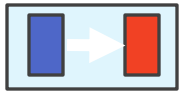
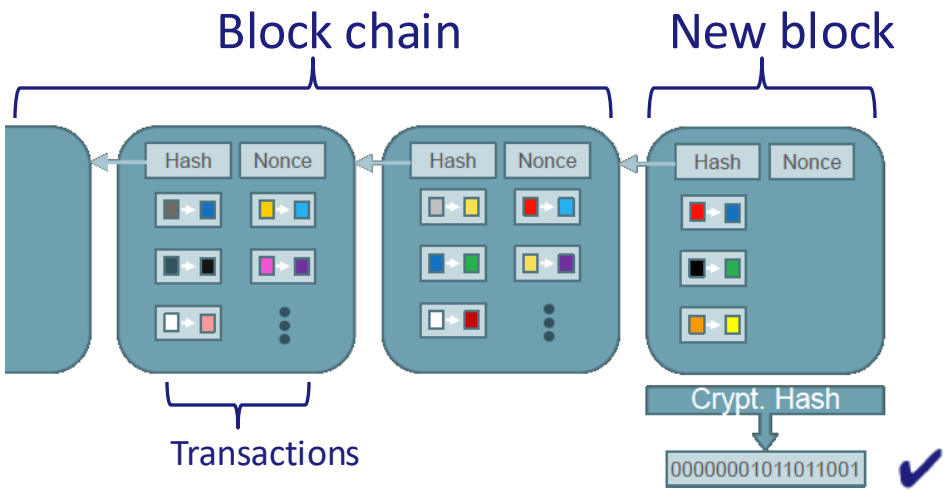
Blockchain & Bitcoin

How Bitcoin Works

Transactions 

Any sender(s) to any receiver(s), transaction fee for the “miner”



Block ingredients:
- Transactions
- Pointer (hash)
- Nonce

The Protocol:

Publish solutions immediately.

If there’s a fork:
- Mine on the longest chain.
- If equal length, mine on what you hear about first.

Incentives for the miners:
- A block reward of 3.125 BTC (~93K USD), originally 50 BTC
- Transaction fees (voluntary tips)

Mining Pools

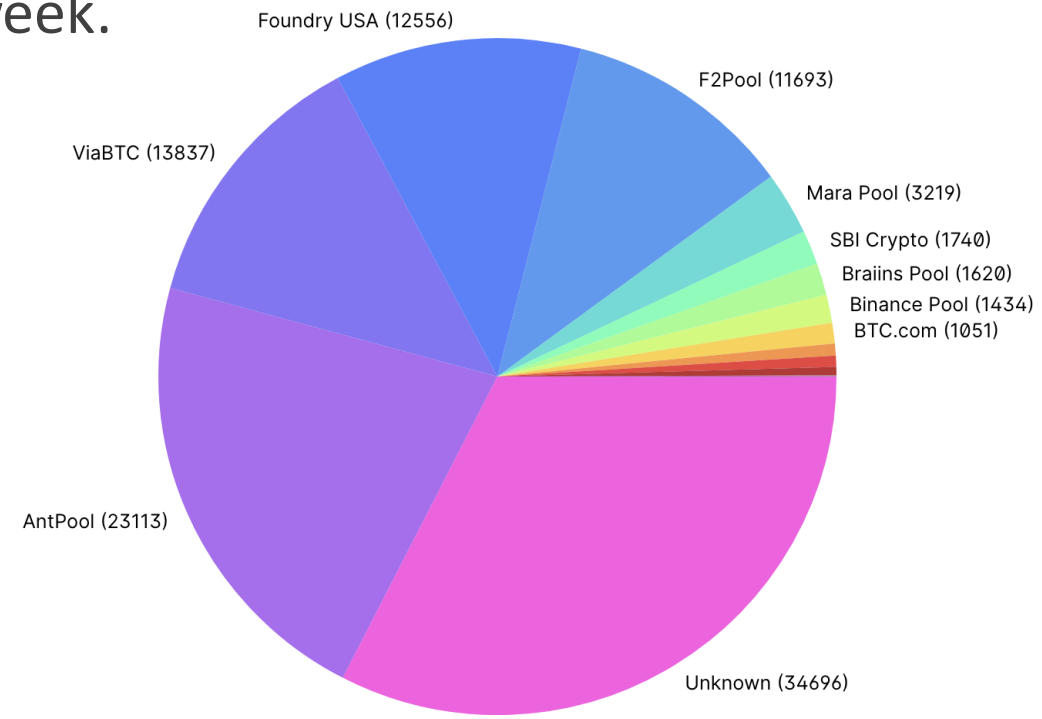
A top-of-the-line GPU finds a block ($292.2K) approximately once in 1mil years.

Instead, join a pool! Make $.005/week.

- Full solutions have hash < target.
- Partial have hash < target/2^20.

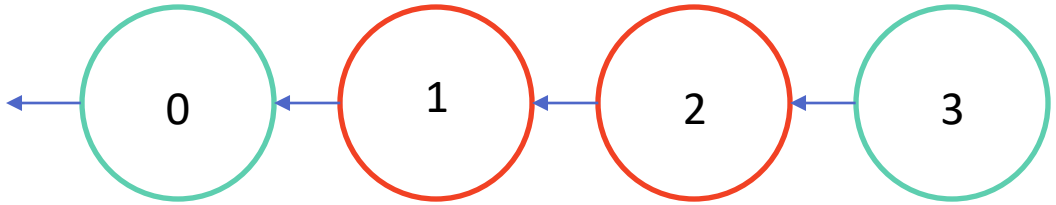
Expectations:

- Miners join a pool.
- Pools have < 50% total hash power.
- Miners in pool paid proportionately.

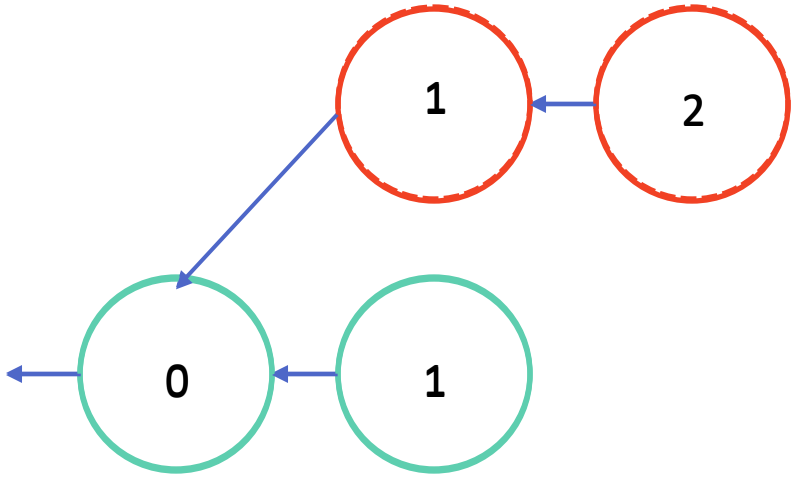


(1) Selfish Mining

Suppose the following event occurs:



Red gets 2/4 blocks. Or instead,



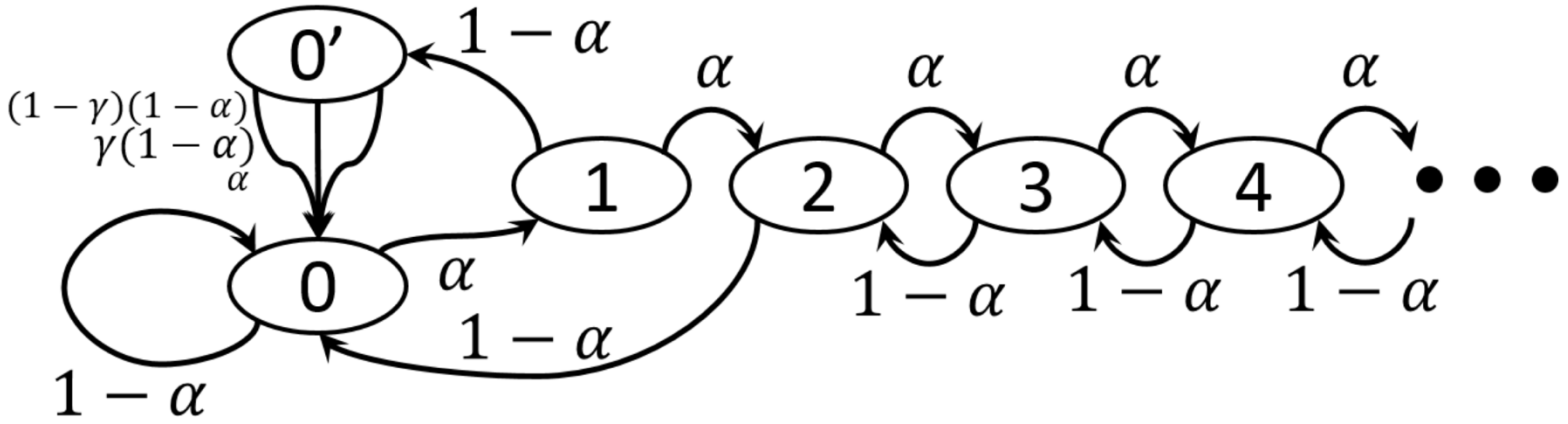
Takeaway: Publishing solved blocks immediately isn't best!

Now red gets 2/3 blocks.

[Eyal Sirer 14]

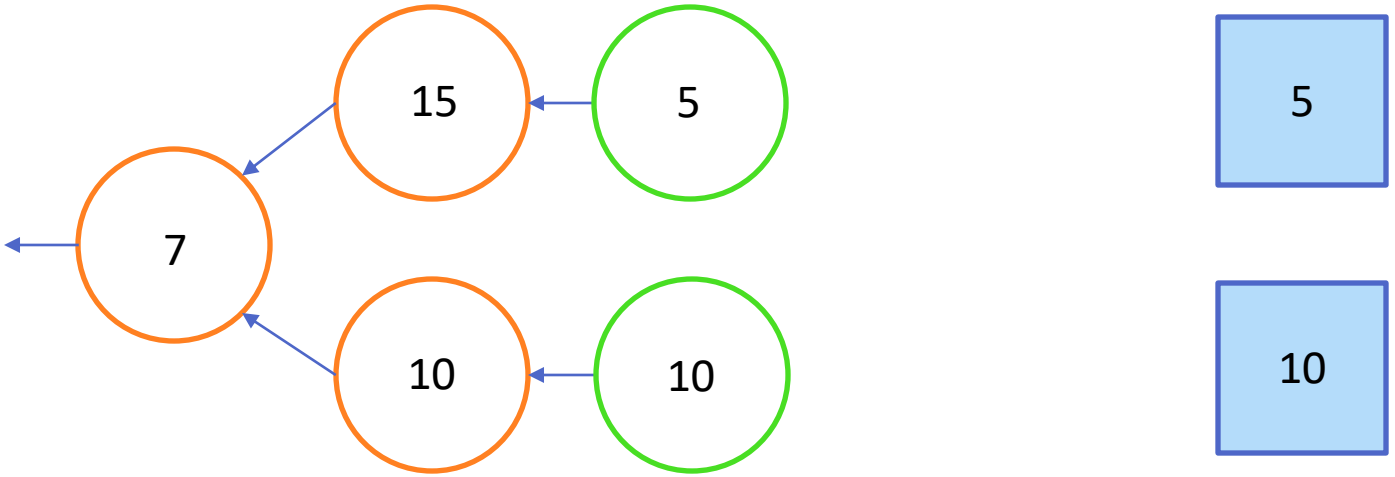
State machine for strategy where my “lead” z is the state:

- If I mine, keep it secret (unless in 0’)
- If honest mines:
  - If $z > 2$: publish 1
  - If $z = 2$: publish both
  - If $z = 0$: switch to longest
  - If $z = 1$: publish and then race! This is state 0’ (could lose race)



(2) Undercutting

Petty tie-breaking:

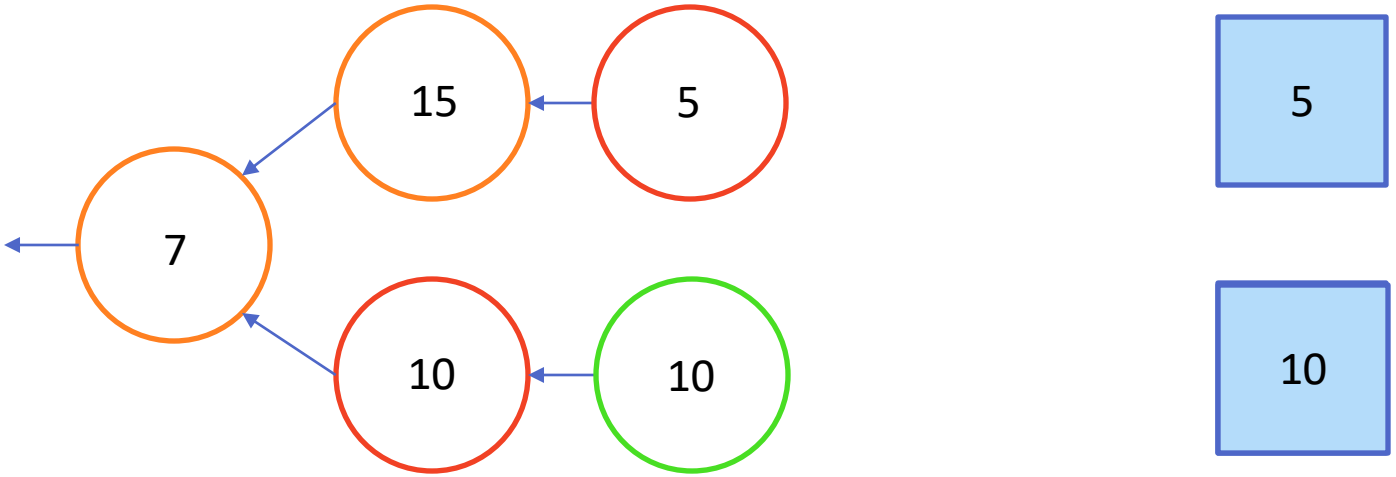


Takeaway: Tie-breaking by what you hear first isn't best.

[Carlsten Kaldoner Weinberg Narayanan 16]

(2) Undercutting

Mining strategy given petty tie-breaking:



Takeaway: Mining on the longest chain isn't best!
Miners might intentional fork the chain, "undercutting."

[Carlsten Kaldoner Weinberg Narayanan 16]

(3) Pool Payment Schemes

Proportional payment rule:

- If each miner i finds p_i partial shares, pay him $p_i / ||\boldsymbol{p}||_1$
- Expected payment is α_i

Example: Suppose $\alpha_i = 1/3$, $\boldsymbol{p} = (2, 4, 4)$, and Pr[solution = full] = 1/100

Reward now = 1/5 vs. E[reward | wait 1 more] = ?

E[reward | wait 1 more] = Pr[next solution full] * 1/10 +

Pr[next solution partial] * [(Pr[i finds it] 3/11 + Pr[not i finds it] (2/11)]

= 1/100 (1/10) + (99/100) [3/11 + (2/6) (2/11)] ≈ 1/3

Takeaway: Reporting full solutions immediately isn't best!

[Schrijvers Bonneau Boneh Roughgarden 16]

(4) Pool Participation

Pool A 50%, Pool B 50%

A earns 50% of blocks

A attacks Pool B with 16%

A earns 40% + 1/4 * 60% = 55%

Takeaway: Contributing truthfully to only your pool isn't best!

[Eyal 15]

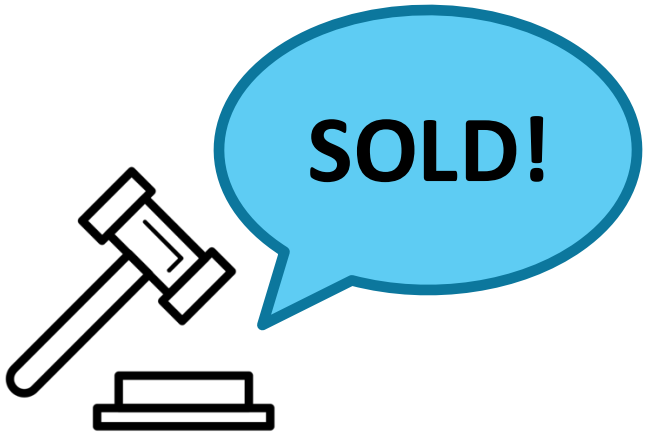
(5) Transaction Fees as Incentives

[Kroll Davey Felten 13] Transaction fees will go to zero (or cost)

Our question: But what if customers have deadlines?

Setting:

- Value
- Deadline
- Different miner each block
- New customers arrive



Interdimensional Mechanism Design

Optimal Seller Revenue

Open Problem: What optimal mechanisms **can** we characterize beyond 1 item?

1 item

2 items

- Simple.
- Easy to compute.
- Only one real option. [Myerson '81]

$5: Pr[🍎]=1

- Uncountably infinite options. [Manelli Vincent '07, Daskalakis Deckelbaum Tzamos '15]
- Intractable to compute. [Daskalakis Deckelbaum Tzamos '13]
- We still know very little about how to do this.

$5.89: (Pr[🍎]=.60, Pr[🍊]=.29)

Optimal Seller Revenue

1) Optimal mechanism characterization
2) Menu complexity

1 item — FedEx — 2 items

easy [Mye'81]

explicit [FGKK'16]

intractable, chaos [DDT'13,'15; MV'07]

Single-Minded [DGSSW '20]

Multi-Bidder FedEx [WZ '21]

Multi-Unit Pricing
1,2,3-cap for documents
[DHP '17, DGSSW '20]

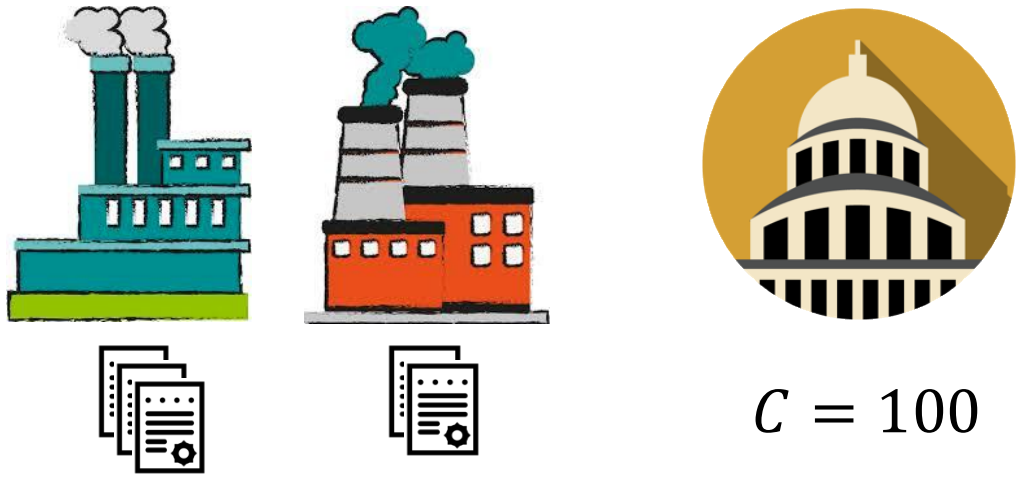
Approximate FedEx [SSW '18]

Budgets
$5, $10, $12 budgets
[DW '17]

Coordinated Valuations
Wifi, +TV, +Cable [w/ g(v)]
[DGSSW '20]

Tournament Design


Tournament Of Champions
March 24th and 29th
(1
(5
(2
(7
Winner
(3
(6
(4
PrintYourBrackets



Strategic Robustness & Carbon Emissions

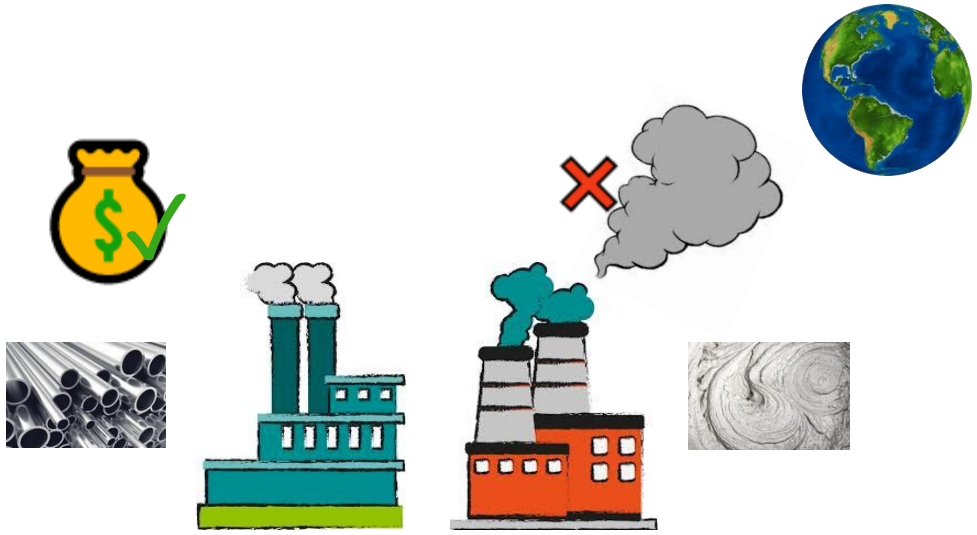
Reducing Carbon Emissions

"Cap and Trade":

- Cap the total amount of carbon pollution per year.
- Require 1 license per 1 metric ton carbon emitted.
- **…how are licenses allocated?**

EU ETS RGGI Inc. WCI KETS

Emissions Trading Schemes



Goal: Optimally trade off economic value and societal cost.

Cap = 100

Emissions Trading Schemes

Most Emissions Trading Schemes worldwide use the **Uniform Price Auction**:

1. Government sets cap C
2. Firms submit (decreasing) bids
3. C highest bids win
4. Price = C^{th} highest bid per license

Modifications:

- **Reserve price:** never sell below $\underline{p}$ (might sell < C)
- **Price ceiling:** can always buy extra for $\overline{p}$ (might sell > C

Due to our objective, can result in more harm than good.

Why it's used

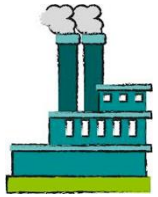
Problems

Objective:

Economic value – societal cost

Value \$112 – Cost \$90 = +\$22

Value \$87 – Cost \$90 = -\$3



1st		\$45	\$32
2nd	\$0	\$35	\$10 ✗
3rd	\$0	\$8 ✗	\$5 ✗

price = \$30

$\underline{p}$ = \$30

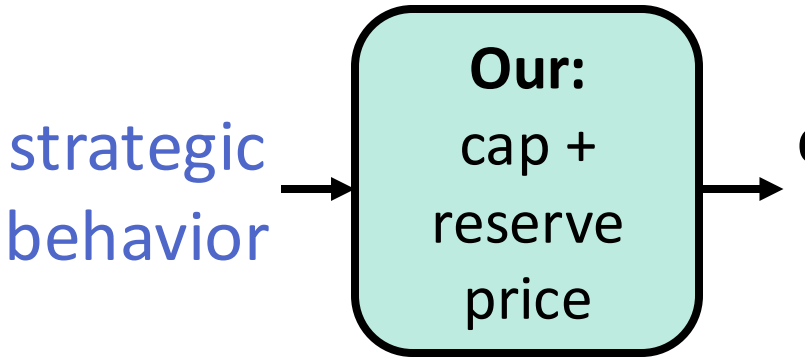
How can we fix this allocation of licenses to be robust to strategic behavior?

Beneficial Deviation

Handling Strategic Behavior

[Goldner Immorlica Lucier ITCS '20]:

Never more harm than good!



$O(1)$-approximation to