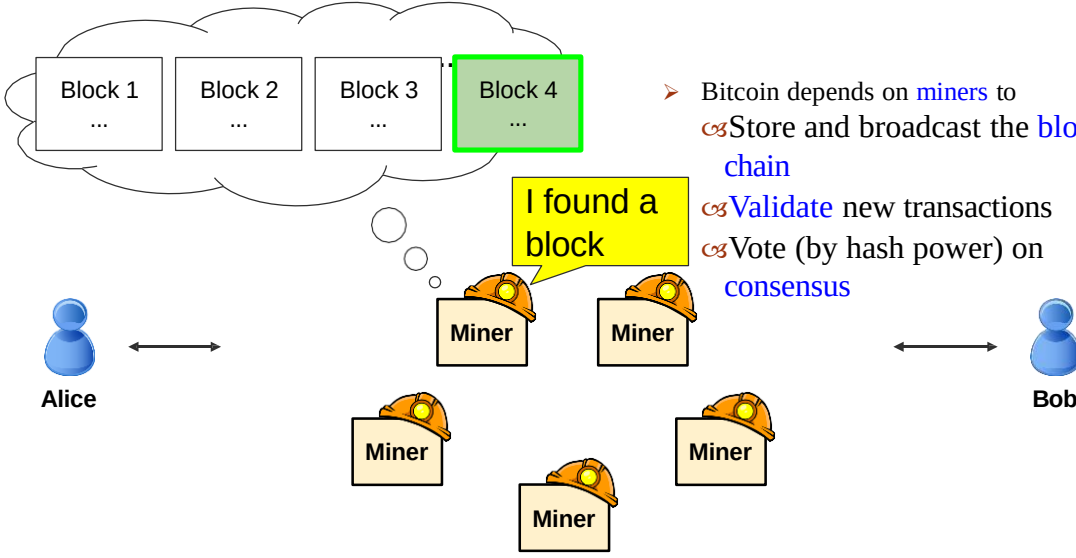
Introduction to Cryptocurrency

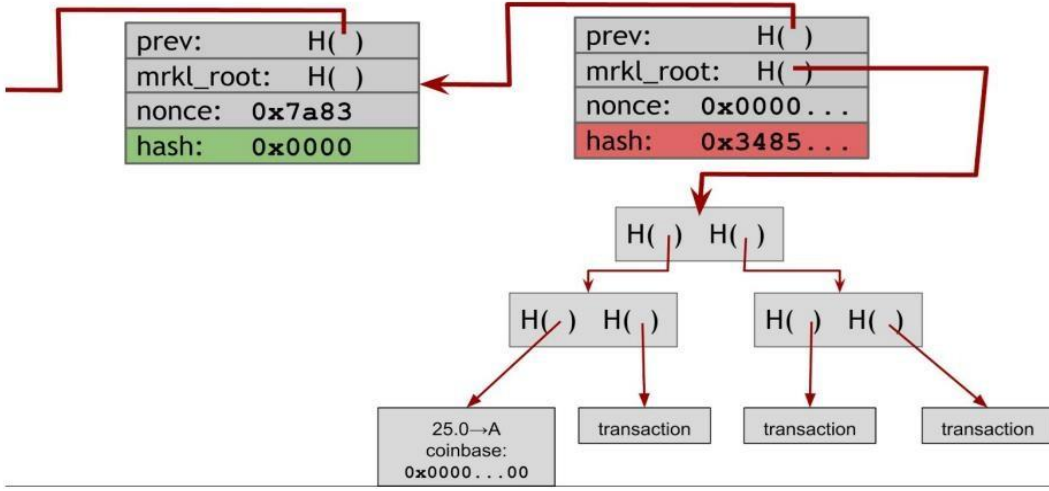
Bitcoin Mining

BITCOIN MINERS

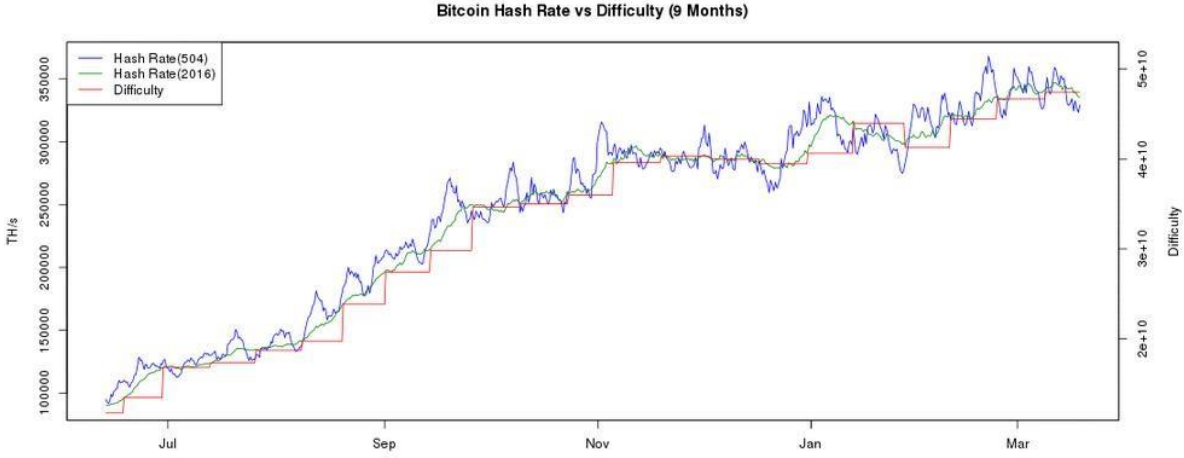


- Bitcoin depends on miners to
  - Store and broadcast the block chain
  - Validate new transactions
  - Vote (by hash power) on consensus

MINING


prev: H( )
mrkl_root: H( )
nonce: 0x7a83
hash: 0x0000
prev: H( )
mrkl_root: H( )
nonce: 0x0000...
hash: 0x3485...
H( ) H( )
H( ) H( )
H( ) H( )
25.0→A
coinbase:
0x0000...00
transaction
transaction
transaction

MINING DIFFICULTY ADJUSTS OVER TIME



SETTING MINING DIFFICULTY

Every two week, compute:

```
next_difficulty= previous_difficulty *
                (2 weeks)/(time to mine last 2016 blocks)
```

Expected number of blocks in 2 weeks at 10 minutes/block

BLOCK HEADER

An 80-byte block header contains:

- 4 bytes: version
- 32 bytes: previous block hash
- 32 bytes: merkle tree of transactions
- 4 bytes: timestamp
- 4 bytes: difficulty target
- 4 bytes: nonce

HASH TARGET

- The encoding has a 1-byte exponent, followed by a 3-byte mantissa (coefficient).
- In block 277,316, for example, the target bits value is 0x1903a30c.
- The first part 0x19 is a hexadecimal exponent, while the next part, 0x03a30c, is the coefficient.

target = coefficient * 2^(8 * (exponent – 3))

Using that formula, and the difficulty bits value 0x1903a30c, we get:

target = 0x03a30c * 2^(0x08 * (0x19 - 0x03))

=> target = 0x03a30c * 2^(0x08 * 0x16)

=> target = 0x03a30c * 2^0xB0

which in decimal is:

=> target = 238,348 * 2^176

CPU MINING

A block is valid if condition is true

```
while (1){
    HDR[kNoncePos]++;
    IF (SHA256(SHA256(HDR)) < max(DIFFICULTY)/ DIFFICULTY)
        return;
}
```

two hashes

Throughput on a high-end PC = 2 **GHz** ≈ $\mathbf{2^{32}}$ Hash/s

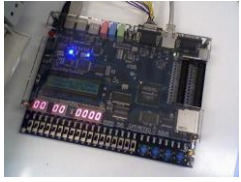
500,000+ years to find a block today!

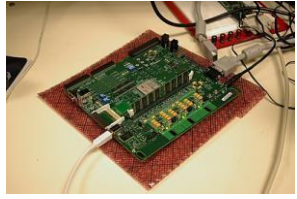
GPU MINING

- GPUs designed for high-performance graphics
  - high parallelism
  - high throughput
- First used for Bitcoin in October 2010

GPU MINING RIG

FPGA MINING





- **F**ield **P**rogrammable **G**ate **A**rea
- First used for Bitcoin in June 2011
- Implemented in Verilog

FPGA MINING

ASIC MINING

BITMAIN

IN STOCK

BITMAIN ANTMINER S19 PRO - 110TH/S

SKU: ANTMINER S19 PRO

$4600.00

IN STOCK

268 SOLD / LIMIT 5 PER CUSTOMER

QUANTITY

- 1 +

Pre-Order Terms: This is a pre-order. 28nm ASIC bitcoin mining hardware products are shipped according to placement in the order queue, and delivery may take 3 months or more after order. All sales are final.

THE LEOPARD

DETAILS :

- **2,5 TH/s**
- Dimensions:
  15" x 13.3" x 13.7"
  (38cm x 34cm x 35cm)
- 28nm ASIC technology
- Silent Cooling
- In-built WiFi Connection (without Antenna)
- Less than 750 watt (0.3 per GH)
- 1 Year Guarantee

- $ 5.800

COMES WITH :

1. Power Supply
2. Free Remote Power Outlet & Smartphone App
3. Free User Guide
4. Free Personal Assistance for Setup

SHIPPING :

- Worldwide, Express
- Included in the price
- Available:
  100 Units: Shipping April (Week 3)

ASIC MINING

- Special purpose
  - less than 10x performance improvement expected
- Designed to be run constantly for life
- Require significant expertise, long lead-times
- Perhaps the fastest chip development ever!

PROFESSIONAL MINING CENTERS

Needs:

- cheap power
- good network
- cool climate

BitFury mining center, Republic of Georgia

EVOLUTION OF MINING

CPU

GPU

FPGA

ASIC

gold pan

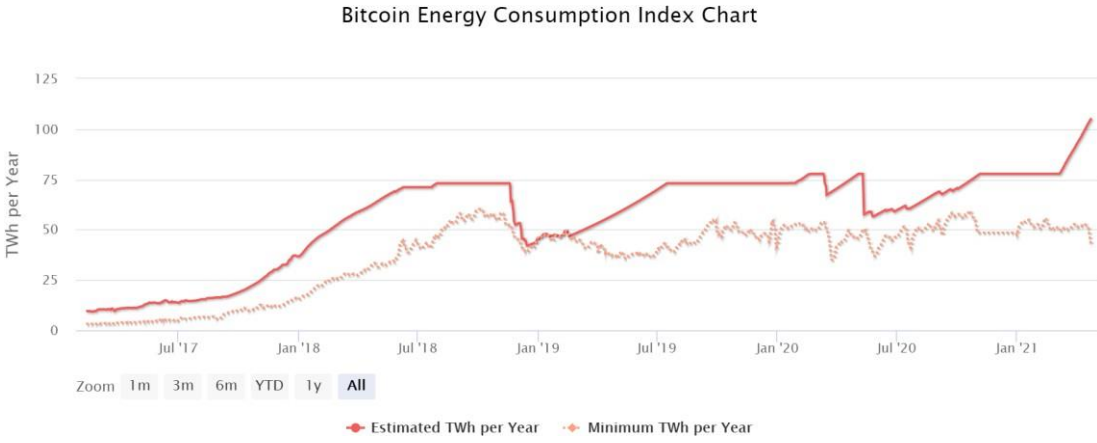
sluice box

placer mining

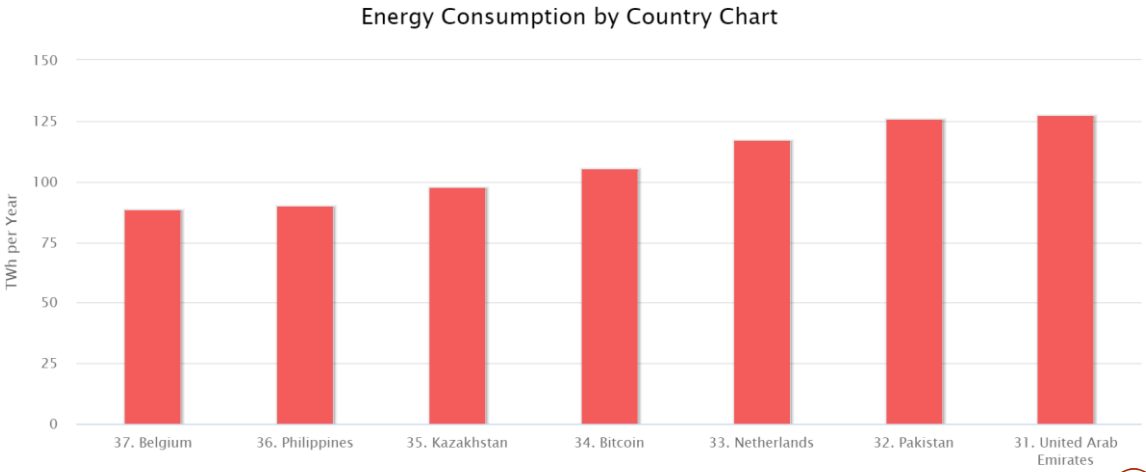
pit mining

MINING

BITCOIN ENERGY CONSUMPTION



BITCOIN ENERGY CONSUMPTION



MINING PROFITABILITY

Currency BTC ETH ETC XMR ZEC DASH LTC

Calculated for
1 BTC = $ 49,552.19

Hashing Power
110 TH/s

Power consumption (w)
3250

Cost per KWh ($)
0.01

Pool Fee (%)
1

PROFIT RATIO PER DAY
3,633%

PROFIT PER MONTH
$ 850.32

Day	Profit per day $ 28.34 (Pool Fee $ 0.2942)	Mined/day Ƀ 0.0005937	Power cost/Day $ 0.7800
Week	Profit per week $ 198.41 (Pool Fee $ 2.06)	Mined/week Ƀ 0.004156	Power cost/Week $ 5.46
Month	Profit per month $ 850.32 (Pool Fee $ 8.83)	Mined/month Ƀ 0.01781	Power cost/Month $ 23.40
Year	Profit per year $ 10.35 k (Pool Fee $ 107.38)	Mined/year Ƀ 0.2167	Power cost/Year $ 284.70

MINING UNCERTAINTY

- Being a small miner
- Example: Antminer S19 pro
- Cost: ~ USD 4,600
- Hash power: 110 TH/s
  Fraction of total hash rate = $110/145{,}000{,}000 \approx 7.6 \times 10^{-7}$
  Expected time to find a block: ~25 years!

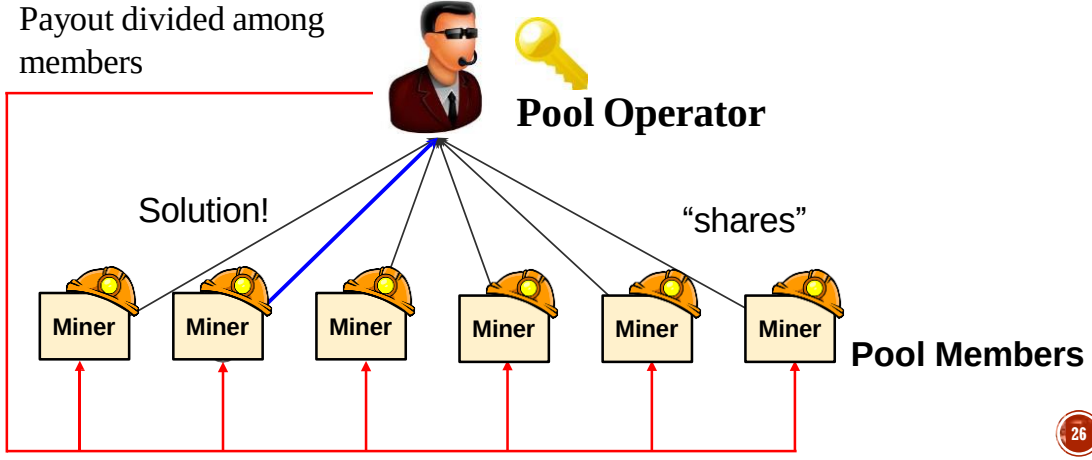
MINING POOLS

- Goal: pool participants all attempt to mine a block with the same coinbase recipient
  - send money to key owned by pool manager

- Distribute revenues to members based on how much work they have performed
  - minus a cut for pool manager

MINING SHARES

- Idea: Prove work with near-valid blocks (shares)



Pool Manager

prev:	H( )
mrkl_root:	H( )
nonce:	0x7a83
hash:	0x0000

coinbase:
25→pool

0x00000000000a877902e...

0x000000000001e8709ce...

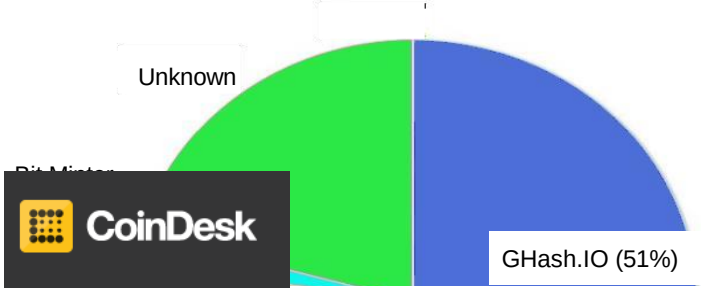
0x00000000000490c6b00...

0x0000000000007313f89...

0x0000000000000003f89...

0x0000000000045a1611f...

MINING POOLS



June 12, 2014

GHash.IO large mining pool crisis

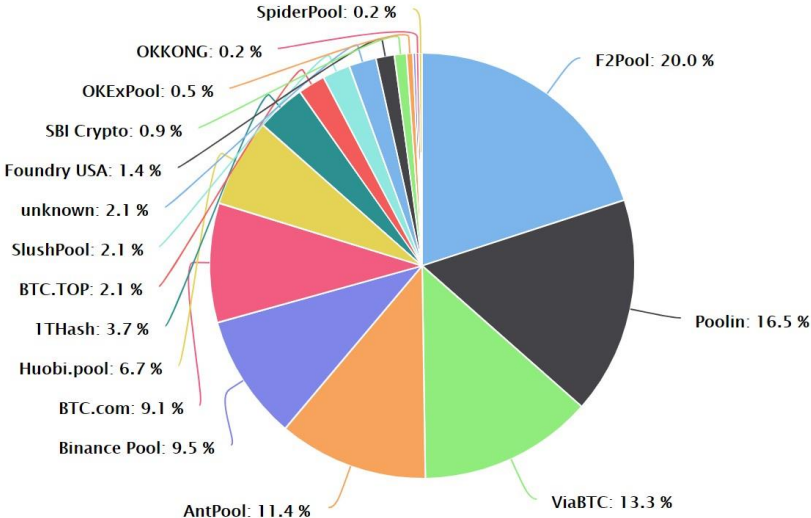
CoinDesk

MINING • NEWS

GHash Commits to 40% Hashrate Cap at Bitcoin Mining Summit

Stan Higgins | Published on July 16, 2014 at 18:40 GMT

MINING POOLS



MINING POOLS

	Pool	Hashrate Share	Hashrate	Blocks Mined	Empty Blocks Count	Empty Blocks Percentage	Avg. Block Size (Bytes)	Avg. Tx Fees Per Block (BTC)	Tx Fees % of Block Reward
0	NETWORK	100.00 %	144.77 EH/s	430	3	0.70 %	1,315,035	1.55783701	24.93 %
1	F2Pool	20.00 %	28.95 EH/s	86	0	0.00 %	1,322,179	1.52945747	24.47 %
2	Poolin	16.51 %	23.90 EH/s	71	1	1.41 %	1,300,951	1.58942627	25.43 %
3	ViaBTC	13.26 %	19.19 EH/s	57	1	1.75 %	1,299,086	1.50795192	24.13 %
4	AntPool	11.40 %	16.50 EH/s	49	0	0.00 %	1,319,934	1.59100892	25.46 %
5	Binance Pool	9.53 %	13.80 EH/s	41	0	0.00 %	1,320,313	1.46012748	23.36 %
6	BTC.com	9.07 %	13.13 EH/s	39	0	0.00 %	1,319,946	1.66646046	26.66 %
7	Huobi.pool	6.74 %	9.76 EH/s	29	0	0.00 %	1,317,926	1.62328039	25.97 %
8	1THash	3.72 %	5.39 EH/s	16	0	0.00 %	1,360,034	1.62348409	25.98 %
9	BTC.TOP	2.09 %	3.03 EH/s	9	1	11.11 %	1,117,161	1.41602713	22.66 %
10	SlushPool	2.09 %	3.03 EH/s	9	0	0.00 %	1,308,928	1.38203378	22.11 %