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
Block Reward = Minting Reward + Tx fees

Minting Reward → Tx Fees

Equivalent?
Block Reward = Minting Reward + Tx fees
Block reward becomes a function of time.
Block reward becomes a function of time.

Block reward = b + at

\[ \text{slope} = a \]
Block reward becomes a function of time.

Block reward = b + at

Miners have costs
Block reward becomes a function of time.

Block reward = b + at
Block reward becomes a function of time.

Block reward = b + at

Block solved
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

Source: Bitcoin wiki, Mining hardware comparison
Evolution of Mining Efficiency

Source: Bitcoin wiki. Mining hardware comparison
Changes in Mining Hardware Fixed Cost

Source: Bitcoin wiki, Mining hardware comparison
When is it rational to start mining?

- Miners independently make this decision
- Instantaneous basis
- When the expected reward/hash $\geq$ cost/hash
When is it rational to start mining?

- Mathematical description
- Simulation
Miner Profits by Gap Size

\[ b = 2 \text{ BTC} \]
\[ a = \frac{40}{600} \text{ BTC} \]

Predicted gap \( \sim 170 \text{ s} \)
What does this mean in the future?

- Miners invest in new hardware
- Behaviour of the gap
Evolution of the Mining Gap

Now (373960)
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
Conclusion

● Needs to be profitable to mine immediately

● Assumption made in this model:
  ○ No backlog of transactions
Thank you.

Any Questions?