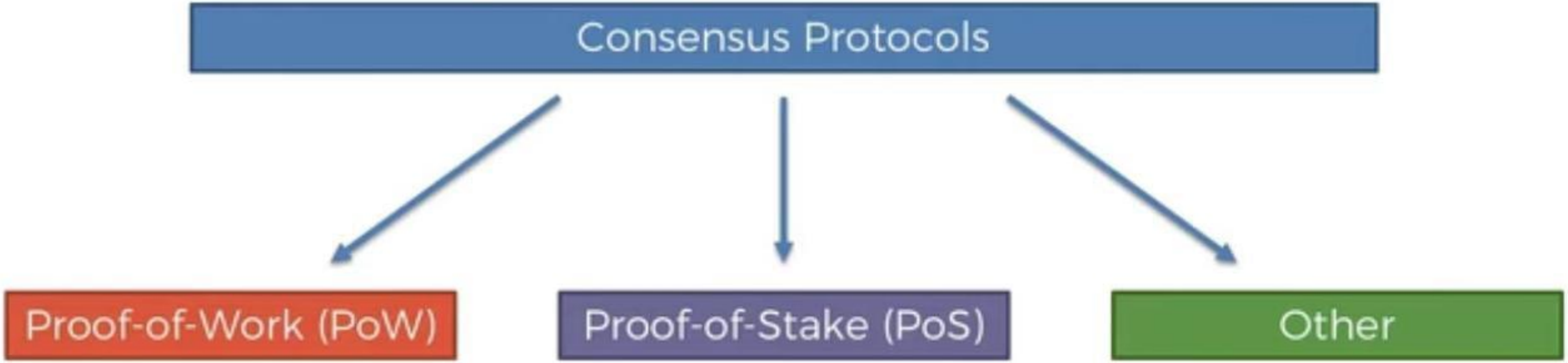
Blockchain and Cryptocurrency

By: Syeda Tayyaba Bukhari



Consensus Protocols

Proof-of-Work (PoW)

Proof-of-Stake (PoS)

Other

Bitcoin Consensus Algorithm

Consensus algorithm (simplified)

1. New transactions are broadcast to all nodes
2. Each node collects new transactions into a block
3. In each round a random node gets to broadcast its block
4. Other nodes accept the block only if all transactions in it are valid (unspent, valid signatures)
5. Nodes express their acceptance of the block by including its hash in the next block they create

Incentive for miners

Incentive 1: block reward

Creator of block gets to

- include <u>special coin-creation transaction</u> in the block
- choose recipient address of this transaction

Value is fixed: currently 12.5 BTC, halves every 4 years

Block creator gets to “collect” the reward only if the block ends up on long-term consensus branch!

Incentive 2: transaction fees

Creator of transaction can choose to make output value less than input value

Remainder is a transaction fee and goes to block creator

Purely voluntary, like a tip

Proof of Work

Consensus protocol used by Bitcoin

Equivalent views of proof of work

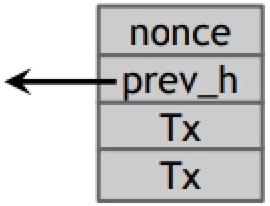
1. Select nodes in proportion to computing power

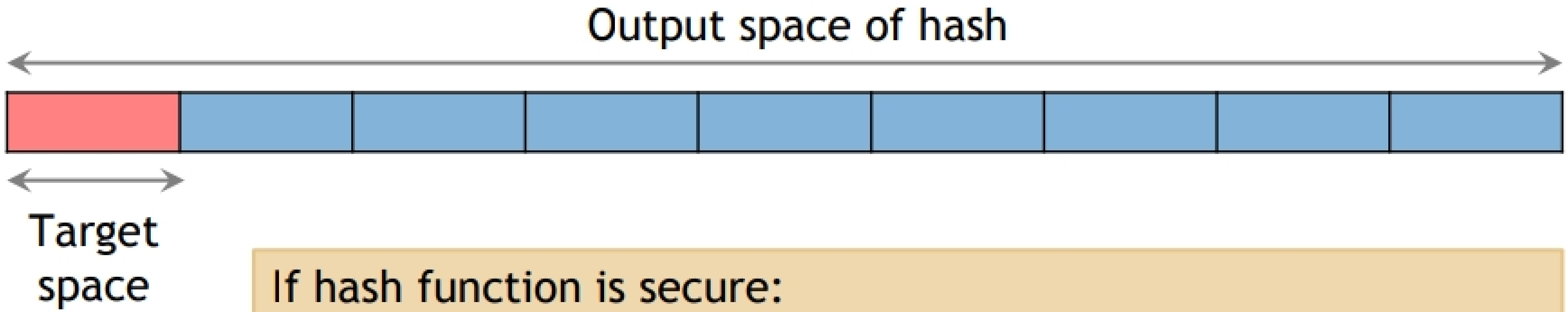
1. Let nodes compete for right to create block

1. Make it moderately hard to create new identities

Hash puzzles

To create block, find nonce s.t.
H(nonce || prev_hash || tx || … || tx) is very small





If hash function is secure:
only way to succeed is to try enough nonces until you get lucky

PoW property 1: difficult to compute

As of Aug 2014: about 10^{20} hashes/block

Only some nodes bother to compete — miners

PoW property 2: parameterizable cost

Nodes automatically re-calculate the target every two weeks

Goal: average time between blocks = 10 minutes

PoW property 3: trivial to verify

Nonce must be published as part of block

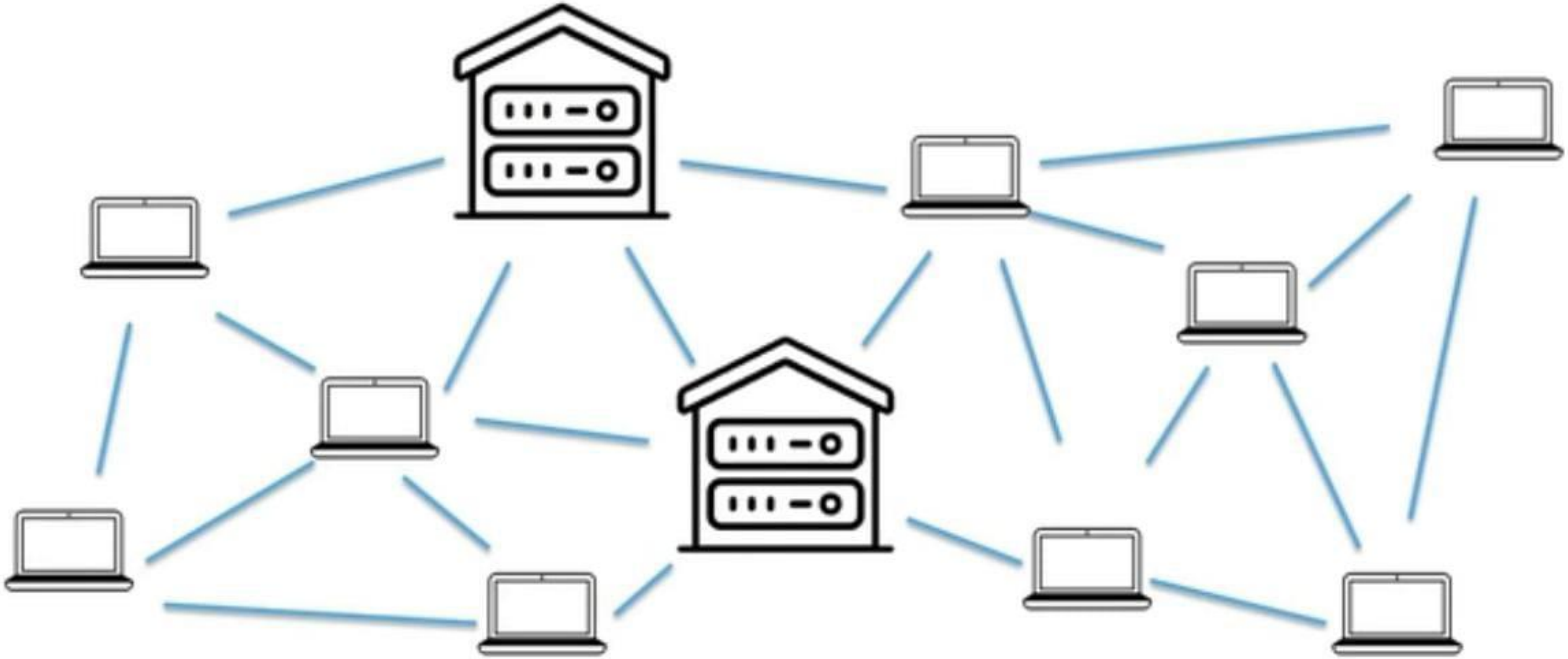
Mining economics

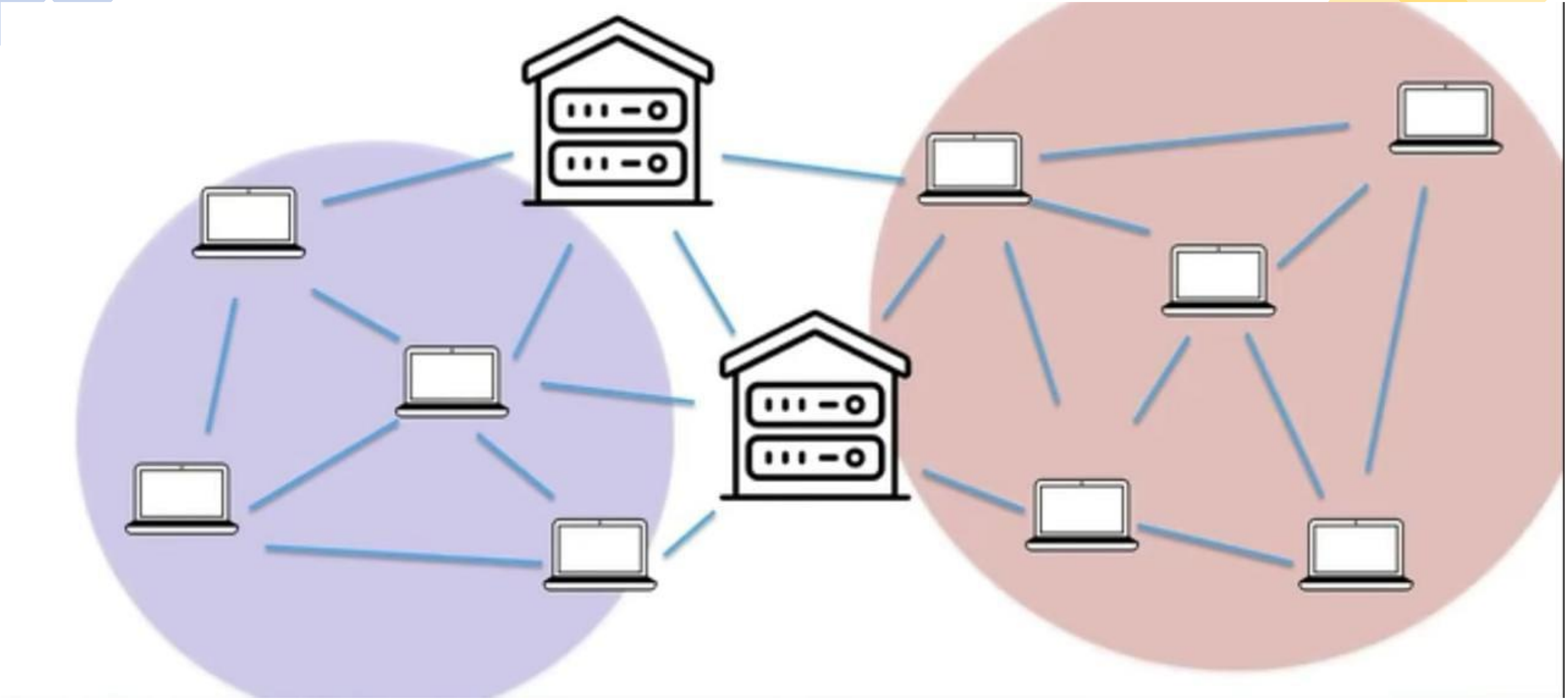
If mining reward (block reward + Tx fees)	>	hardware + electricity cost	→	Profit

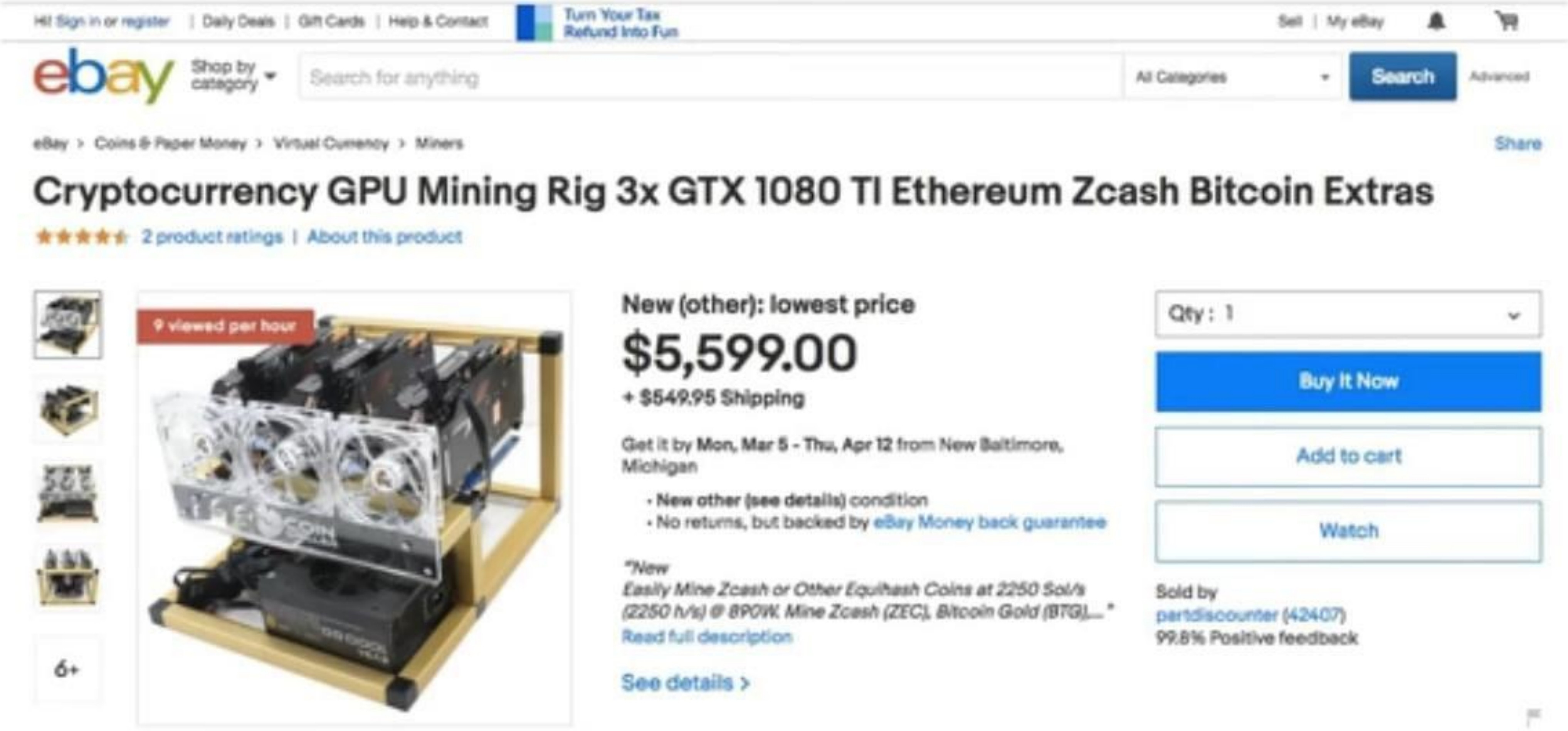
Complications:

- fixed vs. variable costs
- reward depends on global hash rate

Mining Pools







eBay > Coins & Paper Money > Virtual Currency > Miners

Cryptocurrency GPU Mining Rig 3x GTX 1080 TI Ethereum Zcash Bitcoin Extras

2 product ratings | About this product

New (other): lowest price

$5,599.00

+ $549.95 Shipping

Get it by **Mon, Mar 5 - Thu, Apr 12** from New Baltimore, Michigan

- **New other (see details)** condition
- No returns, but backed by eBay Money back guarantee

"New
Easily Mine Zcash or Other Equihash Coins at 2250 Sol/s (2250 h/s) @ 890W. Mine Zcash (ZEC), Bitcoin Gold (BTG)..."

Read full description

See details >

Qty : 1

Sold by
partdiscounter (42407)
99.8% Positive feedback

PoW Strengths

- Proven applicability, predictable block times
- Does not rely on any other node being trustworthy

- Only known vulnerability is the so-called '51% attack'
- Uncensorable and publicly broadcast

PoW Drawbacks

- Enormous waste of resources
  - Bitcoin mining uses much energy as Argentina
- ASIC hardware give advanced miners and mining pools a substantial advantage over the average miner
  - Massive start up costs can result in centralization of pools and resources
  - A regular computer has essentially no hope of ever mining a block

Current PoW Systems

- Bitcoin
- Ethereum (Casper)
- Litecoin
- Bitcoin Cash
- Many, many more

Acknowledgement and Source:

- https://www.udemy.com/course/build-your-blockchain-az/