RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: BAC-R02

The Detrimental Nature of Proofs of Work, and Risks to Cryptocurrencies

Guy Stewart
CTO and Co-founder
EGNI Inc.

Introduction

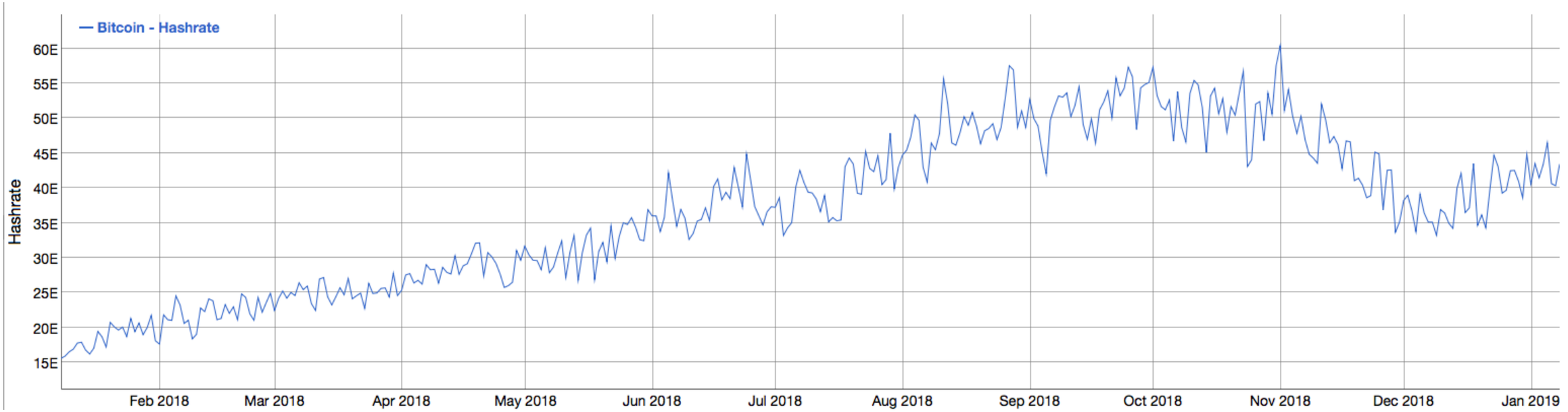
This talk is about the complex reasons behind the crash

… and what to do next …

RSAConference2019

Fluctuations

Fluctuations - Bitcoin hash rate (hash/s per day)



BITCOIN HASH RATE GROWTH CHART

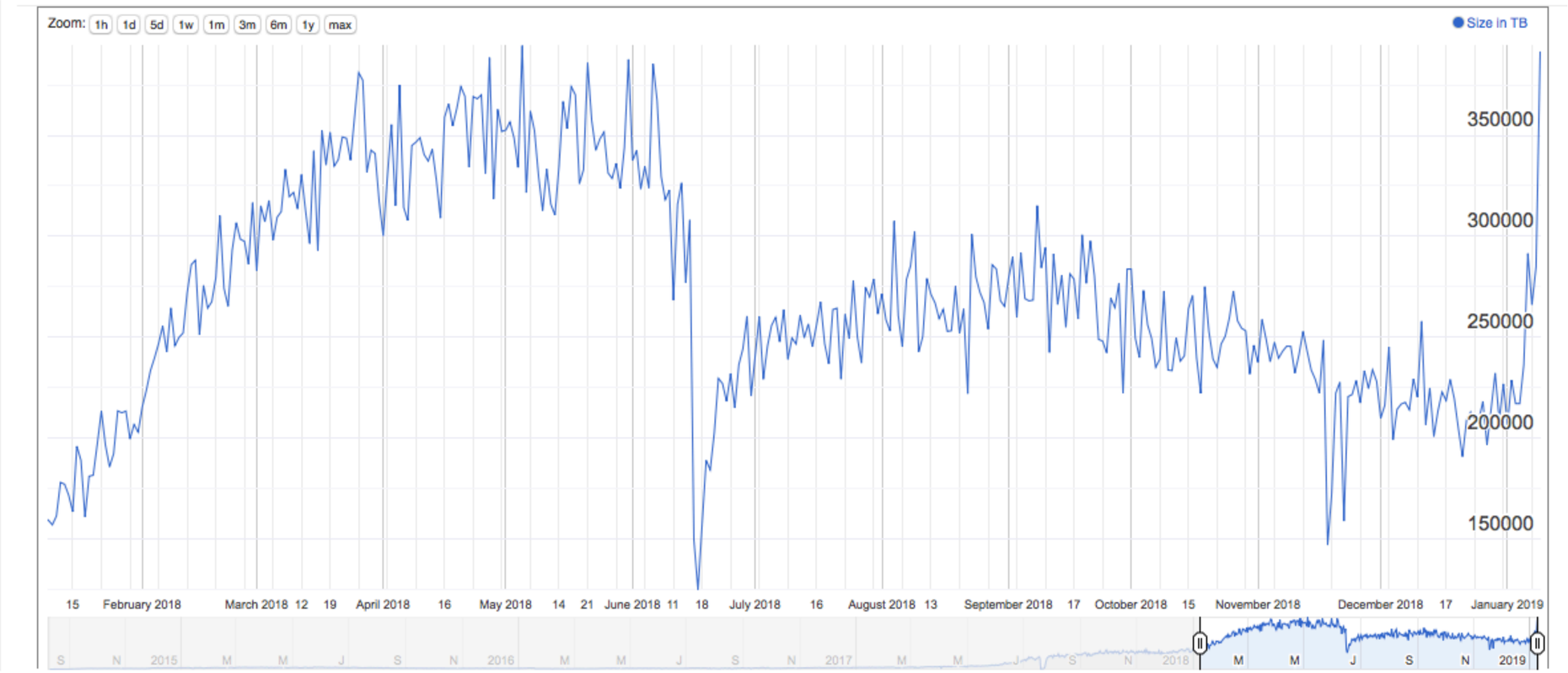
Hash rate fluctuates with market trends

Fluctuations: Ethereum

ETHEREUM NETWORK HASH RATE GROWTH CHART

Hash rate triples during period of irrational exuberance, then falls off dramatically

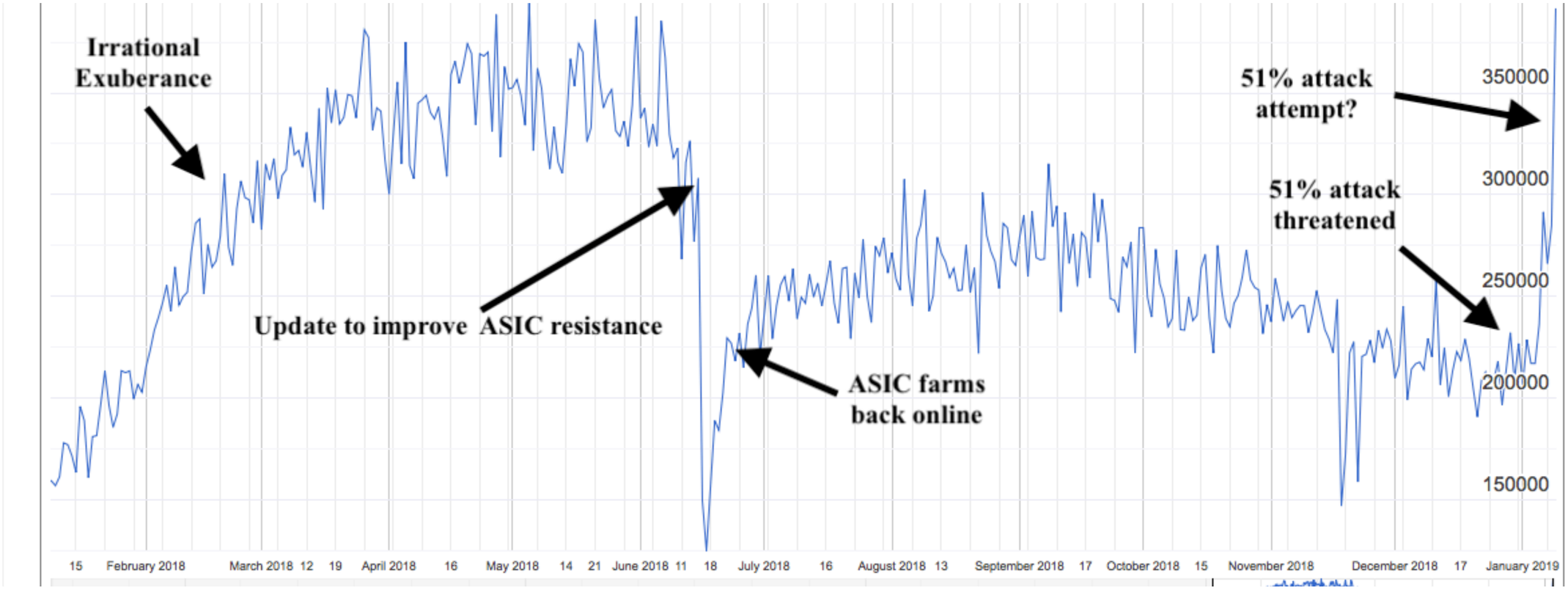
Fluctuations - PoC



NETWORK SIZE IN TB

The number and size of mining instances changes dramatically in response to external stimuli

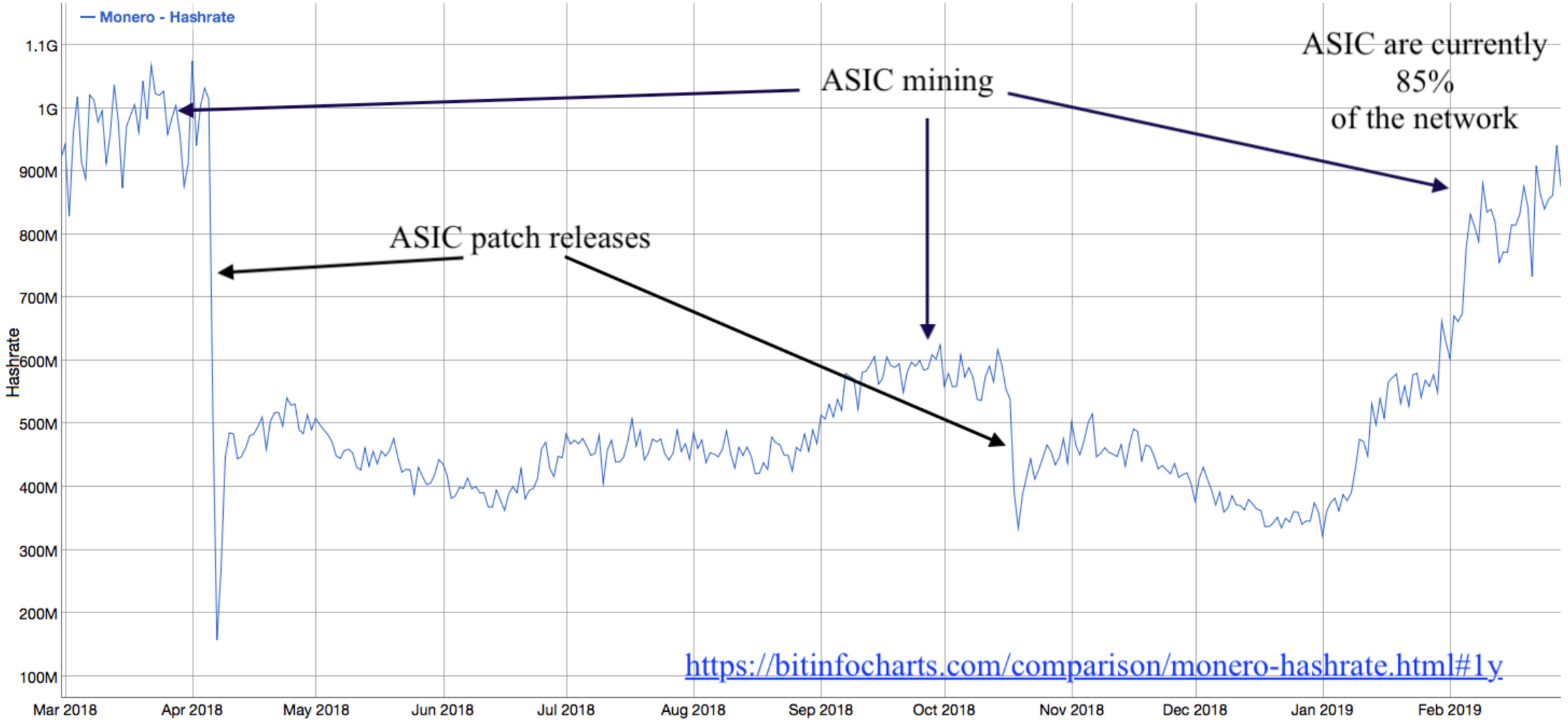
Fluctuation Stimulus Events



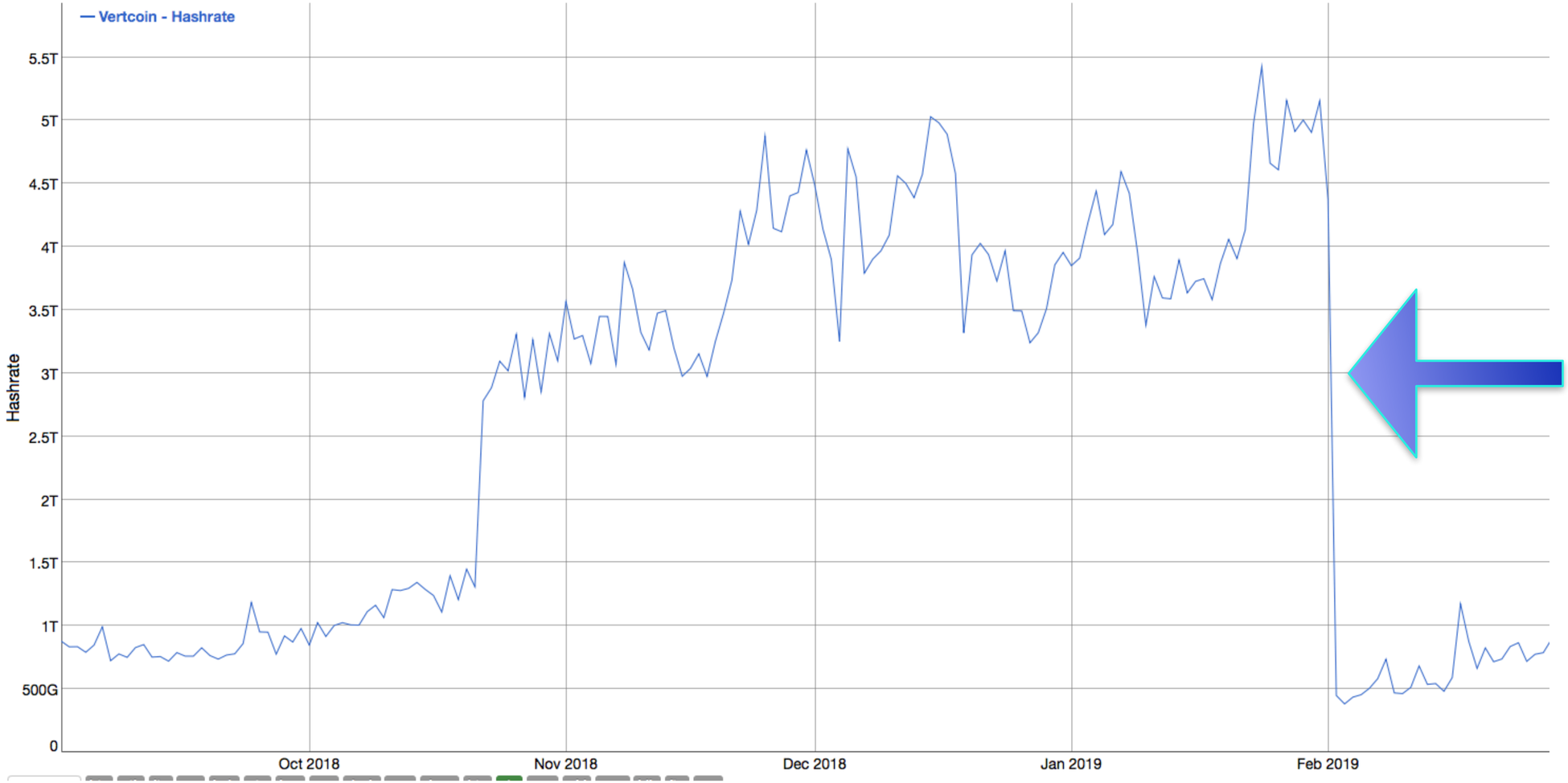
NETWORK RESPONSE TO EVENTS

The size of the mining network fluctuates dramatically in response to internal and external events

Monero anti-ASIC patches



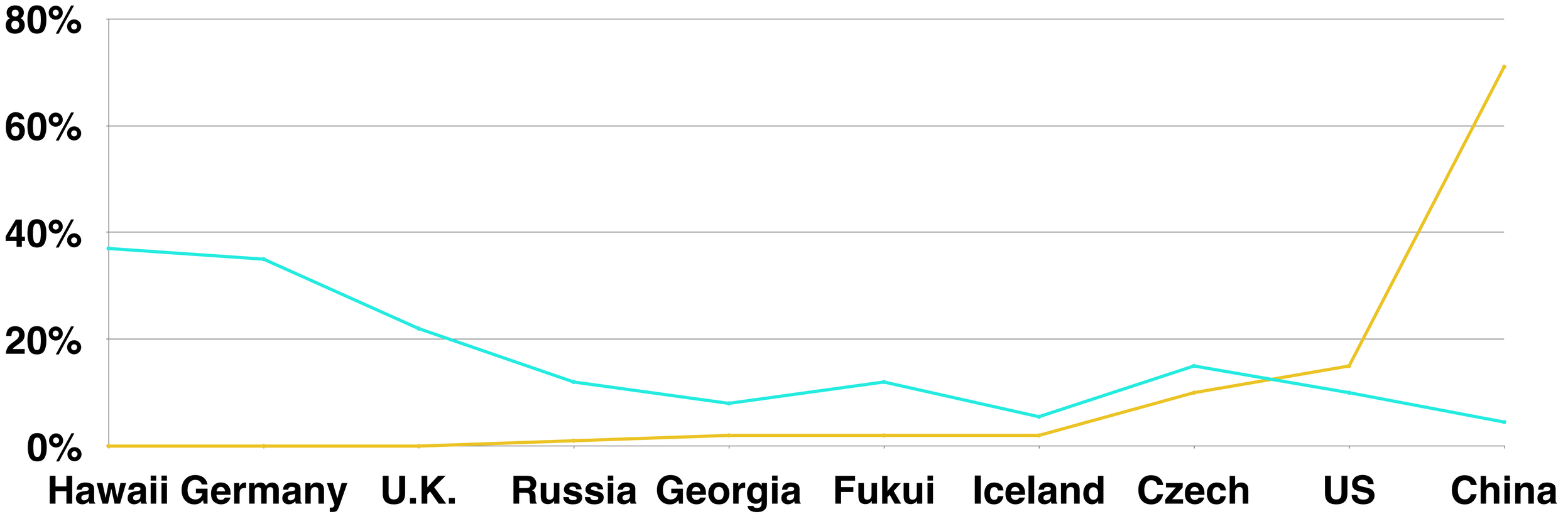
Vertcoin anti-ASIC patch



RSAConference2019

Cost of Power

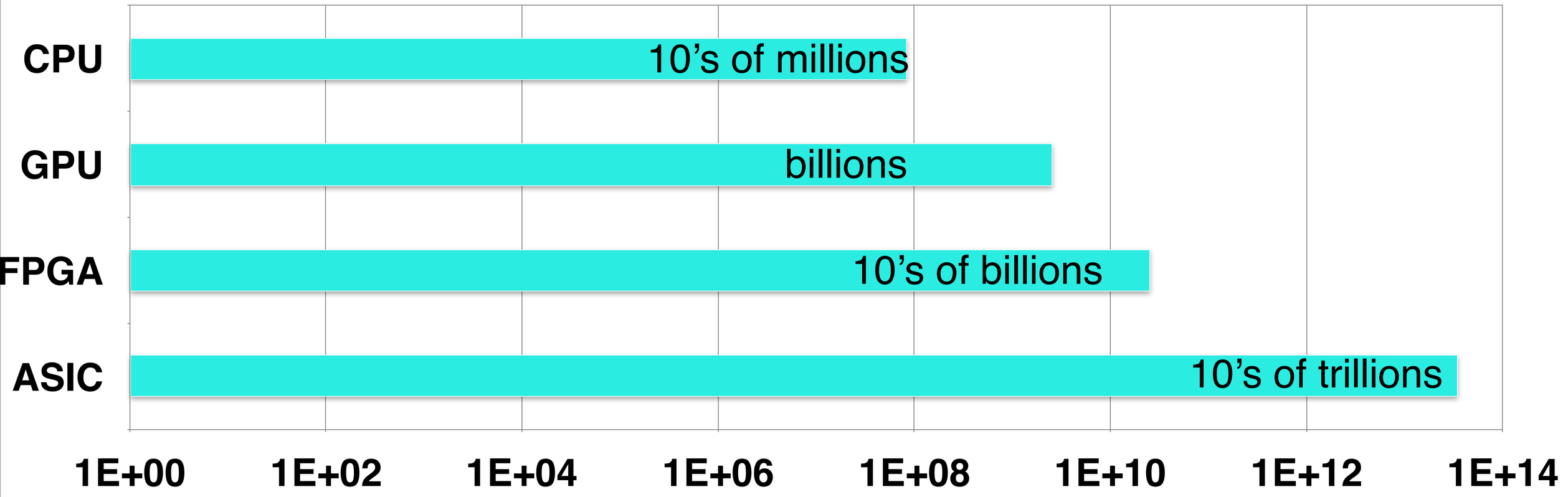
Cost of power —> Centralization



RSAConference2019

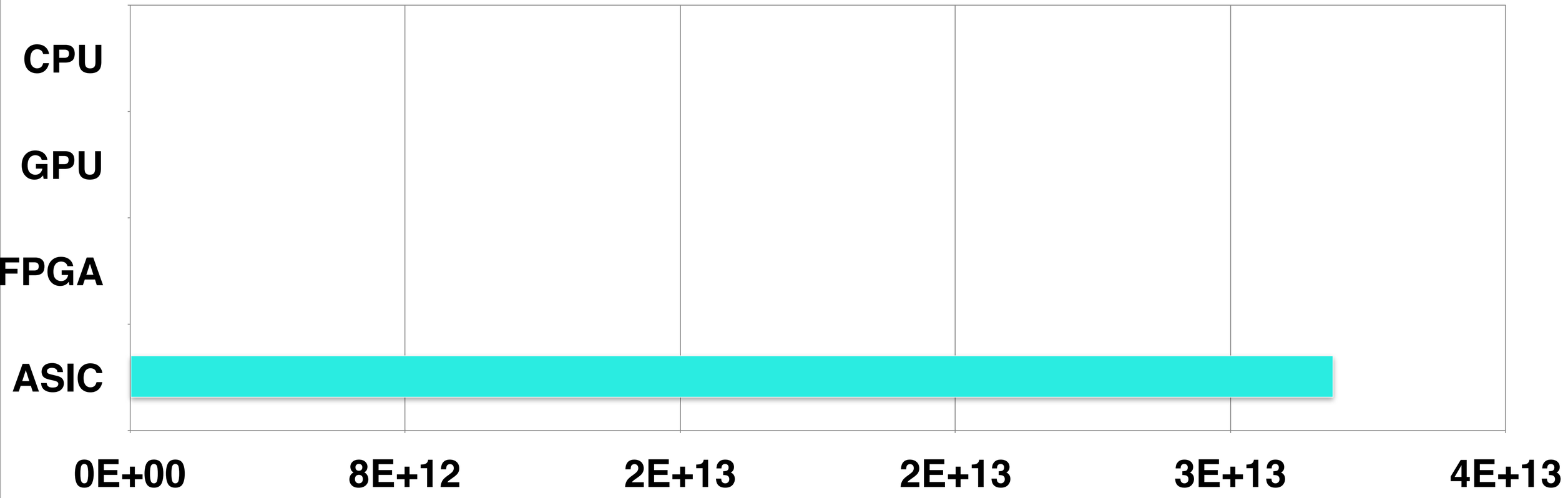
PoS / PoW tradeoffs

ASIC advantage



HASH/S - LOGARITHMIC SCALE

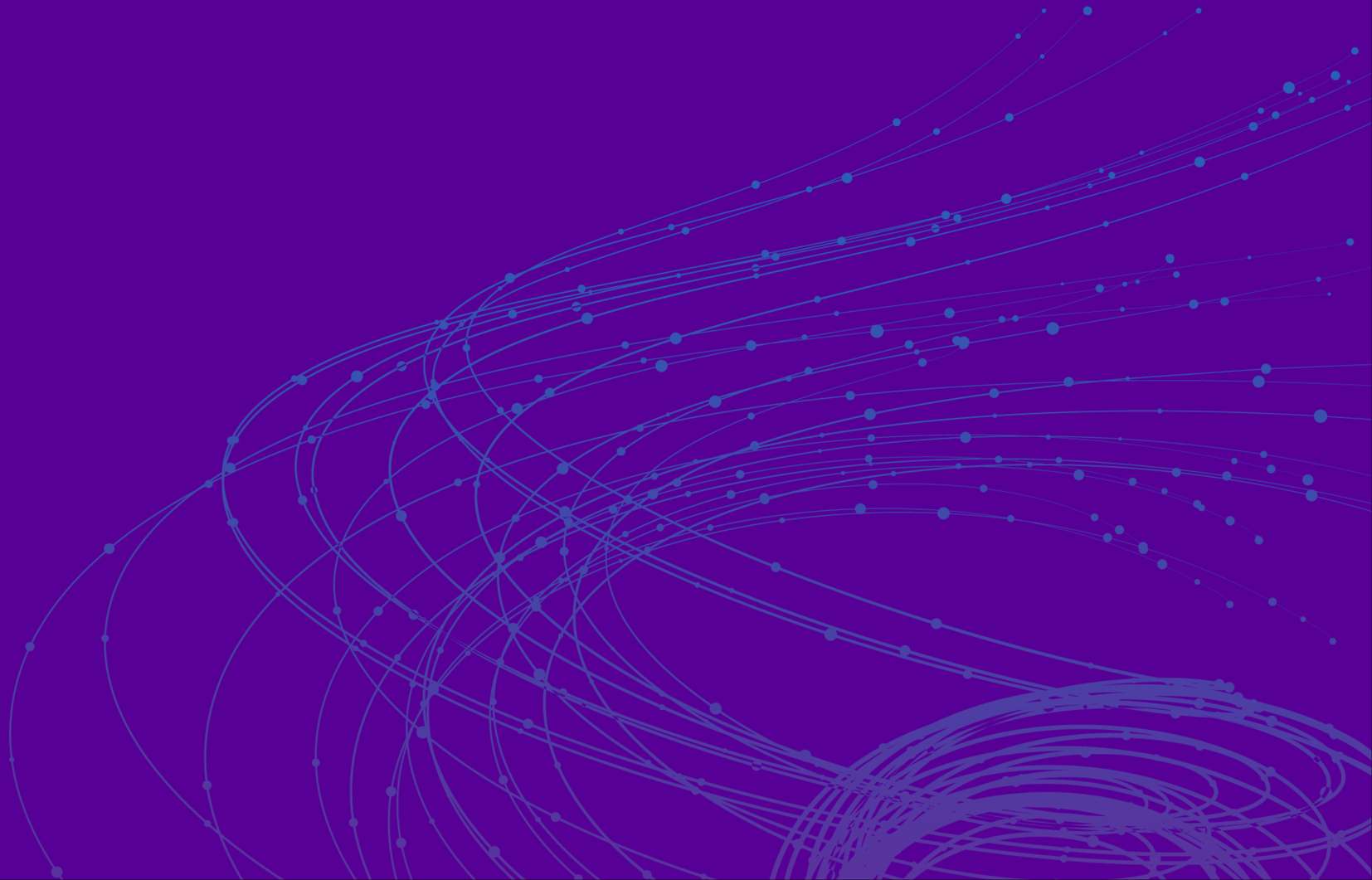
ASIC advantage



MHASH/S - LINEAR SCALE

RSAConference2019

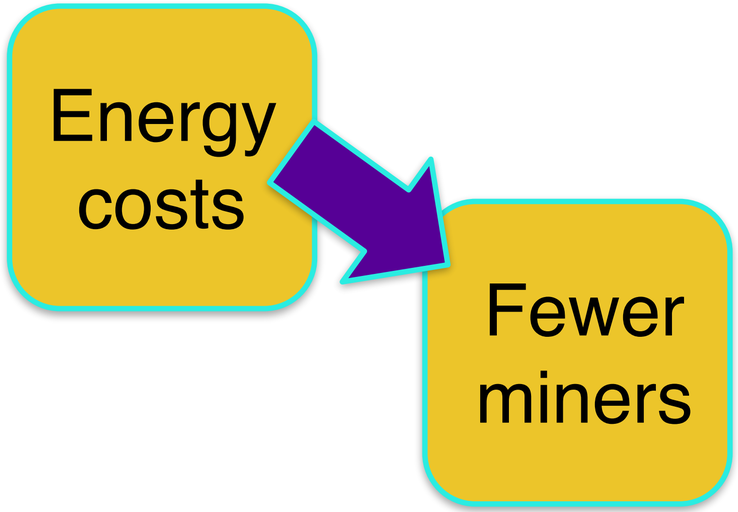
Fragility



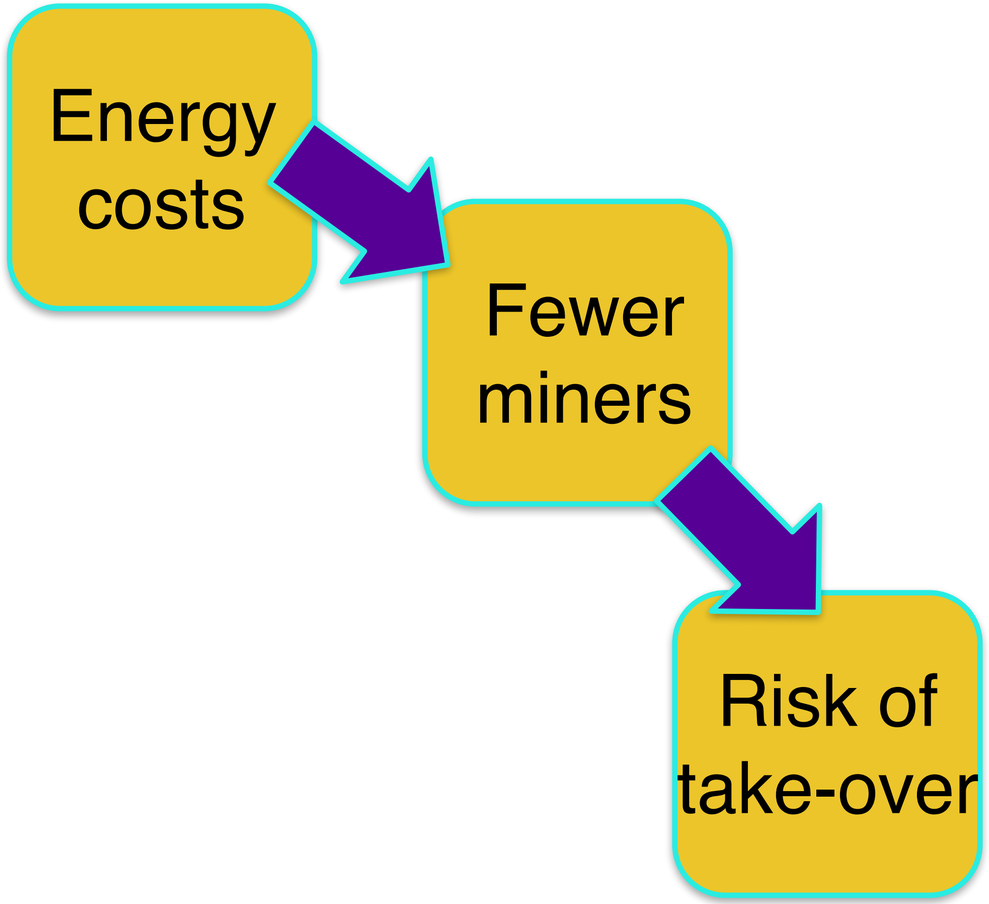
Fragility

Energy costs

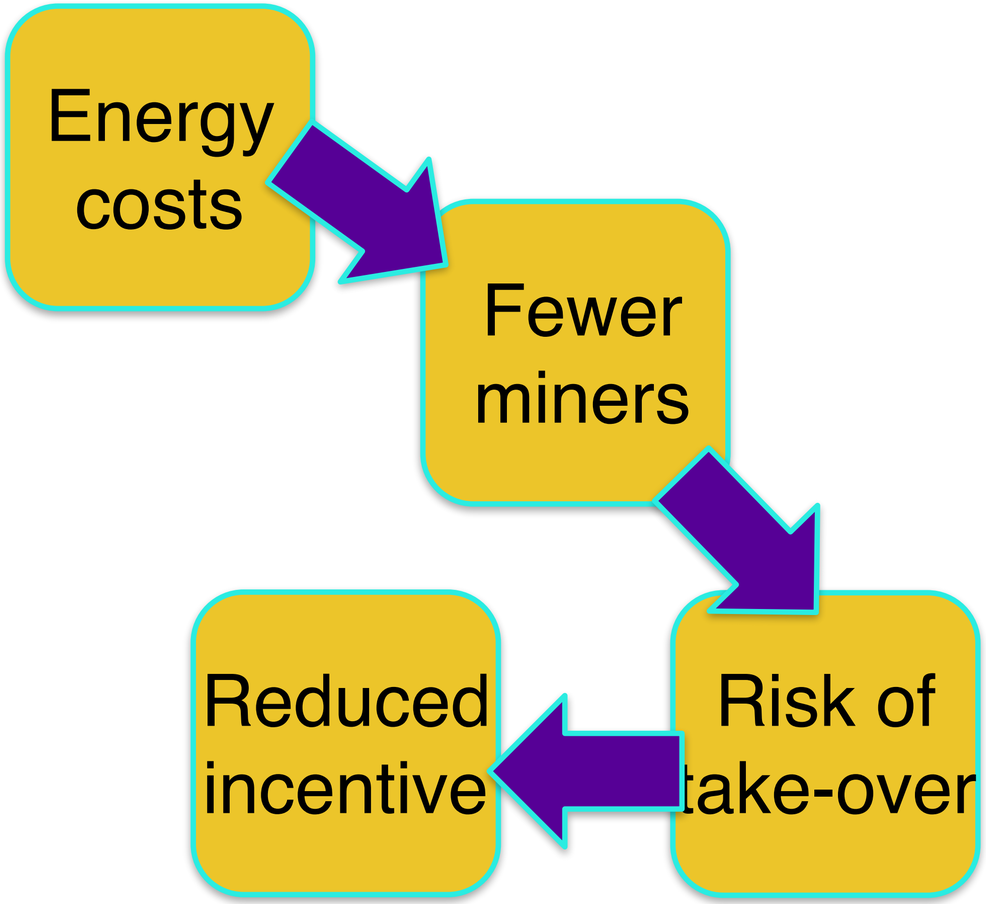
Fragility



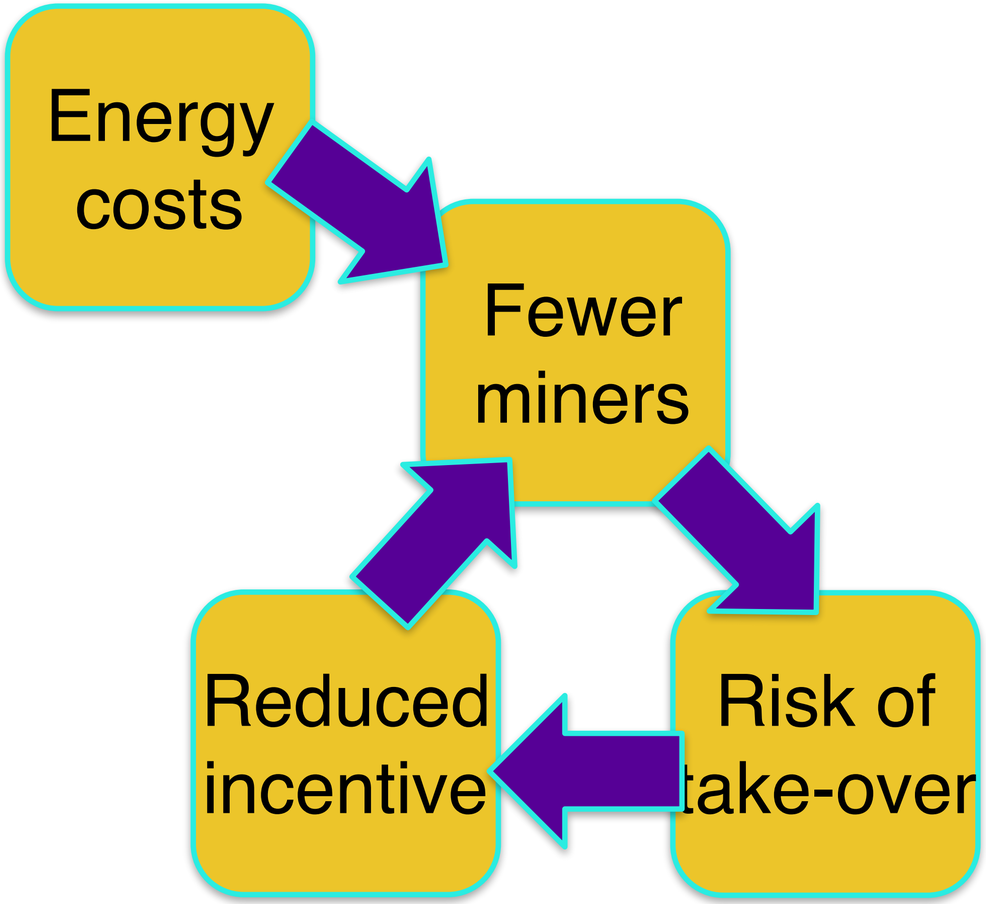
Fragility



Fragility

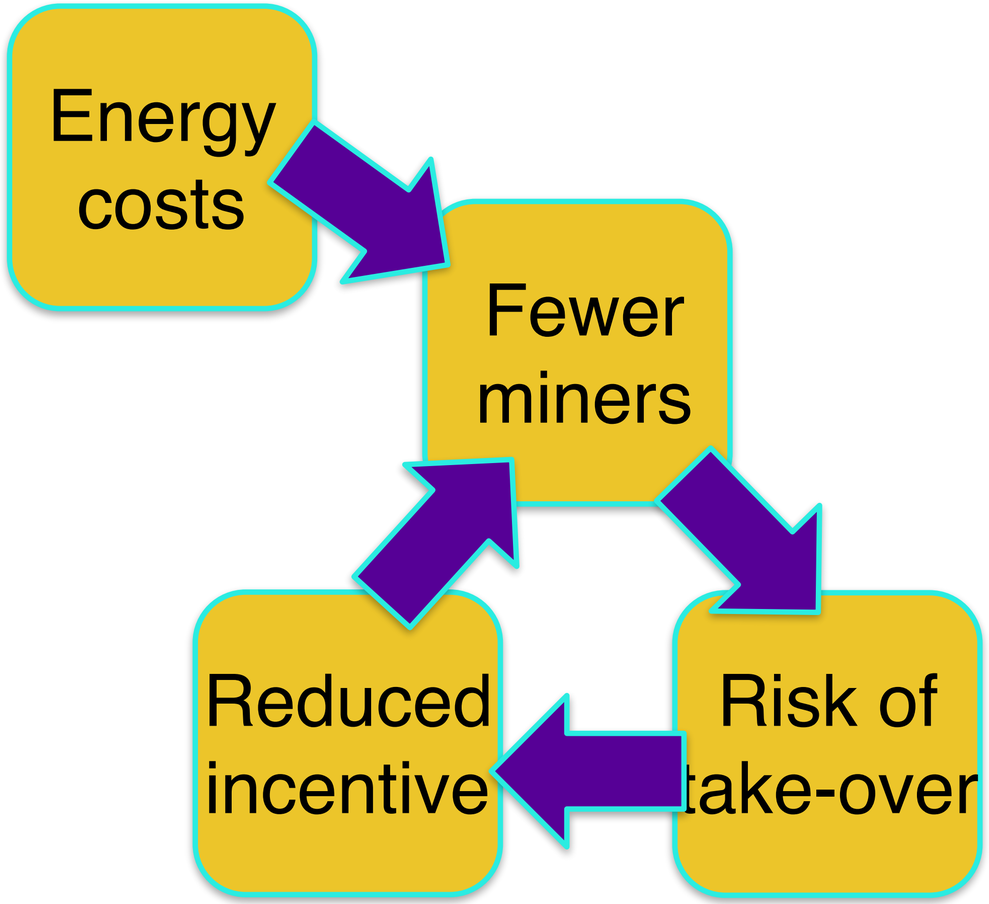

Energy costs
Fewer miners
Risk of take-over
Reduced incentive

Fragility

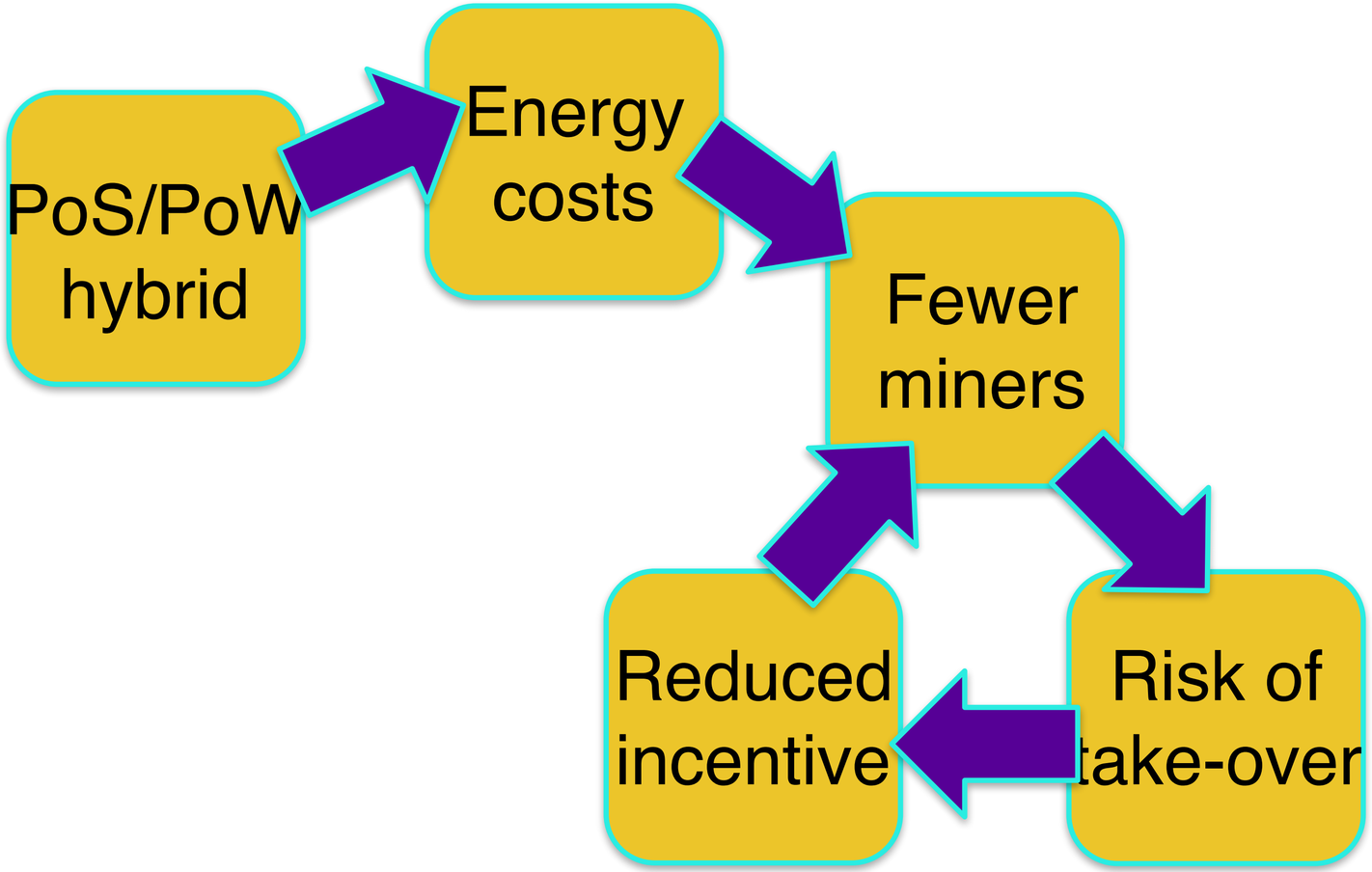

Energy costs
Fewer miners
Risk of take-over
Reduced incentive

Fragility

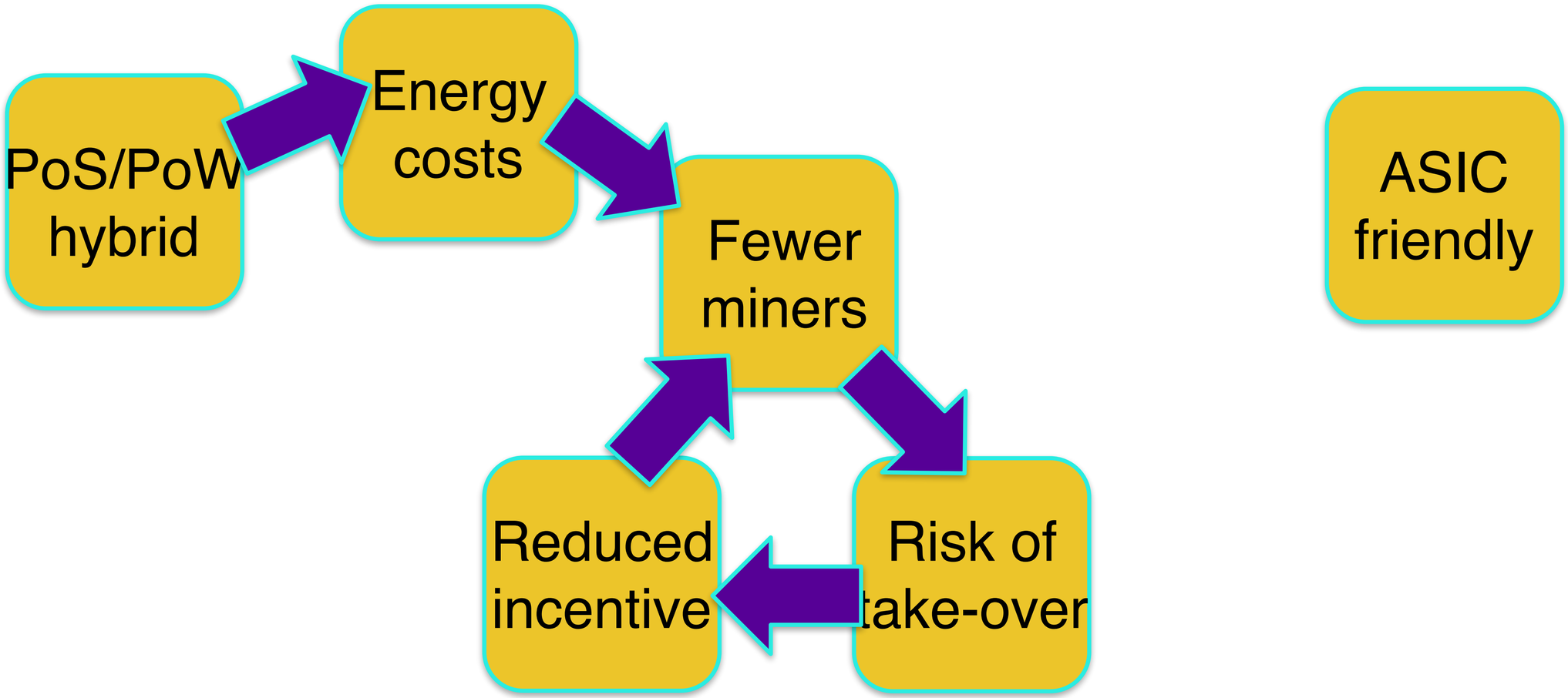
PoS/PoW hybrid



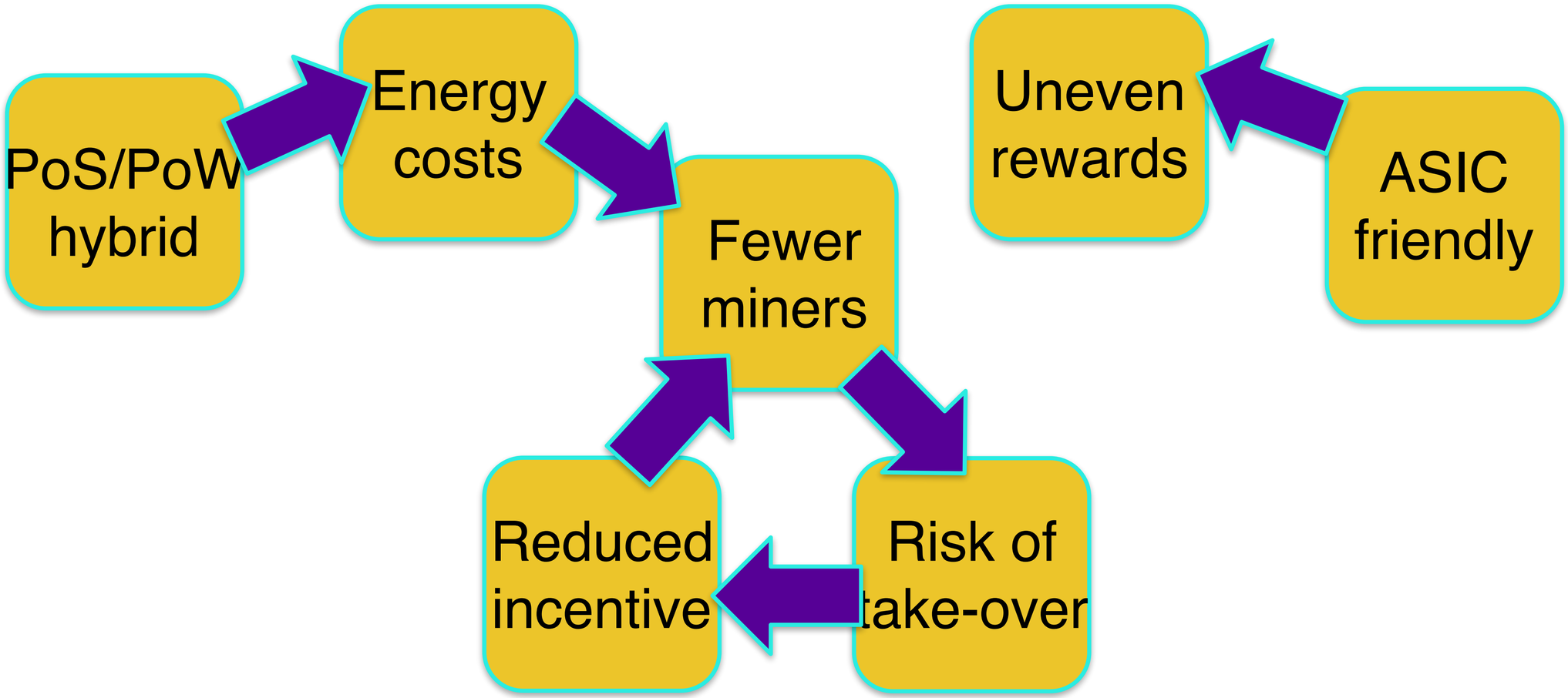
Fragility


PoS/PoW hybrid
Energy costs
Fewer miners
Risk of take-over
Reduced incentive

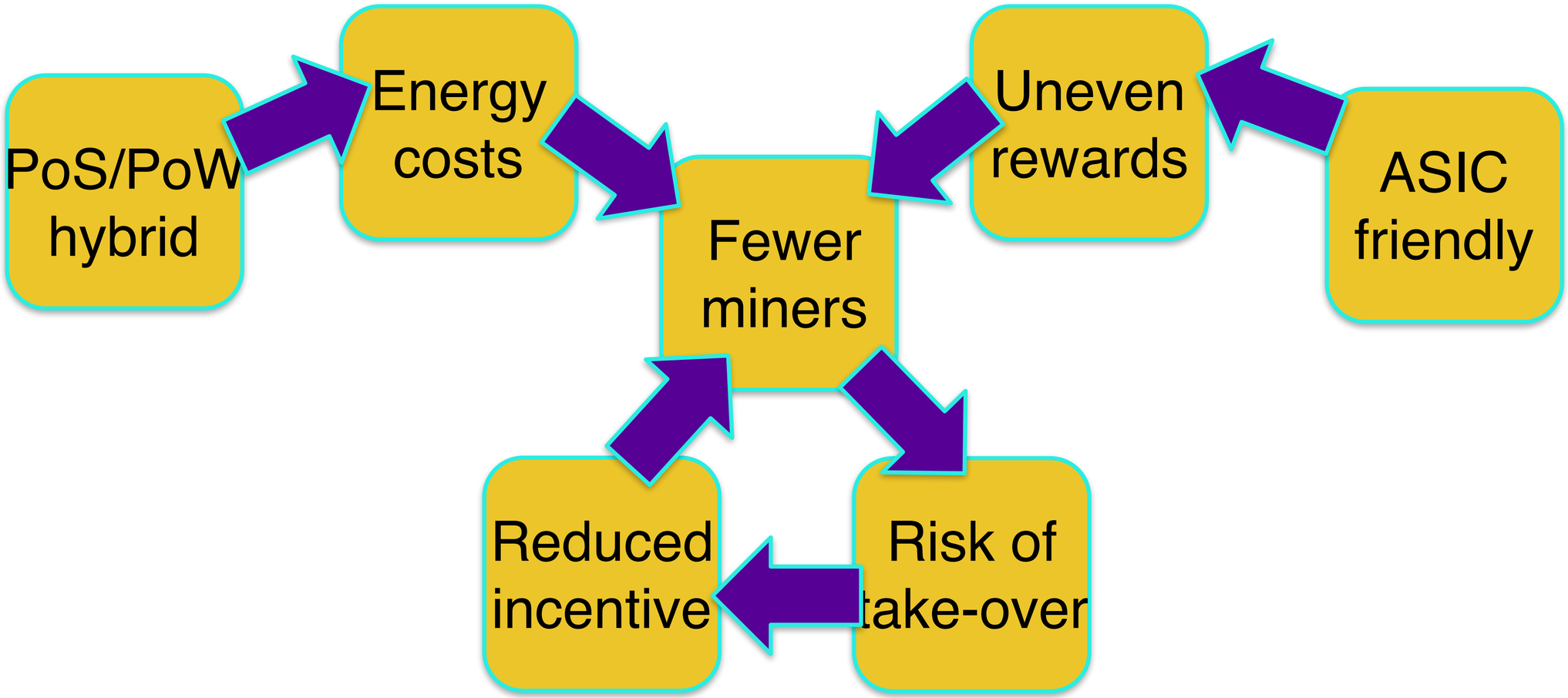
Fragility


PoS/PoW hybrid
Energy costs
Fewer miners
Reduced incentive
Risk of take-over
ASIC friendly

Fragility


PoS/PoW hybrid
Energy costs
Fewer miners
Uneven rewards
ASIC friendly
Reduced incentive
Risk of take-over

Fragility

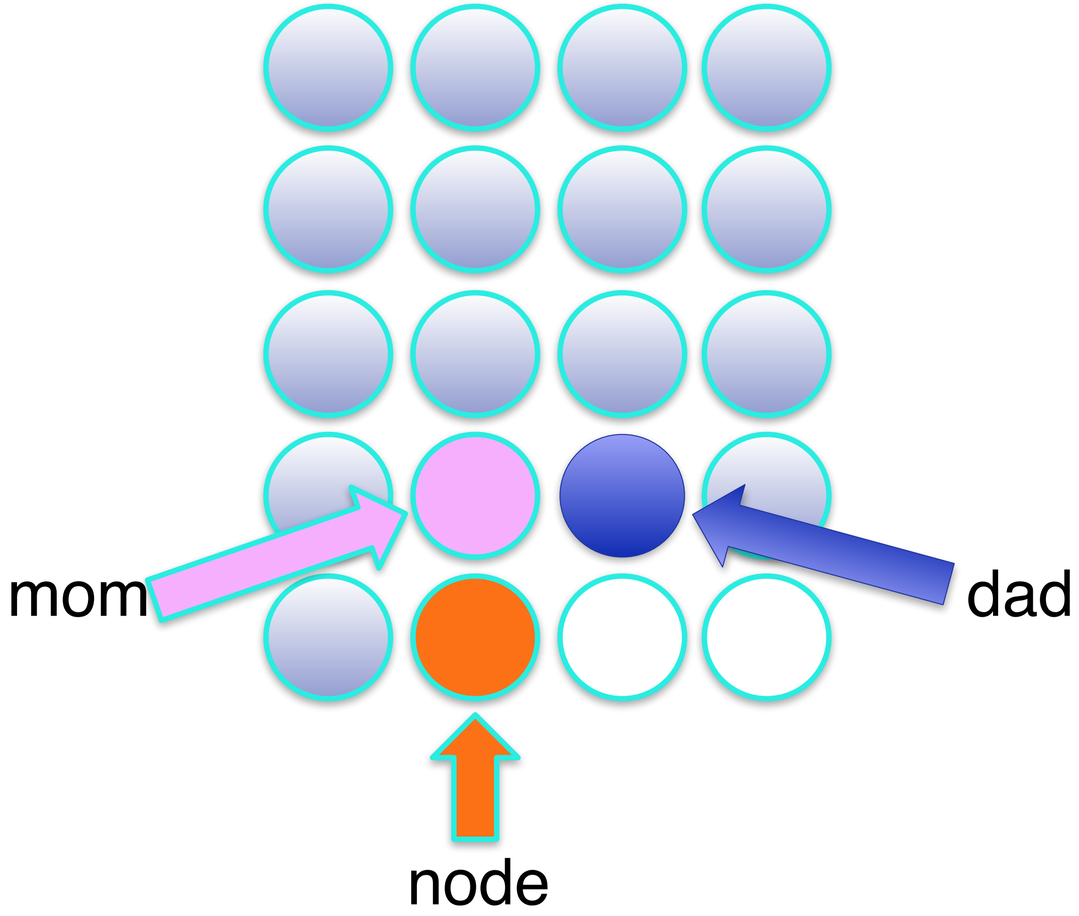

PoS/PoW hybrid
Energy costs
Uneven rewards
ASIC friendly
Fewer miners
Reduced incentive
Risk of take-over

RSAConference2019

Proof of Space (PoS)

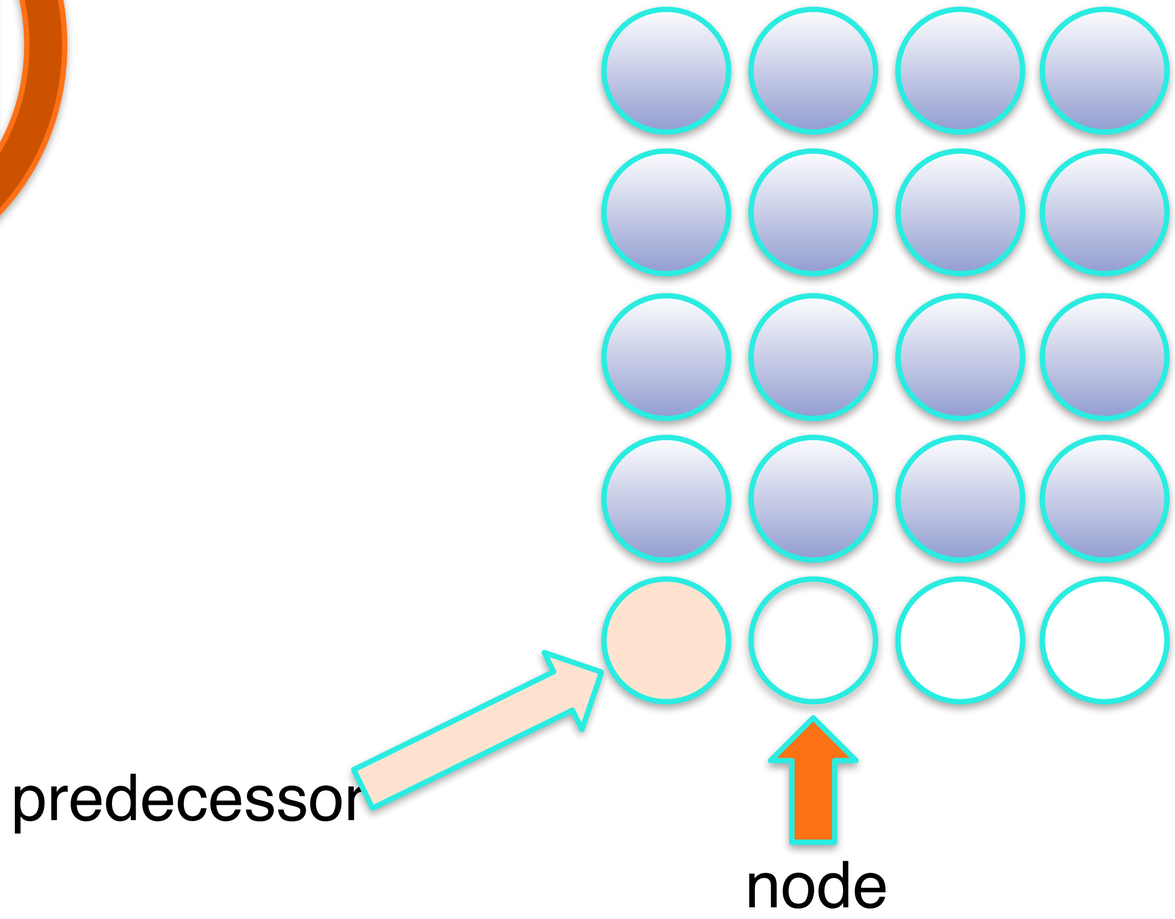
Proof of Space – a look at ASIC resistance

Traditional structure



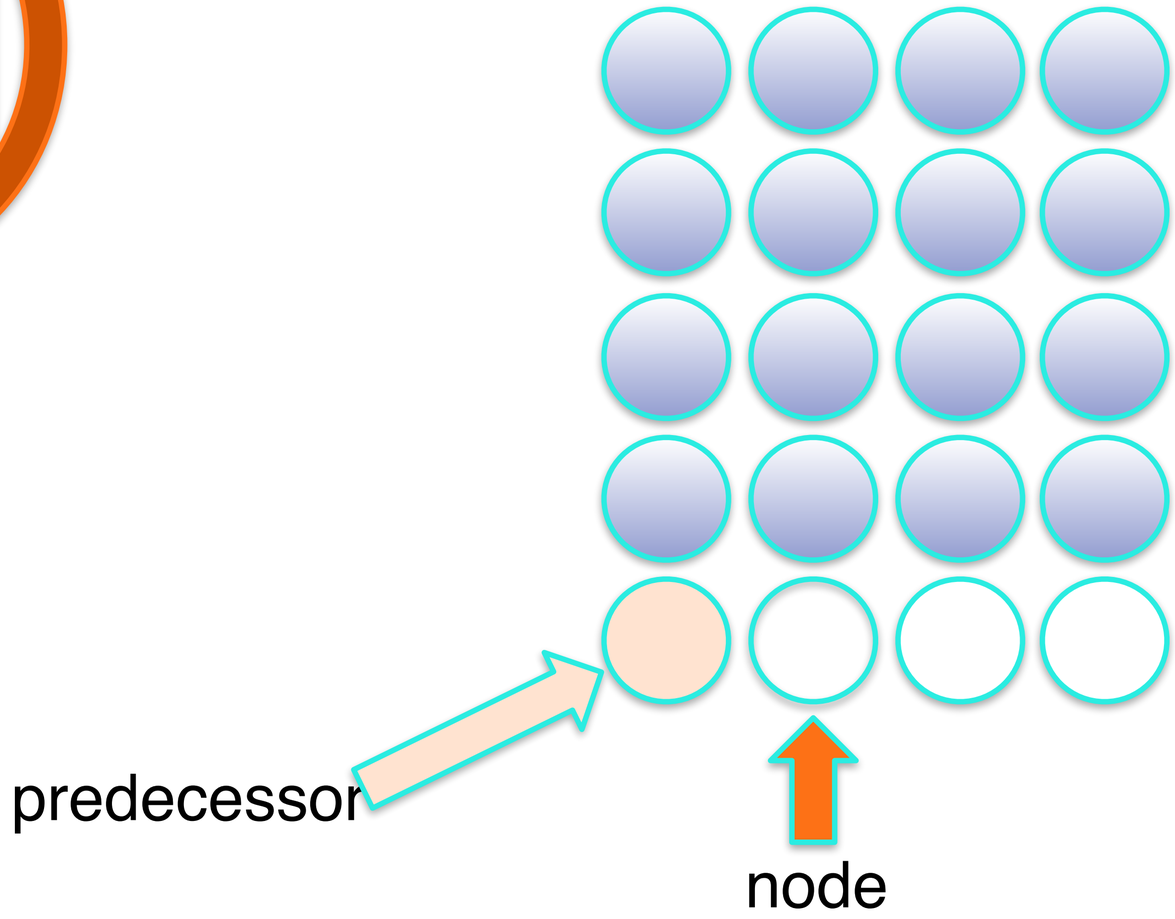
Proof of Space – a look at ASIC resistance

Discouraging ASICs



Proof of Space – a look at ASIC resistance

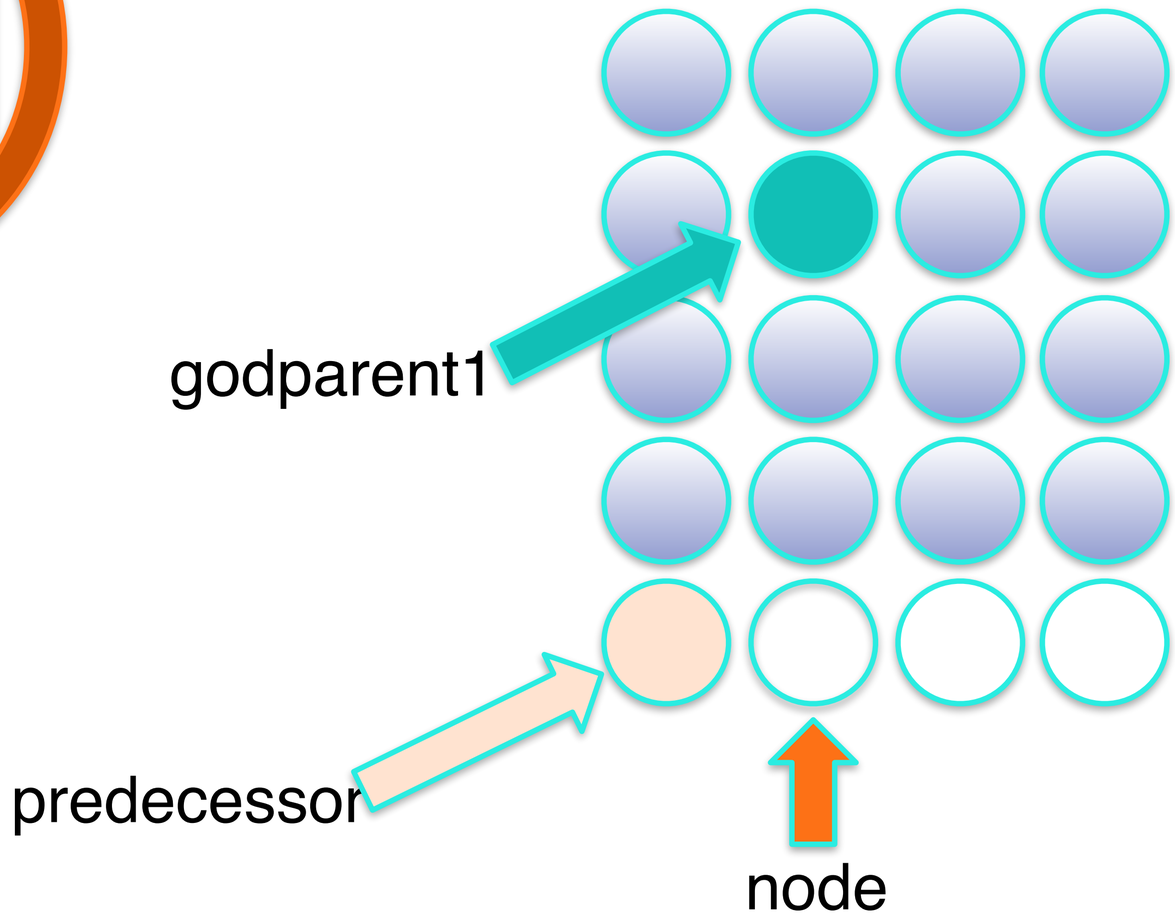
Discouraging ASICs



1. Use hash(G.predecessor) to select the godparent1

Proof of Space – a look at ASIC resistance

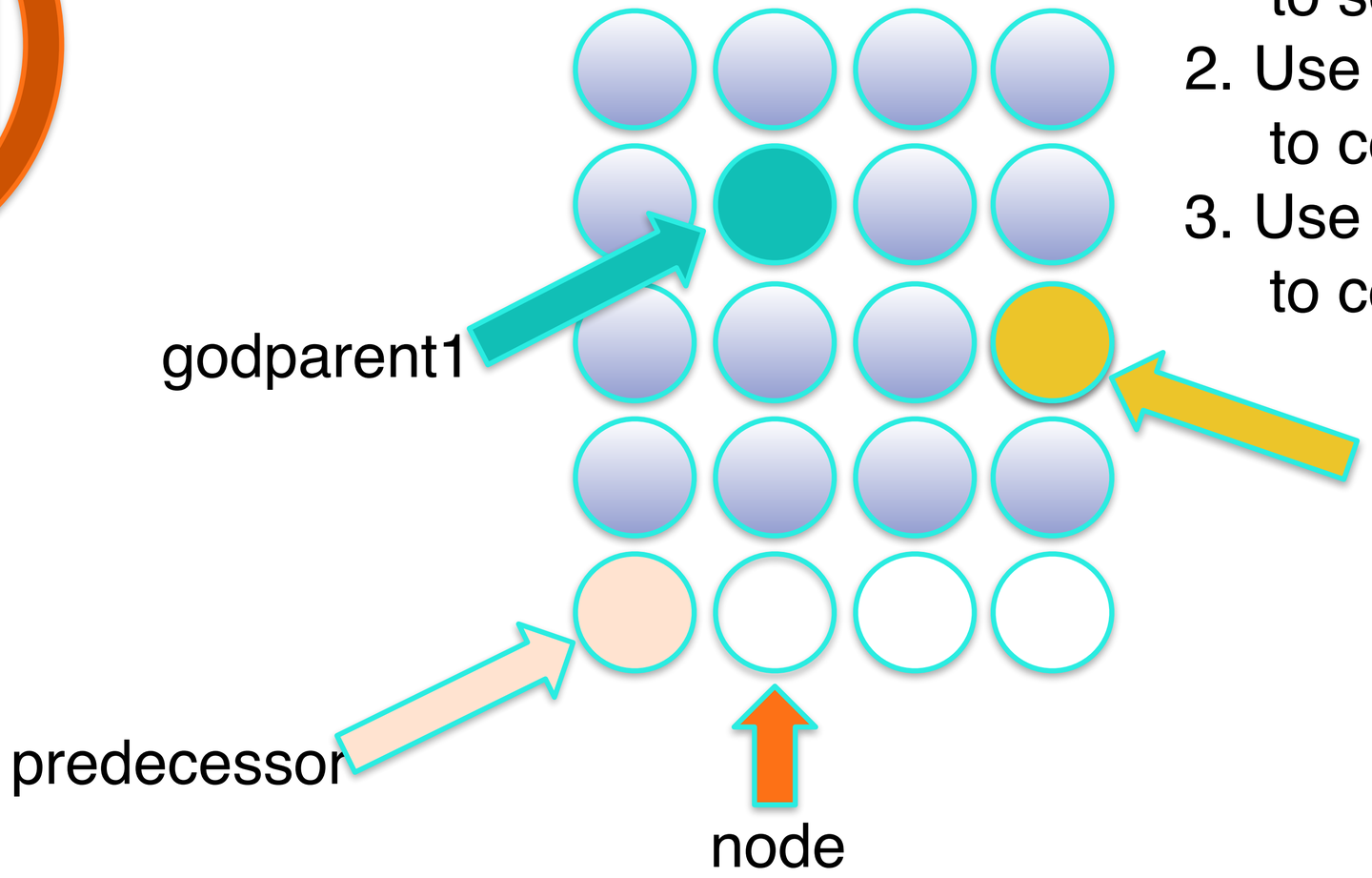
Discouraging ASICs



1. Use hash(G.predecessor) to select the godparent1
2. Use hash(G.godparent1) to compute godparent2

Proof of Space – a look at ASIC resistance

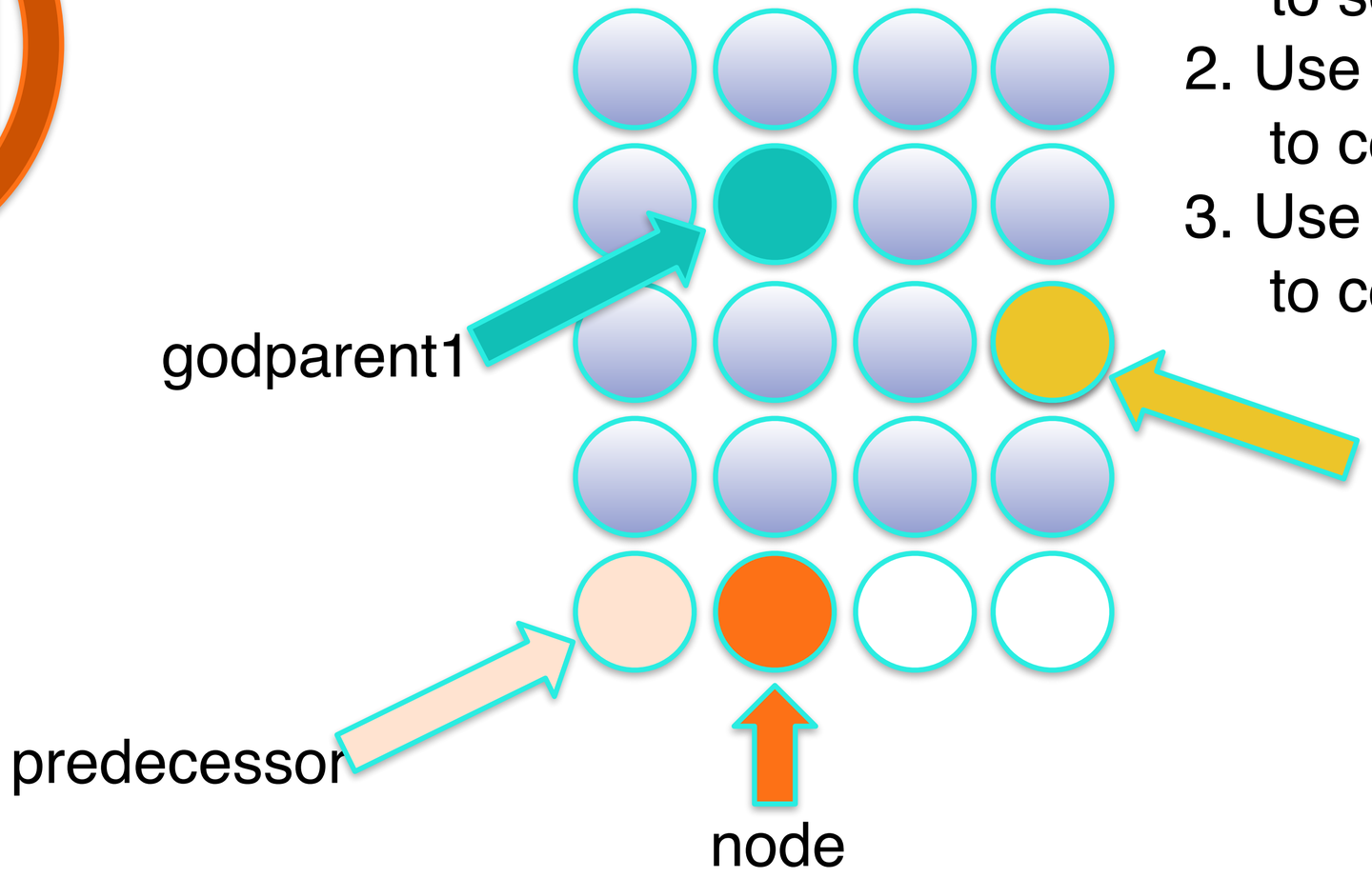
Discouraging ASICs



1. Use hash(G.predecessor) to select the godparent1
2. Use hash(G.godparent1) to compute godparent2
3. Use hash(G.godparent2) to compute G.node

Proof of Space – a look at ASIC resistance

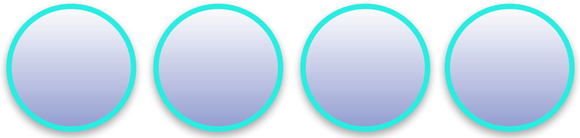
Discouraging ASICs



1. Use hash(G.predecessor) to select the godparent1
2. Use hash(G.godparent1) to compute godparent2
3. Use hash(G.godparent2) to compute G.node

Proof of Space – a look at ASIC resistance

Discouraging ASICs



1. Use hash(G.predecessor) to select the godparent1
2. Use hash(G.godparent1) to compute godparent2
   hash(G.godparent2)
   mpute G.node

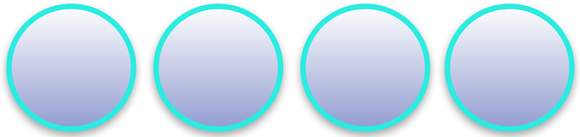
godparent2

Security Intuition

If the node to be used is not in cache, it has to be *computed* or *fetched* from DRAM.

Proof of Space – a look at ASIC resistance

Discouraging ASICs



1. Use hash(G.predecessor) to select the godparent1
2. Use hash(G.godparent1) to compute godparent2
   hash(G.godparent2)
   mpute G.node

godparent2

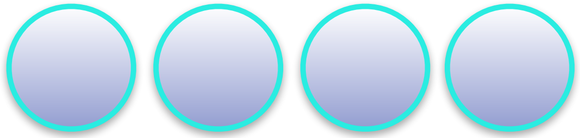
Security Intuition

If the node to be used is not in cache, it has to be *computed* or *fetched* from DRAM.

Fetching from DRAM ”costs” about the same for the ASIC and a general purpose computer.

Proof of Space – a look at ASIC resistance

Discouraging ASICs



1. Use hash(G.predecessor) to select the godparent1
2. Use hash(G.godparent1) to compute godparent2
   hash(G.godparent2)
   mpute G.node

   godparent2

Security Intuition

If the node to be used is not in cache, it has to be *computed* or *fetched* from DRAM.

Fetching from DRAM ”costs” about the same for the ASIC and a general purpose computer.

Computation costs increase if the dependent nodes (predecessor and godparents) are not in cache – avalanche effect. If the avalanche > 2^{20} slowdown then no ASIC benefit.

Proof of Space – a look at ASIC resistance

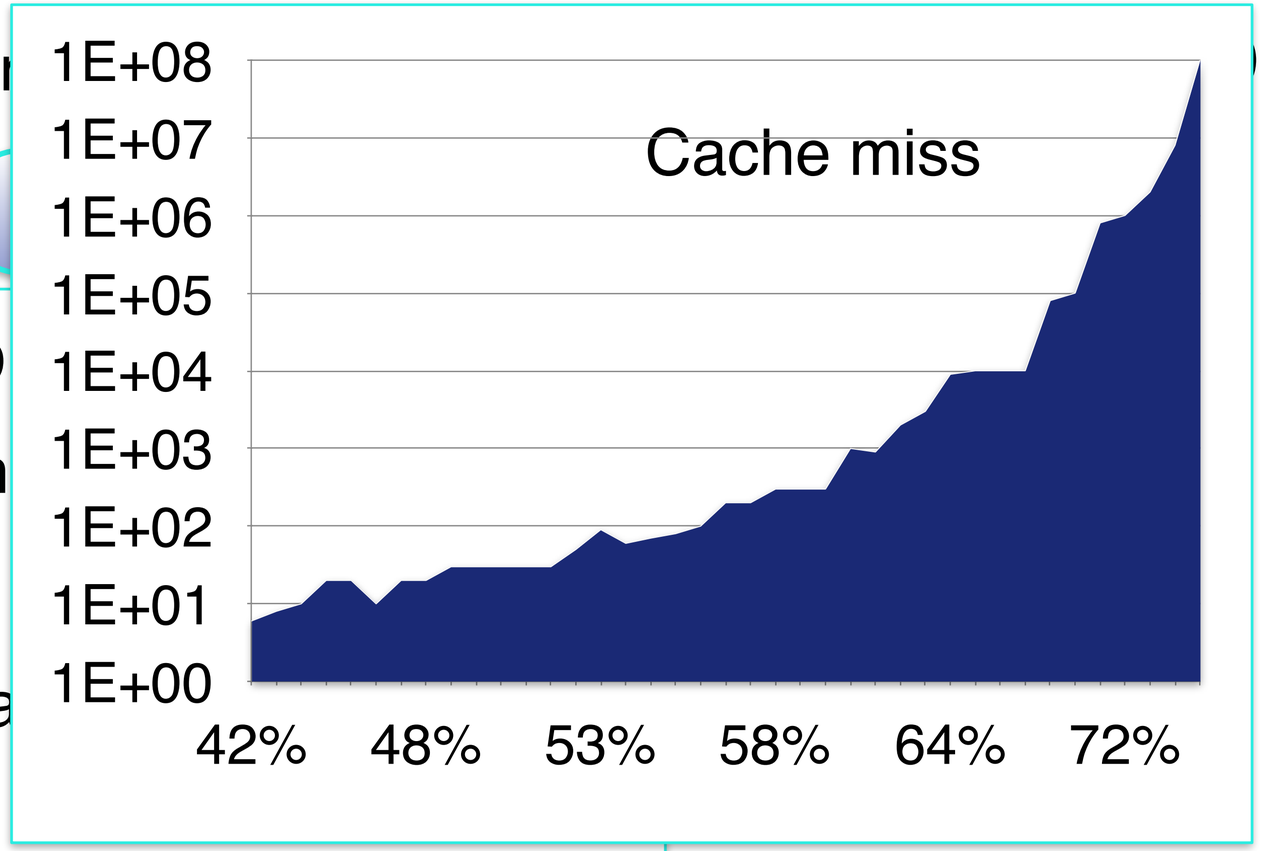
Discour

Security Intuitio

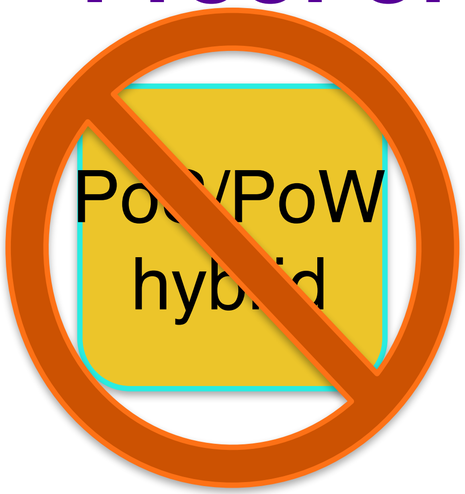
If the node to be used is not in cache, it h
fetched from DRAM.

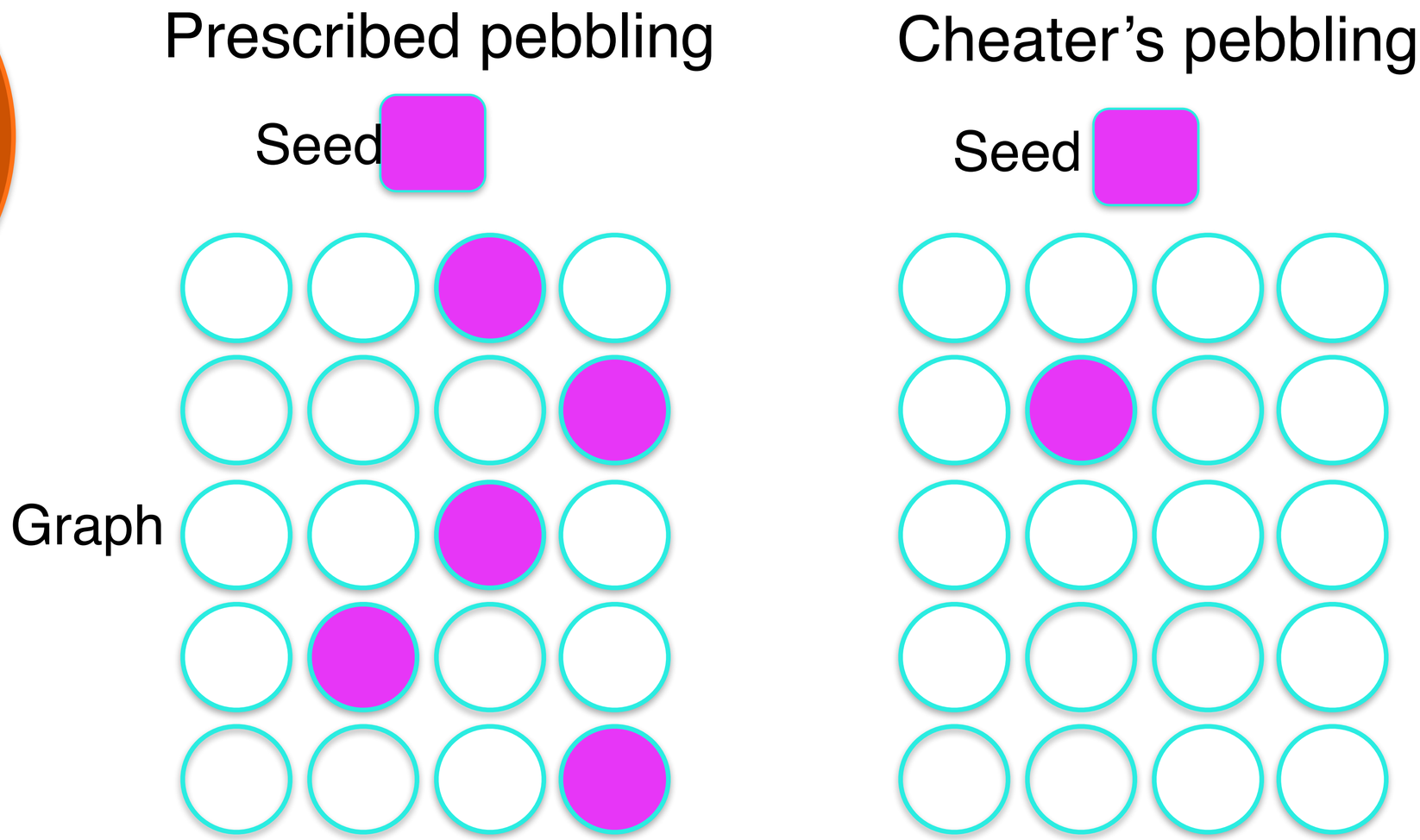
Fetching from DRAM ”costs” about the sa
a general purpose computer.

Computation costs increase if the dependent nodes (predecessor and godparents) are not in cache – avalanche effect. If the avalanche > 2^{20} slowdown then no ASIC benefit.

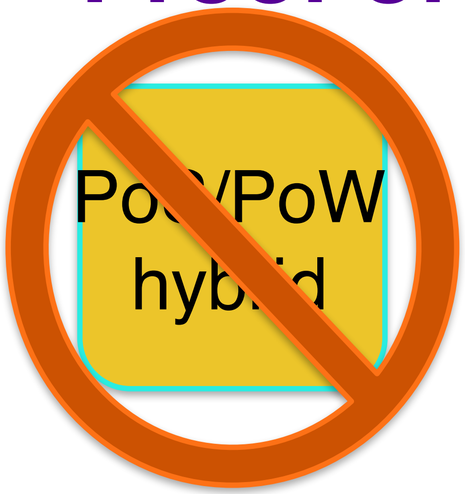


Proof of Space – avoiding PoW hybridization





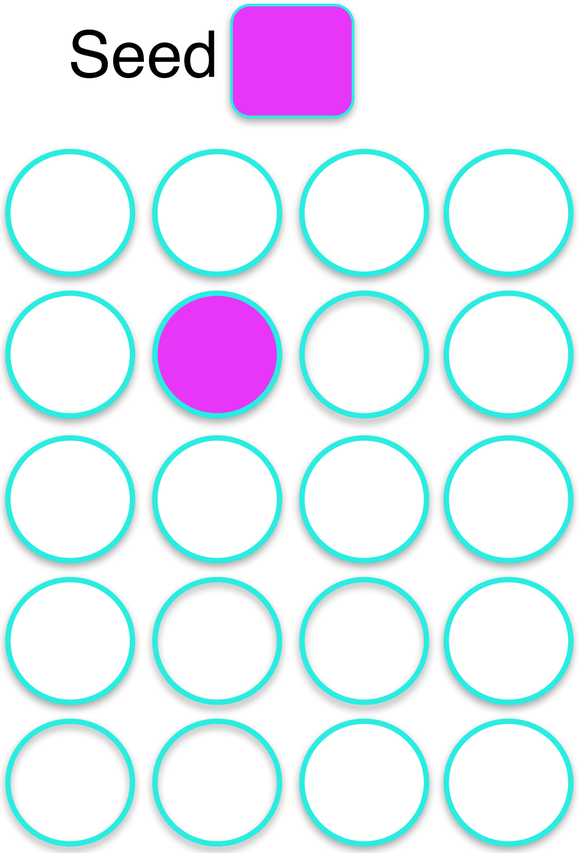
Proof of Space – avoiding PoW hybridization



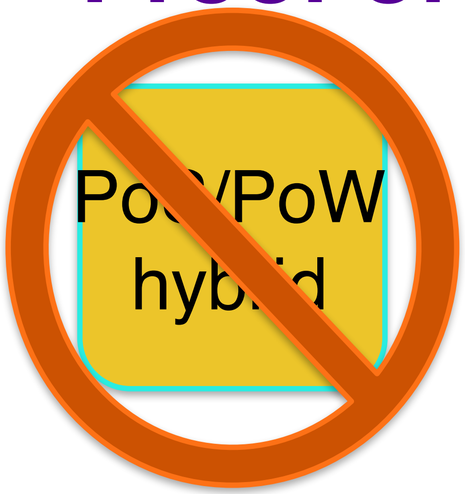
1. Store less than prescribed.
2. Recompute when needed.

(Turns *any* PoS into a PoS-PoW)

Cheater's pebbling



Proof of Space – avoiding PoW hybridization

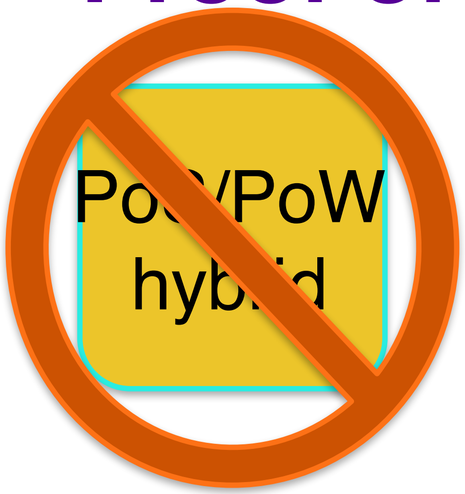


make

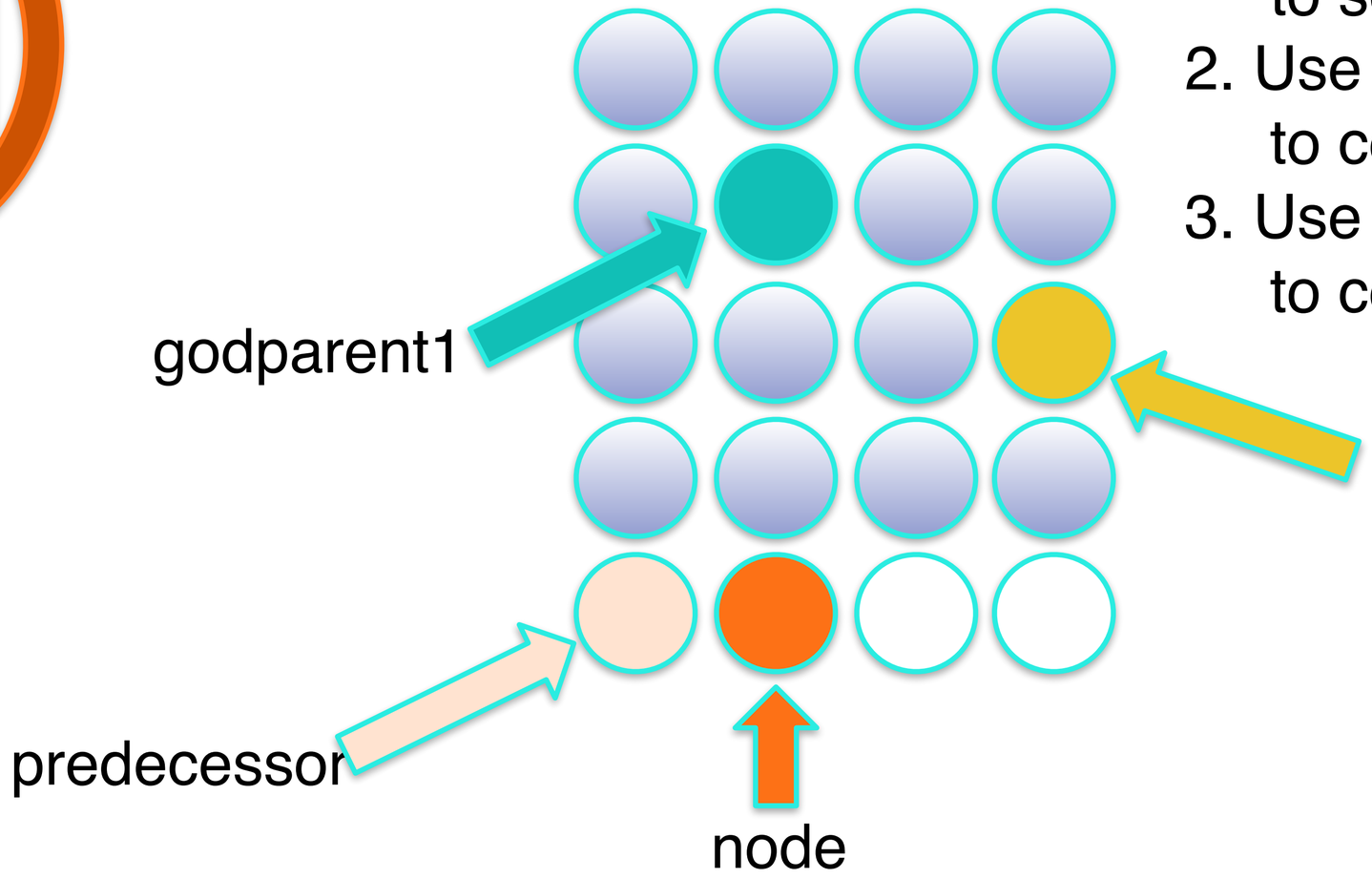
recomputing

painful

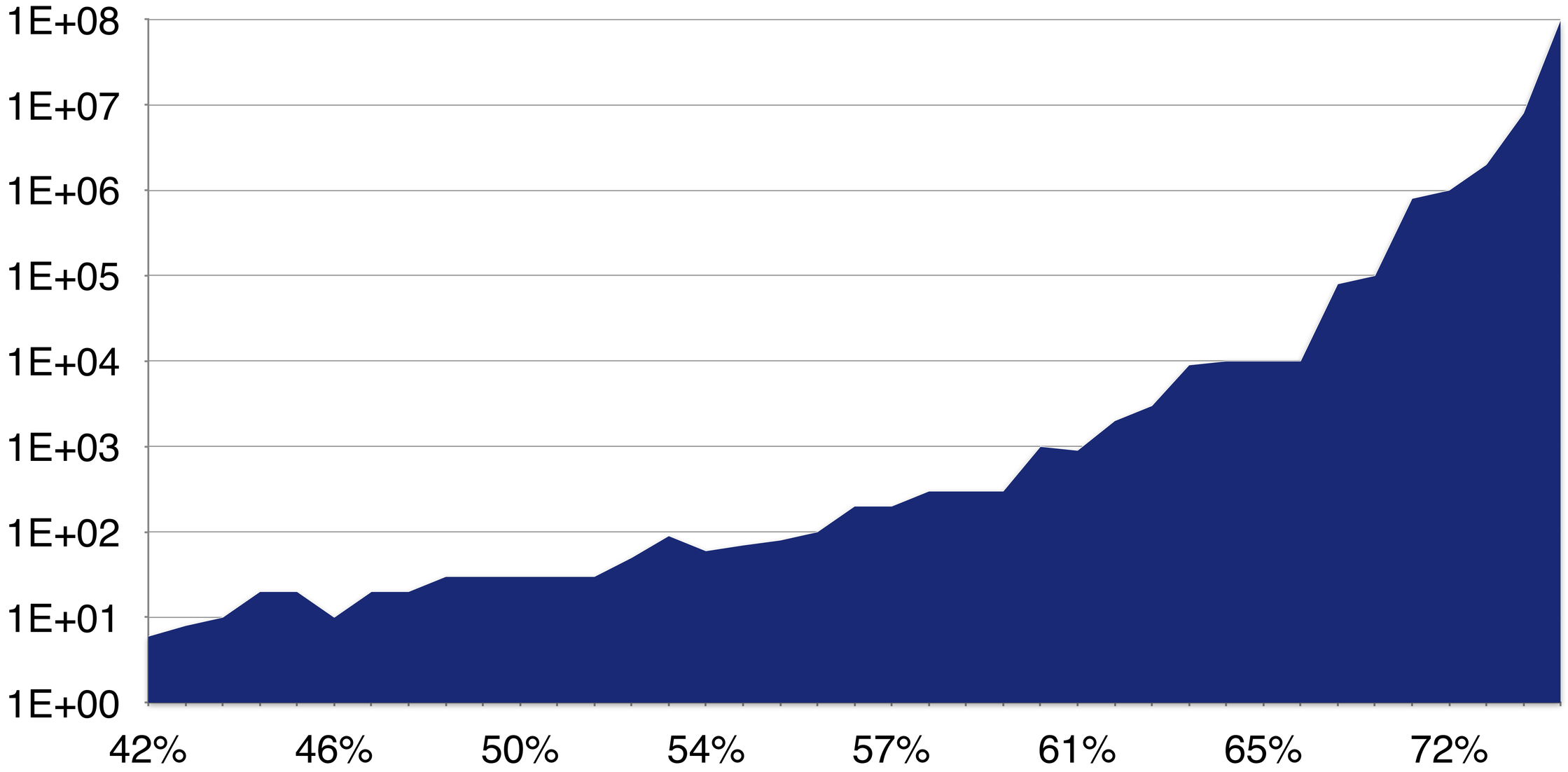
Proof of Space – avoiding PoW hybridization



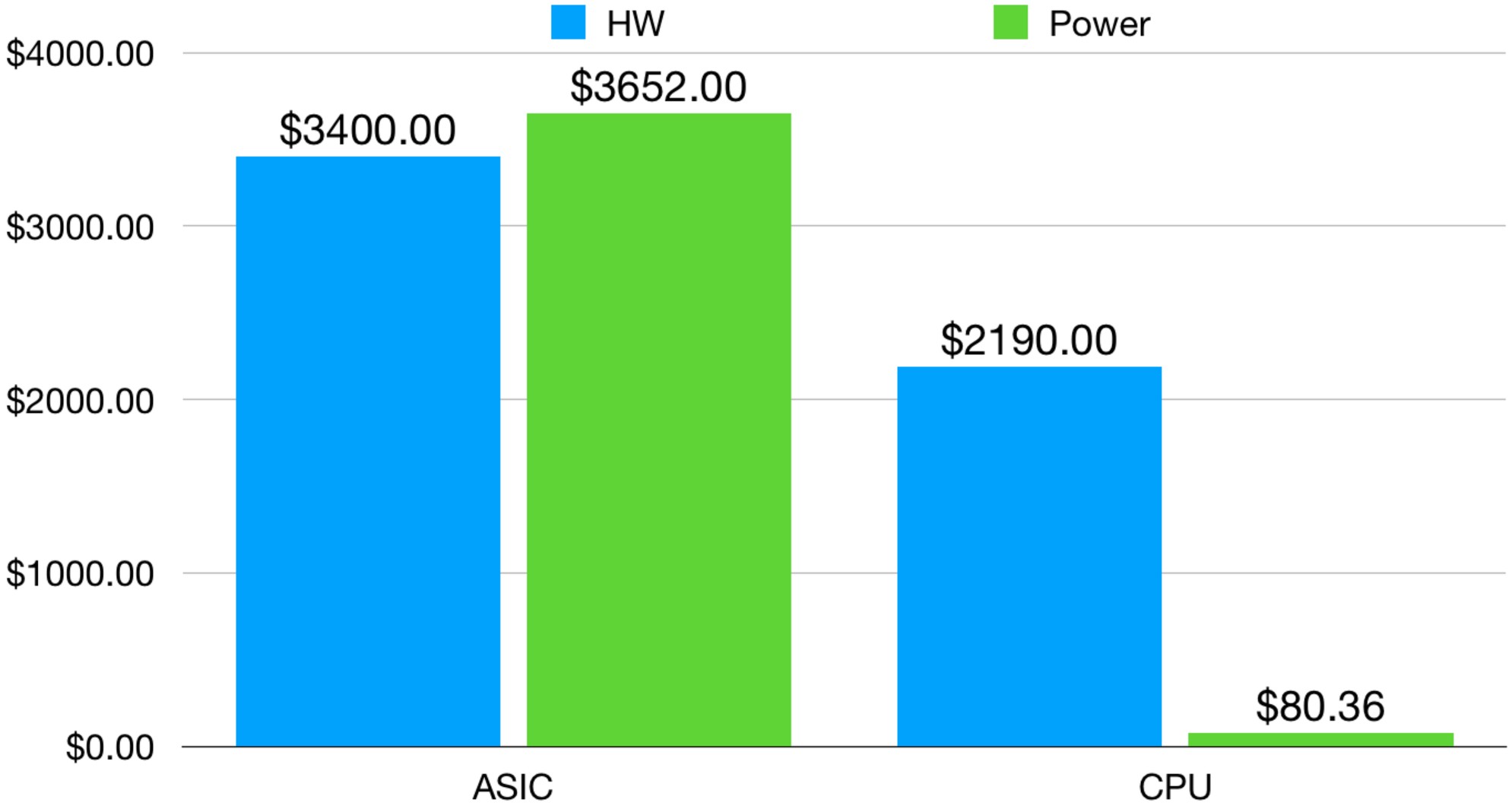
1. Use hash(G.predecessor) to select the godparent1
2. Use hash(G.godparent1) to compute godparent2
3. Use hash(G.godparent2) to compute G.node



Cost of compression with 2^{24} nodes



CPU versus ASIC cost comparison



RSAConference2019

Apply

How can we apply these insights?

- Understand: economic forces have security impact

  In this case, lower crypto values cause instability

How can we apply these insights?

- Understand: economic forces have security impact
- Understand: cheating is rational

In this case, it excludes non-ASICs and causes hybridization

How can we apply these insights?

- Understand: economic forces have security impact
- Understand: cheating is rational
- Design accordingly

  In this case, design to avoid ASICs and hybridization

How can we apply these insights?

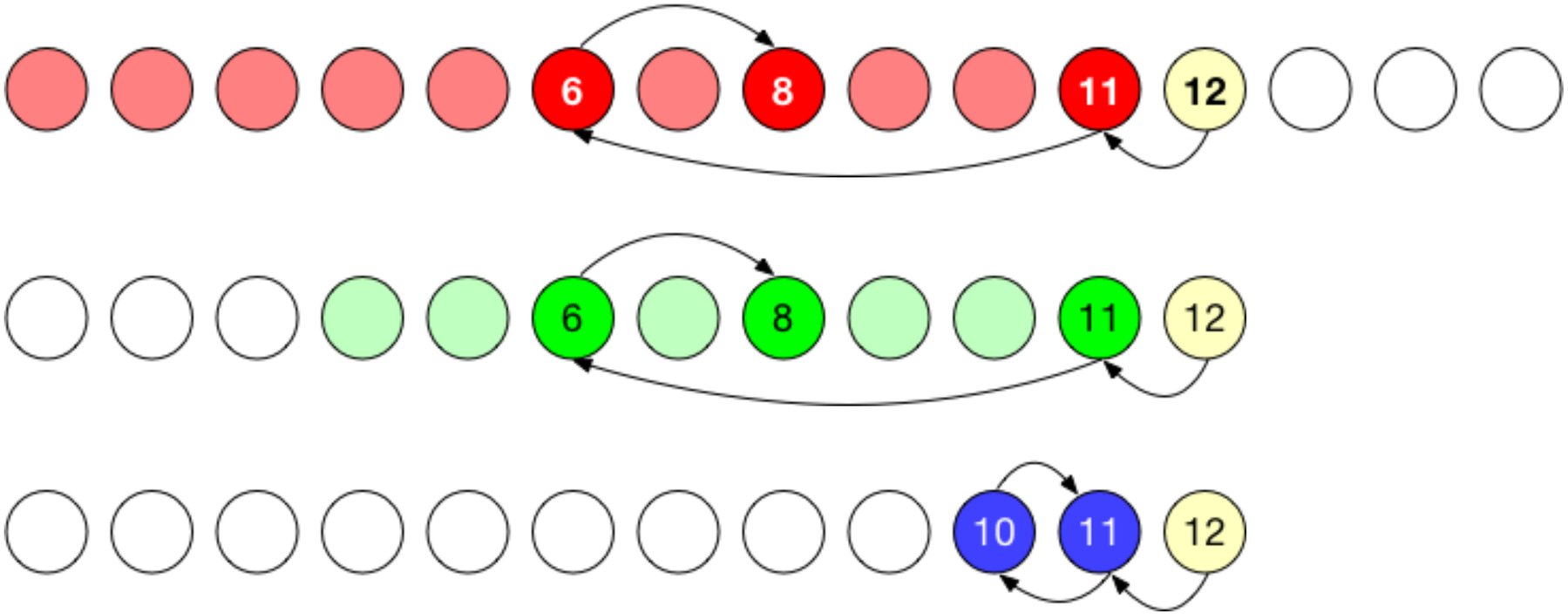
- Understand: economic forces have security impact
- Understand: cheating is rational
- Design accordingly
- Avoid creating crypto value systems within your enterprise that rely on vulnerable cryptocurrency frameworks

RSAConference2019

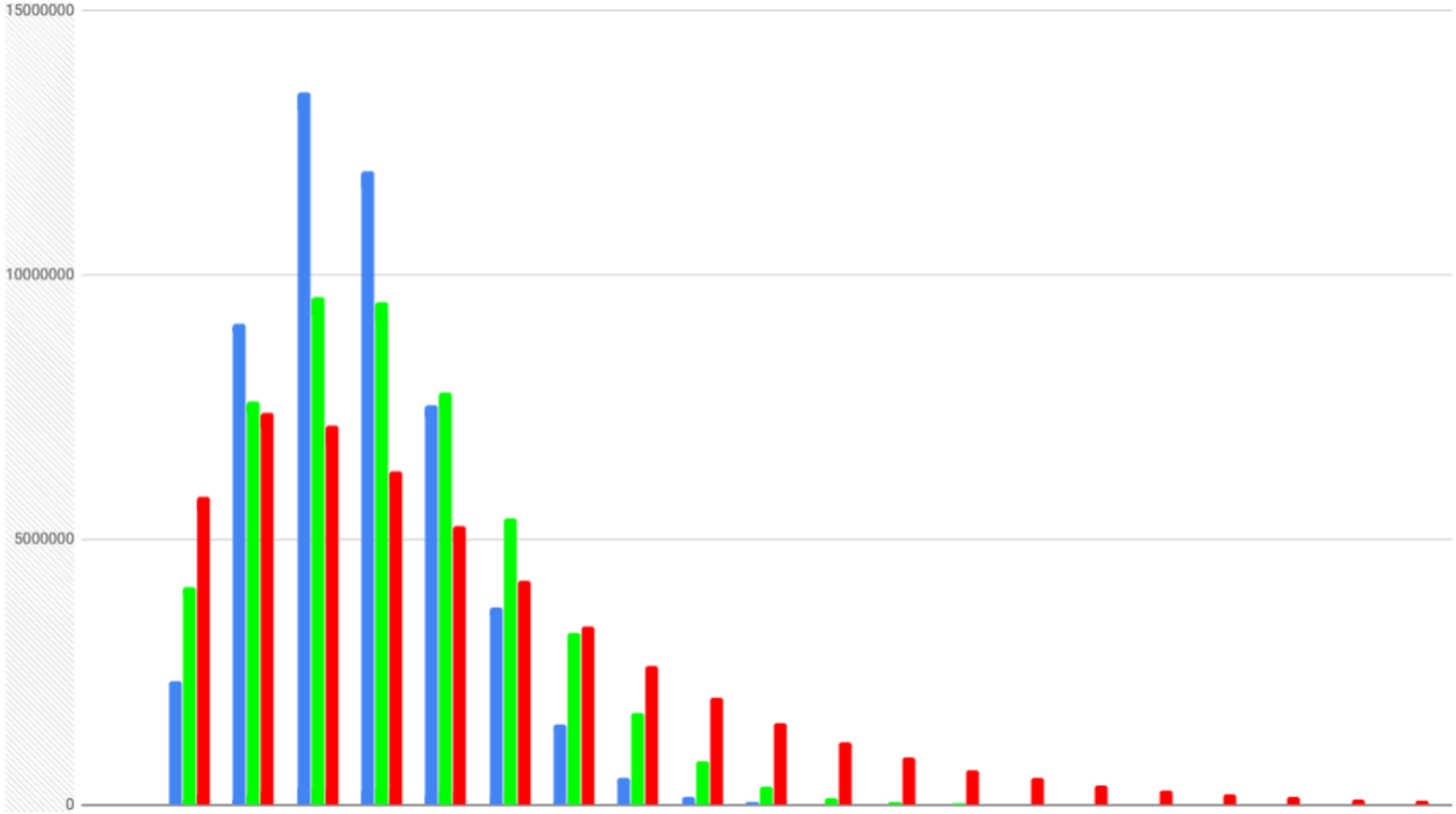
www.egni.io

guy@egni.io

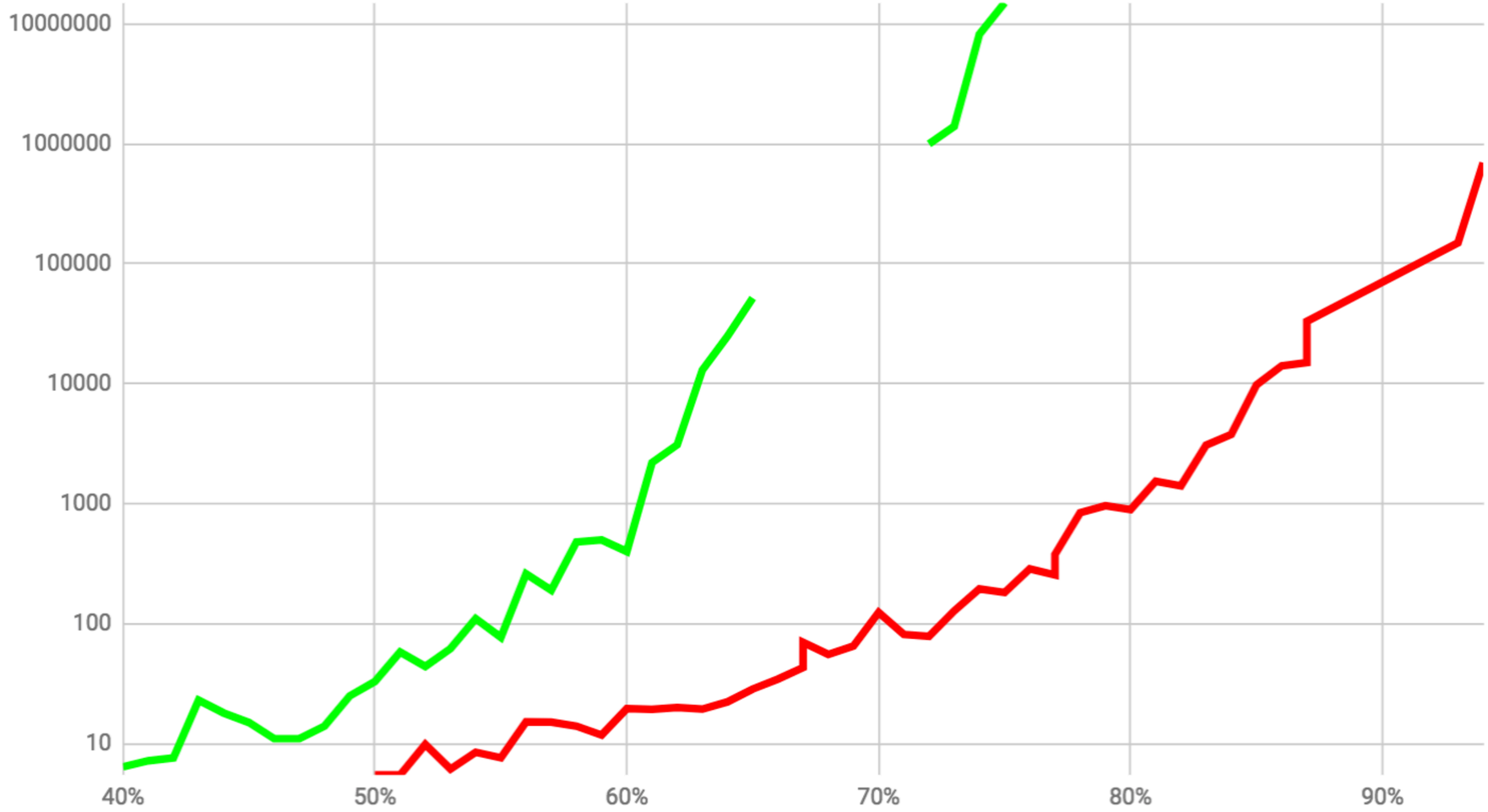
Different godparent selection strategies



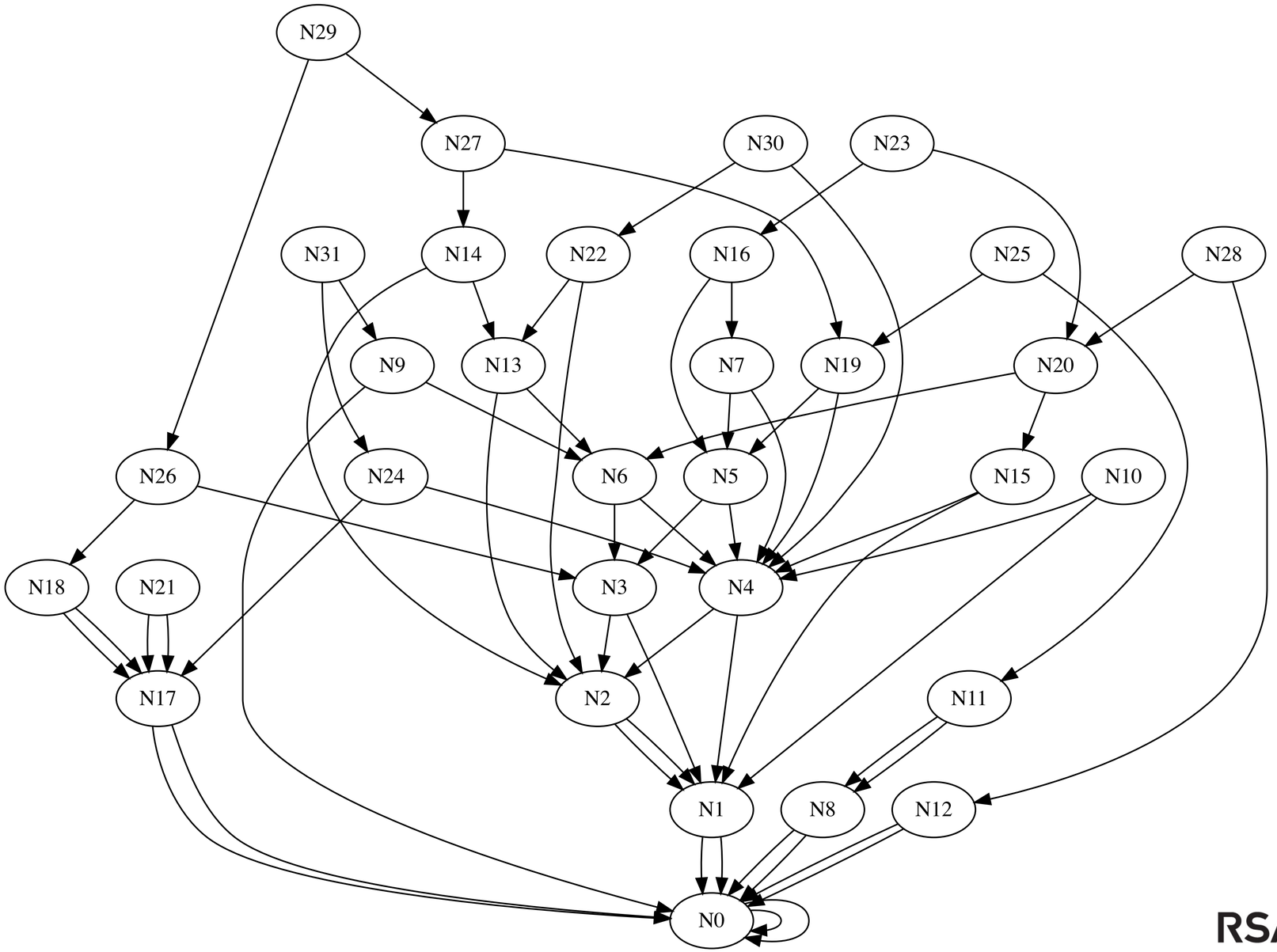
Different godparent selection strategies - godparenthood



Different godparent selection strategies - cost



Graph topology; 32 node example



What about Filecoin, Sia, or other PoStor / PoR?

- PoR: Proof of Replication
- PoStore: Proof of Storage
- These coins have their place. However they have certain drawbacks that make them less than ideal for use when pure proof of space is desired; they are subject to sybil attacks, out-sourcing attacks, and generation attacks. They compete with the existing providers in cost, speed, security and reliability. They solve a problem that has already been solved, and introduce wasteful complexity. Market forces of supply and demand threaten to drive instability. What happens when market forces motivate miners to switch to other currencies and customers lose data? Who is responsible?