



Blockchain and Cryptocurrency

By: Syeda Tayyaba Bukhari

Consensus Protocols

```
graph TD; A[Consensus Protocols] --> B[Proof-of-Work (PoW)]; A --> C[Proof-of-Stake (PoS)]; A --> D[Other];
```

Proof-of-Work (PoW)

Proof-of-Stake (PoS)

Other

TDM	729.89	915.51	185.62	▲25.43%	FLR	660.27	745.28	85.01	▲12.88%
HUM	749.73	924.29	174.56	▲23.28%	UVD	155.59	181.57	25.98	▲16.70%
DMW	833.72	1004.01	170.29	▲20.43%	QUV	440.55	540.21	99.66	▲22.62%
YZJ	903.49	1127.46	223.97	▲24.79%	HZT	285.51	344.98	59.47	▲20.83%
GLY	982.07	1219.39	237.32	▲24.17%	PCW	811.44	1029.66	218.22	▲26.89%
VDA	113.74	143.41	29.67	▲26.09%	AIK	361.77	451.39	89.62	▲24.77%
UVV	468.08	535.41	67.33	▲14.38%	ZJJ	858.36	994.57	136.21	▲15.87%
HJS	545.49	659.05	113.56	▲20.82%	RHJ	894.79	1046.68	151.89	▲16.97%
EQC	566.96	664.69	97.73	▲17.24%	VQV	425.08	509.95	84.87	▲19.97%

PPJ	912.63	1038.36	125.73	▲13.78%	ZBK	391.59	491.48	99.89	▲25.51%
UAQ	1309.55	1655.62	346.07	▲26.43%	BNY	969.21	1130.65	161.44	▲16.66%
DAQ	1295.17	1641.66	346.49	▲26.75%	SDM	735.44	913.39	177.95	▲24.20%
PNR	654.33	775.84	121.51	▲18.57%	TQK	1323.91	1646.42	322.51	▲24.36%
ZTM	161.00	192.00	31.00	▲19.25%	OIS	543.42	667.24	123.82	▲22.79%
					STH	1295.17	1641.66	346.49	▲26.75%

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 special coin-creation transaction 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



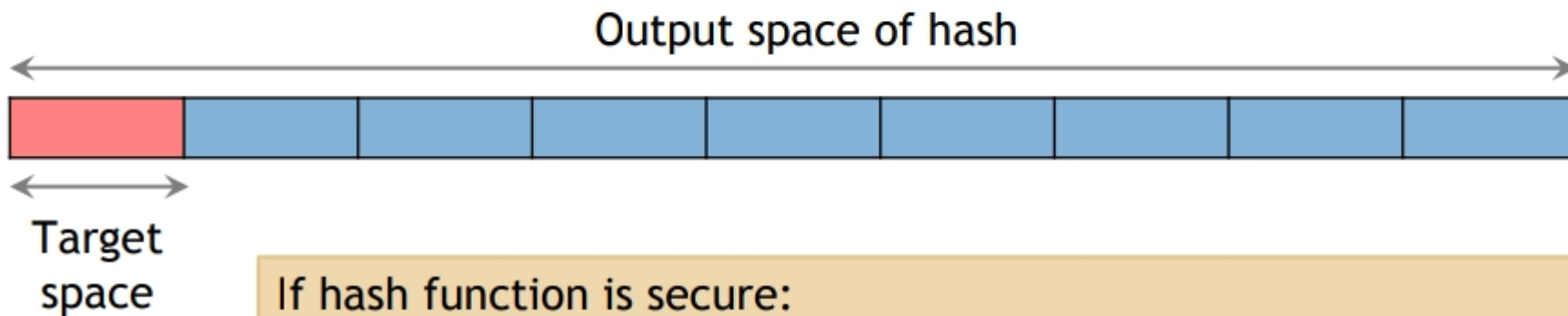
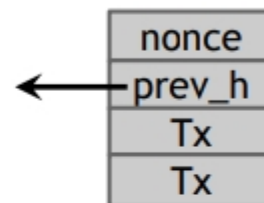


Equivalent views of proof of work

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.
 $H(\text{nonce} \parallel \text{prev_hash} \parallel \text{tx} \parallel \dots \parallel \text{tx})$ 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

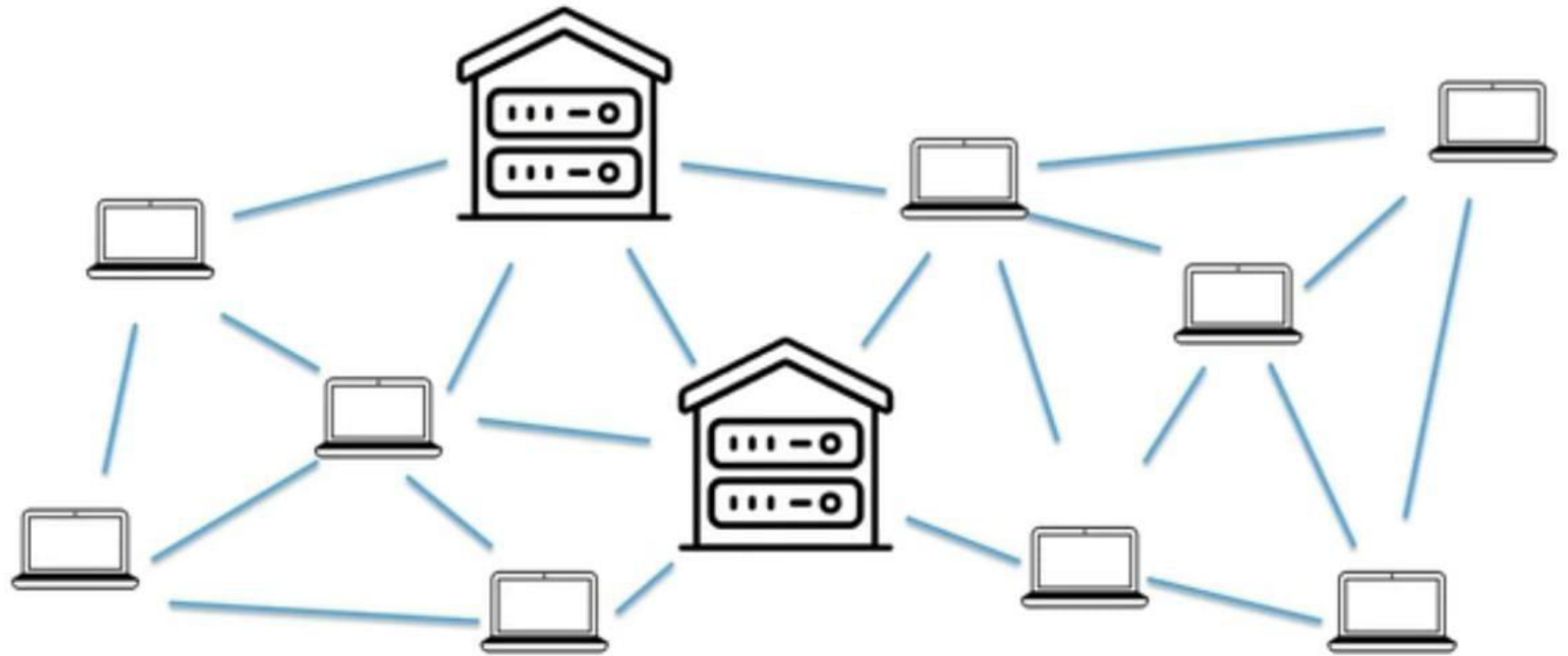
If mining reward (block reward + Tx fees)	>	hardware + electricity cost	→	Profit
--	---	--------------------------------	---	--------

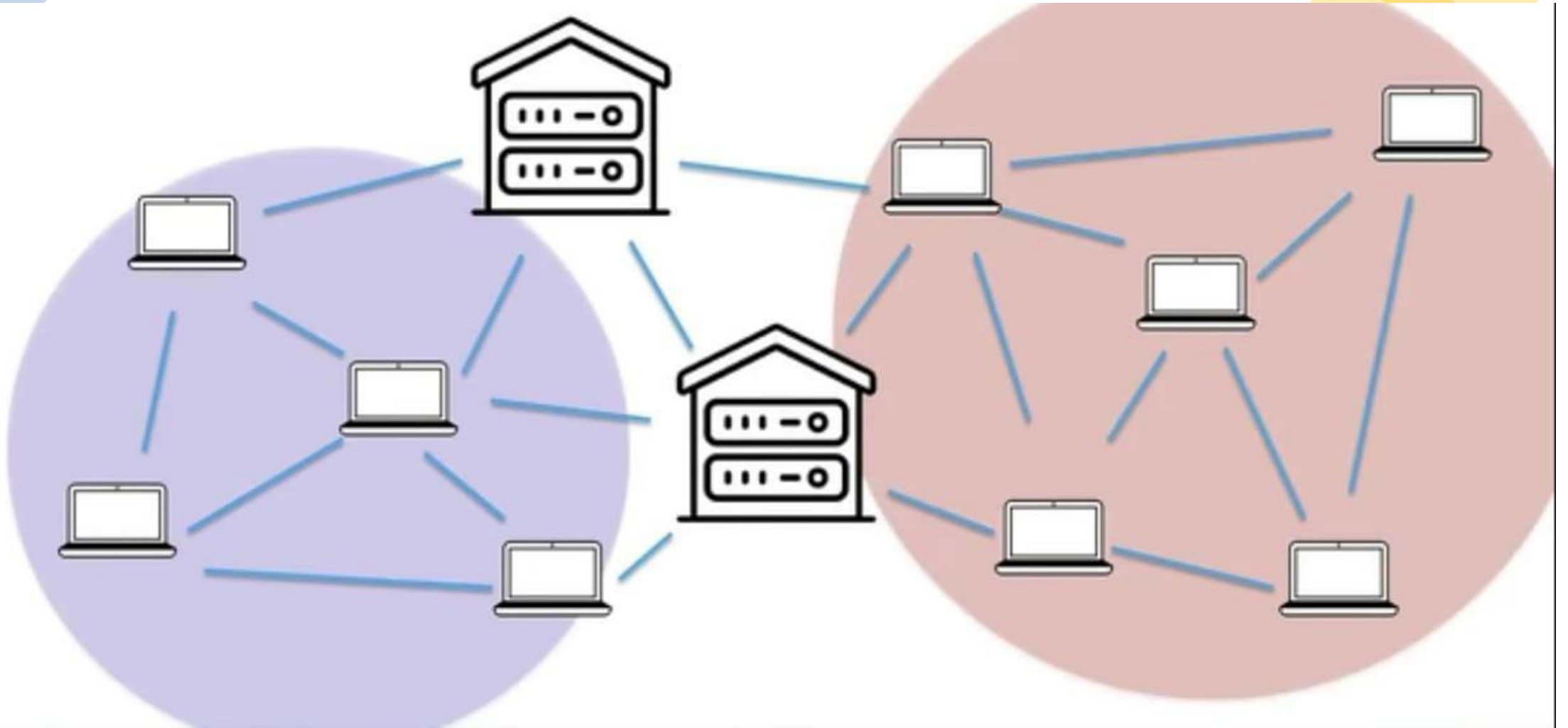
Complications:

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



Mining Pools







Shop by
category

Search for anything

All Categories

Search

Advanced

eBay > Coins & Paper Money > Virtual Currency > Miners

Share

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

★★★★★ 2 product ratings | [About this product](#)



6+

9 viewed per hour



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

Buy It Now


Add to cart

Watch

Sold by
[partdiscourter](#) (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/>