Lecture 4

All about mining

Joseph Bonneau

Recap: Bitcoin miners

Bitcoin depends on miners to:

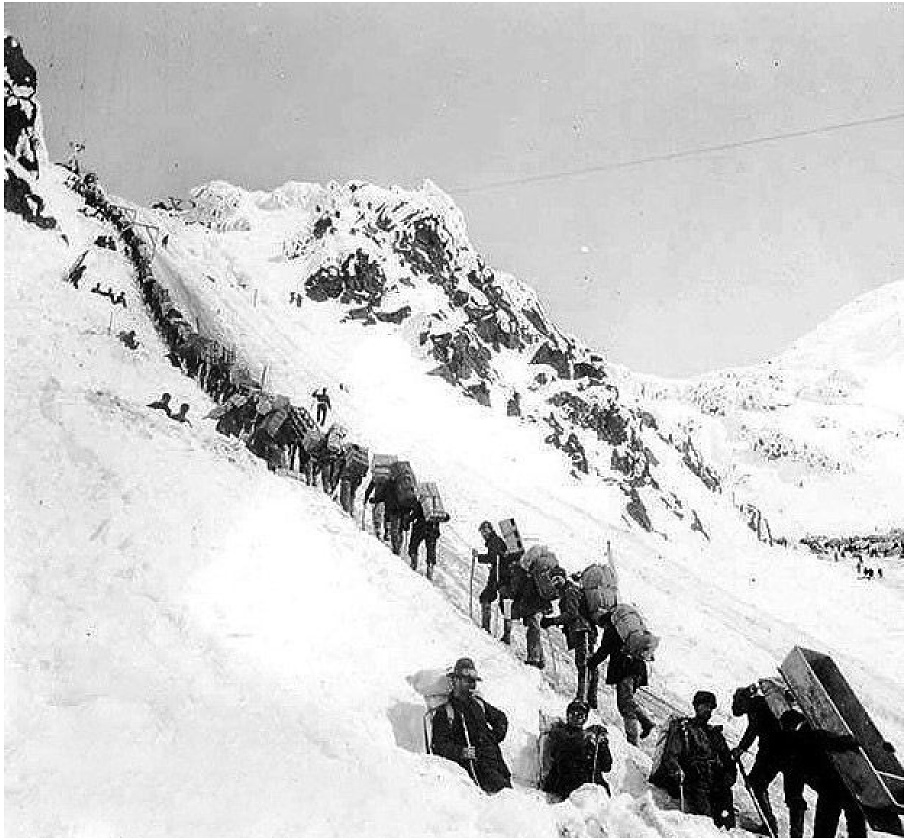
- Store and broadcast the block chain
- Validate new transactions
- Vote (by hash power) on consensus

Who are the miners?

Lecture 4.1:

The task of Bitcoin miners

It’s never easy being a miner



Chilkoot pass,
1898 Klondike gold rush

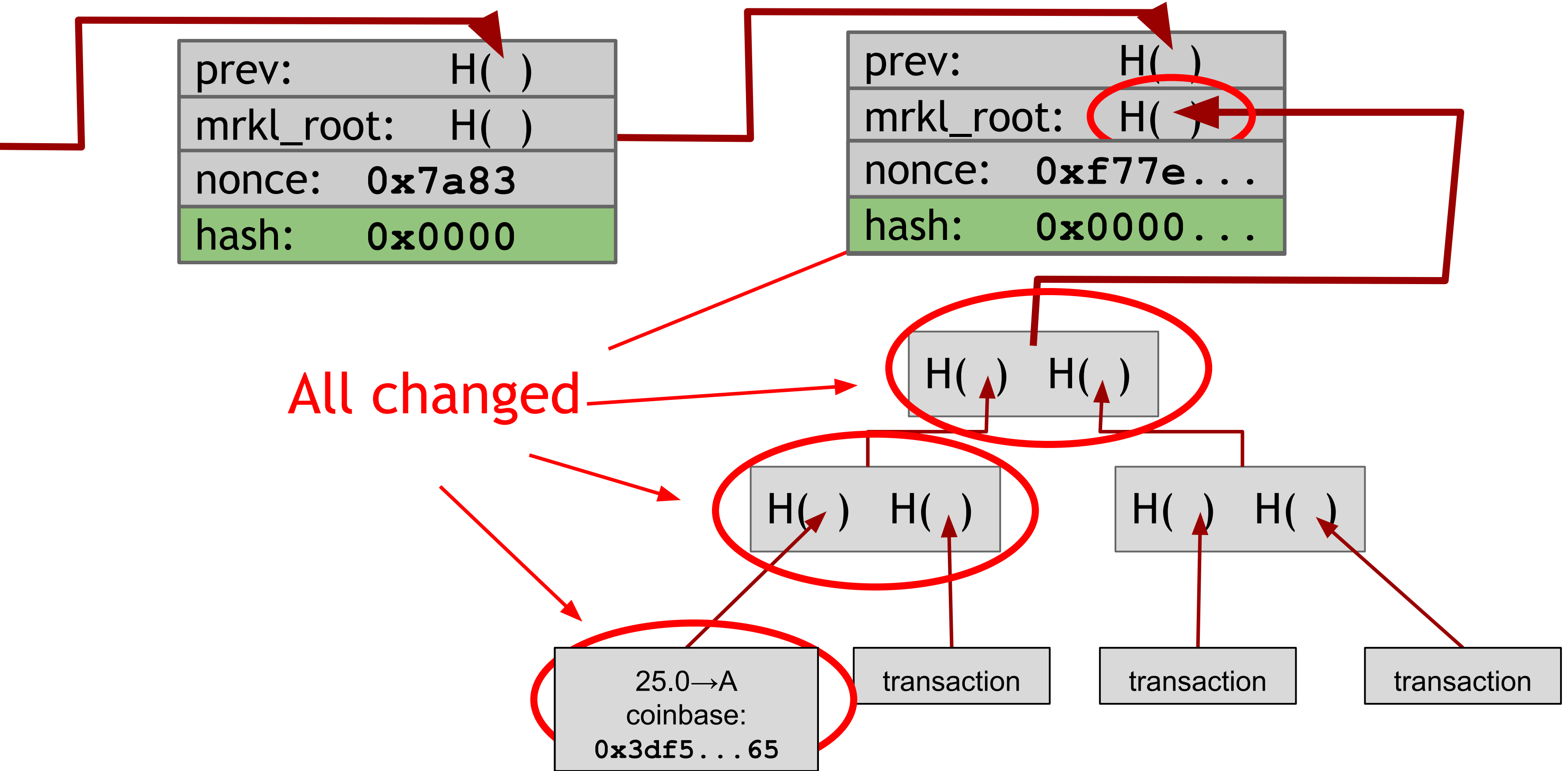
Mining Bitcoins in 6 easy steps

1. Join the network, listen for transactions
    a. Validate all proposed transactions
2. Listen for new blocks, maintain block chain
    a. When a new block is proposed, validate it

Useful to Bitcoin network

3. Assemble a new valid block
4. Find a nonce to make your block valid
5. Hope everybody accepts your new block
6. Profit!

Finding a valid block



Mining difficulty (2016-05-29)

256 bit "target"

0000000000000000058436000000000000000000000000000000000000000000

69+ leading zero bits required

Network hash rate = **1,432,691 TH/s**

Number of blocks tried per 10 min.

$2^{69.6}$ = **903,262,006,880,187,187,200**

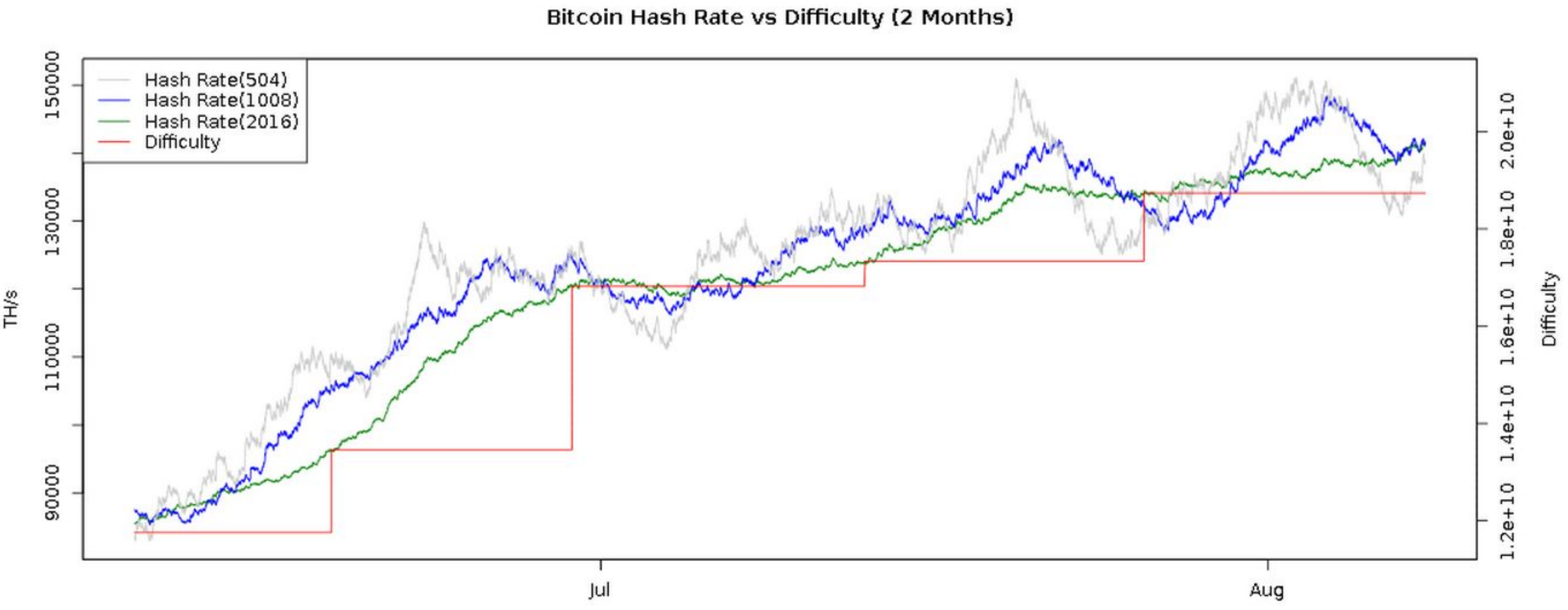
Setting the mining difficulty

Every two weeks, compute:

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

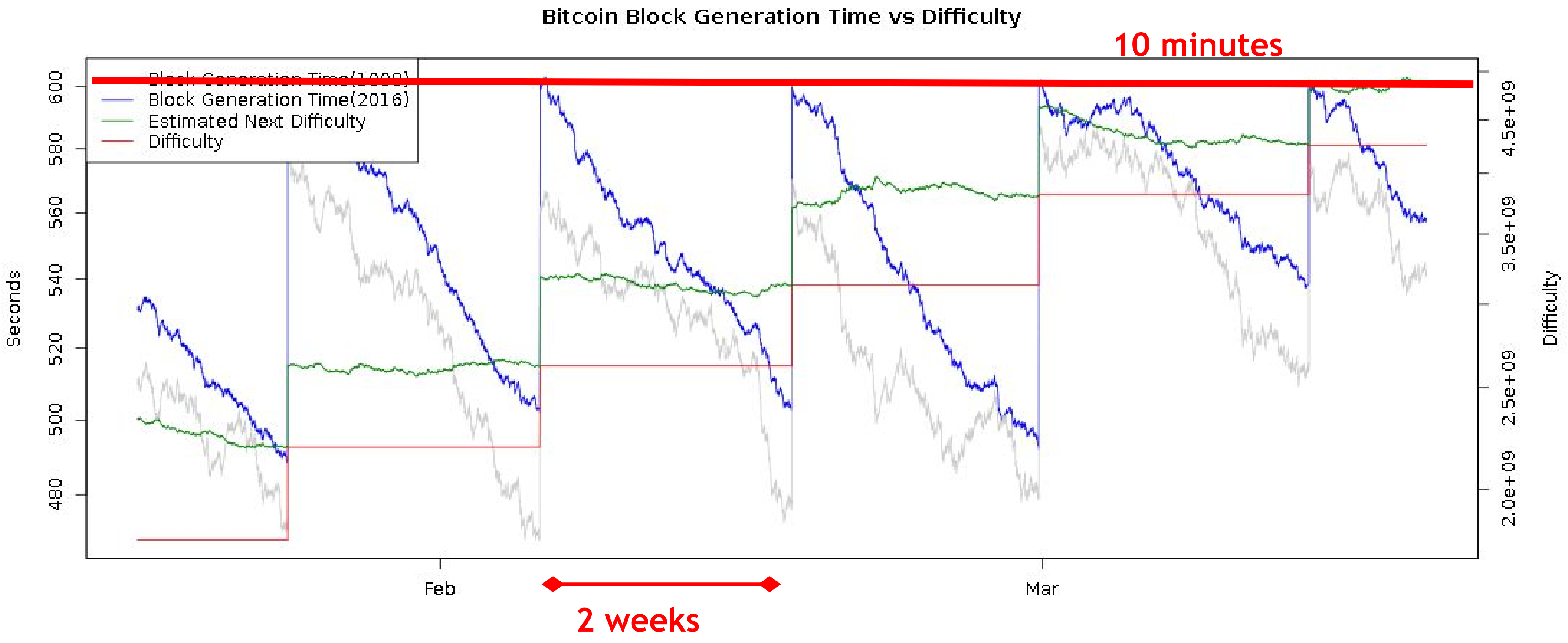
Expected number of blocks in 2 weeks at 10 minutes/block

Mining difficulty over time



bitcoinwisdom.com

Time to find a block



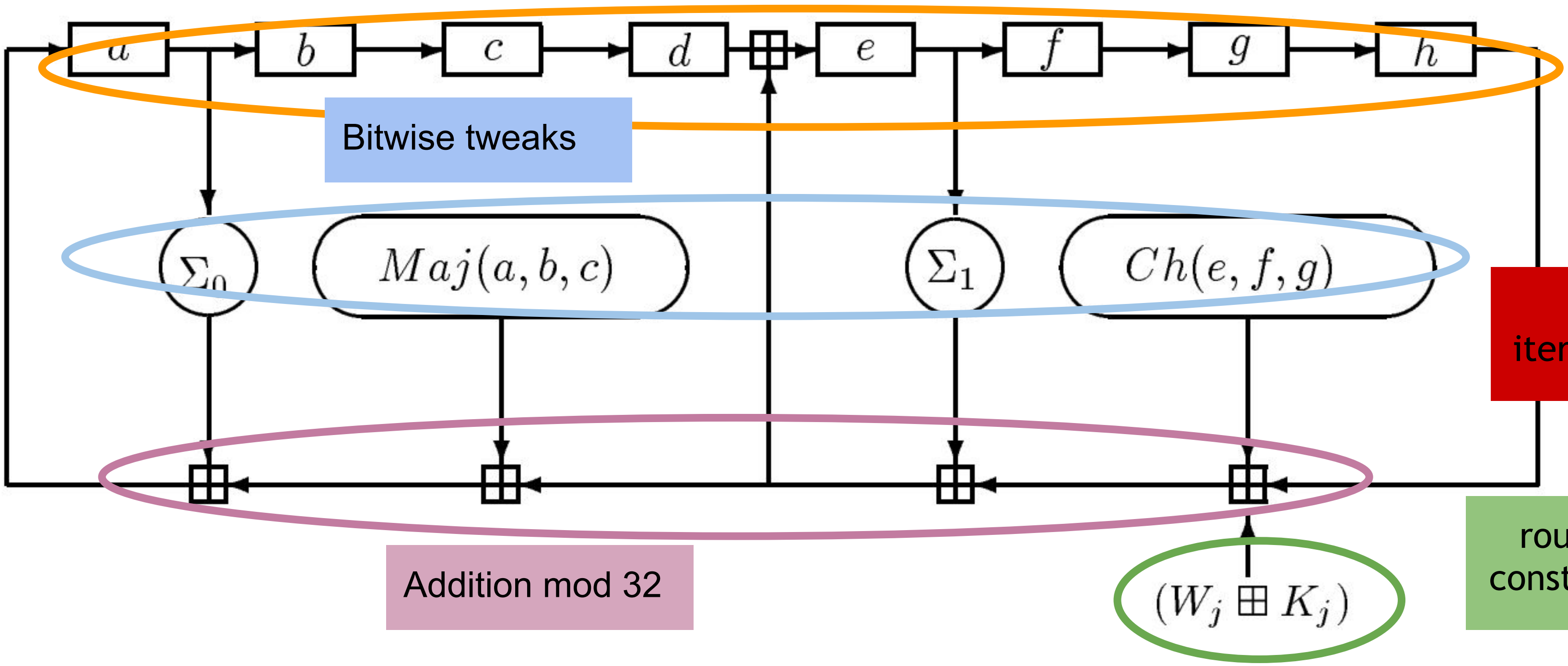
bitcoinwisdom.com

Lecture 4.2:

Mining hardware (Bitcoin)

SHA-256 in more depth

256-bit state



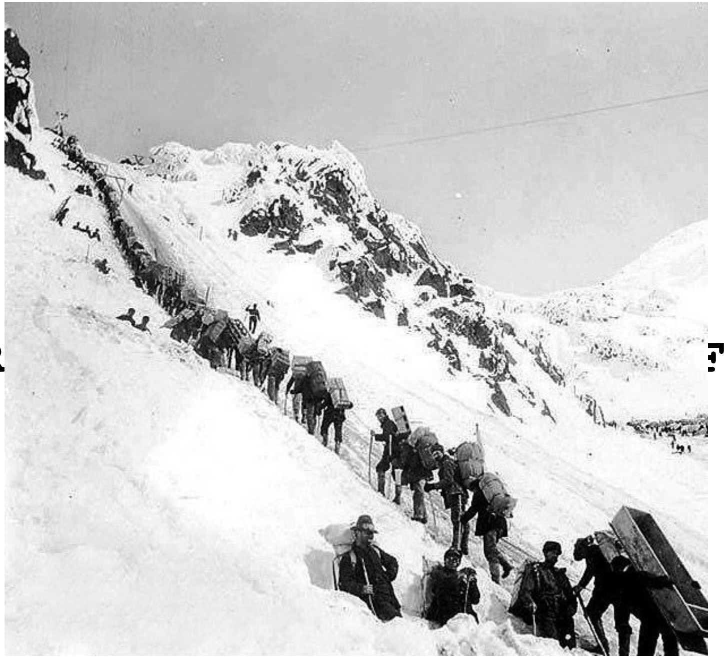
64 iterations

round constants

CPU mining

```
while (1){
    HDR[kNoncePos]++;
    IF (SHA256(SHA256(HDR                    FICULTY)
        return;
}
```

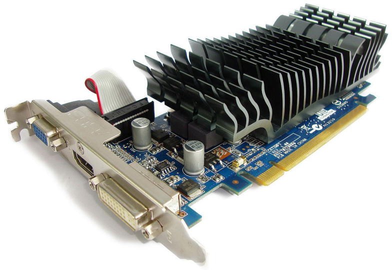
two hashes



Throughput on a high-end PC = 10-20 MHz ≈ 2^{24}

>2 million years to find a block today!

GPU mining



- GPUs designed for high-performance graphics
  - high parallelism
  - high throughput
- First used for Bitcoin ca. October 2010
- Implemented in OpenCL
  - Later: hacks for specific cards

GPU mining advantages

- easily available, easy to set up
- parallel ALUs
- bit-specific instructions
- can drive many from 1 CPU
- can overclock!

“Effective throughput”

Observation: *some* errors are okay (may miss a valid block)

Effective throughput: throughput × success rate

Worth over-clocking by 50% with 30% errors!

Source:
LeonardH,
cryptocurrencies
talk.com

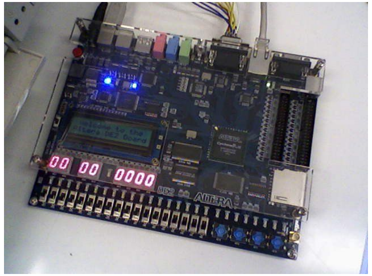
GPU mining disadvantages

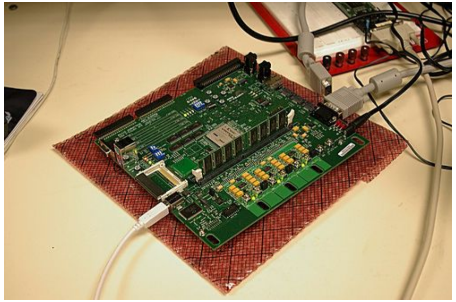
- poor utilization of hardware
- poor cooling
- large power draw
- few boards to hold multiple GPUs

Throughput on a good card = 20-**200 MHz** ≈ **2^{27}**

≈**17,000 years** to find a block w/100 cards!

FPGA mining





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

FPGA mining advantages

- higher performance than GPUs
  - excellent performance on bitwise operations
- better cooling
- extensive customisation, optimisation

Bob Buskirk, thinkcomputers.org

FPGA mining disadvantages

- higher power draw than GPUs designed for
  - frequent malfunctions, errors
- poor optimization of 32-bit adds
- fewer hobbyists with sufficient expertise
- more expensive than GPUs
- marginal performance/cost advantage over GPUs

Throughput on a good card = 100-**1000 MHz** ≈ **2^{30}**

2,000 years to find a block w/100 boards!

Bitcoin ASICs

- special purpose
  - approaching known limits on feature sizes
  - 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!

Market dynamics (2013/2014)

- Most boards obsolete within 3-6 months
  - Half of profits made in first 6 weeks
- Shipping delays are devastating to customers
- Most companies require pre-orders
- Most individual customers should have lost...

But... rising prices saved them!

Bitcoin ASICs

TerraMiner™ IV – 2TH/s Networked ASIC Miner

$5,999

Shipping June 2014

300 GH Bitcoin Mining Card

The Monarch BPU 300 C

$1,497.00

Qty: 1 ADD TO CART

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 :

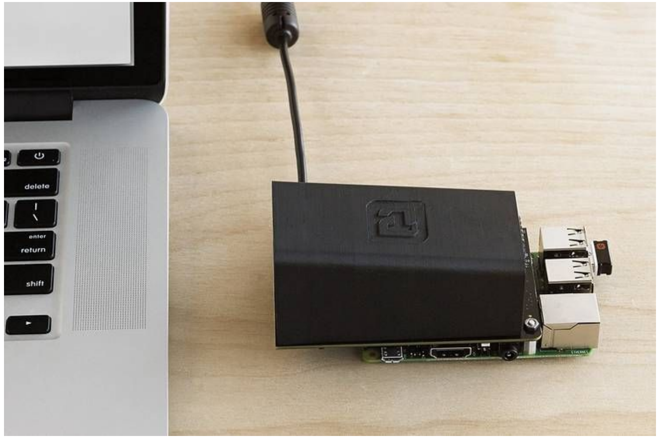
1. Power Supply
2. Free Remote Power Outlet & Smartphone App
3. Free User Guide
4. Free Personal Assistance for Setup

SHIPPING :

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

Current hardware (2015/2016)

	AntMiner S7	Avalon6	SP20 Jackson
			
Advertised Capacity:	4.73 Th/s	3.5 Th/s	1.3-1.7 Th/s
Power Efficiency:	0.25 W/Gh	0.29 W/Gh	0.65 W/Gh
Weight:	8.8 pounds	9.5 pounds	20 pounds
Guide:	Yes	No	Yes
Price:	$595.99	$750.95	$248.99
	Buy from amazon.com	Buy from amazon.com	Buy from amazon.com
Appx. BTC Earned Per Month:	0.3994	0.2955	0.1593



Case study: Ant Miner S7

- First shipped 2015
- 4.7 TH/s
- 1210 W
- Cost: US$619

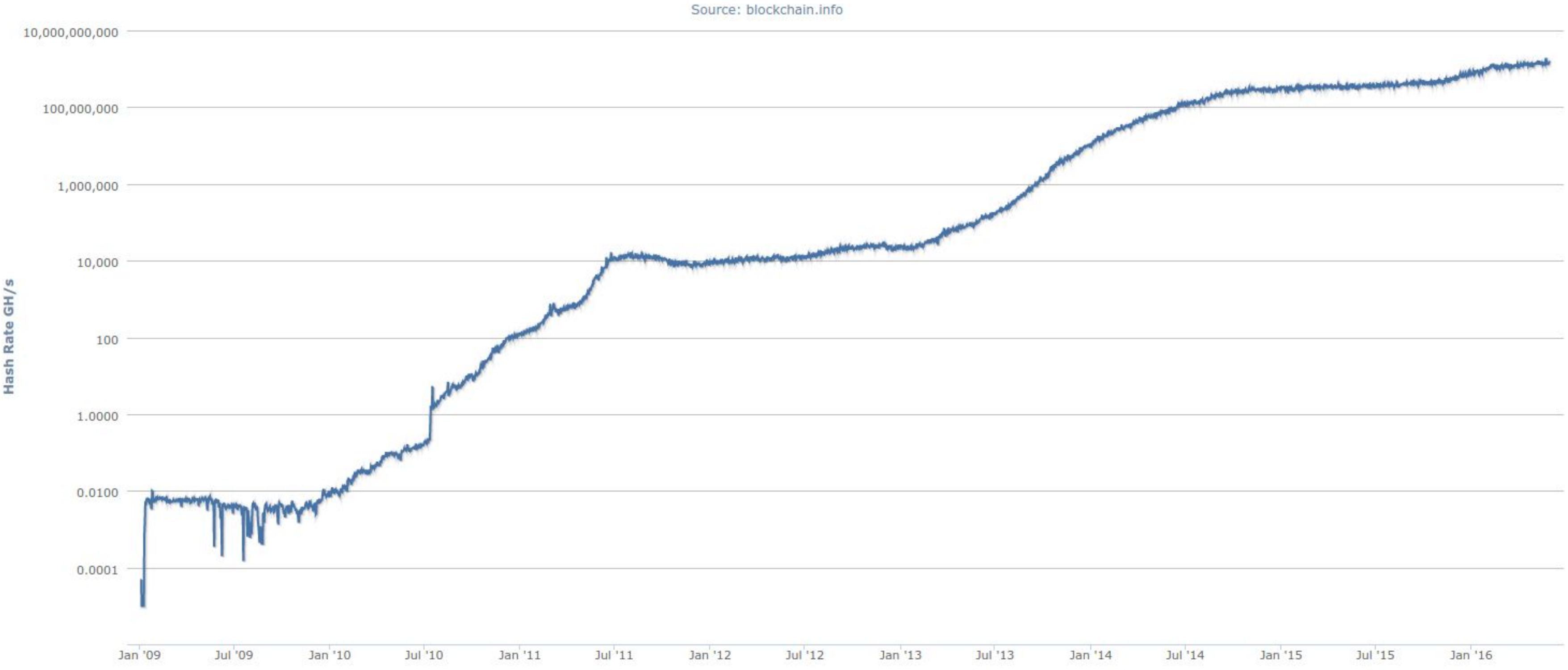
Still, **4.8 years** to find a block!

Market dynamics (2015/2016)

- Growth rate leveling off
- Mining hardware approaching fab. limits
- Mining becoming professionalized

[Taylor 2013]
Bitcoin and the Age of Bespoke Silicon.

Market dynamics (2015/2016)



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

Philosophical questions

- Can small miners stay in the game?
- Do ASICs violate the original Bitcoin vision?
- Would we be better off without ASICs?

Lecture 4.3:

Energy consumption & ecology

Energy aspects of Bitcoin mining

- **Embodied energy:** used to manufacture mining chips & other equipment
  - should decrease over time
  - returns to scale
- **Electricity:** used to perform computation
  - should increase over time
  - returns to scale
- **Cooling:** required to protect equipment
  - costs more with increased scale!

Estimating energy usage: top-down

- Each block worth approximately **US$15,000**
- Approximately **$25/s** generated
- Industrial electricity (US): **$0.03/MJ**
    - **$0.10/kWh**

Upper bound on electricity consumed:

900 MJ/s = **900 MW**

Estimating energy usage: bottom-up

- Best claimed efficiency: **0.25 GHz/W**
- Network hash rate: **150,000,000 GHz**
- (excludes cooling, embodied energy)

Lower bound on electricity consumed:

375 MW

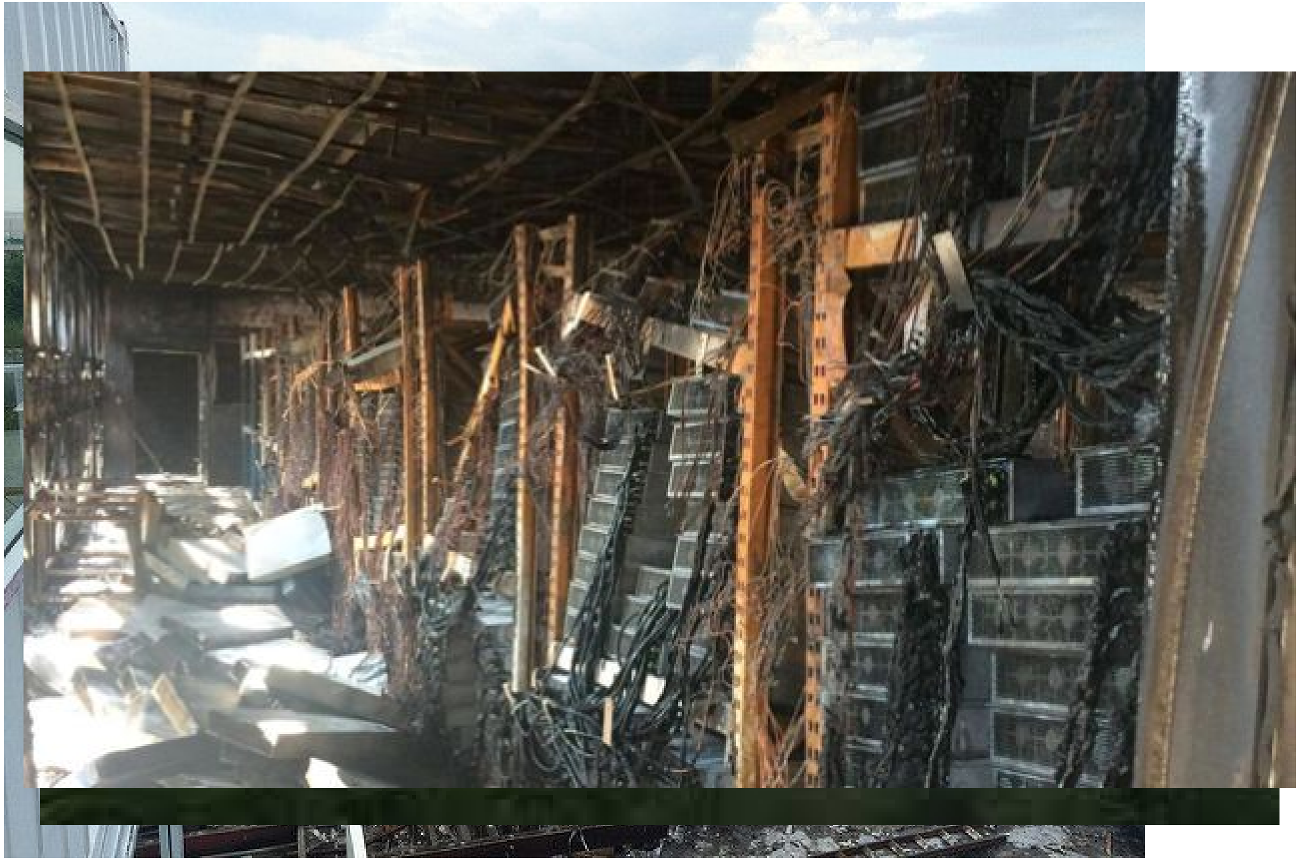
How much is a MW?

Three Gorges Dam = 10,000 MW
typical hydro plant ≈ 1,000 MW

Kashiwazaki-Kariwa
nuclear power plant = 7,000 MW
typical nuclear plant ≈ 4,000 MW

major coal-fired plant ≈ 2,000 MW

Cooling costs matter as well!



All payment systems require energy

Data furnaces

- ASICs are ~as efficient as electric heaters
- Why not install mining rigs as home heaters?
- Challenges:
  - Ownership/maintenance model
  - Gas heaters still at least 10x more efficient
  - What happens in summer?

Open questions

- Will Bitcoin drive out electricity subsidies?
- Will Bitcoin require guarding power outlets?
- Can we make a currency with no proof-of-work?

Lecture 4.4:

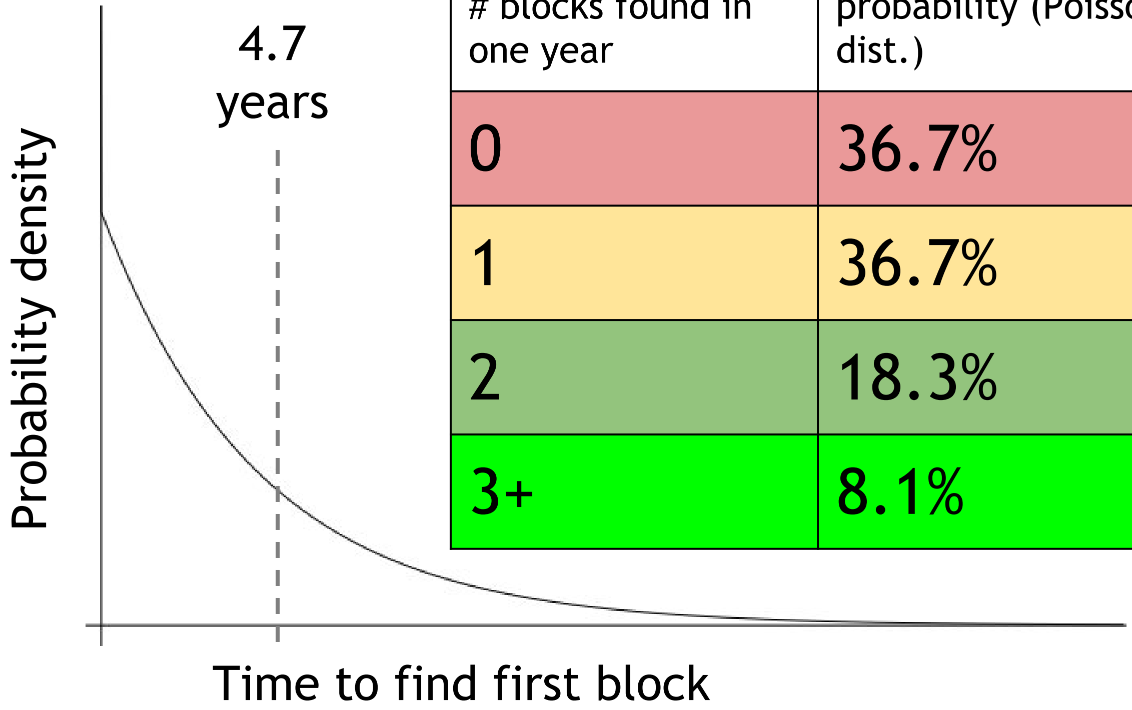
Mining pools

Economics of being a small miner

Ant Miner S7

- Cost: ≈US$619
- Expected time to find a block: ≈4.7 years
- Expected revenue: ≈$88/month
- Electricity cost:
  - $71/month (USA)
  - $140/month (EU)

Mining uncertainty (4.7 year mean)



# blocks found in one year	probability (Poisson dist.)
0	36.7%
1	36.7%
2	18.3%
3+	8.1%

Risk aversion

vs.

guaranteed

50% chance

Expectation(Utility) ≠ Utility(Expectation)

Idea: could small miners pool risk?

Mining pools

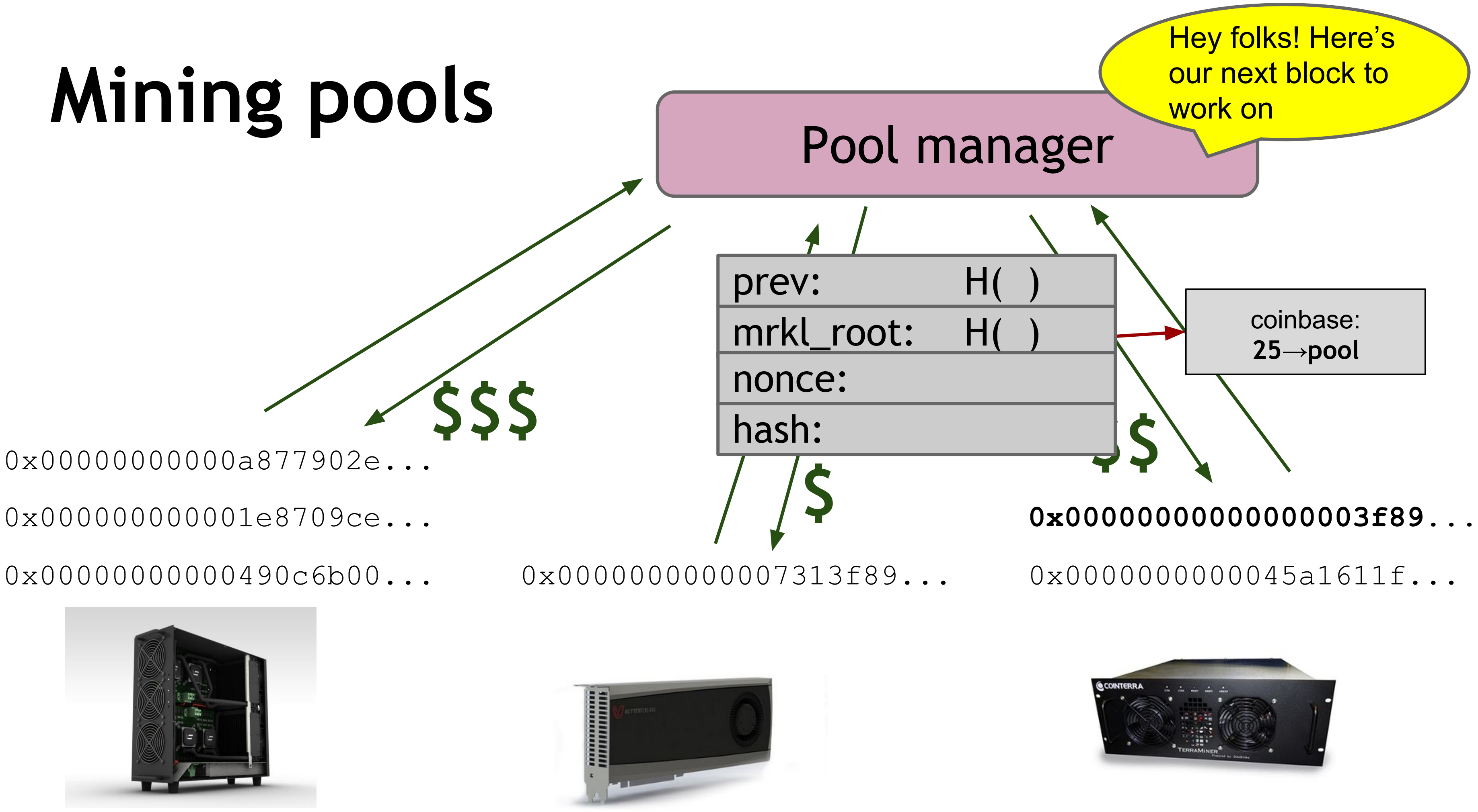
- **Goal:** pool participants all attempt to mine a block with the same coinbase recipient
  - send money to key owned by pool manager
- Distribute revenues to members based on how much work they have performed
  - minus a cut for pool manager

How do we know how much work members perform?

Show work with near-valid blocks (shares)

4AA087F0A52ED2093FA816E53B9B6317F9B8C1227A61F9481AFED67301F2E3FB
D3E51477DCAB108750A5BC9093F6510759CC880BB171A5B77FB4A34ACA27DEDD
0000000000008534FF68B98935D090DF5669E3403BD16F1CDFD41CF17D6B474255
BB34ECA3DBB52EFF4B104EBBC0974841EF2F3A59EBBC4474A12F9F595EB81F4B
00000000002F891C1E232F687E41515637F7699EA0F462C2564233FE082BB0AF
0090488133779E7E98177AF1C765CF02D01AB4848DF555533B6C4CFCA201CBA1
460BEFA43B7083E502D36D9D08D64AFB99A100B3B80D4EA4F7B38E18174A0BFB
000000000000000078FB7E1F7E2E4854B8BC71412197EB1448911FA77BAE808A
652F374601D149AC47E01E7776138456181FA4F9D0EEDD8C4FDE3BEF6B1B7ECE
78552640214 3A291CFD60DA09CC80DD066BC723FD5FD20F9B50D614313529AF3
000000000041EE59343468 6000AF77F54CDE839A6CE30957B14EDEC10B15C9E5
9C20B06B01A0136F192BD48E0F372A4B9E6BA6ABC36F02FCED22FD9780026A8F

Mining pools



Mining pool variations

- **Pay per share:** flat reward per share
  - Typically minus a significant fee
  - What if miners never send in valid blocks?
- **Proportional:** typically since last block
  - Lower risk for pool manager
  - More work to verify
- **Pay per-last-N-shares**
  - Minimize “pool hopping”
  - Some pool hopping still exists!

Rewards structure for pools

Goals:

- Limit risk carried by pool
- Incentivize participants to always submit blocks
- Incentivize participants to mine consistently
    - no “pool-hopping”
- Don’t discourage new participants

Impossibility result (in progress):

- No system can satisfy all these goals

[Schrijvers, Bonneau, Roughgarden, Boneh 2016]
Incentive Compatibility of Bitcoin Mining Pool Reward Functions

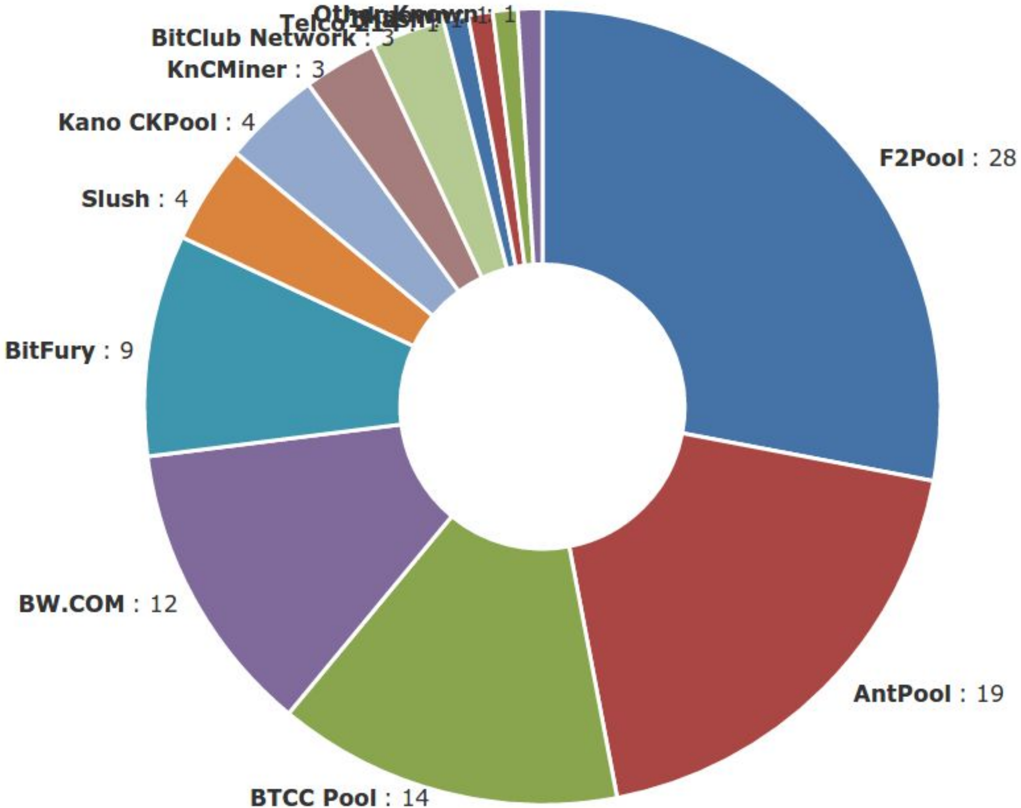
Mining pool protocols

- API for fetching blocks, submitting shares
  - Stratum
  - Getwork
  - Getblockshare
- Proposed for standardization with a BIP
- Increasingly important; some hardware support

Mining pool history

- First pools appear in late-2010
    - Back in the GPU era!
- By 2014: around 90% of mining pool-based
- June 2014: GHash.io exceeds 50%

Mining pools (May 2016)



Are mining pools a good thing?

- Pros
  - Make mining more predictable
  - Allow small miners to participate
  - More miners using updated validation software
- Cons
  - Lead to centralization
  - Discourage miners from running full nodes

Can we prevent pools?

Lecture 4.5:

Mining incentives and strategies

Game theory in one slide

Modeling strategies for interactions between rational, utility-maximizing agents

	Prisoner B stays silent (*cooperates*)	**Prisoner B betrays (*defects*)**
Prisoner A stays silent (*cooperates*)	Each serves 1 year	Prisoner A: 3 years Prisoner B: goes free
Prisoner A betrays (*defects*)	Prisoner A: goes free Prisoner B: 3 years	Each serves 2 years

Game theory poorly suited to Bitcoin

Usual assumptions:

- known set of players
- known utility functions
- synchrony

Most Bitcoin “game theory” is really unilateral optimization

Strategy space for miners

- Which transactions to include in a block
  - Default: any above minimum transaction fee
- Which block to mine on top of
  - Default: longest valid chain
- How to choose between colliding blocks
  - Default: first block heard
- When to announce new blocks
  - Default: immediately after finding them

Deviant mining strategies

Assume you control $0 < \alpha < 1$ of mining power and the remainder is “compliant”

Can you profit from a non-default strategy?

For some α, **YES**, though not observed in practice

What can you do with $\alpha > 51\%$?

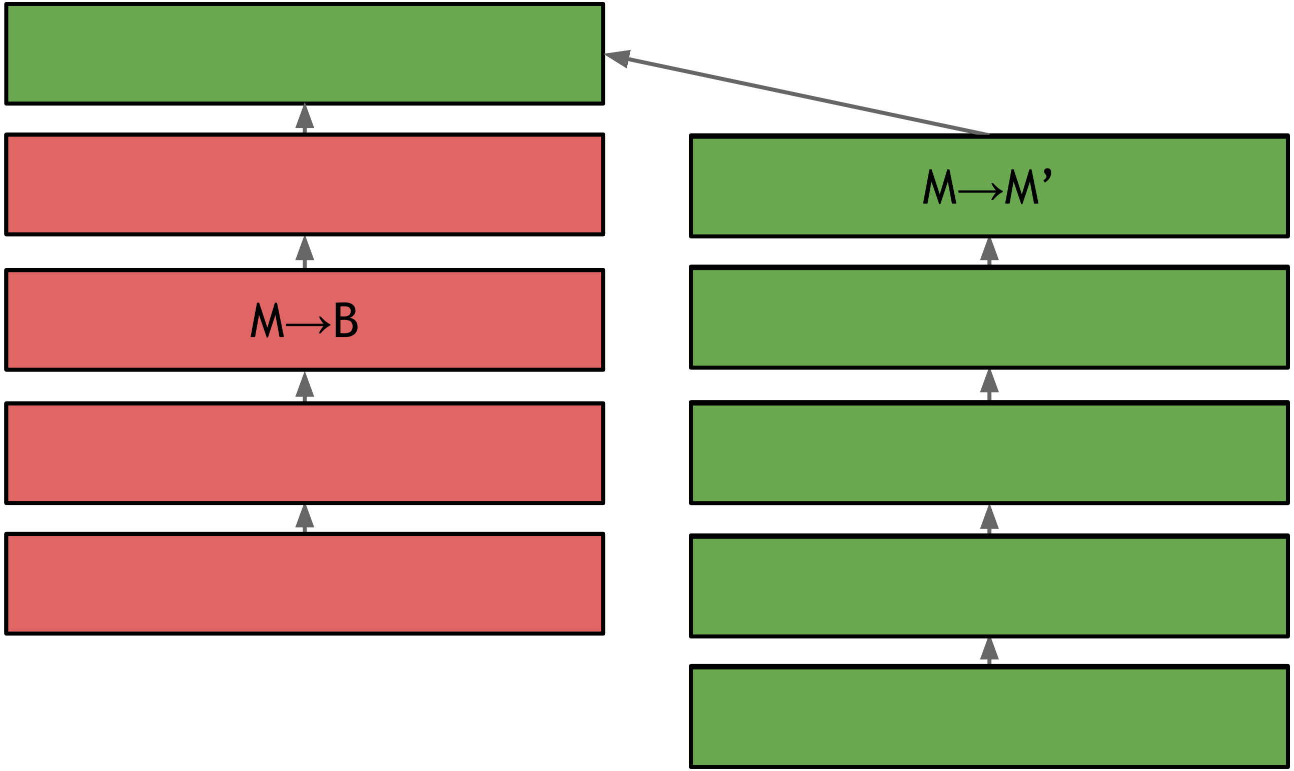
- Fork the blockchain and double-spend
  - Undermine exponential convergence

- Reject all other miners’ blocks
  - Undermine fairness

- Demand exorbitant transaction fees
  - Undermine liveness

All of these attacks are highly visible

Forking attacks



Attackers care about the exchange rate

Source: blockchain.info

Mining hardware is illiquid

- ➔ High **entry costs**
- ➔ Low **salvage value**

Result: Miners care about future exchange rate

What if you *want* to crash Bitcoin?

Goldfinger Attack

[Kroll, Davey, Felten 2013]

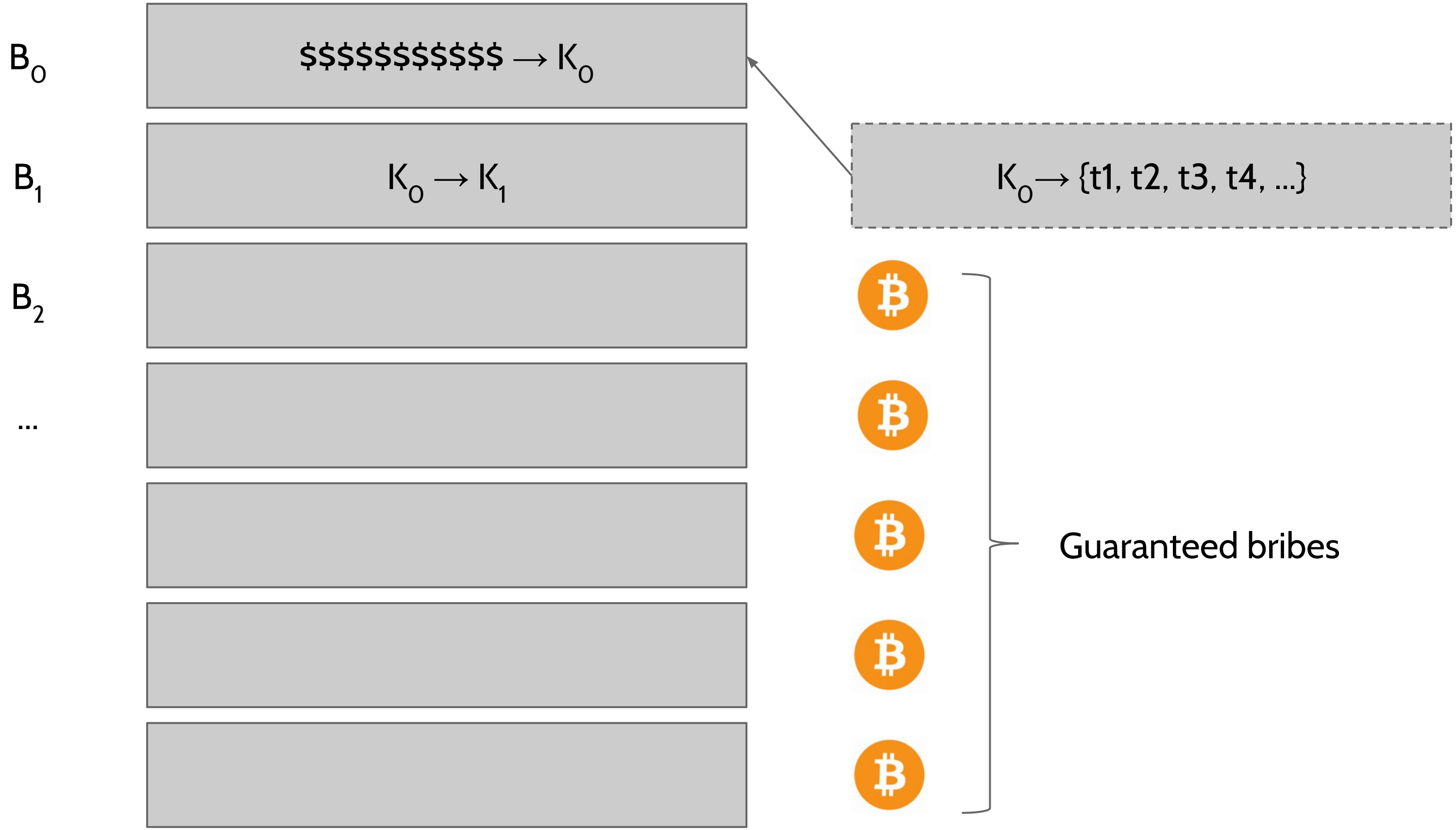
The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries

Forking attacks via bribery

- Buying $\alpha > 0.5$ is expensive. Why not rent?
- Payment techniques:
  - Out-of-band bribery
  - Run a mining pool at a loss
  - Insert large “tips” in the block chain

[Bonneau 2016]
Why buy when you can rent? Bribery attacks on Bitcoin consensus

In-band bribery possible with scripts



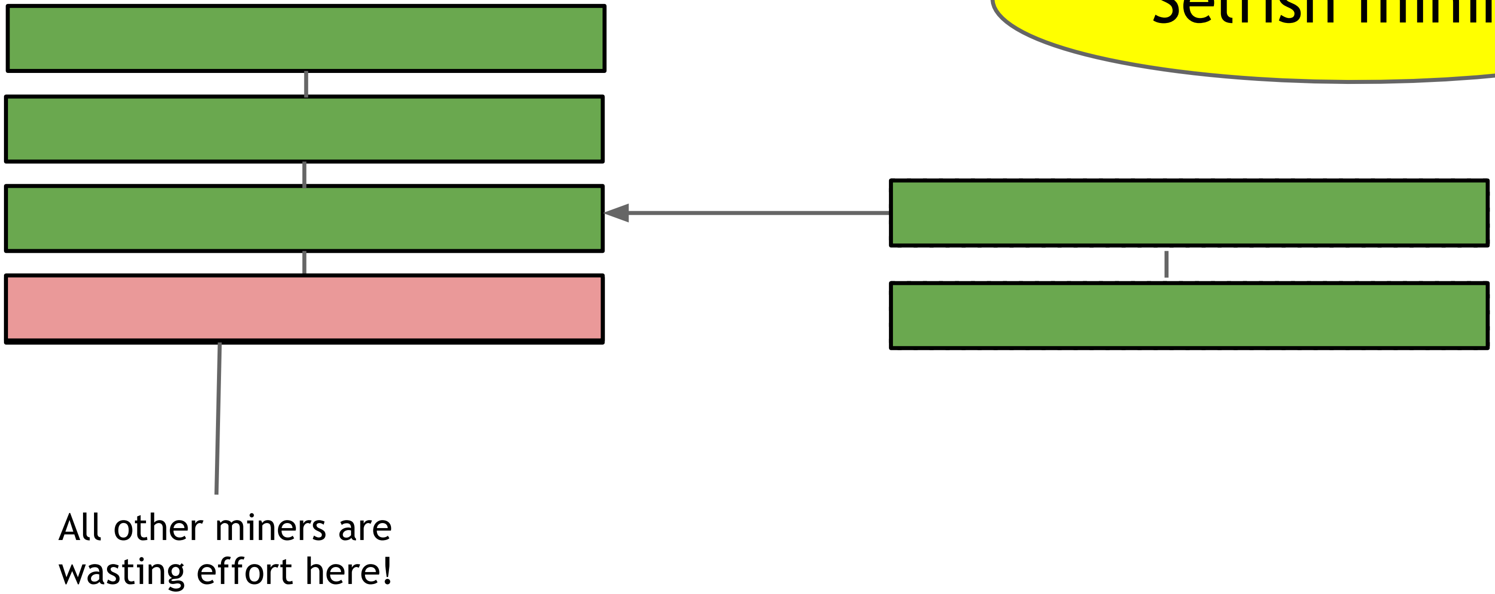
Can we do anything with α < 50%?

Surprising answer: Yes!

Temporary block-withholding attacks

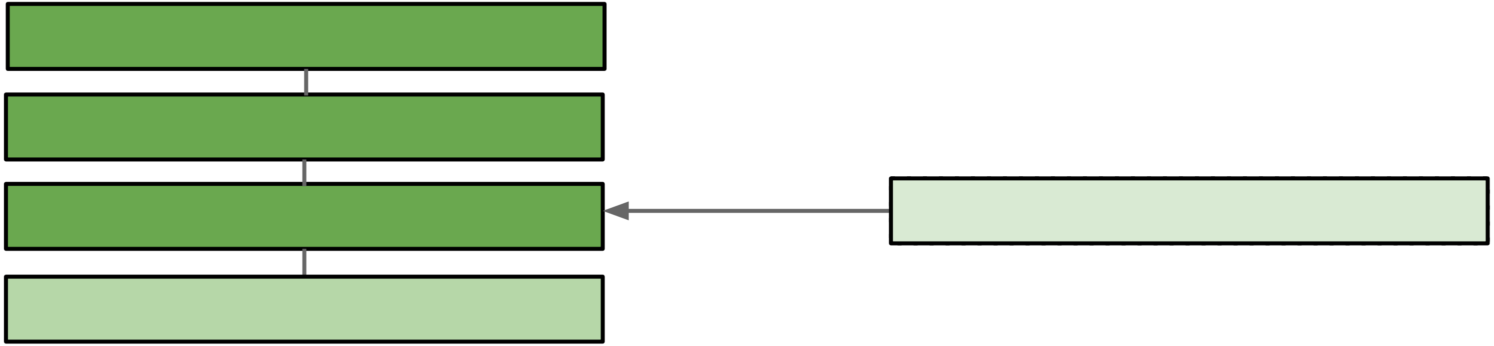
Strategy: don’t announce blocks right aw

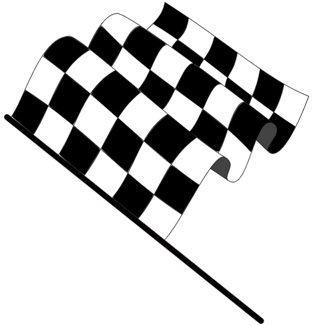
“Selfish mining”



Temporary block-withholding, take 2

What happens if a block is announced when you're ahead by 1?





Network race

Assume you win races with prob. γ

- Always withhold if $\gamma = 1$
  - Ideal network position
  - Obtainable through bribery?
- Withhold for α **> 0.25** if $\gamma > 0.5$
- Always withhold for α **> 0.33**

Surprising theoretical finding, never observed!

[Eyal, Sirer 2014]

Majority is not enough: Bitcoin mining is vulnerable.

Optimal withholding strategies

Table 4: Optimal actions (abbreviated to their initials) for an attacker with $\alpha = 0.45, \gamma = 0.5$, for states $(l_a, l_h, \cdot)$ with $l_a, l_h \leq 7$. See legend in Subsection 5.2.[10]

l_a \ l_h	0	1	2	3	4	5	6	7
0	***	*a*	***	***	***	***	***	***
1	w**	*m*	a**	***	***	***	***	***
2	w**	*mw	*m*	w**	a**	***	***	***
3	w**	*mw	*mw	wm*	w**	a**	***	***
4	w**	*mw	*mw	omw	wm*	w**	w**	a**
5	w**	*mw	*mw	*mw	omw	wm*	w**	w**
6	w**	*mw	*mw	*mw	*mw	omw	wm*	w**
7	w**	*mw	*mw	*mw	*mw	*mw	ooo	w**

[Sapirshtein, Sompolinsky, Zohar 2016]

Optimal Selfish Mining Strategies in Bitcoin

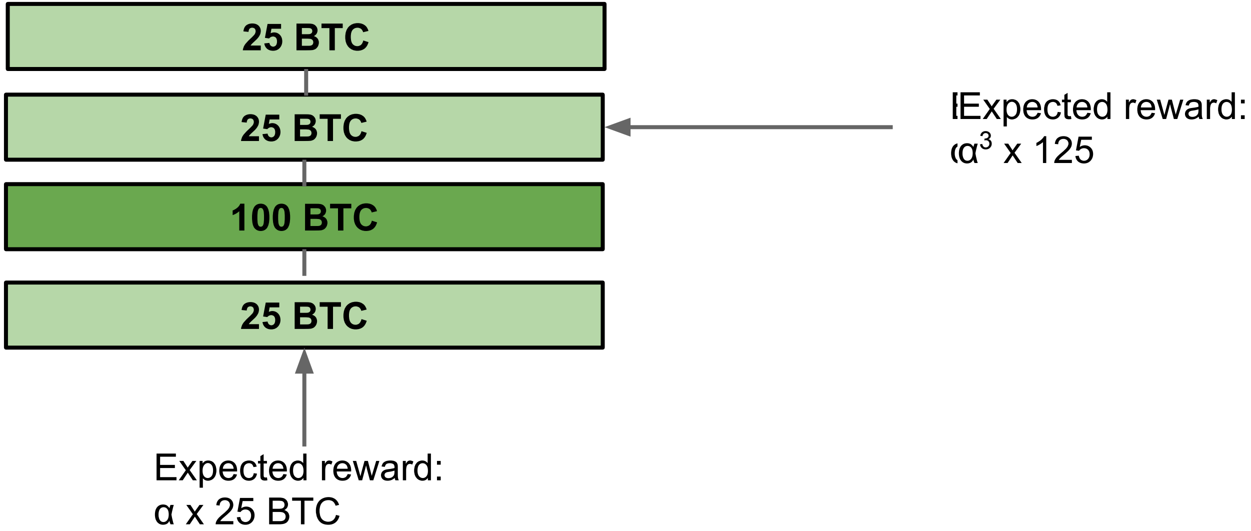
Whale mining

The Story of the 'Accidental' $137K Bitcoin Payment Just Got Very Strange

April 26, 2016 // 05:21 PM EST

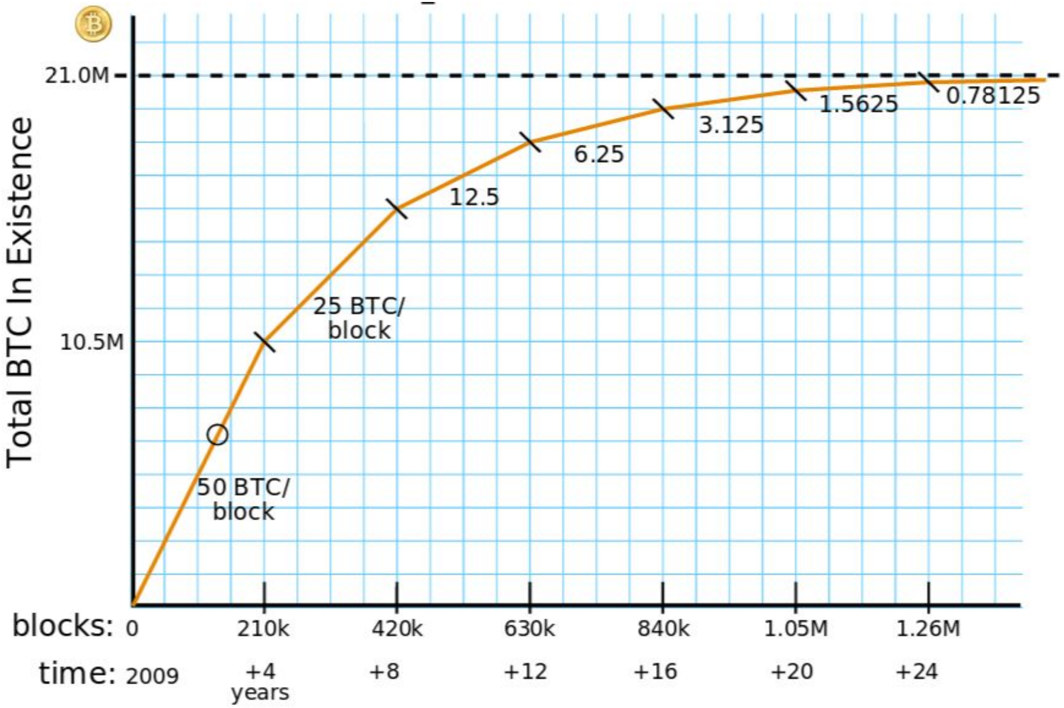
There are bad days, and then there are days when you accidentally send $137,000 worth of bitcoin to somebody with no way to retrieve it.

Risks of uneven transaction fees



Transaction fees will matter more

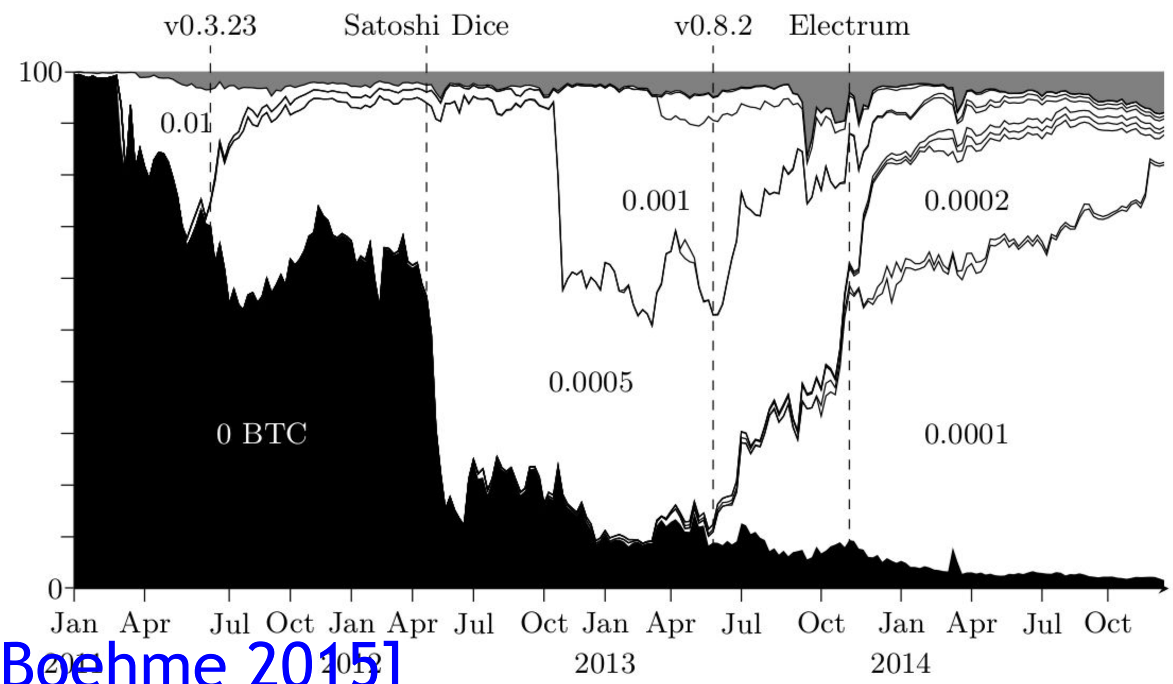
Currently, block rewards are > 99% of miner revenue. But:



Eventually, transaction fees will dominate

Courtesy:
Brian Warner

Transaction fees already increasing



[Moeser, Boehme 2015]
Trends, Tips, Tolls: A Longitudinal Study of Bitcoin Trans. Fees

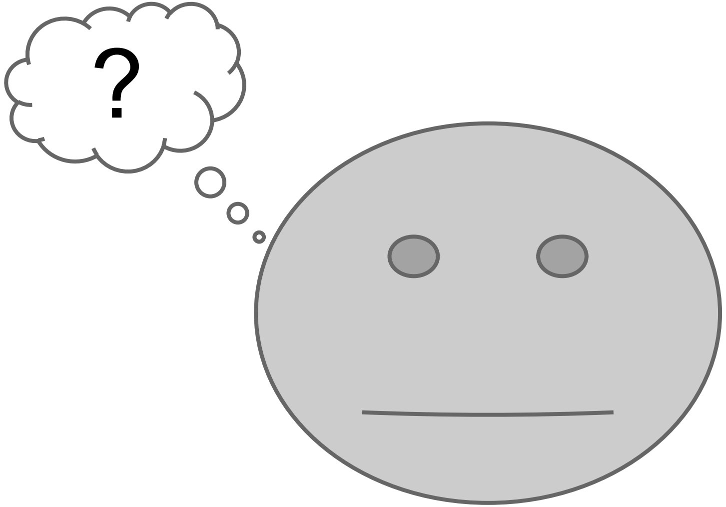
Current default policy is arbitrary

Default policy:

```
priority = sum(input_value * input_age)/size_in_bytes
```

Accept without fees if:

```
priority > 0.576
```



What will set transaction fees?

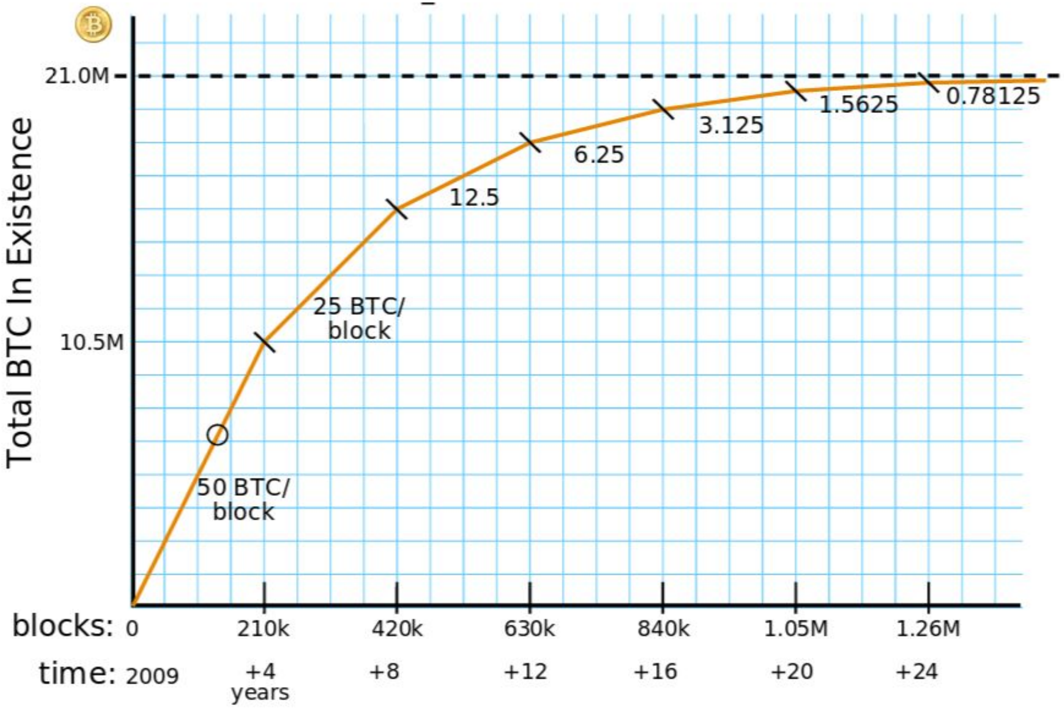
- Marginal cost of inclusion in a block?
  - $\rightarrow 0$ if block size is big enough
  - Otherwise, auction for limited space

- Cartel of miners?
  - Optimize fees x volume
  - Pressure from other currencies?

- Exogenous security requirements?
  - Not known/proven

Transaction fees will matter more

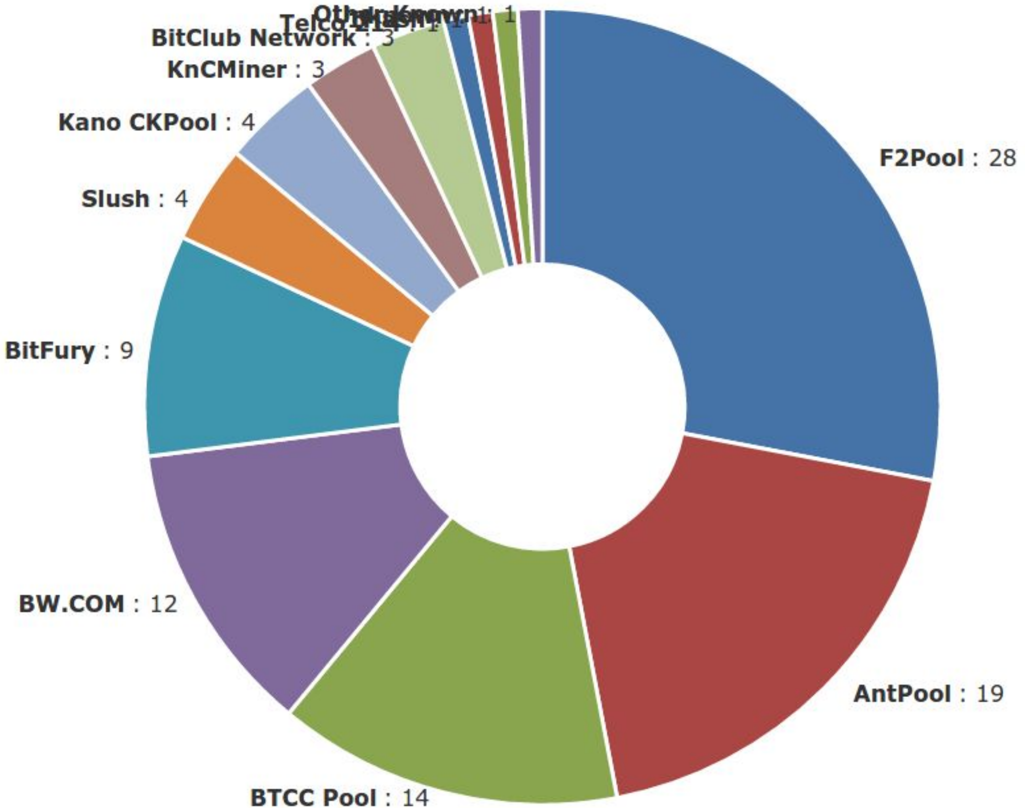
Currently, block rewards are > 99% of miner revenue. But:



Eventually, transaction fees will dominate

Courtesy:
Brian Warner

Will miners cooperate to enforce fees?



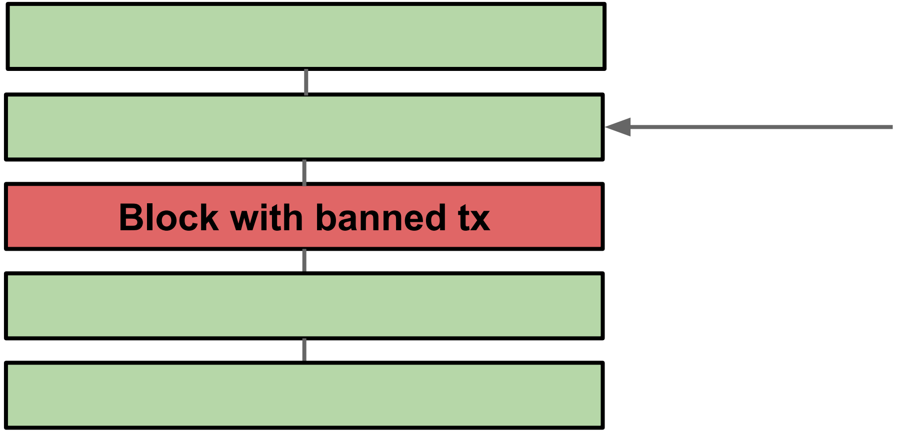
Feather-forking

Goal: blacklist/censor some addresses

Strategies:

- Announce you will try to fork if blacklisted addresses appear in a block
- Will try to make fork work until *k* blocks behind

Feather forking



Feather forker works here

Chance of success down to α^3, give up

Feather-forking

Goal: blacklist/censor some addresses

Strategies:

- Announce you will try to fork if blacklisted addresses appear in a block
- Will try to make fork work until *k* blocks behind

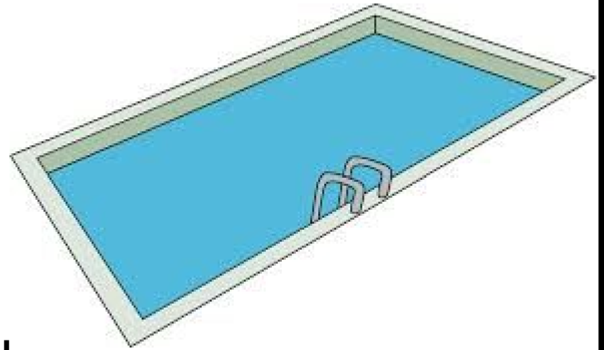
Apparent outcome:

- Blacklister will lose some mining revenue
- Others will also lose! Optimal strategy is to enforce blacklist (unless Tx fees are very high)

Mining pools may attack each other

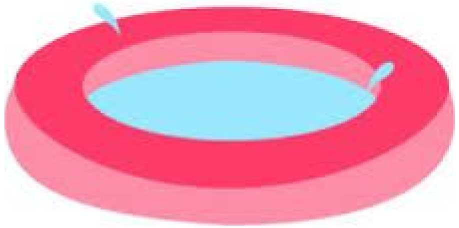
Goals:

- Increase profitability of your pool
- Increase size of your pool by damaging others

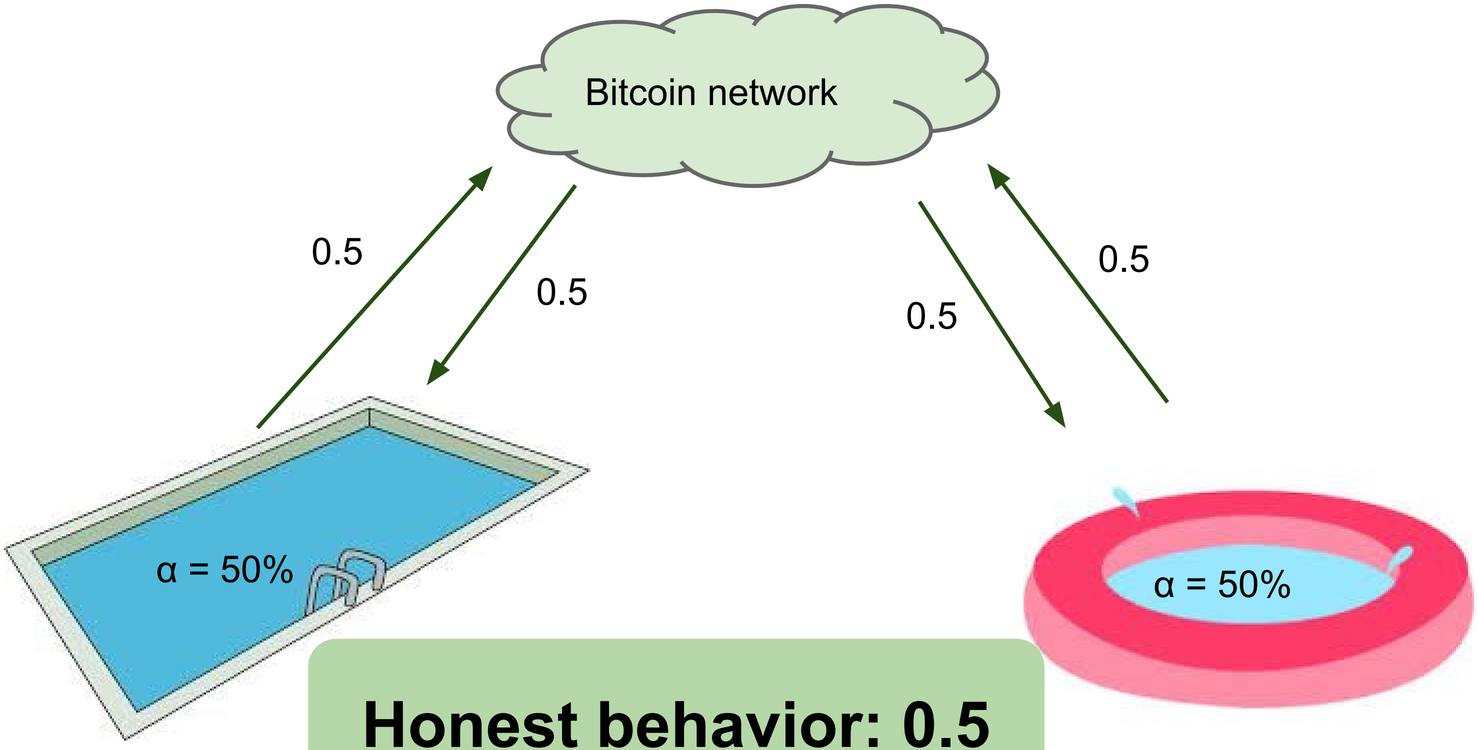


Strategies:

- Participate in rival pool but withhold valid blocks
- Denial of service on the network to delay rival pools

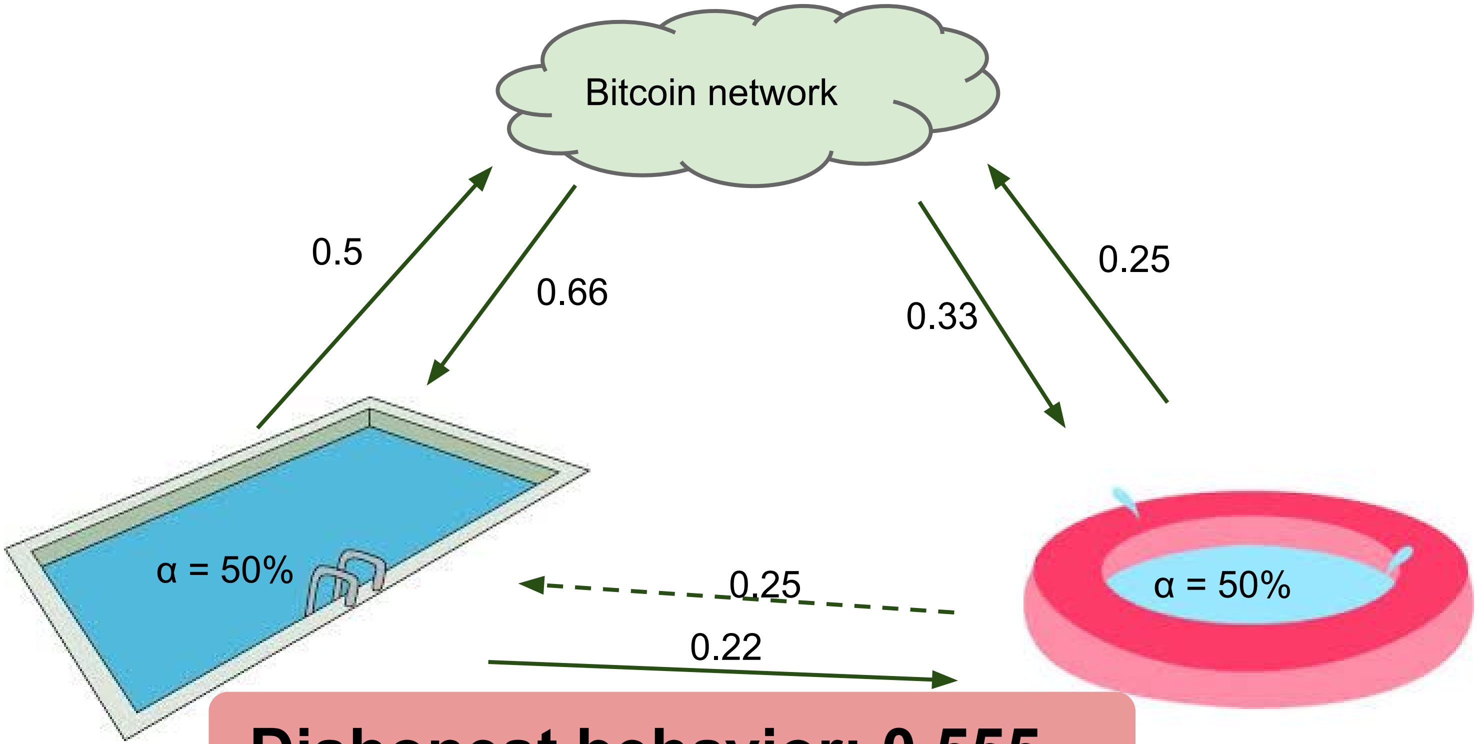


Mining pool sabotage



Honest behavior: 0.5

Mining pool sabotage



Dishonest behavior: 0.555...

Mining pool sabotage

Surprising result:

- For realistic pool sizes, incentives favor sabotage
- Infeasible to prevent with pools as we know them
- Result is an iterated prisoner's dilemma!

[Eyal 2015]
The Miner's Dilemma

Do we want pools?

Pros:

- Allow smaller miners to participate by lowering variance

Cons:

- Fewer fully-validating nodes
- Mining pools may become too powerful

Interesting result [Miller et al. 2015]:
we can design a cryptocurrency so that pools are impossible

None of these attacks observed yet…

If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.

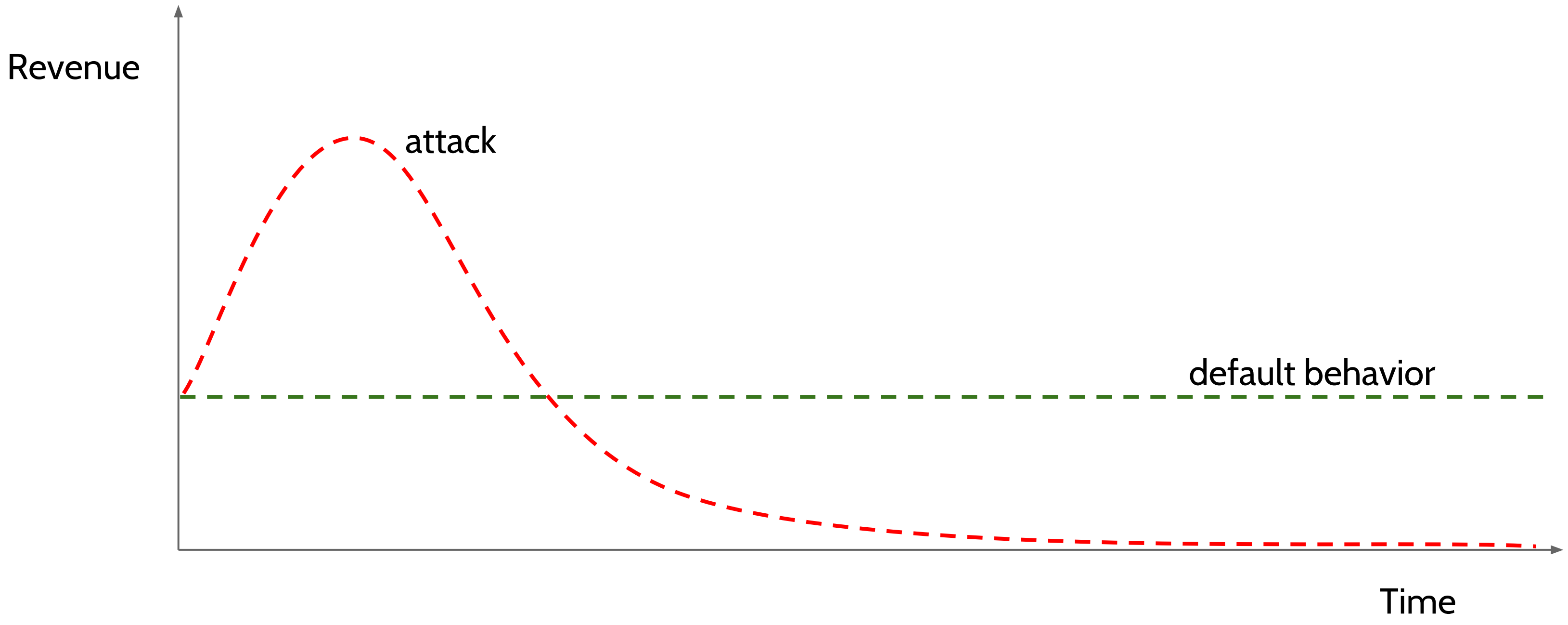
--Satoshi Nakamoto

Mining hardware is illiquid

- → High **entry costs**
- → Low **salvage value**

Conclusion: Miners care about future exchange rate

To attack, or not to attack?



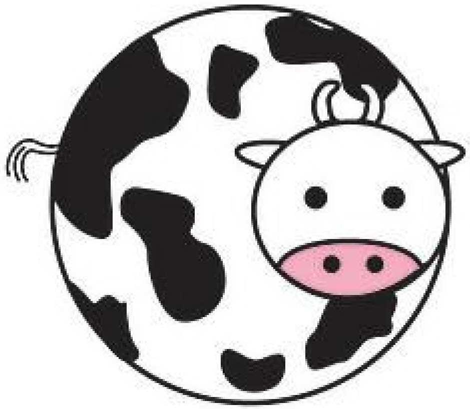
Attacks are lucrative in a simple model

Infinite:

- ➔ attacker capital
- ➔ attacker risk tolerance

Negligible:

- ➔ double-spend overhead
- ➔ bribery premium



Many explanations for lack of attacks in practice

Miners are too simplistic?

Too much risk and capital needed?

Hard to profit from double-spends?

Honor among miners?

Games at two levels

- Human level
  - Slow
  - Can change rules/code
  - Exchange rates matter
  - Other currencies exist

- Algorithmic level
  - Fast
  - Rules are fixed
  - Closed world
  - Exchange rate fixed?

Summary

- Miners are free to implement any strategy
- Very little non-default behavior in the wild
- No complete game-theoretic model exists
- Game changes as fixed rewards dwindle

Things might be about to get interesting...