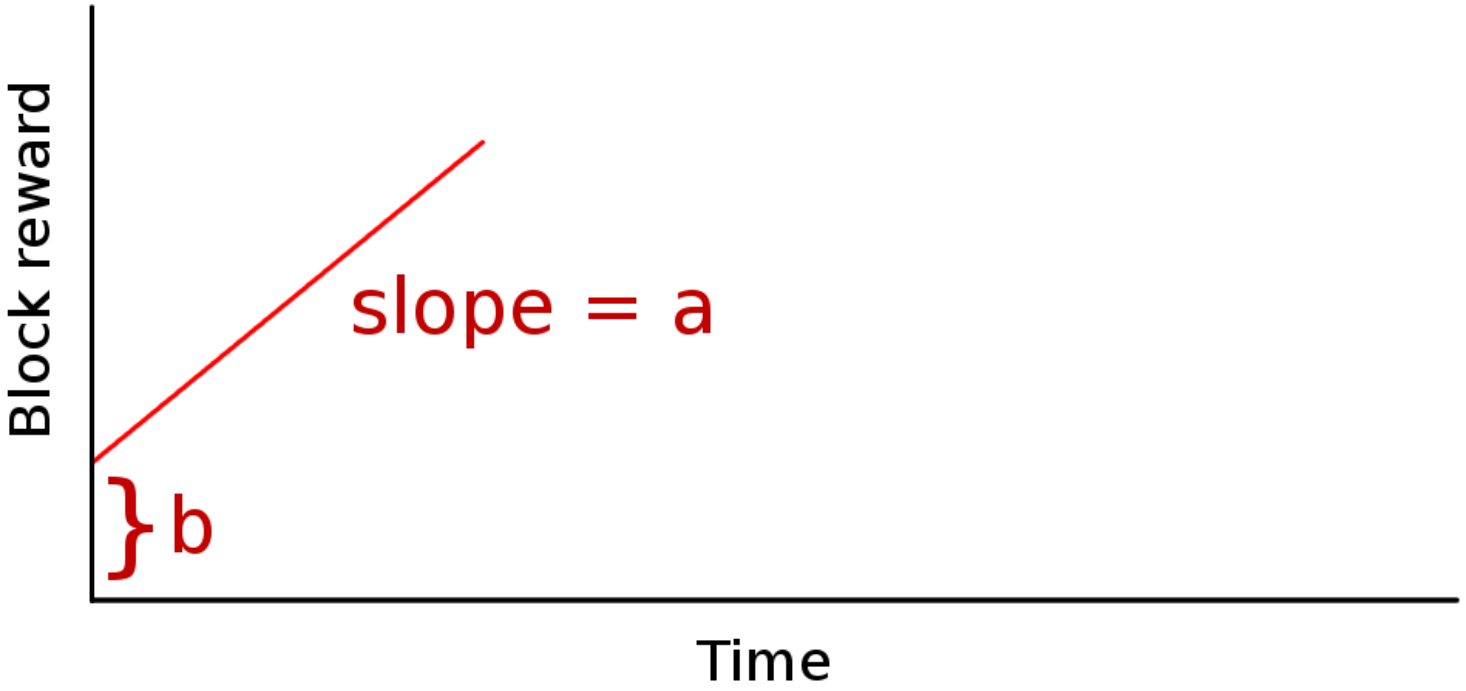
Minting Reward

Tx Fees

Block reward becomes a function of time.

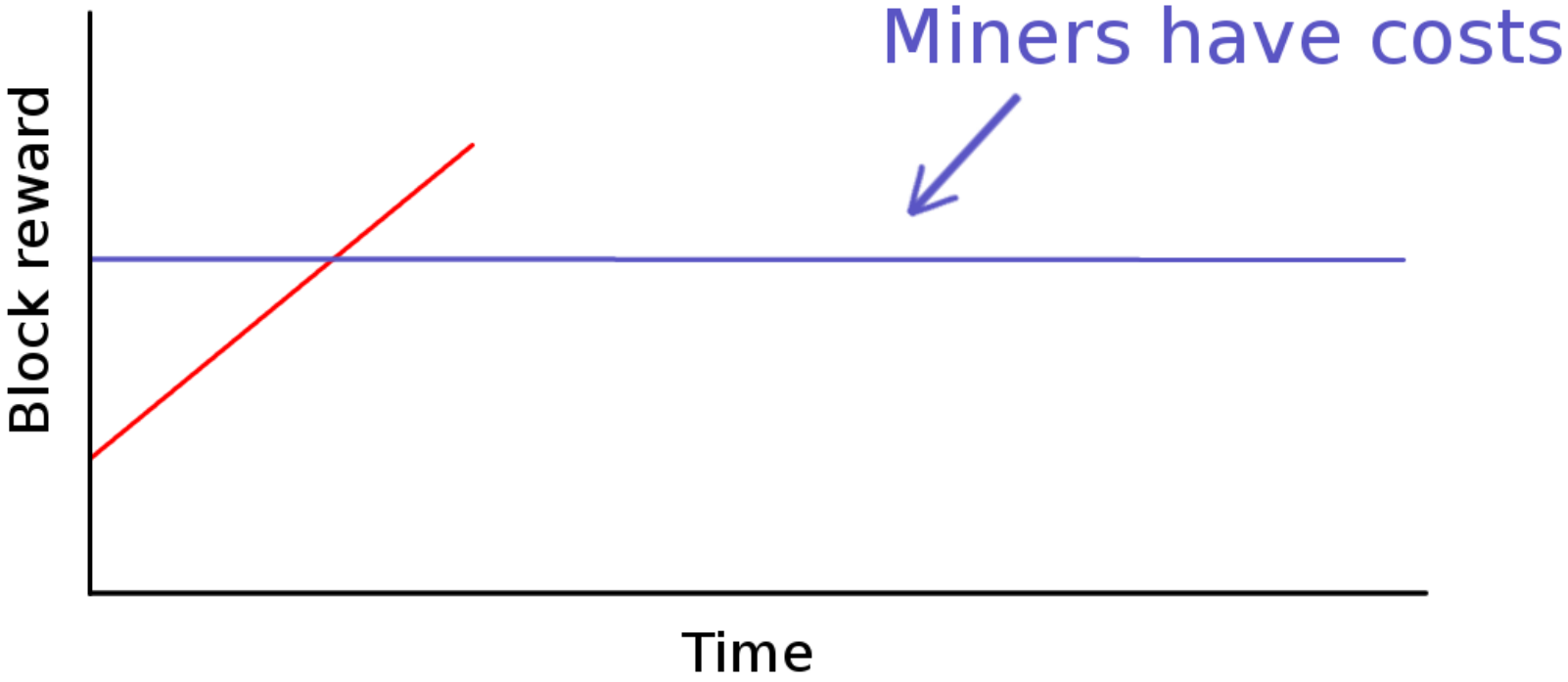
Block reward becomes a function of time.

Block reward = b + at



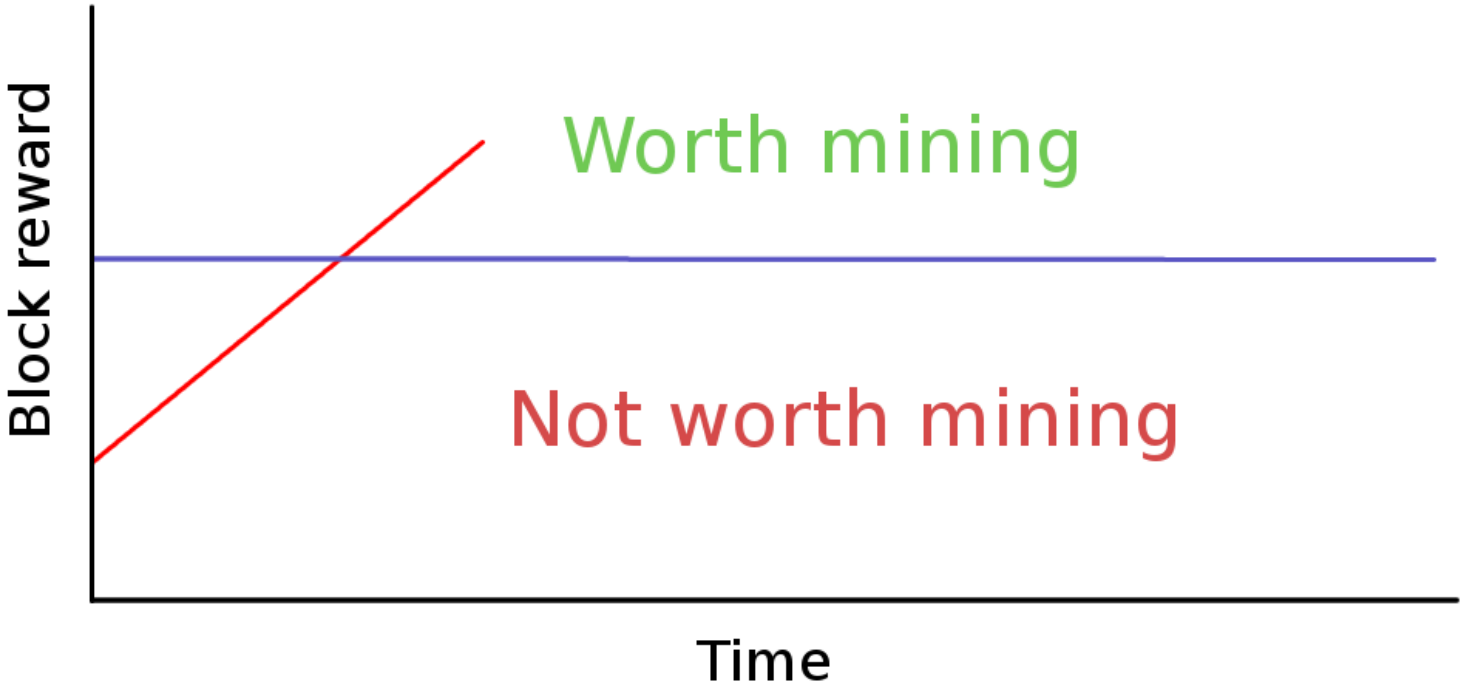
Block reward becomes a function of time.

Block reward = b + at



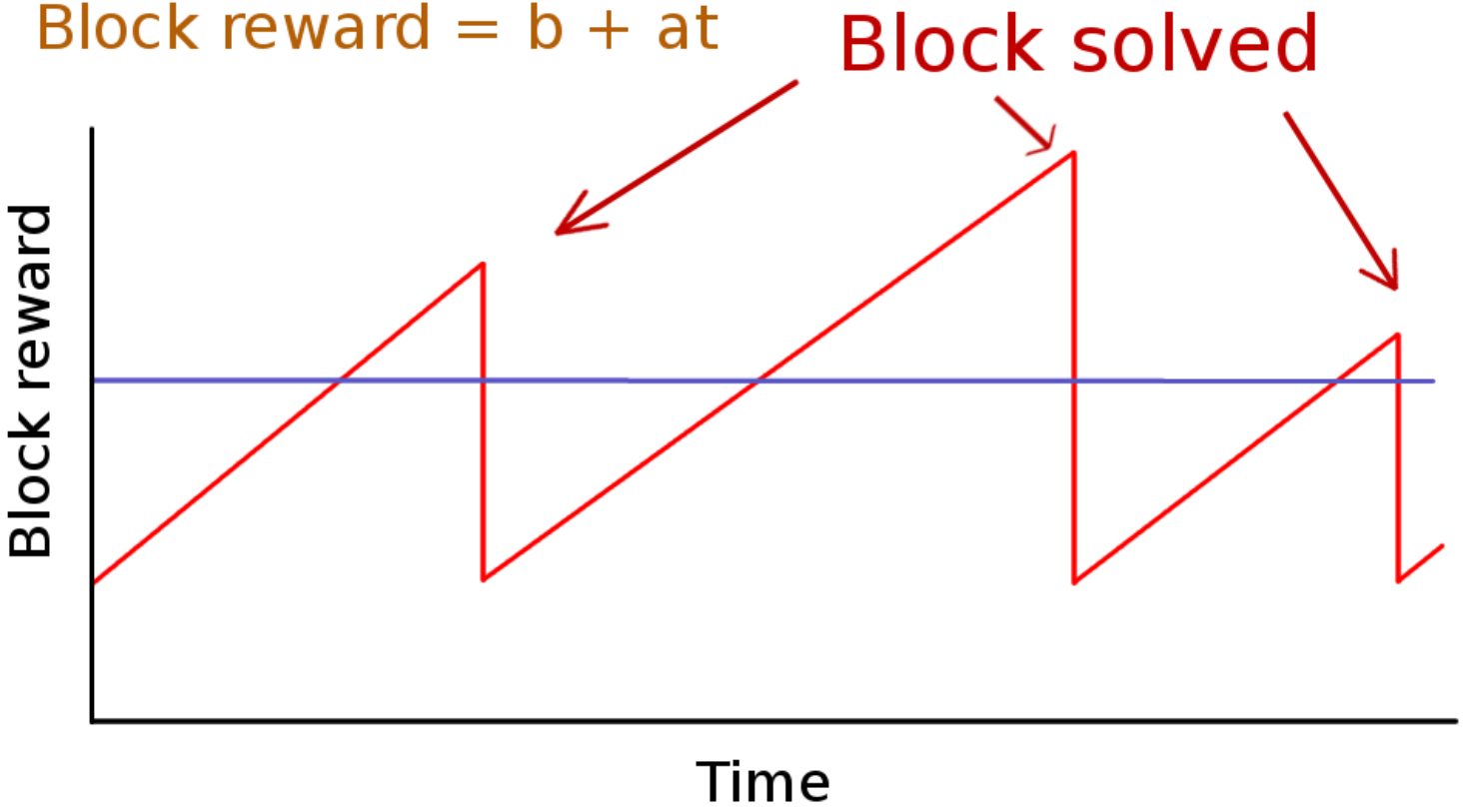
Block reward becomes a function of time.

Block reward = b + at



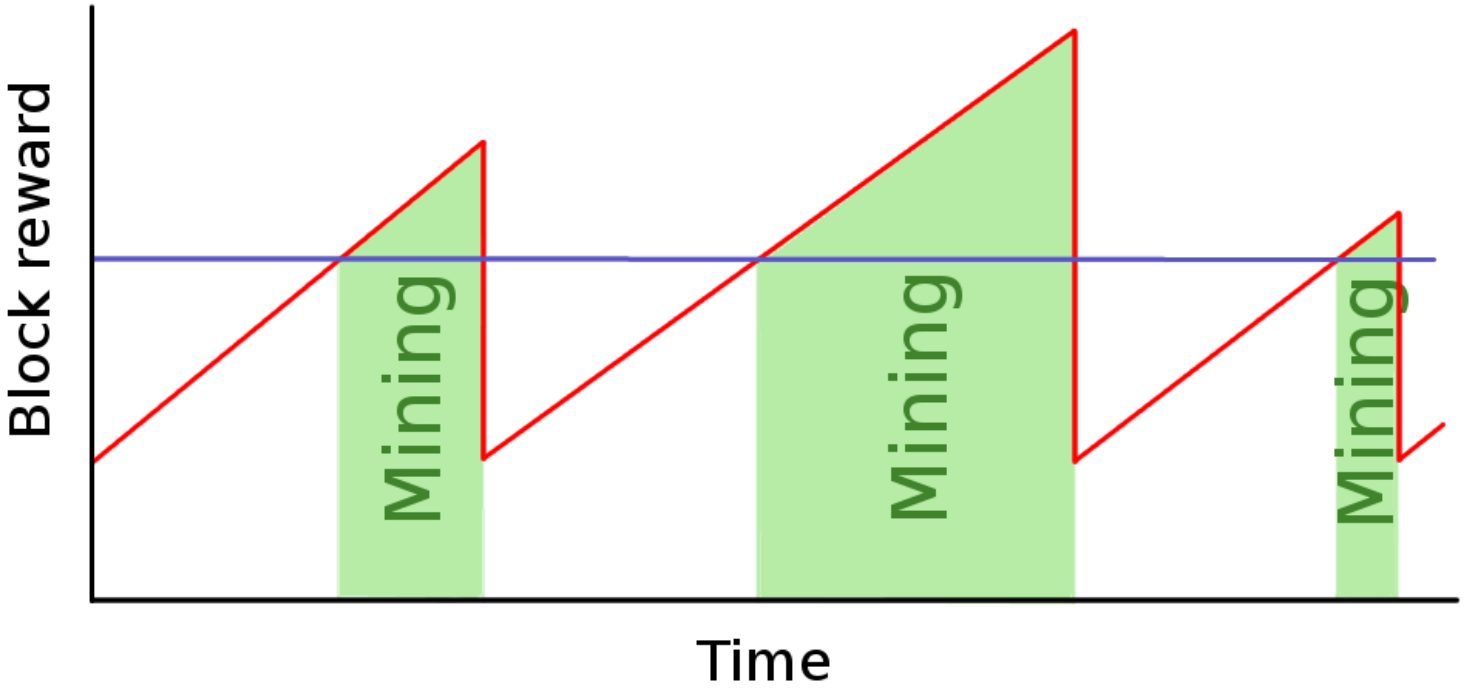
Block reward becomes a function of time.

Block reward = b + at



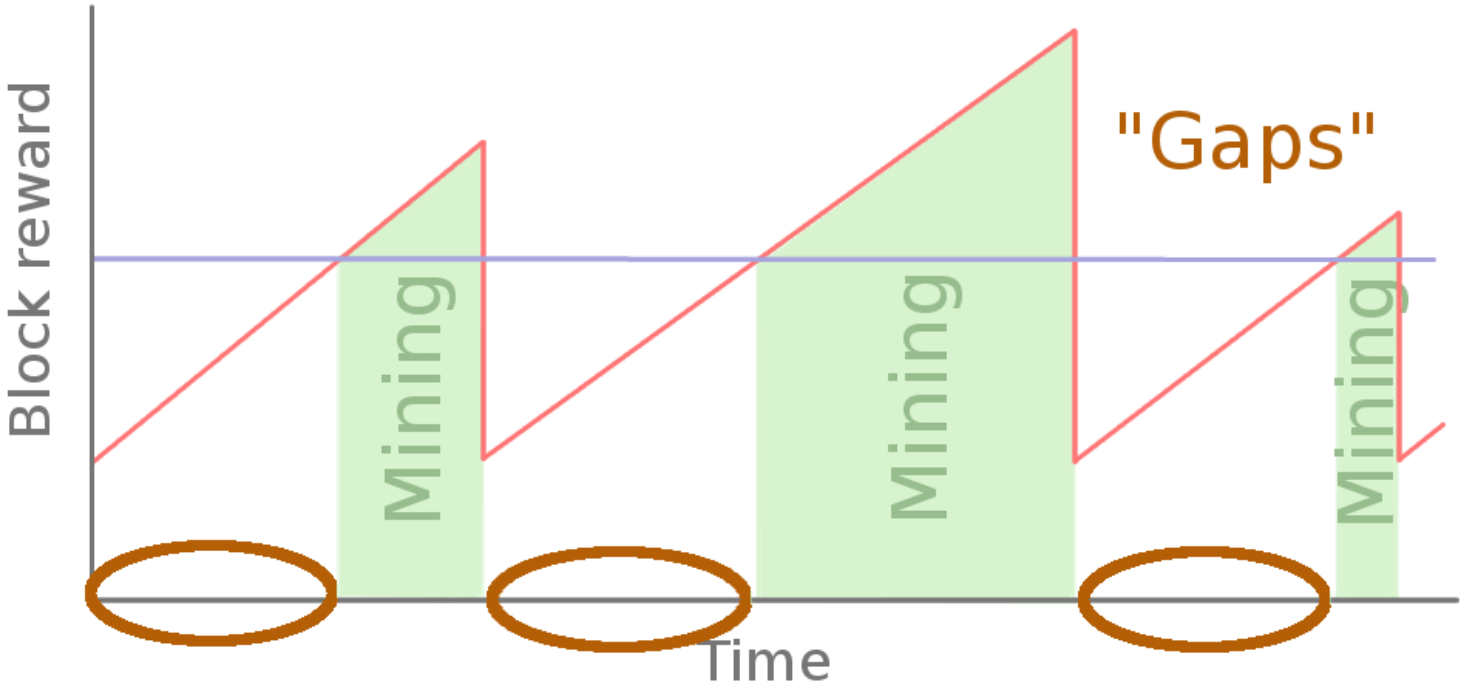
Block reward becomes a function of time.

Block reward = b + at



Block reward becomes a function of time.

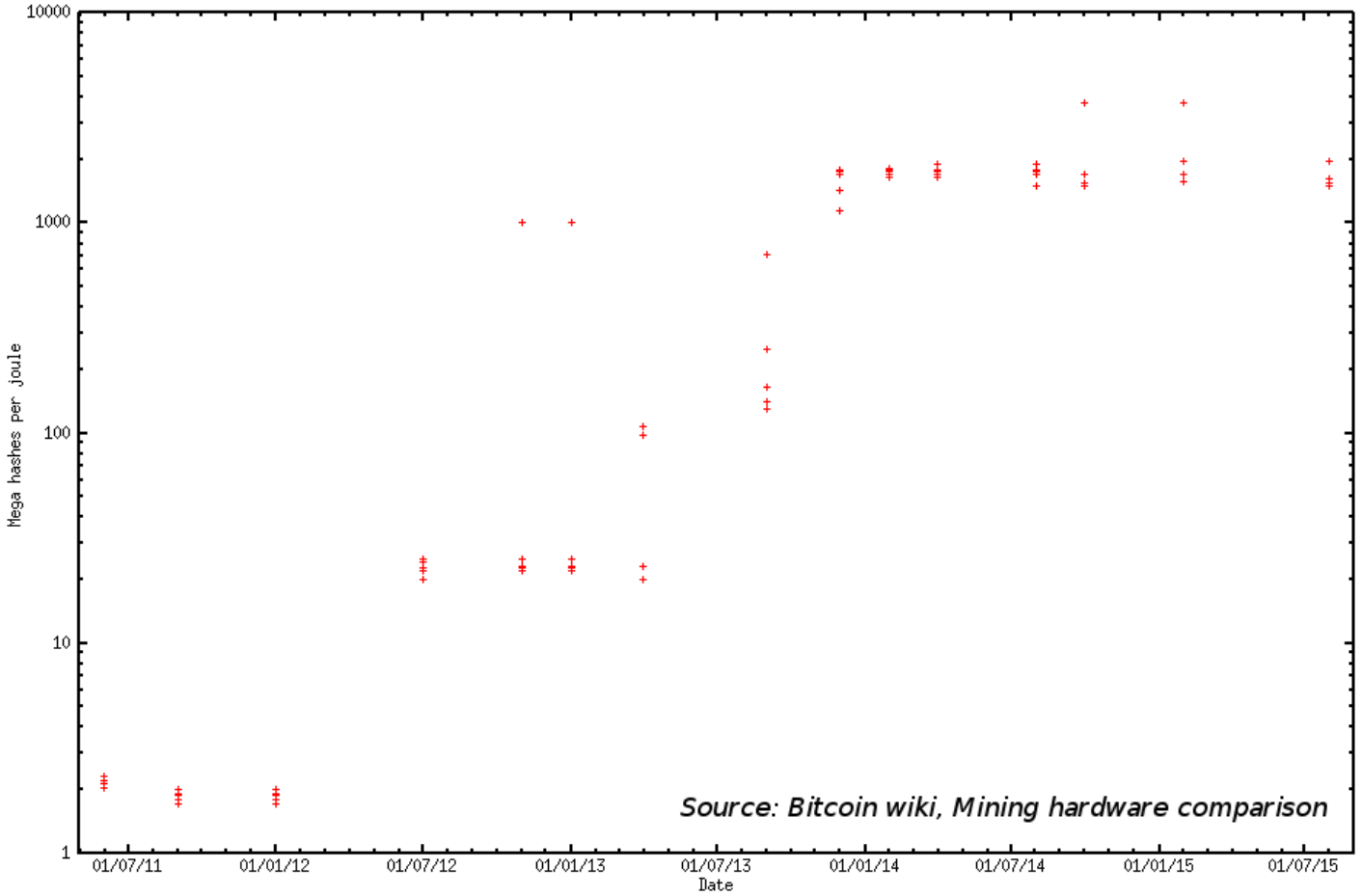
Block reward = b + at



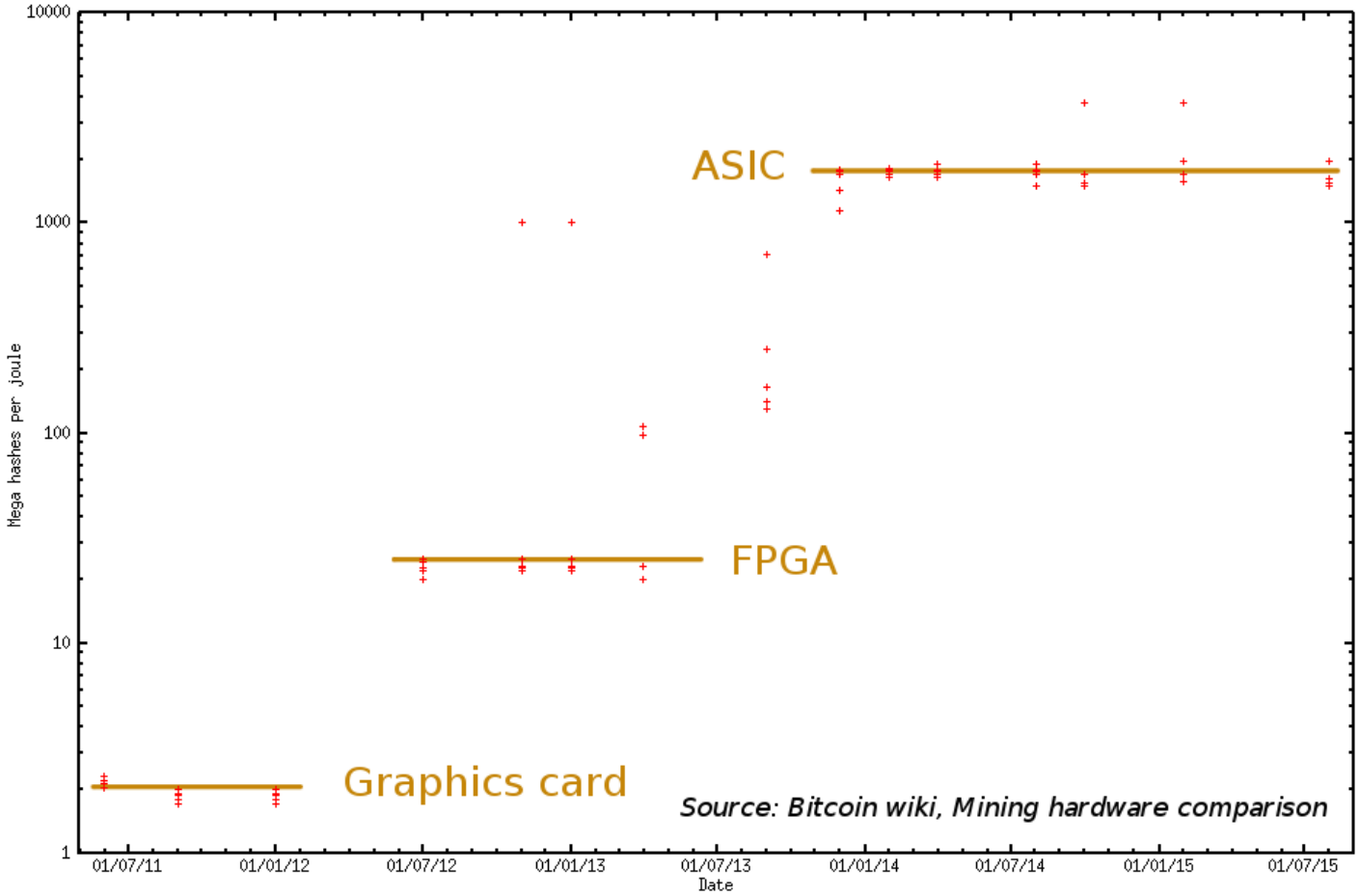
The future of hardware

- Mining hardware will become commoditized
- Moore’s Law is dead here
- Cheaper, longer lasting hardware

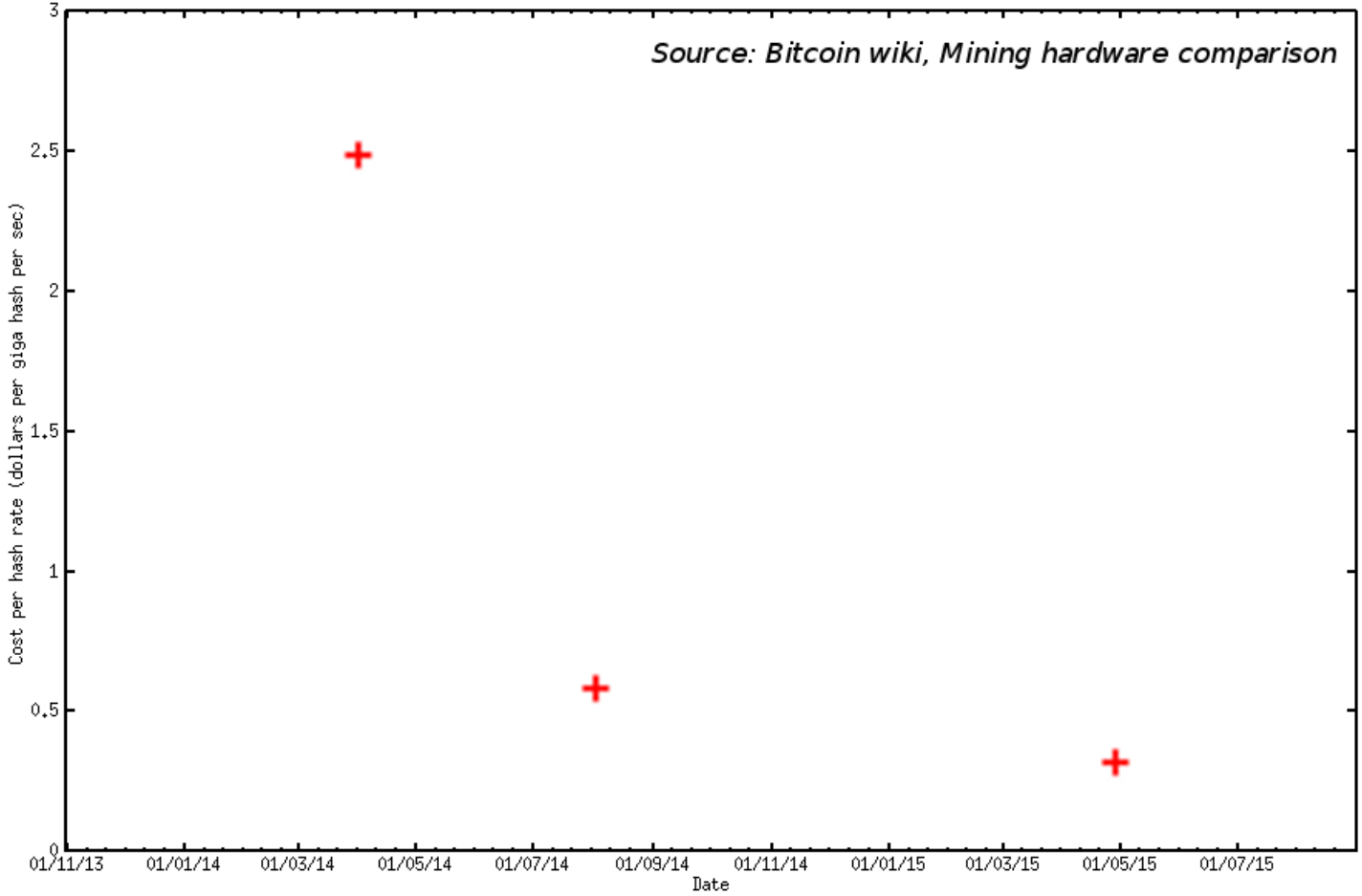
Evolution of Mining Efficiency



Evolution of Mining Efficiency



Changes in Mining Hardware Fixed Cost



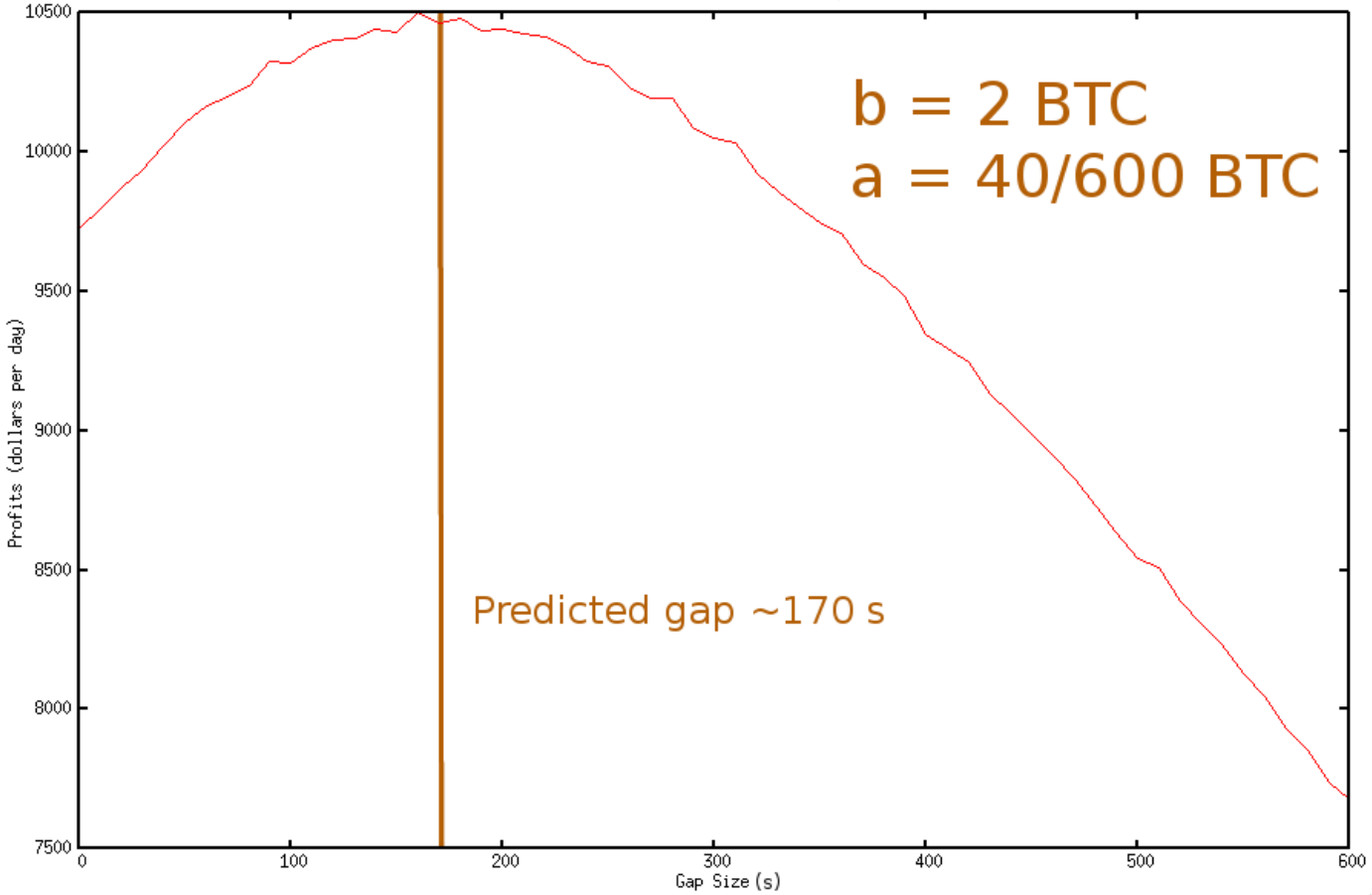
When is it rational to start mining?

- Miners independently makes this decision
- Instantaneous basis
- When the expected reward/hash >= cost/hash

When is it rational to start mining?

- Mathematical description
- Simulation

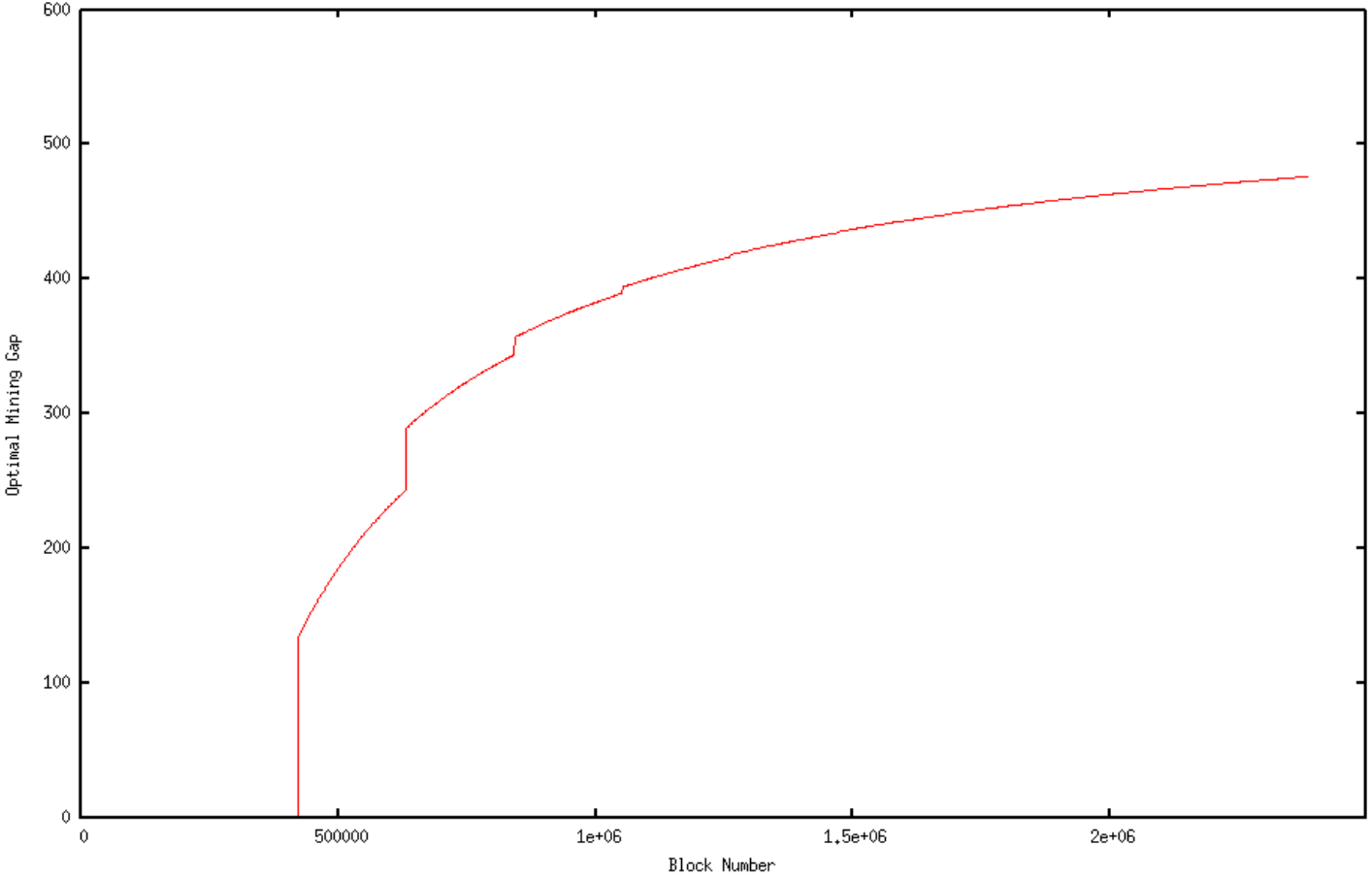
Miner Profits by Gap Size



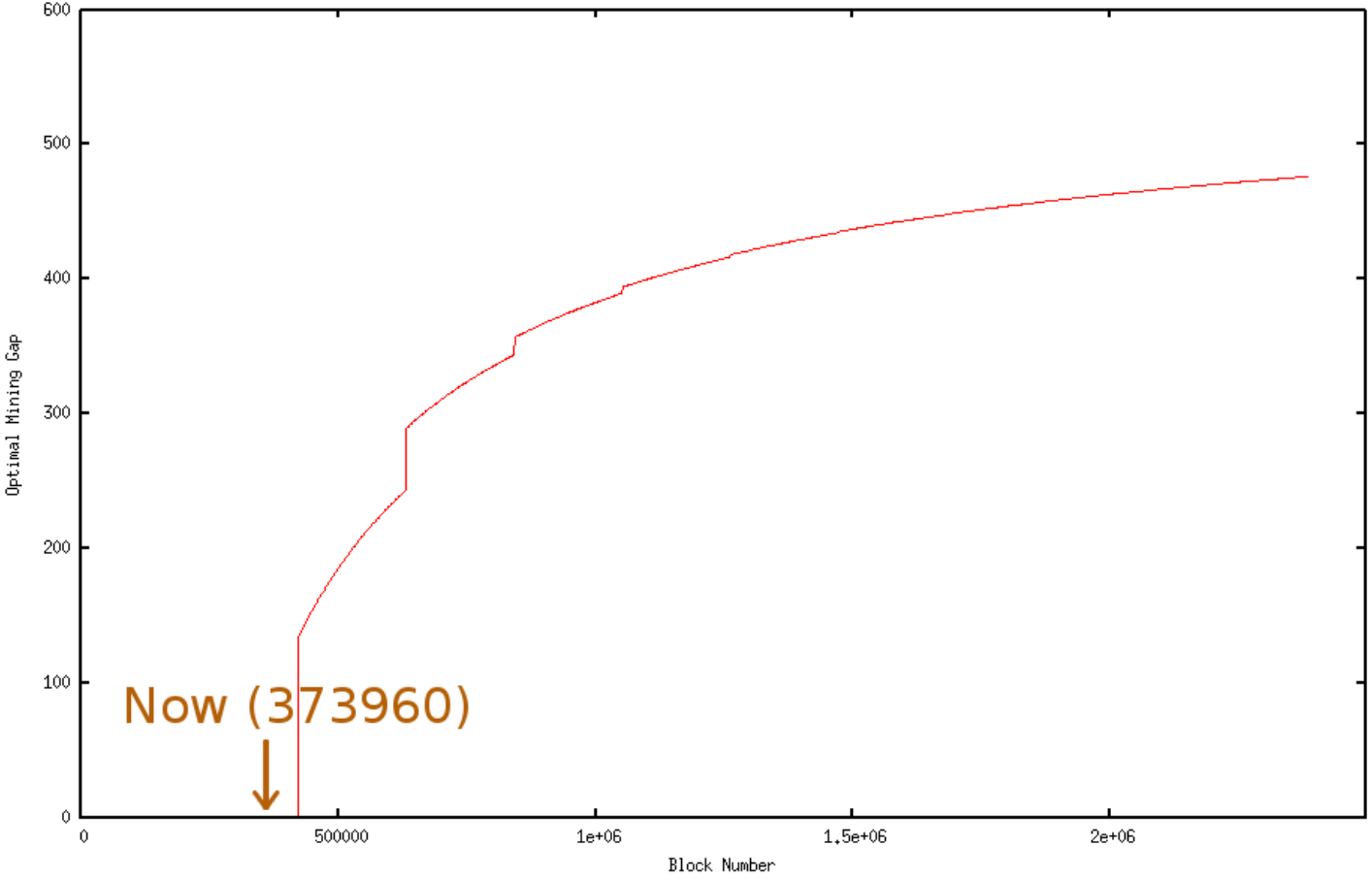
What does this mean in the future?

- Miners invest in new hardware
- Behaviour of the gap

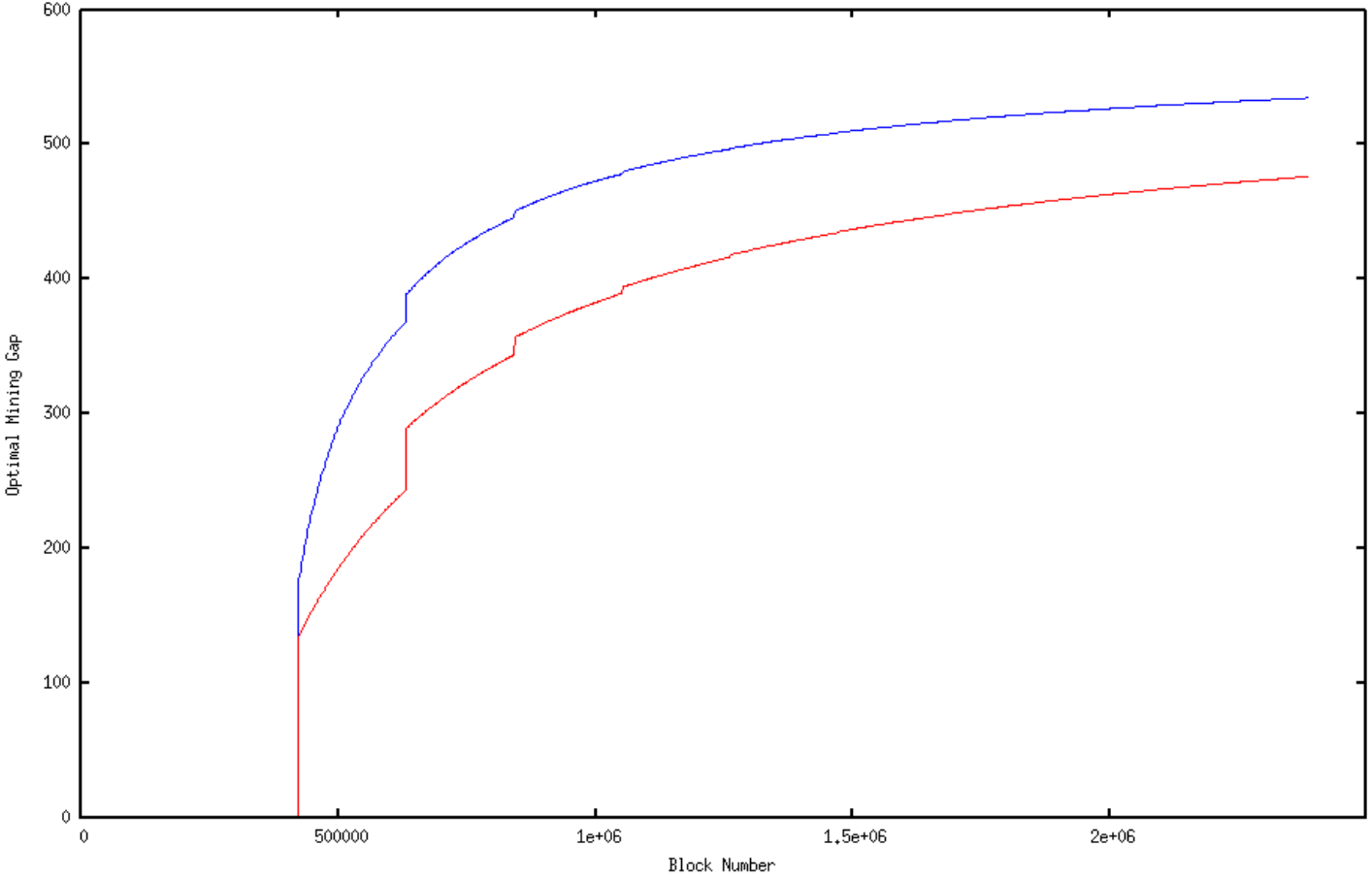
Evolution of the Mining Gap



Evolution of the Mining Gap



Evolution of the Mining Gap

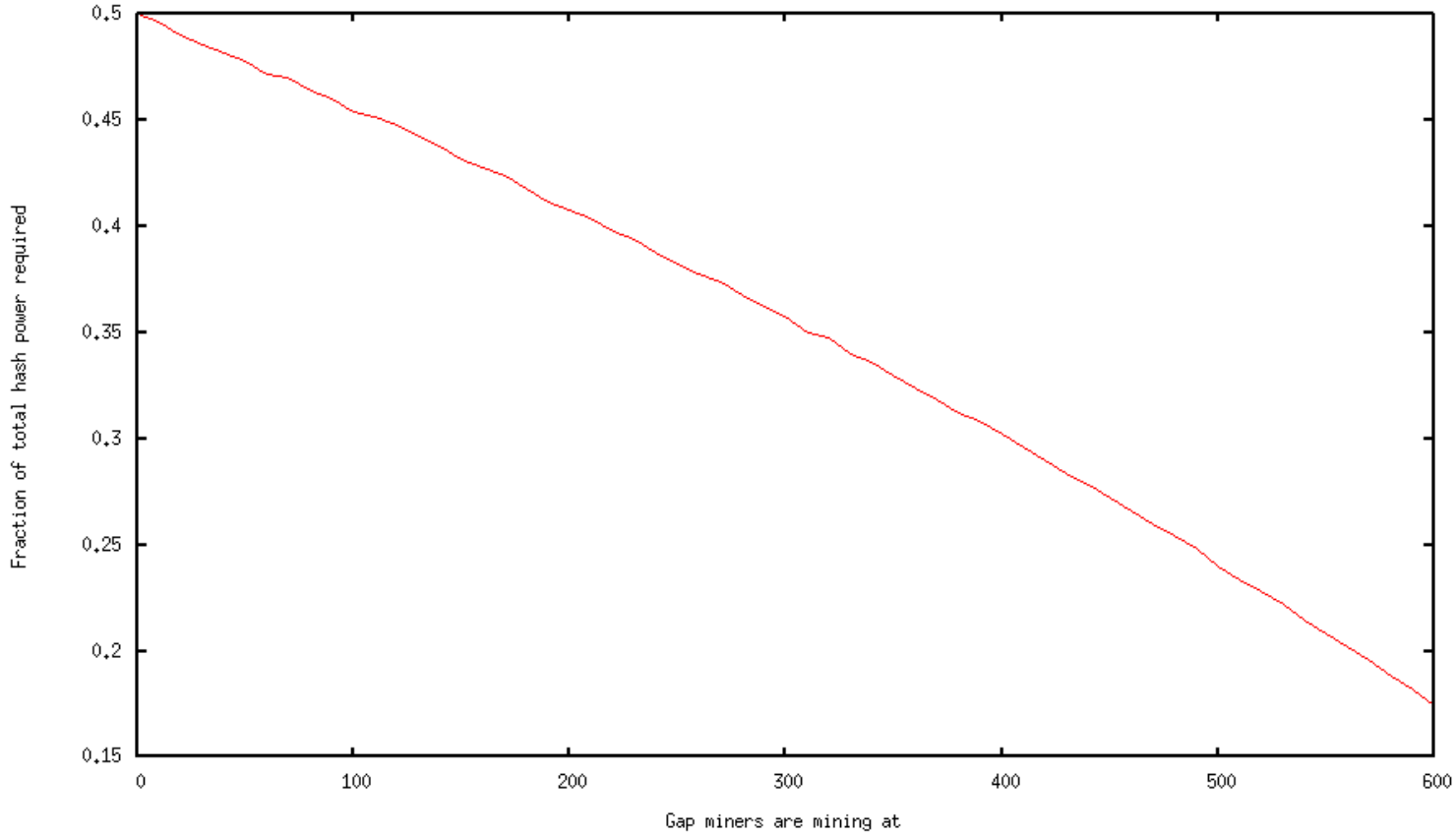


Take-aways from the prediction

- Gap at next reward halving
- Gap approaches 600 s in the future
- Exacerbated by commoditization of hardware

Security implications

- Increased vulnerability to attacks
- Amplified attackers perceived hashrate


Hash Power Required for 51% Attack
Fraction of total hash power required
0.5
0.45
0.4
0.35
0.3
0.25
0.2
0.15
0
100
200
300
400
500
600
Gap miners are mining at

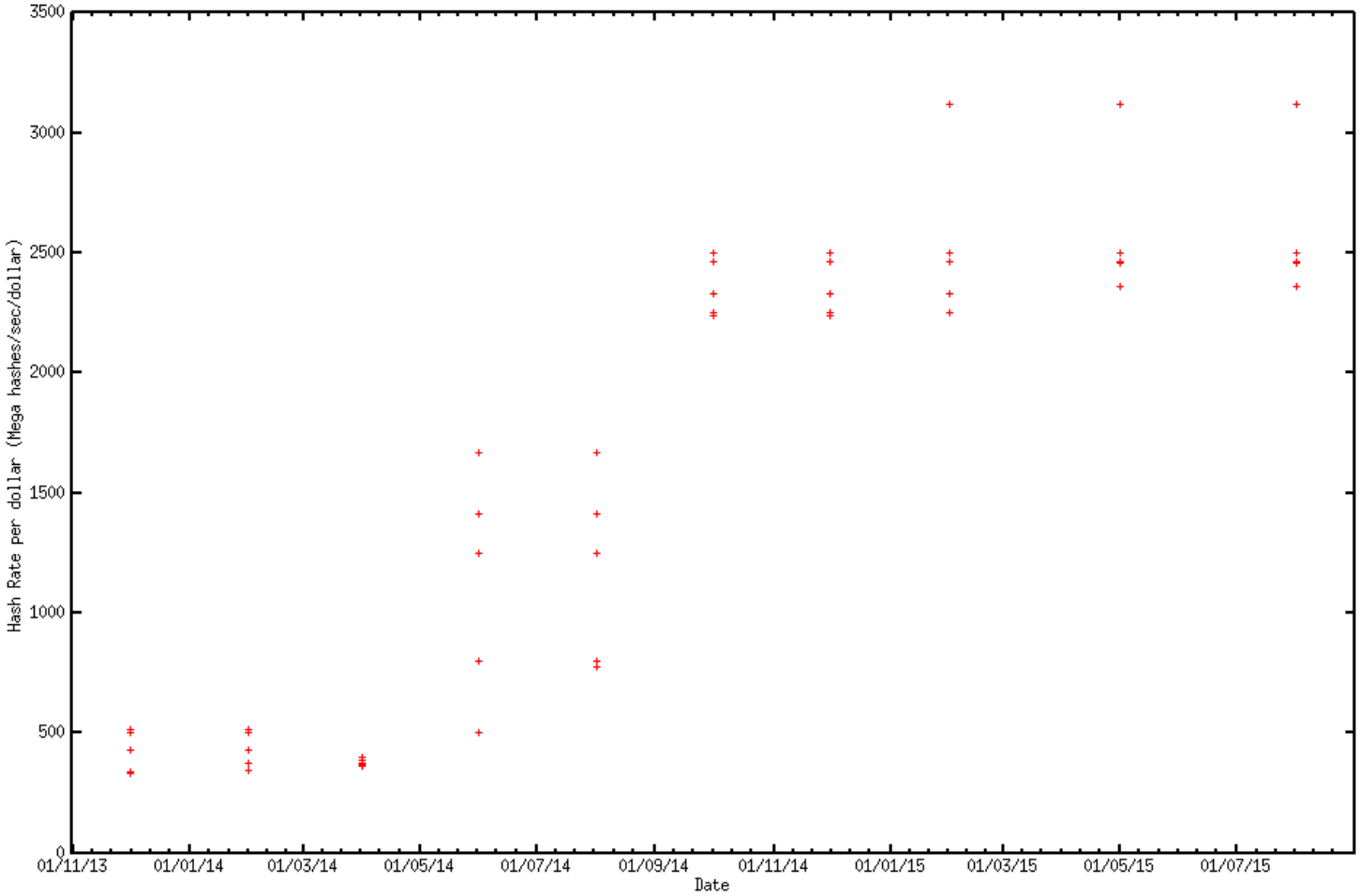
Conclusion

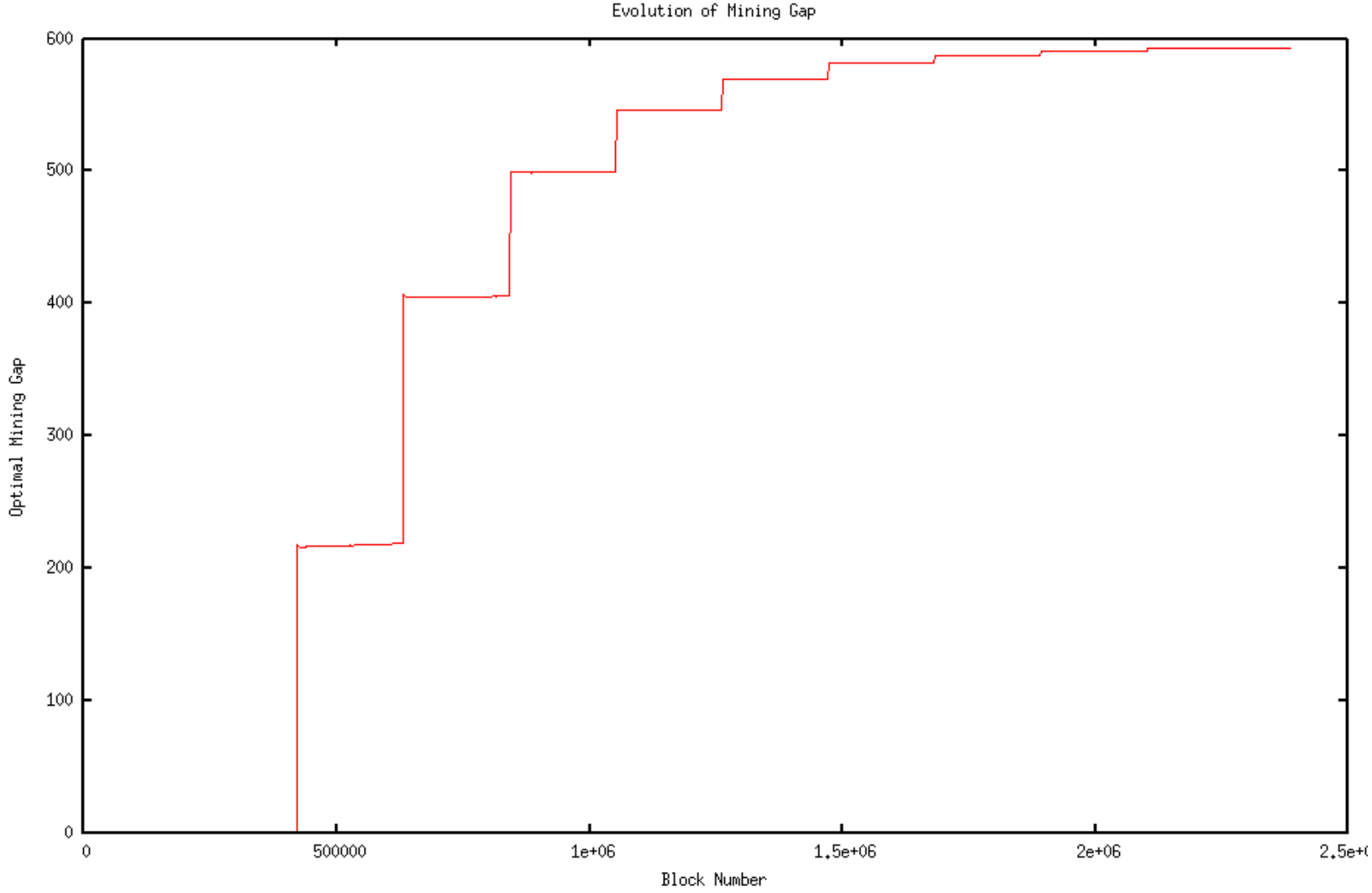
- Needs to be profitable to mine immediately
- Assumption made in this model:
  - No backlog of transactions

Thank you.

Any Questions?

Change in Fixed Cost of Mining Hardware




Evolution of Mining Gap
Optimal Mining Gap
Block Number
600
500
400
300
200
100
0
0
500000
1e+06
1.5e+06
2e+06
2.5e+0