

## Bitcoin Mining

---

- The Task of Bitcoin Miners
  - Mining Hardware
  - Energy Consumption & Ecology
  - Mining Pools
  - Mining Incentives and Strategies
- 

## Recap: Bitcoin Miners

---

Bitcoin depends on **miners** to

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

But who are the miners?!

## Bitcoin Mining

---

- The Task of Bitcoin Miners
  - Mining Hardware
  - Energy Consumption & Ecology
  - Mining Pools
  - Mining Incentives and Strategies
- 

## So, you want to be a Miner?

---



Gold miners ascending  
the Chilkoot pass

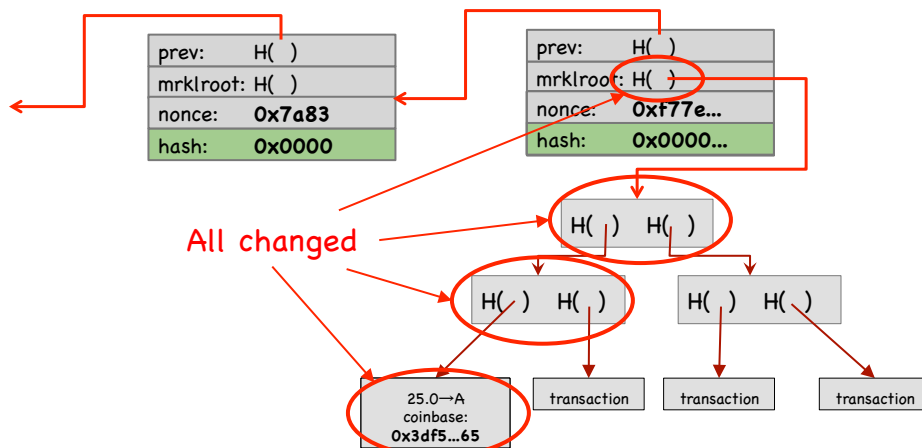
Klondike gold rush of  
1898

## Mining Bitcoins in 6 Easy Steps

Useful to Bitcoin network

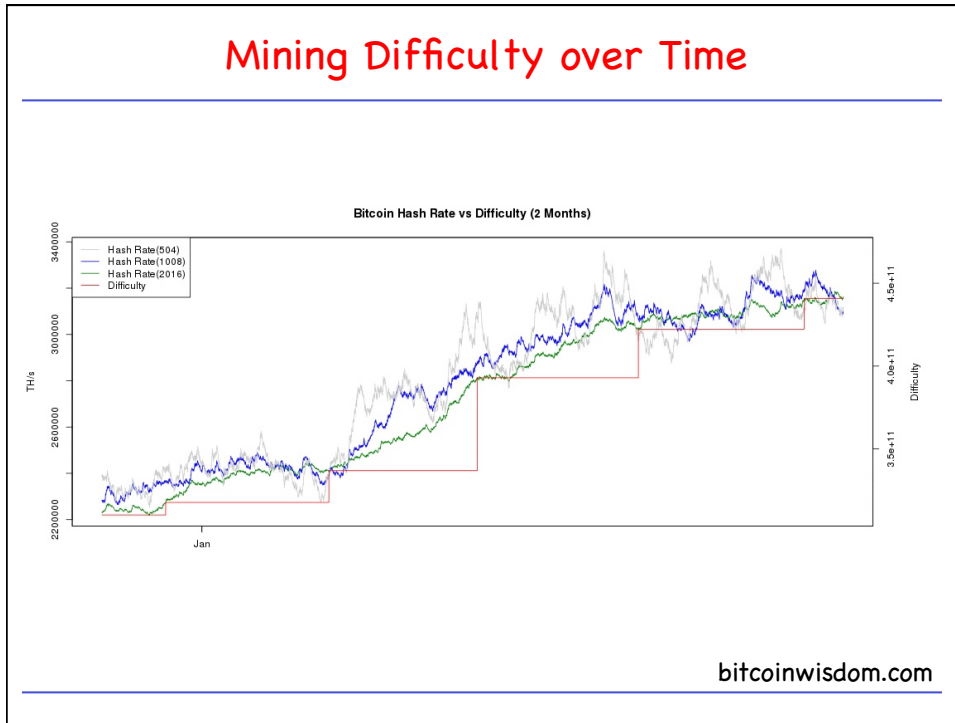
1. Join the network, **listen** for transactions
  - a. **Validate** all proposed transactions
2. Listen for new blocks, **maintain** block chain
  - a. When a new block is proposed, **validate** it
3. **Assemble** a new valid block
4. Find the **nonce** to make your block valid
5. **Hope** everybody accepts your new block
6. **Profit!**

## Finding a valid Block

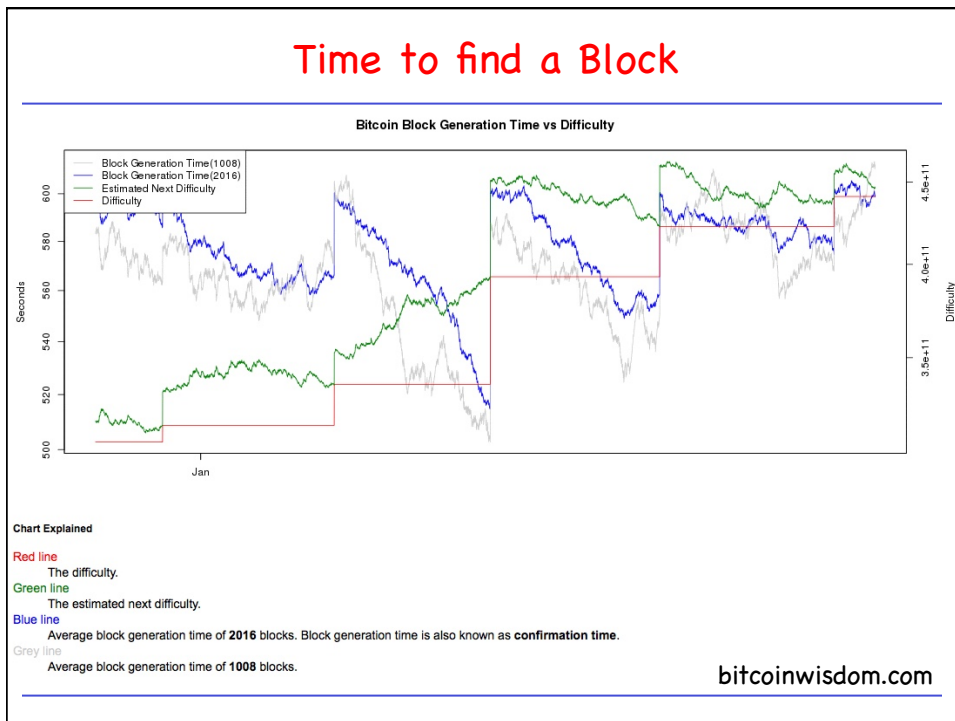




## Mining Difficulty over Time



## Time to find a Block



## Bitcoin Mining

---

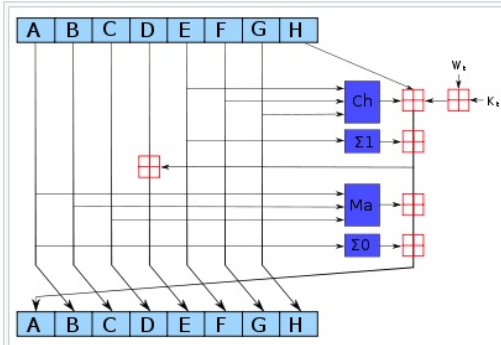
- The Task of Bitcoin Miners
  - Mining Hardware
  - Energy Consumption & Ecology
  - Mining Pools
  - Mining Incentives and Strategies
- 

## SHA-256

---

- General purpose hash function
    - Part of [SHA-2 family](#): SHA-256,SHA-384,SHA-512
  - Published in 2001
  - Designed by the NSA
  - Remains unbroken cryptographically
    - Weaknesses known
  - SHA-3 (replacement) under standardization
-

### SHA-256: Details



Iterate through compression 64 times.

$K_i$ : constants of the algorithm

$W_i$ : computed from input string

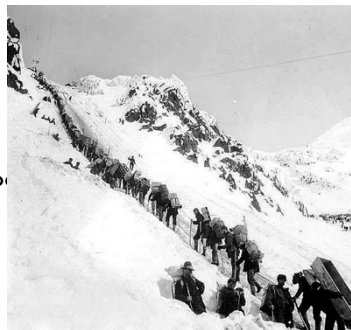
One iteration in a SHA-2 family compression function. The blue components perform the following operations:  
 $Ch(E, F, G) = (E \wedge F) \oplus (\neg E \wedge G)$   
 $Ma(A, B, C) = (A \wedge B) \oplus (A \wedge C) \oplus (B \wedge C)$   
 $\Sigma_0(A) = (A \gg 2) \oplus (A \gg 13) \oplus (A \gg 22)$   
 $\Sigma_1(E) = (E \gg 6) \oplus (E \gg 11) \oplus (E \gg 25)$   
 The bitwise rotation uses different constants for SHA-512. The given numbers are for SHA-256.  
 The red  $\oplus$  is addition modulo  $2^{32}$  for SHA-256, or  $2^{64}$  for SHA-512.

wikipedia.org

### CPU Mining

```
while (nonce < MAX) {
    if (SHA256(SHA256(block))) {
        return nonce;
        nonce++;
    }
}
```

↑  
two hashes

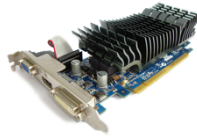


Throughput on a high-end PC = 10-20 MHz  $\approx 2^{24}$

**139,461 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

---

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



## “Goodput”

- Observation:
  - Some errors are okay. May miss a valid block, though.
- Goodput: throughput  $\times$  success rate
- Worth over-clocking by 50% with 30% errors!

## GPU Mining Rigs



Source: LeonardH, [cryptocurrenciestalk.com](http://cryptocurrenciestalk.com)

## GPU Mining Disadvantages

1. Poor **utilization** of hardware
2. Poor **cooling**
3. Large **power** draw
4. **Few boards** to hold multiple GPUs

Throughput on a good card = 20-200 MHz  $\approx 2^{27}$   
 $\approx$  **173 years** to find a block w/100 cards!

## FPGA Mining

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



## FPGA Mining Advantages

---

1. Higher performance than GPUs
  2. Excellent performance on bitwise operations
  3. Better cooling
  4. Extensive customization, optimization
- 

## FPGA Mining Rigs

---



Bob Buskirk, thinkcomputers.org

## FPGA Mining Disadvantages

---

1. Higher **power** draw than GPUs
2. Poor optimization of **32-bit adds**
3. Fewer hobbyists with sufficient **expertise**
4. More **expensive** than GPUs
5. **Marginal performance/cost advantage** over GPUs

Throughput on a good card = 100-1000 MHz  $\approx 2^{30}$

**25 years** to find a block w/100 boards!











---

## Bitcoin ASICs

---

### Bitcoin Miners for Sale on eBay

If you're a hobby miner who wants to buy a couple rigs for your house, eBay has some decent deals on mining hardware.

Miner	Hash Power	Price	Buy
 Antminer S5	1.16 TH/s	\$139.99	
 Antminer S7	4.73 TH/s	\$489.99	
 Antminer S9	14.0 TH/s	\$3,000	
 Avalon6	3.50 TH/s	\$559.95	
 SP20 Jackson	1.3-1.7 TH/s	\$90.00	

---

## 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!
- 

## Case Study: TerraMiner IV

---



- First shipped Jan 2014
- 2TH/s
- Cost: US\$6000

Still, **14 months** to find a block!

---

## Professional Mining Centers



Needs:

- cheap power
- good network
- cool climate

BitFury mining center, Republic of Georgia

## Evolution of Mining



gold pan

sluice box

placer mining

pit mining

## The Future

---

Q: Can small miners stay in the game?

Q: Do ASICs violate the original Bitcoin vision?

Q: Would we be better off without ASICs?

---

## Bitcoin Mining

---

- The Task of Bitcoin Miners
  - **Mining Hardware**
  - Energy Consumption & Ecology
  - Mining Pools
  - Mining Incentives and Strategies
-

## Thermodynamic Limits

---

**Landauer's Principle:** Any **non-reversible** computation must **consume** a minimum amount of energy.

Specifically, each bit changed requires  $(kT \ln 2)$  joules.

SHA-256 is not reversible

Energy consumption is **inevitable!**

---

## 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 (2014)

---

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

electricity consumed:  
**900 MJ/s = 900 MW**

### Estimating Energy Usage: top-down (2017)

---

- Each block worth approximately US\$28,500
- Approximately \$47.5/s generated
- Industrial electricity (US): \$0.10/kWh, or \$0.03/MJ
- Bitcoin miners could buy about 1580 MH/s

electricity consumed:  
**1580 MJ/s = 1580 MW**

### Estimating Energy Usage: bottom-up (2014)

---

- Best claimed efficiency: 1 W / GH/s  
(excluding cooling, embodied energy)
- Network hash rate: 150,000,000 GH/s (150 PH/s)

electricity consumed:

**150 MW**

---

### Est. Energy Usage: bottom-up (early 2015)

---

- Best claimed efficiency: 1/3 W / GH/s  
(excluding cooling, embodied energy)
- Network hash rate: 350,000,000 GH/s (350 PH/s)

electricity consumed:

**117 MW**

---

## Est. Energy Usage: bottom-up (2017)

- Good claimed efficiency: 0.1 W/GH/s  
(Artminer S9, excluding cooling, embodied energy)
- Network hash rate: 3,200,000,000 GH/s (3.2 EH/s)

electricity consumed:  
**320 MW**

## How much is a MW?



Three Gorges Dam = 10,000 MW  
typical hydro plant  $\approx$  1,000 MW

Kashiwazaki-Kariwa  
nuclear power plant = 7,000 MW  
typical nuclear plant  $\approx$  4,000 MW



major coal-fired plant  $\approx$  2,000 MW

## All Payment Systems require Energy

---



## "Data Furnaces"

---

**Observation:** In the limit, computing devices produce heat almost as well 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?
- 

## Bitcoin Mining

---

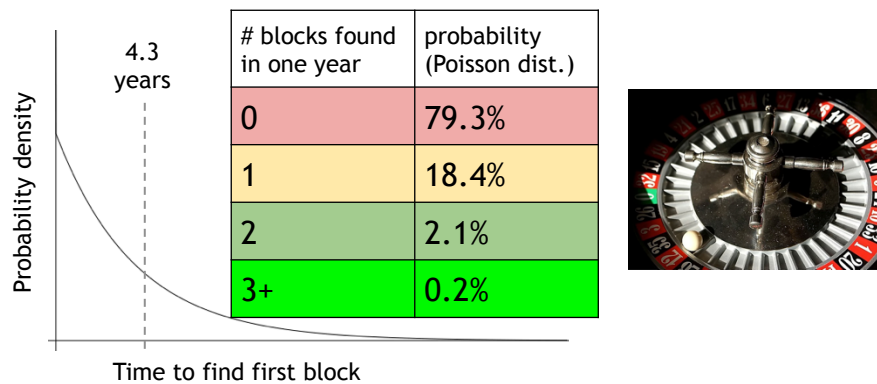
- The Task of Bitcoin Miners
  - Mining Hardware
  - Energy Consumption & Ecology
  - Mining Pools
  - Mining Incentives and Strategies
-

## Economics of being a Small Miner



- Example: Antminer S9
- Cost: ~ US\$ 3,000
- Hash power: 14 TH/s
- Fraction of total hash rate =  $14/3,200,000 = 4.4 * 10^{-6}$
- Expected time to find a block: ~4.3 years!
- Expected revenue: \$538/month
- (assume no energy costs!)

## Problem: Mining Uncertainty



## 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

**Q:** How do we know how much work members perform?

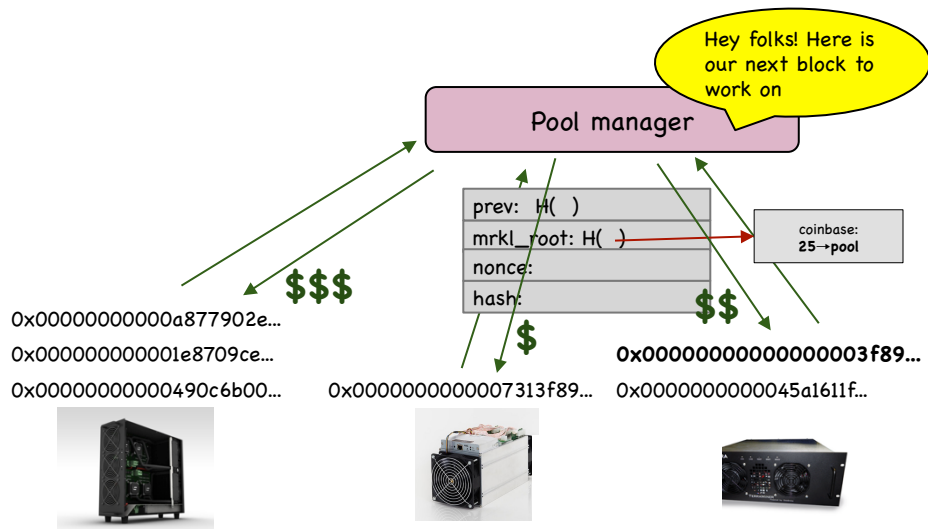
## Mining Shares

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

```

4AA087F0A52ED2093FA816E53B9B6317F9B8C1227A61F9481AFED67301F2E3FB
D3E51477DCAB108750A5BC9093F6510759CC880BB171A5B77FB4A34ACA27DEDD
0000000008534FF68B98935D090DF5669E3403BD16F1CDFD41CF17D6B474255
BB34ECA3DBB52EFF4B104EBBC0974841EF2F3A59EBBC4474A12F9F595EB81F4B
0000000002F891C1E232F687E41515637F7699EA0F462C2564233FE082BB0AF
0090488133779E7E98177AF1C765CF02D01AB4848DF555533B6C4CFCA201CBA1
460BEFA43B7083E502D36D9D08D64AFB99A100B3B80D4EA4F7B38E18174A0BFB
000000000000000078FB7E1F7E2E4854B8BC71412197EB1448911FA77BAE808A
652F374601D149AC47E01E7776138456181FA4F9D0EEDD8C4FDE3BEF6B1B7ECE
785526402143A291CFD60DA09CC80DD066BC723FD5FD20F9B50D614313529AF3
00000000041EE593434686000AF77F54CDE839A6CE30957B14EDEC10B15C9E5
9C20B06B01A0136F192BD48E0F372A4B9E6BA6ABC36F02FCED22FD9780026A8F
    
```

## Mining Pools





## Mining Pool Protocols

---

- **API** for fetching blocks, submitting shares
    - Stratum
    - Getwork
    - Getblockshare
  - Proposed for standardization with a **Bitcoin Improvement Proposal (BIP)**
  - Increasingly important; some hardware support
- 

## Mining Pool Variations

---

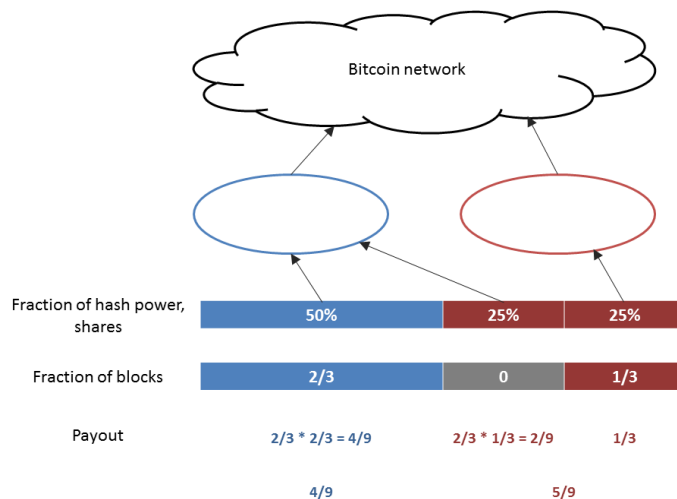
- Pay per share:** flat reward per share
    - Typically minus a significant fee
    - What if miners never send in valid blocks?
  - Proportional:** typically since last block
    - Lower risk for pool manager
    - More work to verify
  - "Luke-jr" approach:** no management fee
    - Miners can only get paid out in whole BTC
    - Pool owner keeps spread
-

## Block-Withholding Attacks: Assumptions

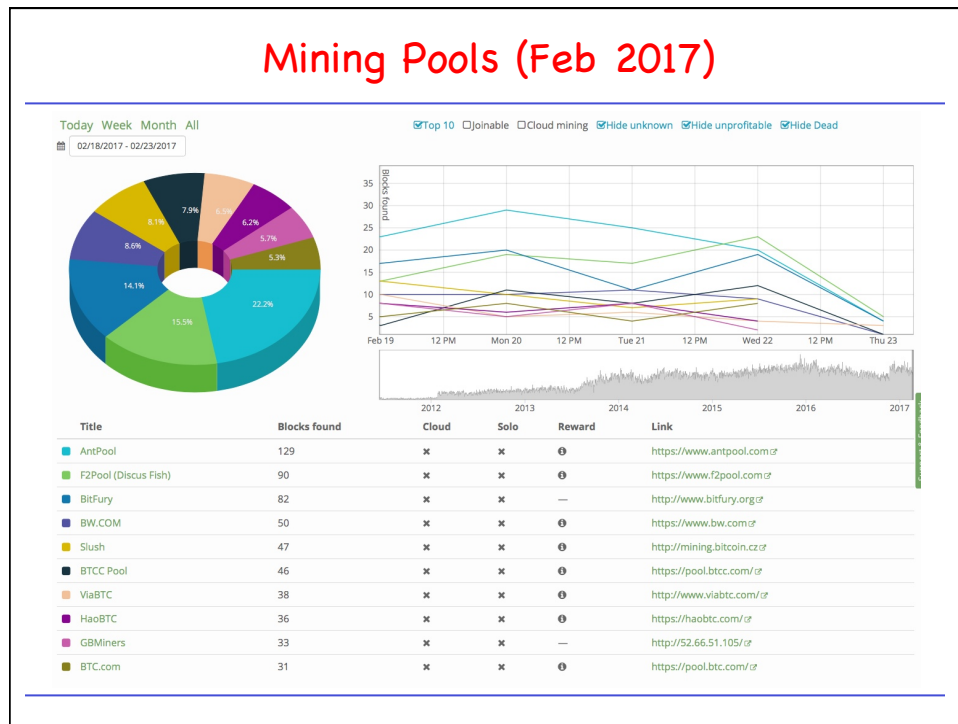
**Rules** that govern pooled mining:

1. A **pool's revenues** are proportional to the number of Bitcoin blocks that its members mine, measured as a fraction of the total blocks mined in that period.
2. A **miner's rewards** are proportional to the **number of "shares"** submitted, as a fraction of the total shares submitted by all members of that pool.
3. Miners can easily **create numerous pseudo-identities** ("sybils"), each contributing a very small amount of mining power.  
Therefore **pools can't easily detect if a miner is withholding valid blocks** (and can't punish a miner for doing so).

## Block-Withholding Attacks: Example



Arvind Narayanan, "Bitcoin and game theory: we're still scratching the surface", March 31, 2015



### 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**

**Q:** Can we **prevent** mining pools?

## Bitcoin Mining

---

- The Task of Bitcoin Miners
  - Mining Hardware
  - Energy Consumption & Ecology
  - Mining Pools
  - Mining Incentives and Strategies
- 

## Game-Theoretical Analysis of Mining

---

Several **strategic decisions**

- **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
-

## Game-Theoretical Analysis of Mining

---

Assume you control  $0 < \alpha < 1$  of mining power.

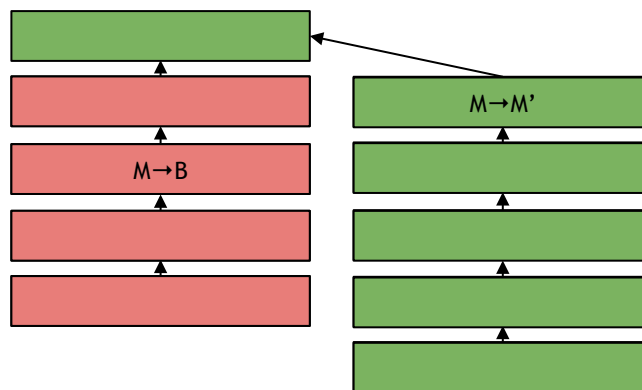
**Q:** Can you profit from non-default strategy?

**A:** For some  $\alpha$  yes, though analysis is ongoing!

---

## Forking Attacks

---



## Forking Attacks

---

- Certainly possible if  $\alpha > 0.5$ 
  - may be possible with less
  - avoid block collisions
- Attack is detectable
- Might be reversed
- Might crash exchange rate



*Goldfinger Attack?*

## Forking Attacks via Bribery

---

**Idea:** Building  $\alpha > 0.5$  is expensive.  
Why not rent it instead?

Payment techniques:

1. Out-of-band bribery
2. Run a mining pool at a loss
3. Insert large "tips" in the block chain

This is an open problem!

---

## Checkpoint Lockin

- Once in a while, old block is **hardcoded** into Bitcoin software.
- Prevents DOS attacks that **flood** unusable chains.
- Prevents attacks involving **isolating** nodes and giving fake chains.
- Also, **optimizes** initial blockchain download.

**satoshi**  
Founder  
Sr. Member  
Activity: 364

**Bitcoin 0.3.2 released**  
July 17, 2010, 09:35:51 PM

Download links available now on bitcoin.org. Everyone should upgrade to this version.

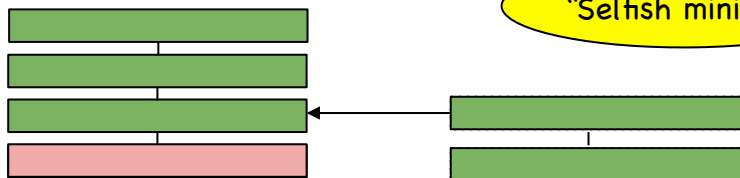
- Added a simple security safeguard that locks-in the block chain up to this point.
- Reduced addr messages to save bandwidth now that there are plenty of nodes to connect to.
- Spanish translation by milkiway.
- French translation by aidos.

Default clients ship with built-in checkpoint

## Temporary Block-withholding Attacks

Strategy: don't announce blocks right away

"Selfish mining"

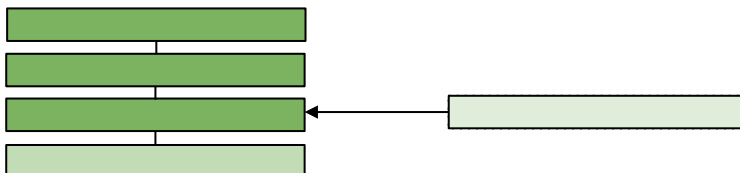


All other miners are wasting effort here!

## Temporary Block-withholding Attacks (cont)

---

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



The race is on!

## Temporary Block-withholding Attacks

---

- Improved strategy for any  $\alpha$  if you can win every race
  - Need ideal network position
  - Bribery?
- With a 50% chance of winning races, improves over default strategy for  $\alpha > 0.25$ .
- Not yet observed in practice!

**Note:** This is a surprising departure from previous assumptions!



## Punitive Forking

---

Suppose you want to **blacklist** transactions from address  $X$ .  
- Freeze an individual's money forever

**Extreme strategy:** Announce that you will **refuse** to mine on any chain with a transaction from  $X$ .

With  $\alpha < 0.5$  you will soon **fall behind** the network.

---

## Feather-forking Strategy

---

Punitive forking does **not** work **without majority** of hash power.

To **blacklist transactions from  $X$** , announce that you will **refuse to mine directly** on any block with a transaction from  $X$ .

- but you'll **concede** after  $n$  confirming blocks

The chance of pruning an offending block is  $\alpha^2$ .

---

## Response to Feather Forking

For other miners, including a transaction from  $X$  induces an  $\alpha^2$  chance of losing a block.

So, it may be safer to join in on the blacklist!

... Unless  $X$  is willing to compensate with appropriate transaction fee.

Interesting: You can force a blacklist with  $\alpha < 0.5$ !

Depends on convincing other miners that you will fork.

## What is Feather-forking good for?

For freezing individual Bitcoin owners:

- ransom / extortion
- law enforcement

Or for Enforcing a minimum transaction fee . . .

Example:

Default policy:

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

New: accept without fees only if

```
priority > 0.56789
```

## Summary

---

Miners are free to implement **any strategy**.

**Very little** non-default behavior in the wild.

**No** complete **game-theoretic models** exist.

---