MINING PROCESS AND MINING POOLS

ENSURING THE FUTURE OF BLOCKCHAIN

Network Difficulty, Mining Mechanics, CPU/GPU and ASIC Mining, Solo vs. Pool Mining

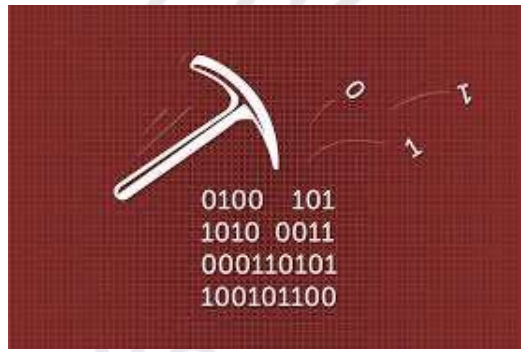
1. Understanding Mining
   - Mining process, **network difficulty**
   - Exercise: **Write a Simple Miner**
2. Mining Methods
   - **Solo** mining vs. **pool** mining
   - Mining **farms**
   - Exercise: **Mine Ethereum in a Pool**
3. Mining equipment CPU, GPU, ASICs
   - Exercise: **What to Mine?**

What is Bitcoin Mining?

https://youtu.be/GmOzih6I1zs

How Does a Cryptocoin Mining Work?

- Mining is a part of the **PoW** consensus
  - Miners **verifying transactions**
  - They create **new blocks**
  - Miners get paid with **fees** and newly mined **coins** (through a coinbase transaction)
- **Proof of Stake** networks do not perform mining
  - Instead, blocks are build by **verifiers** (not miners)



How Does the Bitcoin Mining Work?

- A miner **calculates SHA-256** on the **block header**
  - The only **mutable** elements in the header are the **nonce** and **timestamp**
  - …and the **coinbase TX**
- The **hash result** should be **smaller** than the **target value**

Block “n” → Header n:
- Nonce (**0**)
- [hash(header(n-1))]
- Etc…

→ SHA 256 →

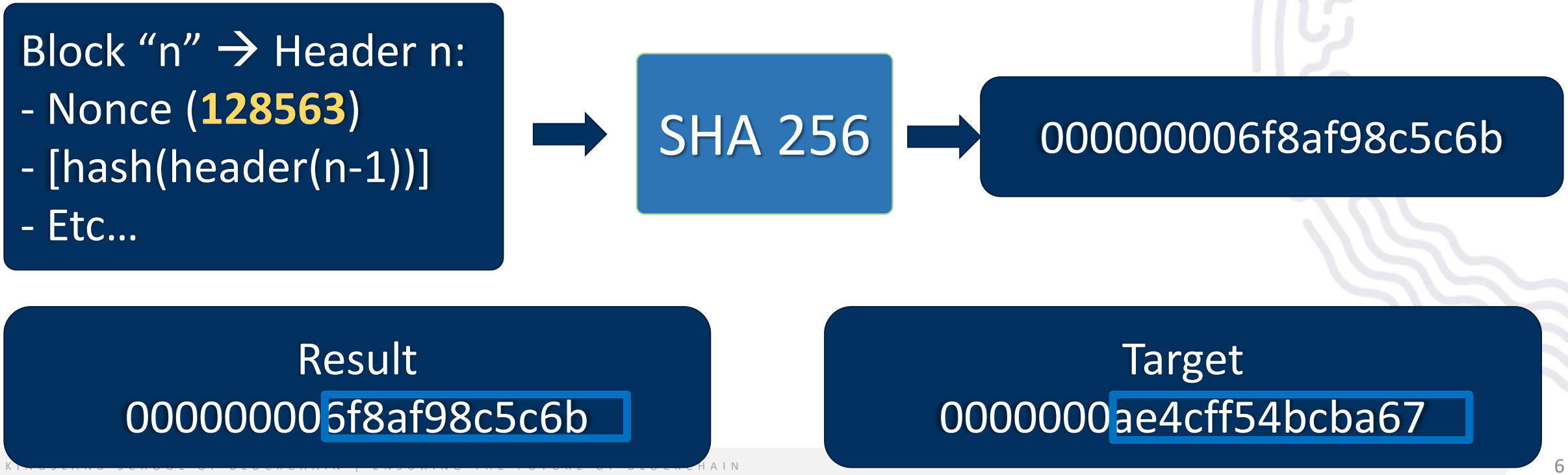
00aacf3be5ce032f5a6b

Result
00aacf3be5ce032f5a6b

Target
0000000ae4cff54bcba67

How Does the Bitcoin Mining Work? (2)

- The miner **increments the nonce** until a satisfying result is found
  - This may take a lot of time and hashing power!
- Finally, the **nonce is found** and the hash meets the target



How Does the Bitcoin Mining Work? (3)

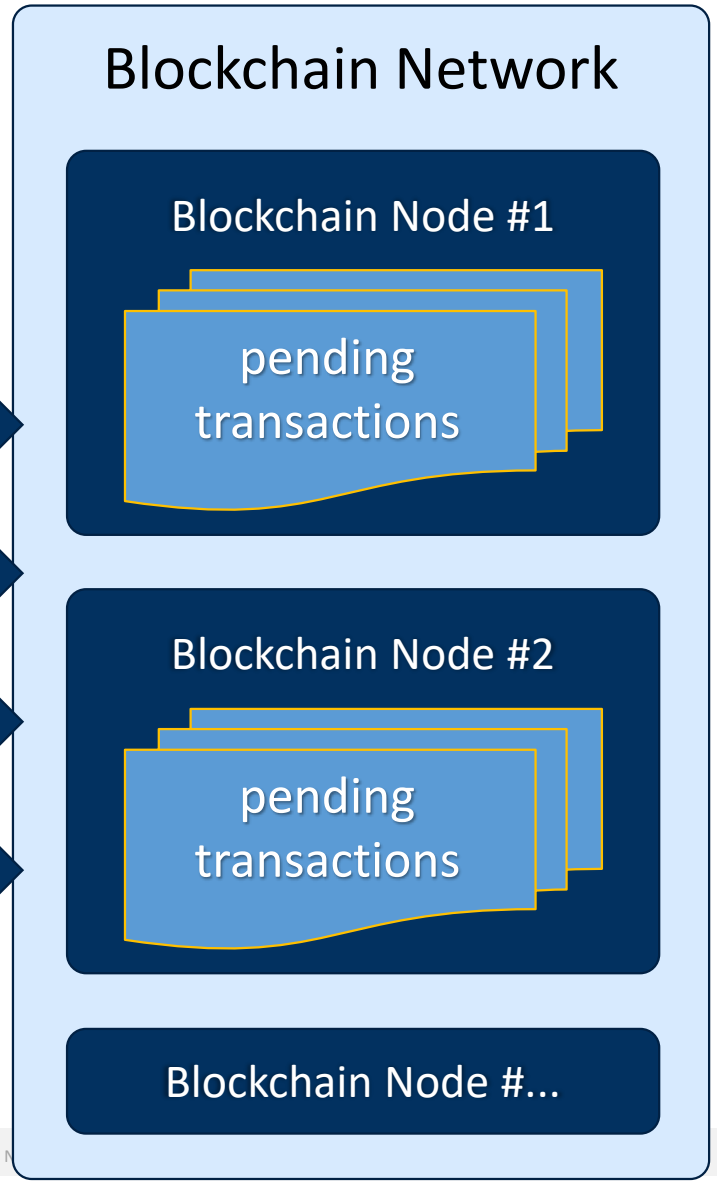
- Miners **compete** each other in order to find a correct **nonce**
- Once a correct nonce is found
  - The lucky miner builds the next block
  - Broadcasts it for **verification** by the other miners in the network
  - Transaction **fees** + **mining award** are collected by the miner
- The network **validates** the new block
  - **Valid** block → miners start mining the next block
  - **Invalid** block → miners continue mining the current block

PoW Mining in the Blockchain

Blockchain clients **create** and **sign** transactions

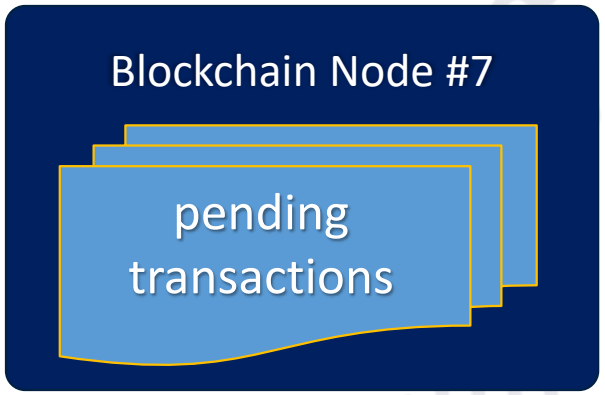
- Transaction A
- Transaction B
- Transaction C
- Transaction …

Transactions are **sent** to the network

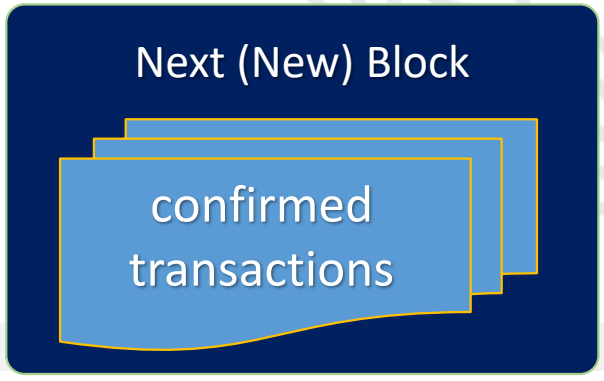


PoW mining process

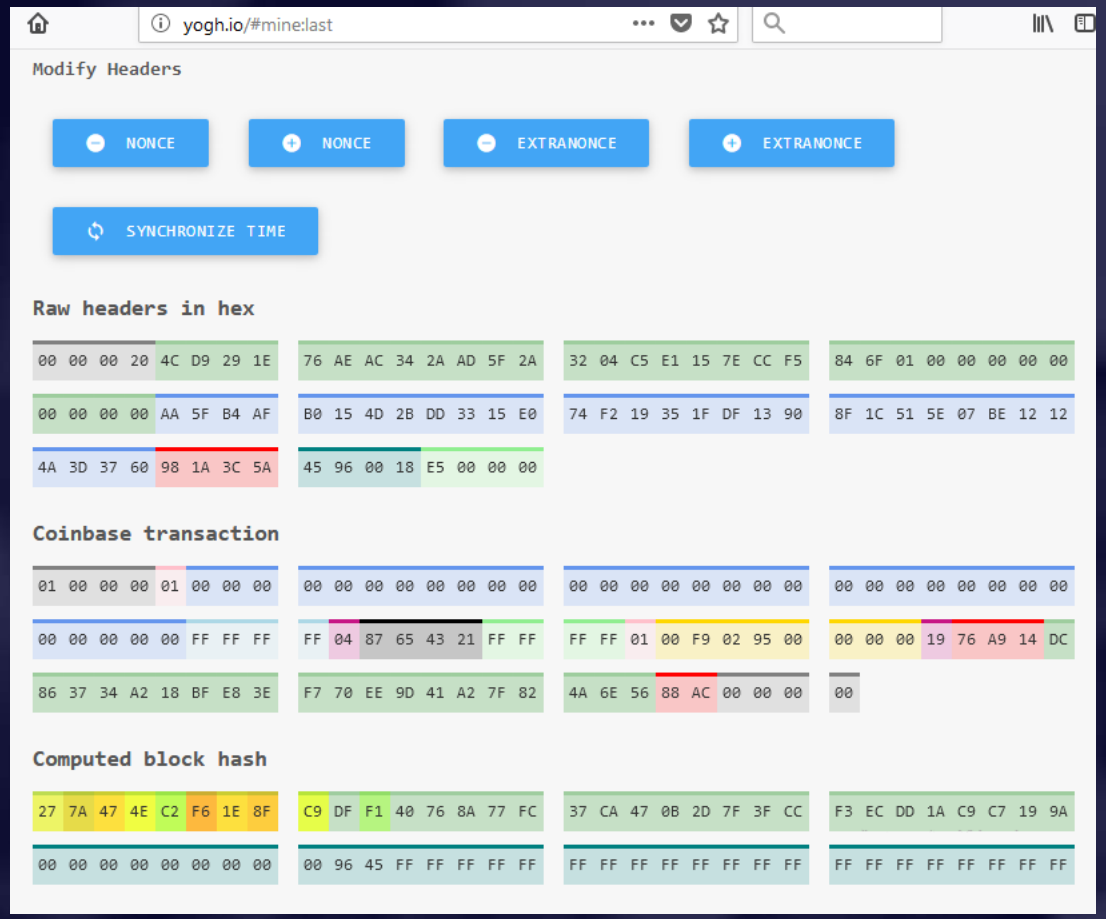
Selects the **winning node** (a lucky miner)



Validates the pending transactions and creates the **next block**



Propagate for validation



HOW DOES CRYPTOCOIN MINING WORK?

Live Demo: http://yogh.io/#mine:last

Mining Rewards

- Miner who mined the block **receives** coins from two streams:
  - The **new bitcoins** created by the coinbase transaction
    - The reward began at **50 BTC**
    - The reward is **halved every 210,000 blocks**
    - It will take about **132 years** to mine all 6,929,999 block subsidies, and the last subsidy will be mined in **2140**
  - The **fees** paid on the transactions

What is Network Difficulty?

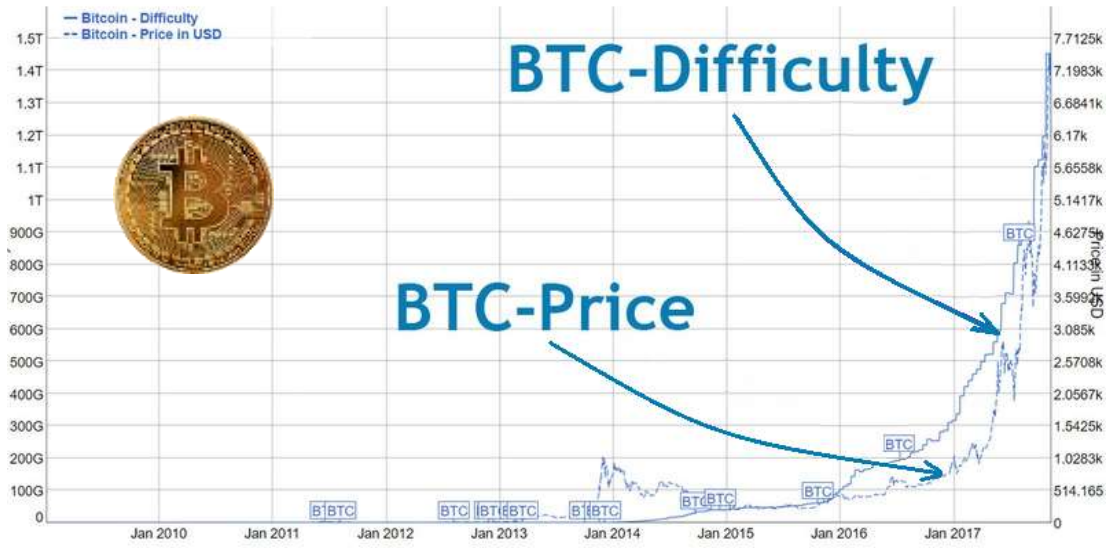
- The mining **target** is also called "**network difficulty**"
  - The difficulty is defined by the magnitude of the target value
- In Bitcoin system if more **computational power** is added to the network, system **increases its difficulty** (so as to keep block time constant)

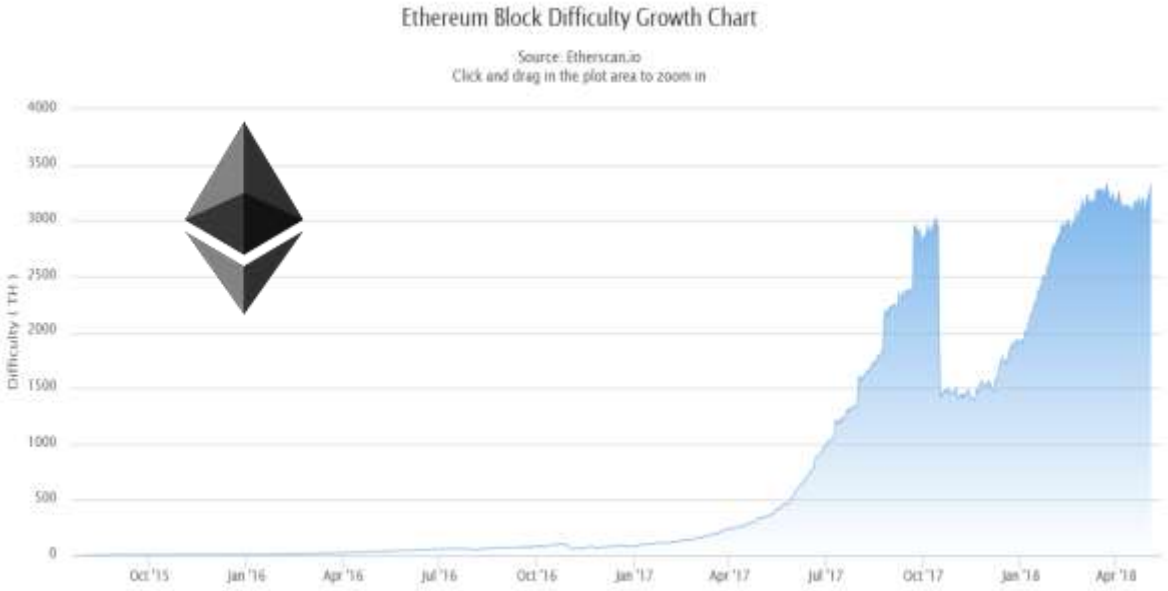
Target (Difficulty)
000dlks3nfolr0jdgf5h6h

Target (Difficulty)
000000gdjhfhj57kjytt9

Cryptocurrency Difficulty Growth

- Growing number of miners **raises the network difficulty**





BUILDING A MINER FOR SIMPLE JS BLOCKCHAIN

JavaScript Blockchain with Simple Miner

Implementing Mining: Block Structure

```
class Block {
  constructor(index, timestamp, data, previousHash = '') {
    this.index = index;
    this.previousHash = previousHash;
    this.timestamp = timestamp;
    this.data = data;
    this.nonce = 0;
    this.hash = this.calculateHash();
}
```

Data is stored in the **block** (typically holds transactions)

Miners search for **nonce** calculate **PoW hash** and to **mine** the block

Implementing Mining: Proof of Work

```
mineBlock(difficulty) {
  while (this.hash.substring(0, difficulty) !==
      Array(difficulty + 1).join("0")) {
    this.nonce++;
    this.hash = this.calculateHash();
  }
  console.log("BLOCK MINED: " + this.hash);
}
```

Search for more zeroes than the **difficulty**

Increment the **nonce** to try again

Implementing Mining: Block Hash

```
calculateHash() {
  return SHA256(this.index +
    this.previousHash +
    this.timestamp +
    JSON.stringify(this.data) +
    this.nonce
  ).toString();
}
```

Miners use the block fields to calculate the **block hash**

The **nonce** is part of the block hash

EXERCISE: PROOF OF WORK MINER

JavaScript Blockchain with PoW Miner

MINING POOLS

Solo Mining and Mining Pools

Solo Mining vs. Pool Mining

- Proof of work mining takes on two forms:

Solo mining

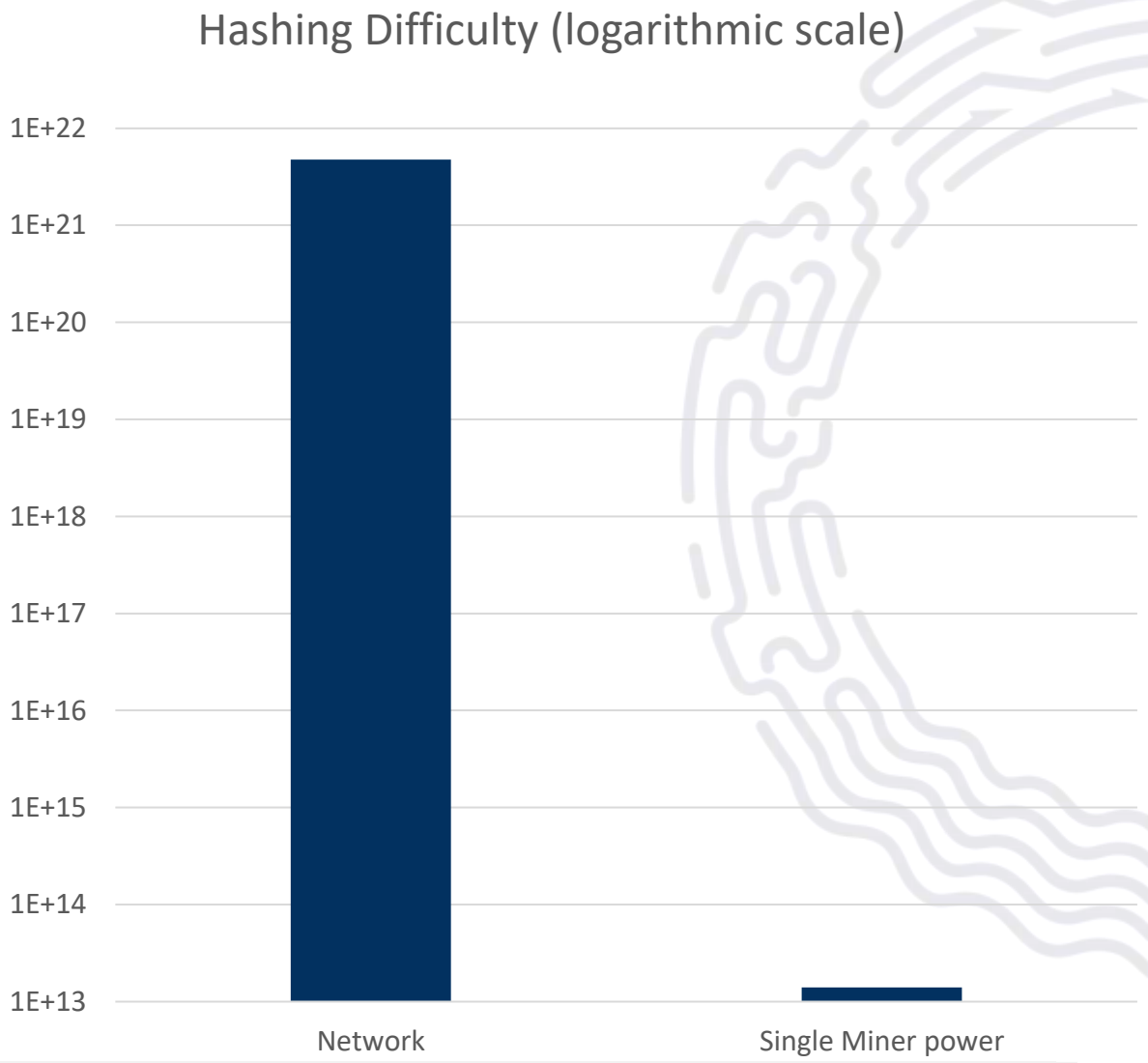
Pool mining

What is Solo Mining?

- **Solo miners** have a **low probability** to "find" a block
  - Do **not share** the block reward
  - Do **not pay fees** to a pool
- Solo miners can run a single **CPU** / **GPU** or a large **farm**
- Works well early after a PoW cryptocurrency is launched

Solo Mining is Like a Lottery!

- **Extremely low chance** to find a block, see an example:
  - Bitcoin block #487465 (09/2017)
  - Network **difficulty** = 1103400932964.29 ≈ **1.1034×10^{12}**
  - Average **time to find a block** ≈ 3 917 days = **10.7 years**

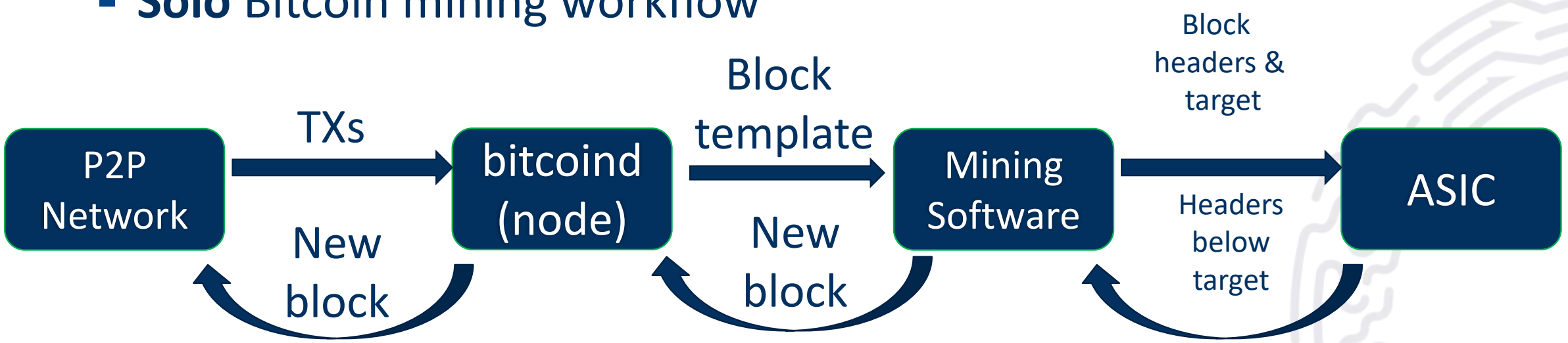


Mining in a Pool is More Predictable

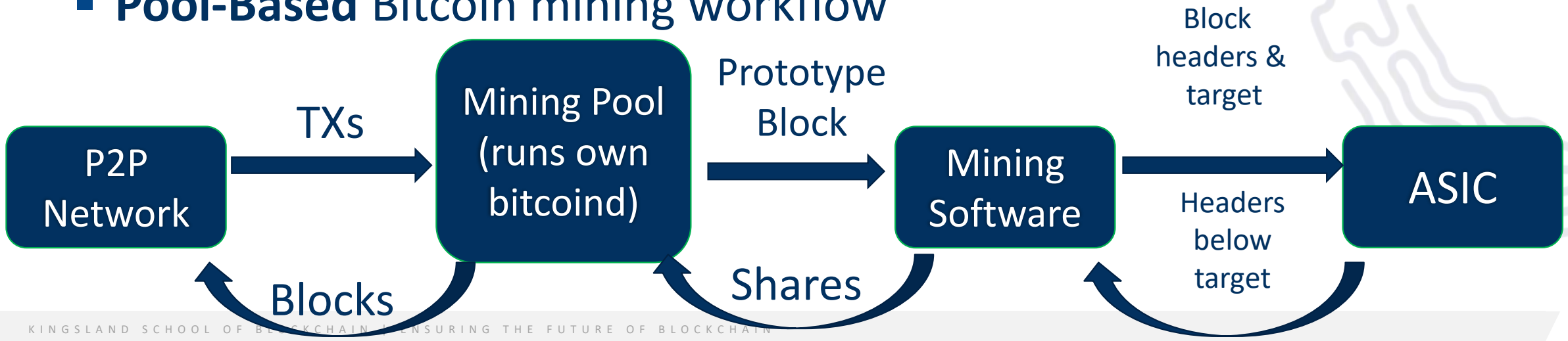
- It could **take years** for slower miners to mine a block
- What is a **mining pool**?
  - Miners **share** their processing **power** over a network
  - Pools **split the reward** between the miners
  - Pools take a **pool fee** from the miners
- In Jan 2018 the Antpool mines
  ~ 25 blocks / day
  - Recall that ~ 144 new Bitcoin blocks are mined per day

Bitcoin Solo vs. Pool Mining

- **Solo** Bitcoin mining workflow



- **Pool-Based** Bitcoin mining workflow



Proof of Some Work

- Pool accepts shares at **lower difficulty** than the actual chain
- Shares **mostly useless**, except they **prove workers aren't slacking off**
- Some shares will **exceed the requirements** by so much that they will be valid **even** on the actual chain
  - When this happens, the pool has **found a block**
  - **Reward split** between people who submitted shares

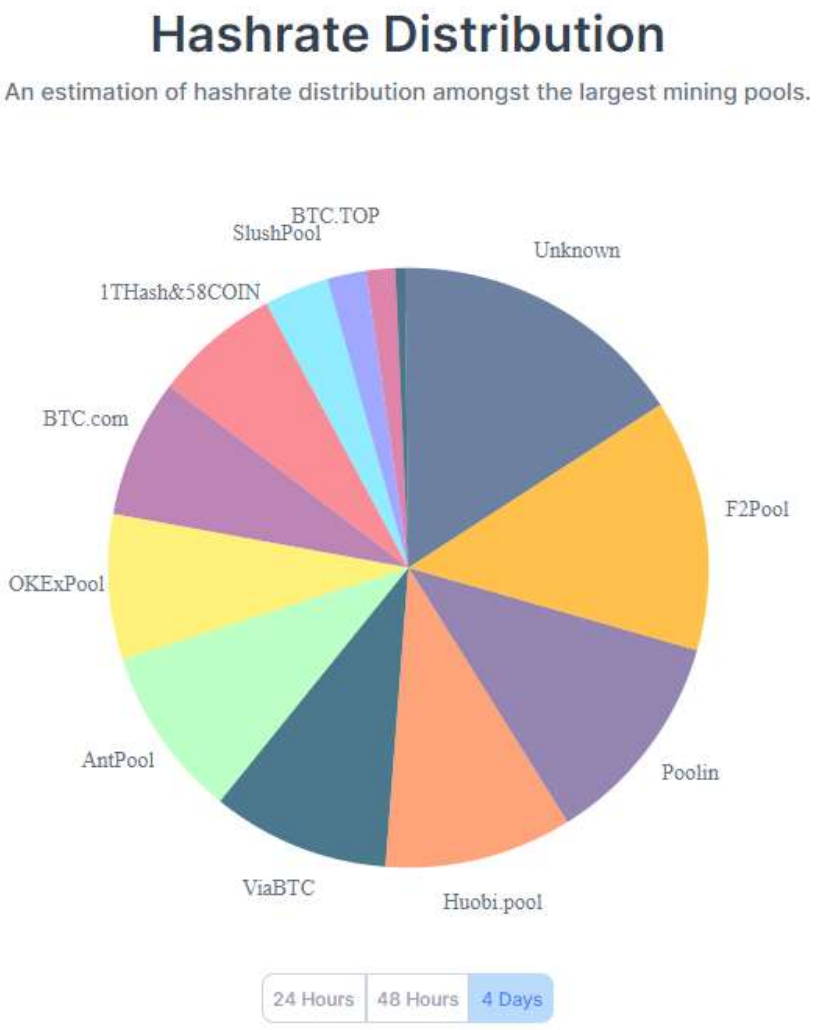
Mining Pool Methods

- **Pay-per-Share** (PPS)
  - Instant, guaranteed payout for each share, solved by a miner
- **Proportional**
  - Miners earn shares until the pool finds a block
  - After that **each user** gets reward
- **Bitcoin Pooled mining** (“Slush's system")
  - Older shares from the beginning of a block round are given less weight than more recent shares
  - Reduces the ability to cheat the mining pool system by **switching pools** during a round

Mining Pool Methods (2)

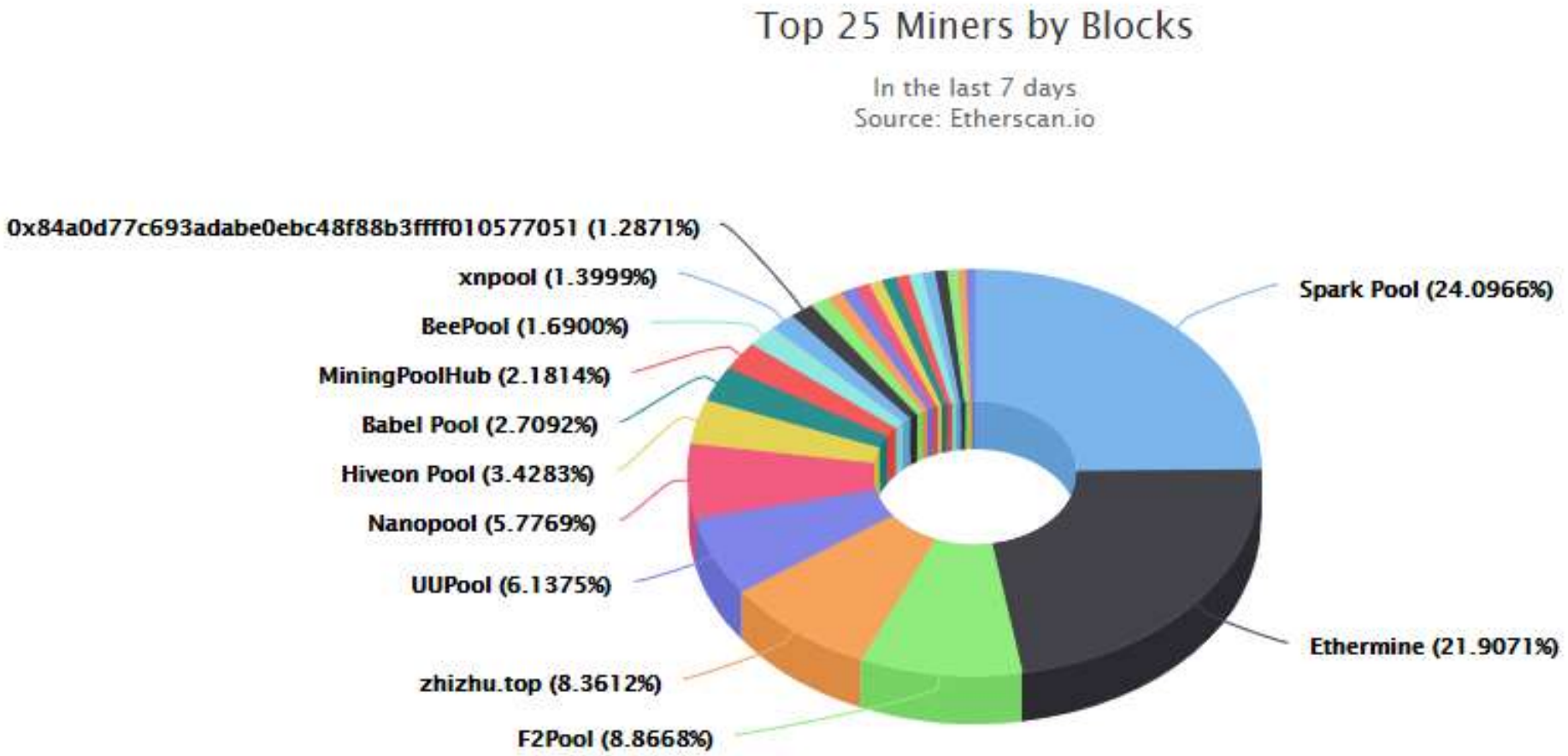
- **Pay-per-last-N-shares** (PPLNS)
  - Reward calculated on a basis of **N last shares**, instead of all shares for the last round
- **Geometric Method**
  - Similar to PPS: score granted for every new share
- **Double Geometric Method**
  - Generalized version of Geometric and PPLNS methods

Bitcoin Mining Pools



Source: https://blockchain.info/pools (September 2020)

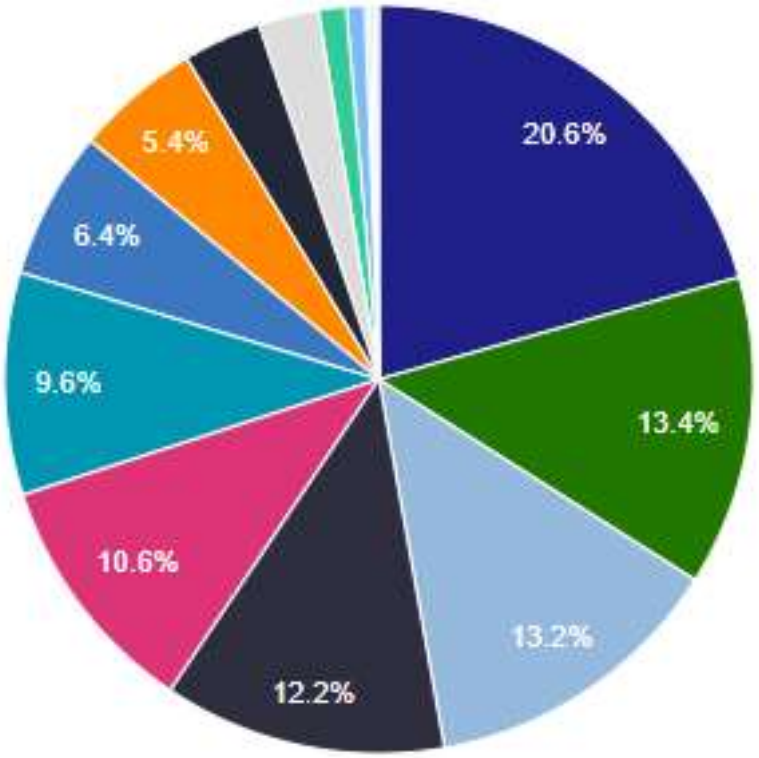
Ethereum Mining Pools



Source: https://etherscan.io/stat/miner (September 2020)

Litecoin Mining Pools

Hash Rate Distribution (last 21 hours)



Poolin	~ 55.1 TH/s
F2Pool	~ 35.9 TH/s
Easy2Mine	~ 35.3 TH/s
Antpool	~ 32.7 TH/s
LTC.top	~ 28.4 TH/s
ViaBTC	~ 25.7 TH/s
BTC.com	~ 17.1 TH/s
LitecoinPool.org	~ 14.5 TH/s
Huobi	~ 9.1 TH/s
LaKd2Pa578...	~ 7.0 TH/s
Show all pools...	
Total	~ 267.7 TH/s

Source: https://www.litecoinpool.org/pools (September 2020)

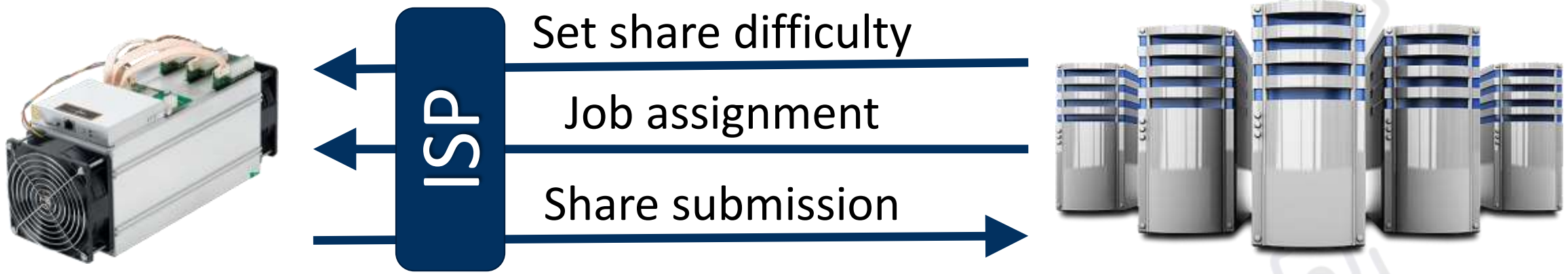
29

Stratum Protocol

- Created by **Slush pool** to **support pooled mining** as a replacement for obsolete "getwork" protocol in late 2012
- Originally designed for lightweight Bitcoin client **Electrum**
- Line-based protocol using plain **TCP socket**, with payload **encoded as JSON-RPC messages**
  - **Client opens TCP socket** and **writes requests** to the server in the form of **JSON messages** finished by the newline character **\n**
  - **Client receives** a valid JSON-RPC fragment containing the response

The "Stratum" Mining Protocol

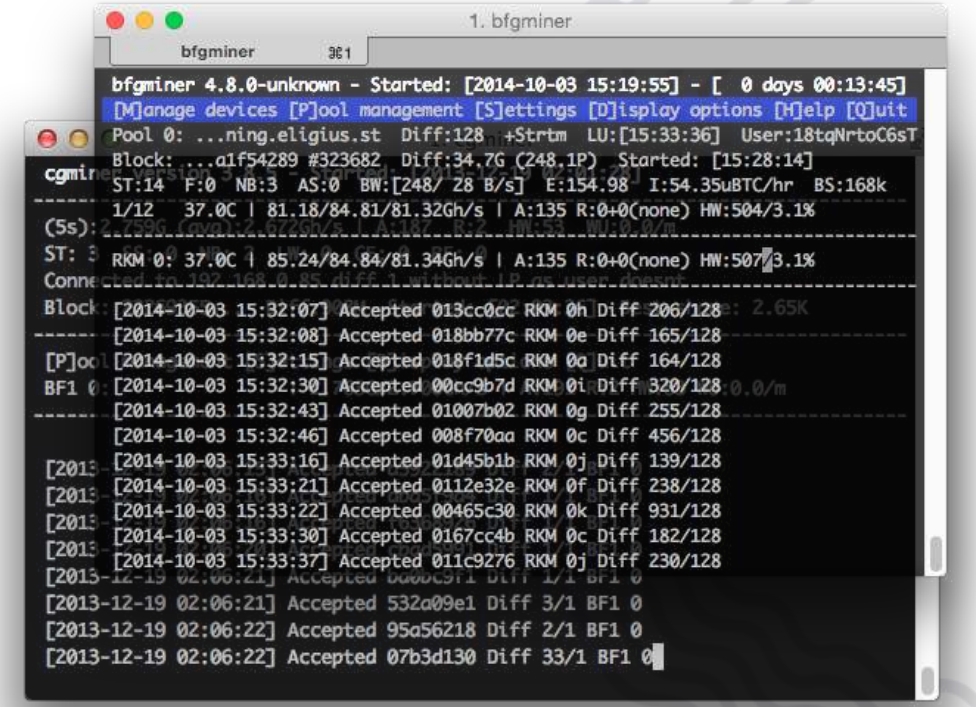
- Stratum == popular mining protocol, used by PoW pools and miners
  - Simple, easy to **implement**, easy to **debug**, easy to **extend**



- Miners can **locally generate work** by rolling the **extranonce**
- Serve **18 EHash/s** (exa-hashes/s) **mining rig from a single TCP connection**
- **Disadvantage**: miners **cannot** choose the **transactions** on their own

Stratum Protocol Compatible Miners

- Miners with **native** support of the **Stratum protocol**:
  - bfgminer
  - cgminer (ver. 2.8.1 and newer)
  - poclbm (ver. 20120920 and newer)
- All current **getwork-compatible miners** can use **Stratum mining proxy** running locally on mining computer
  - One **mining proxy** can handle (almost) **unlimited number** of connected workers



Setup Miner Examples

- Connect **cgminer** to single pool examples

```
Single pool with a standard http proxy:
cgminer -o "http:proxy:port|http://pool:port" -u username -p passwd

Single pool with a socks5 proxy:
cgminer -o "socks5:proxy:port|http://pool:port" -u username -p passwd

Single pool with stratum protocol support:
cgminer -o stratum+tcp://pool:port -u username -p password
```

- **Claymore's** Dual Ethereum miner supports all **Stratum** versions for **Ethereum** (**HTTP mode** is necessary for **solo mining only**)

EXERCISE

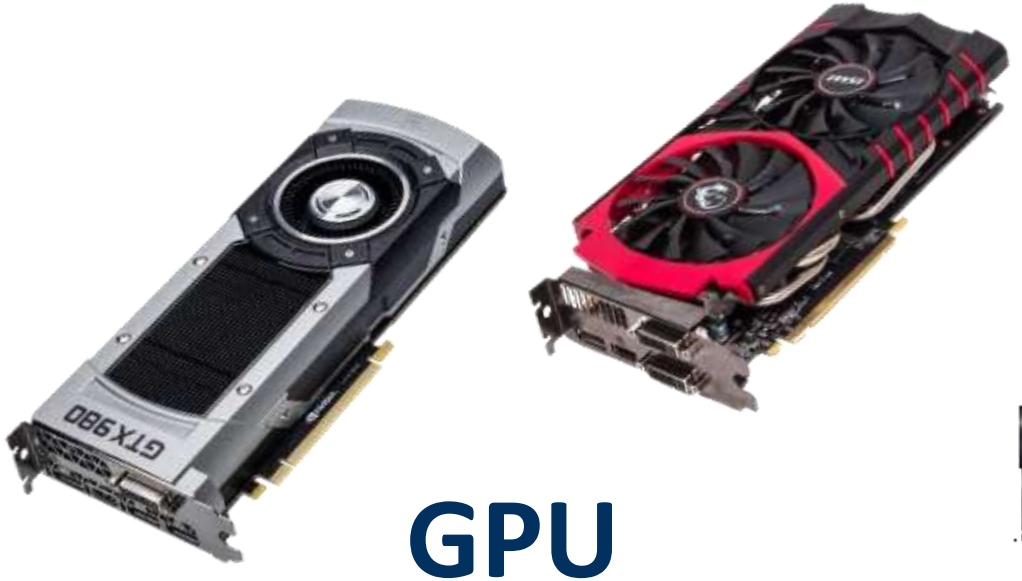
Mine Ethereum and Monero in a Pool

MINING EQUIPMENT

CPU, GPU, ASIC

Mining Equipment

- Different **equipment** is more effective with different **PoW algorithms**



GPU

ASIC

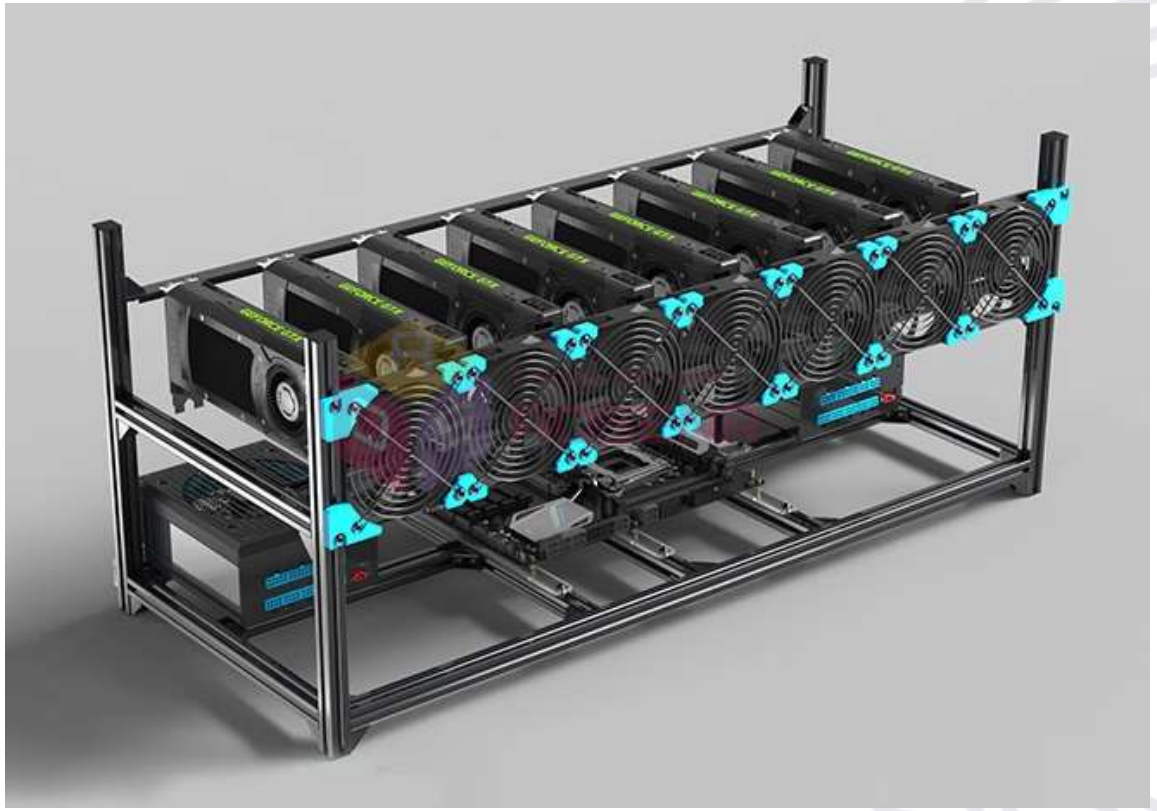
CPU

Central Processing Unit (CPU)

- In the **beginning**, mining with a **CPU** was the only way to mine
  - Very **inefficient** for most algorithms
  - Some coins (like Monero) using **CryptoNight** and **X11** can still be mined **using CPU**

Graphics Processing Unit (GPU)

- GPU **rigs** can mine many hashing algorithms
- Ethereum miners mostly use **GPUs**
- Some GPUs are **hard to find**

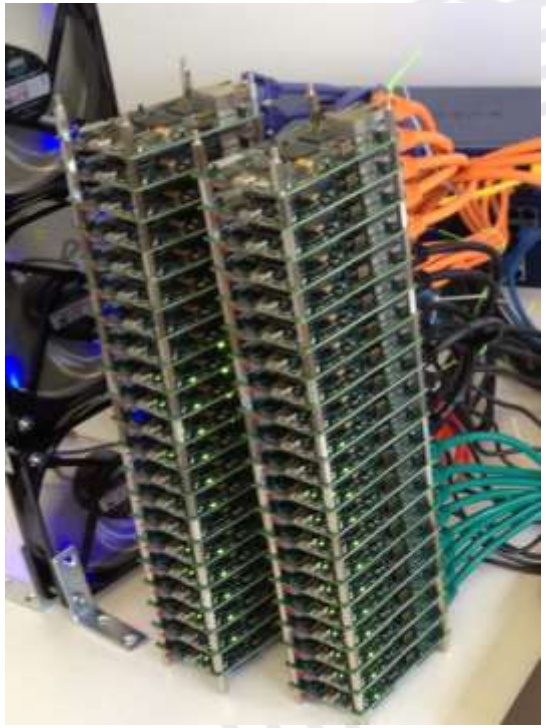


Example of **GPU mining rig**

Example of video card (**GPU**)

Field-Programmable Gate Arrays – FPGA

- **FPGA** can implement complex digital computations
  - **FPGA** == field-programmable integrated circuit
  - Array of **programmable logic blocks**
  - Allows to build your own specialized CPU
- First **mining farms** were based on FPGA
  - FPGA miners used **much less power** than CPUs and GPUs with higher hashrate



Application-Specific Integrated Circuit (ASIC)

- **ASIC** miners are an integrated circuits customized particularly for **mining**
  - Hardware designed for mining
- Very **powerful**
  - Effective with less algorithms

13.5Th/s 1400w

Newest BM1387 chip with 0.09w/GH

Popular Proof-of-Work Cryptocurrencies

- Different **cryptocurrencies** use different **hashing algorithms**
  - **Bitcoin**, **Bitcoin Cash** – SHA256 – ASIC mineable
  - **Ethereum**, **Ethereum Classic** – ETHash – GPU* mineable
  - **ZCash**, **Bitcoin Gold** – Equihash – GPU and ASIC mineable
  - **Monero**, **ByteCoin** – CryptoNight – GPU and ASIC mineable
  - **Litecoin**, **Dogecoin** – SCrypt – GPU and ASIC mineable
  - **Dash** – X11 – ASIC, CPU and GPU mineable
  - **Stratis** – X13 – ASIC, CPU and GPU mineable

Learn more at: cryptorival.com/algorithms

Proof of Work: Potential ASIC Speedup

PoW Mining Algorithm	Potential ASIC Efficiency Gain
SHA256 (Bitcoin, Bitcoin Cash)	1000 X
Scrypt (Litecoin)	1000 X
X11 (Dash)	1000 X
Equihash (Zcash, Bitcoin Gold)	100 X
Cuckoo Cycle (Aeternity)	100 X
CryptoNight (Monero)	50 X
ETHash (Ethereum)	2 X

Source: https://github.com/ifdefelse/ProgPOW

Mining: from Enthusiasts to Giant Enterprises

Why are Mining Farms So Popular?

- Crypto **mining** has become a more specialized activity
- Industry invented **faster** Bitcoin **mining equipment like FPGAs** and **ASICs**
- More **profitable**

What to Mine?

- Miners often switch what cryptocurrency to mine
  - Depending mostly on the **profitability**
- Many sites and apps can estimate the mining expenses, expected incomes and profitability, e.g.
  - whattomine.com
  - cryptocompare.com/mining/calculator
  - cryptoground.com/mining-calculators

EXERCISE: WHAT TO MINE?

Play with whattomine.com

Summary

- Miners **calculate hashes with** different **nonce** till find enough zeroes
- **Difficulty** → the number of zeroes in the beginning of the target
  - Growing number of miners **raises** the network difficulty
- **Solo miner** has a **low probability** to "find" a block
  - Do not share the **reward**
- **Pools** split the reward between their members
  - Mining usually works in pools, which **shares the reward**
- Different **equipment** is effective for different **hash algorithms**

Questions?

Resources

- Bitcoin Mining: https://bitcoin.org, https://en.bitcoin.it/wiki/, https://www.weusecoins.com/en/mining-guide/
- Ethereum Mining: https://www.ethereum.org/
- Proof of Work: https://en.bitcoin.it/wiki/Proof_of_work, https://www.cryptocoinsnews.com/proof-of-work/
- Mining Pool Methods: https://en.bitcoin.it/wiki/Comparison_of_mining_pools, https://en.wikipedia.org/wiki/Mining_pool
- Stratum protocol: https://en.bitcoin.it/wiki/Stratum_mining_protocol, https://slushpool.com/help/manual/stratum-protocol, https://docs.google.com/document/d/17zHy1SUlhgtCMbypO8cHgpWH73V5iUQKk_0rWvMqSNs/edit?hl=en_US
- Mining components comparison: https://whattomine.com/

50

KINGSLAND
SCHOOL OF BLOCKCHAIN

THANK YOU

ENSURING THE FUTURE OF BLOCKCHAIN

ENSURING THE FUTURE OF BLOCKCHAIN