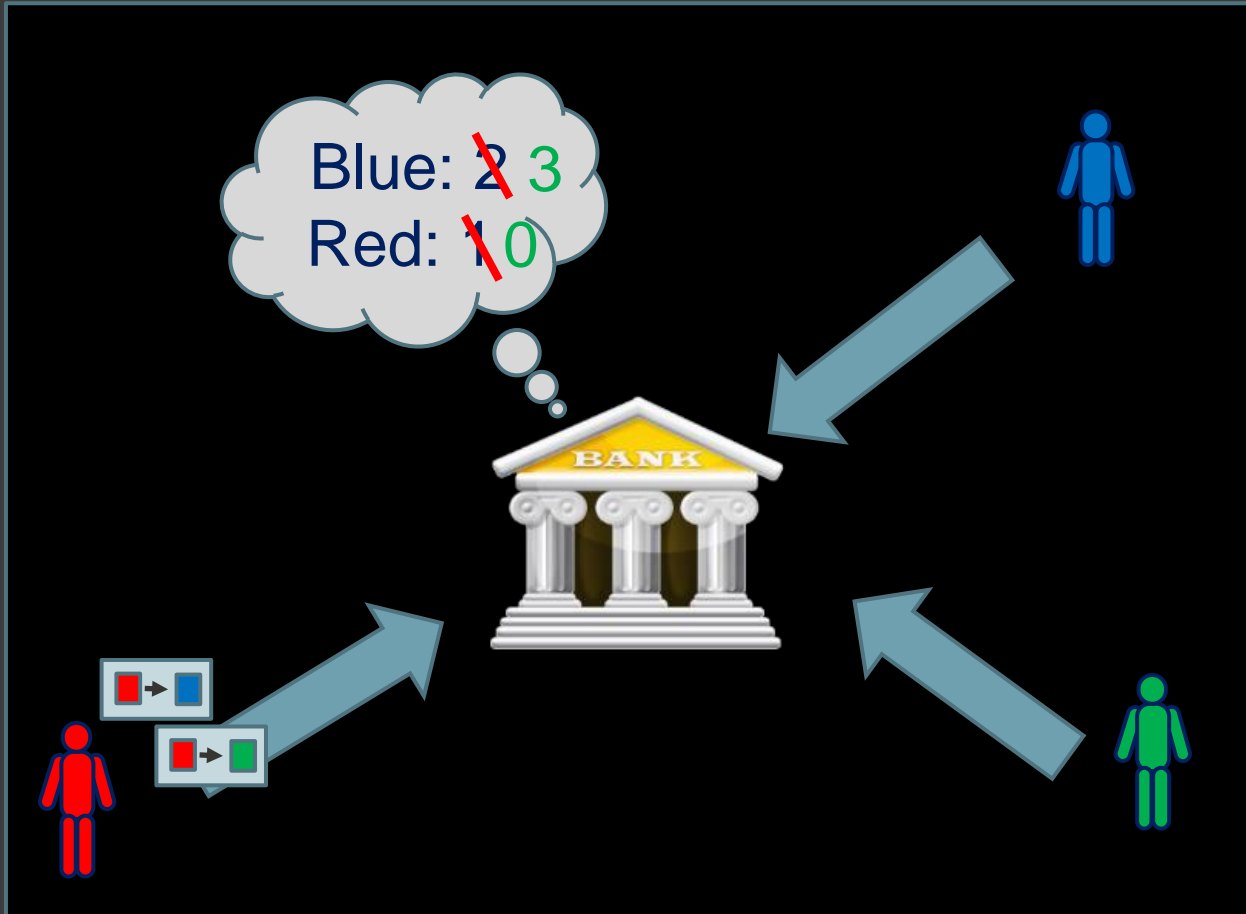


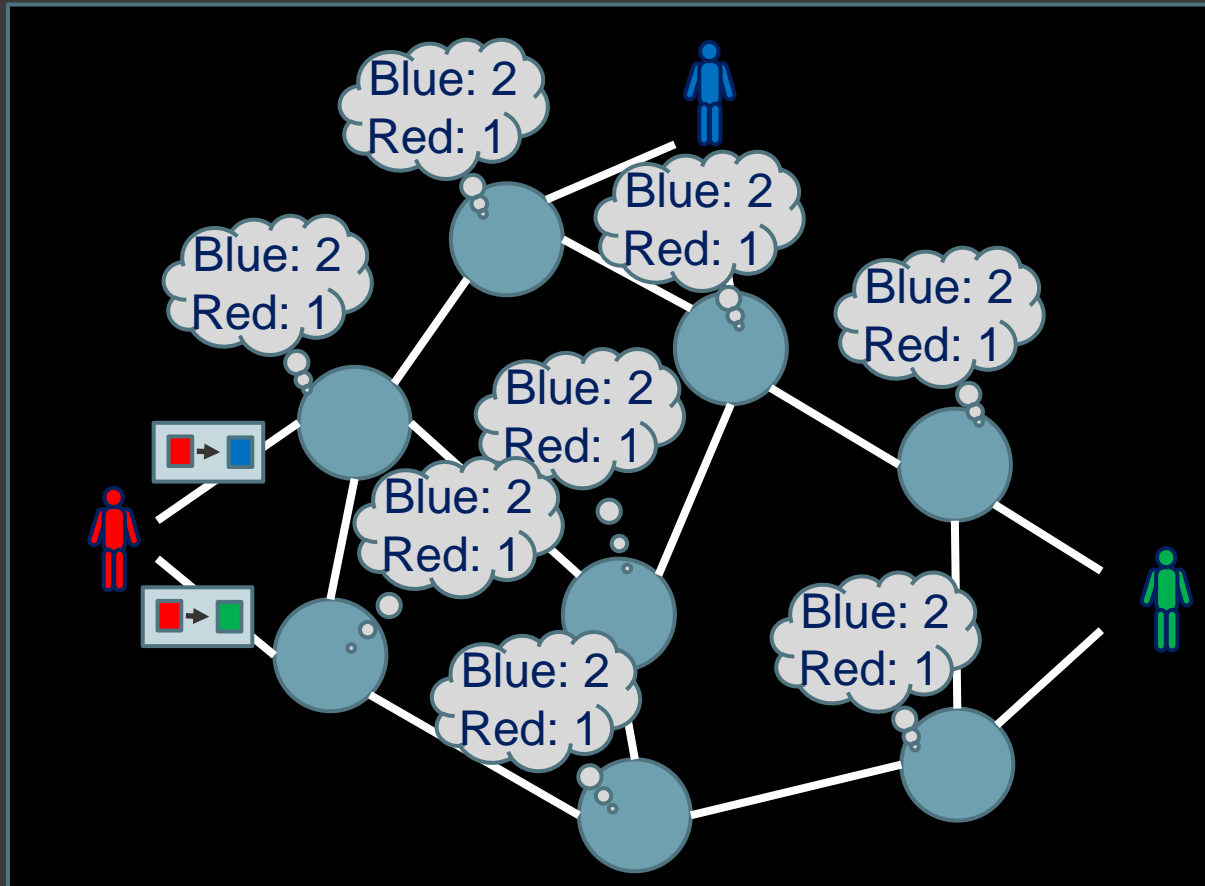
INCENTIVES IN BITCOIN

Aviv Zohar

The Hebrew University of Jerusalem
& Microsoft Research Israel

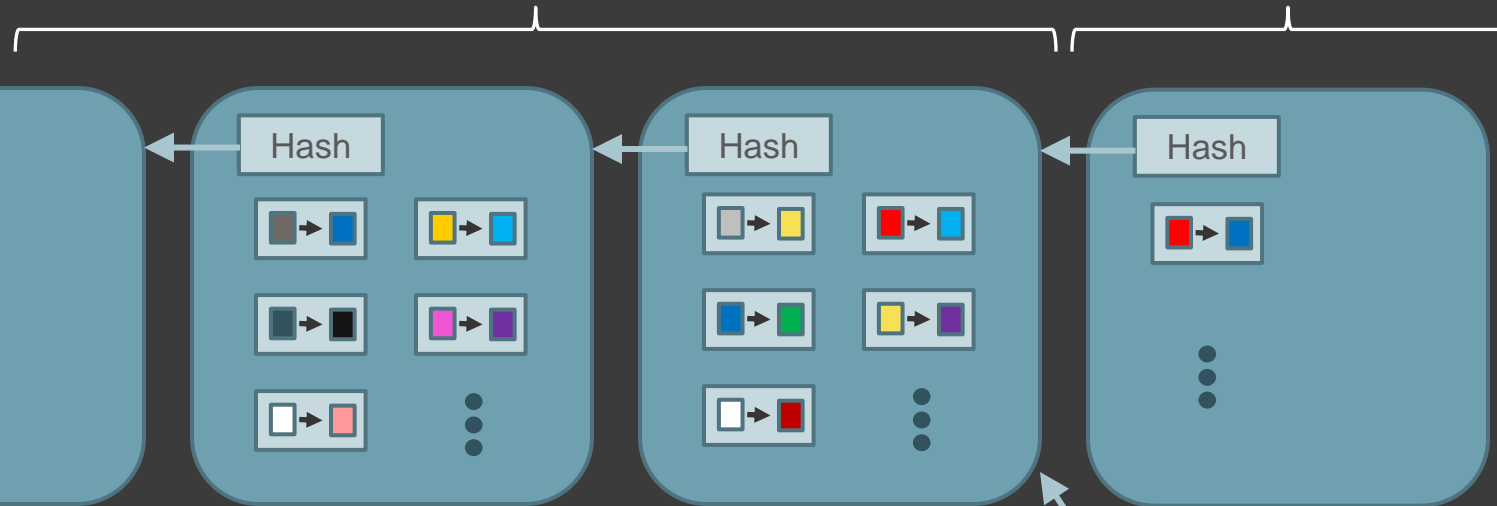


The double spending problem

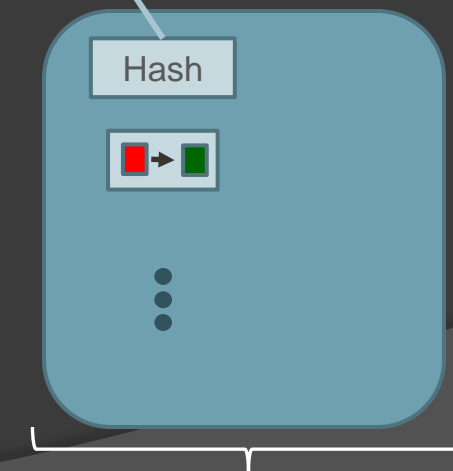


Block Chain

New Block

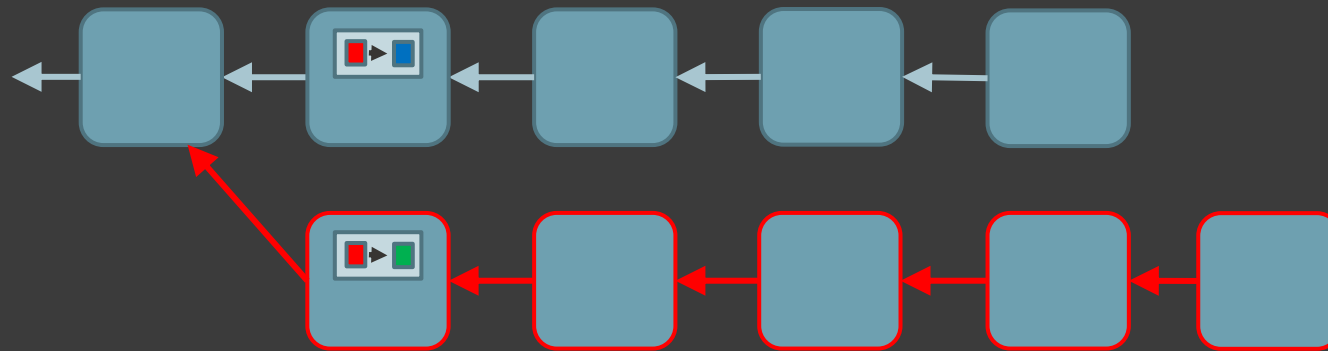


1. Make block creation hard (once every 10 minutes) via computational “puzzles”
2. Quickly send blocks to all nodes
3. Adopt (conflicting) blocks iff they make up a longer chain

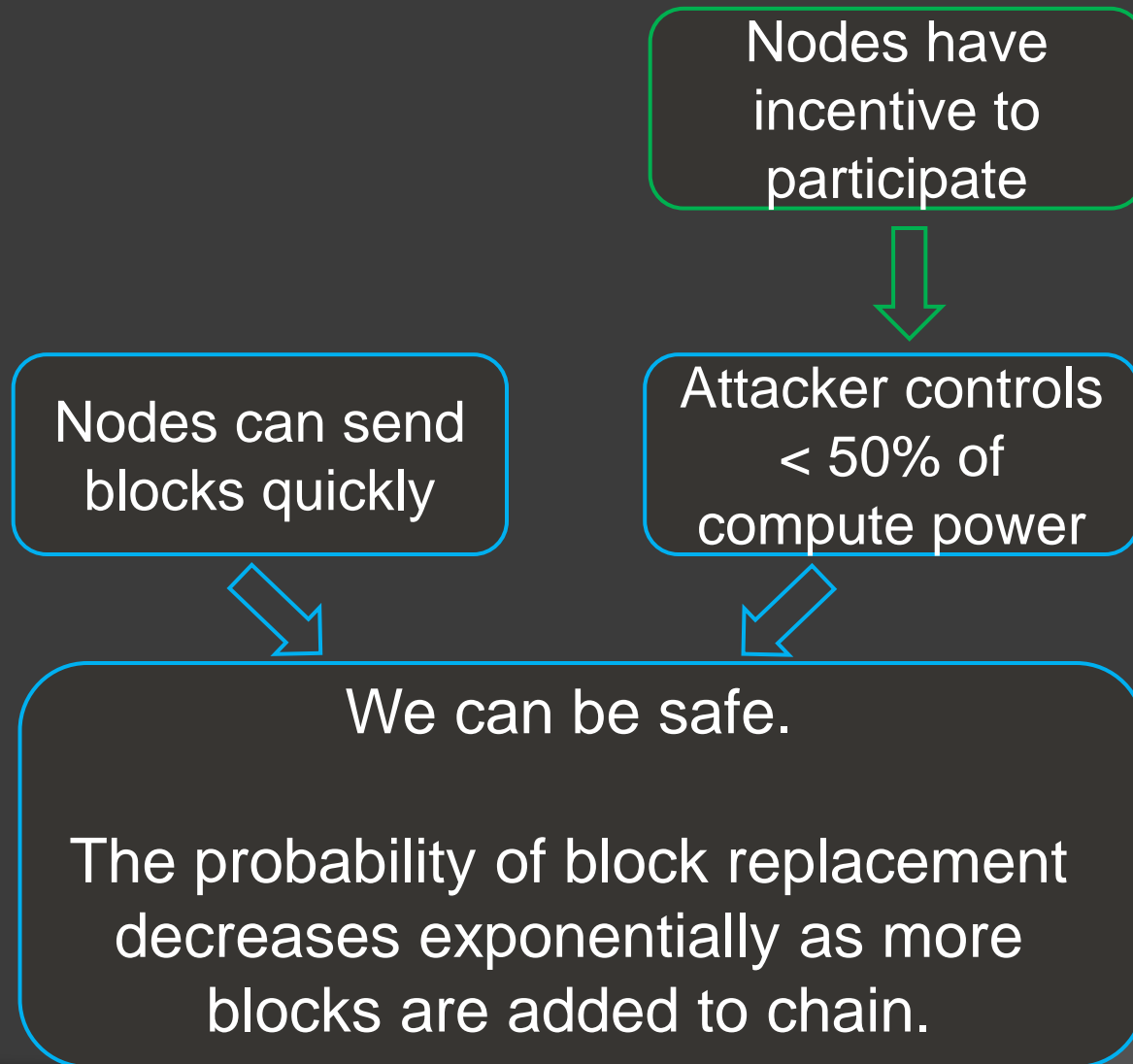


Another Node's Block

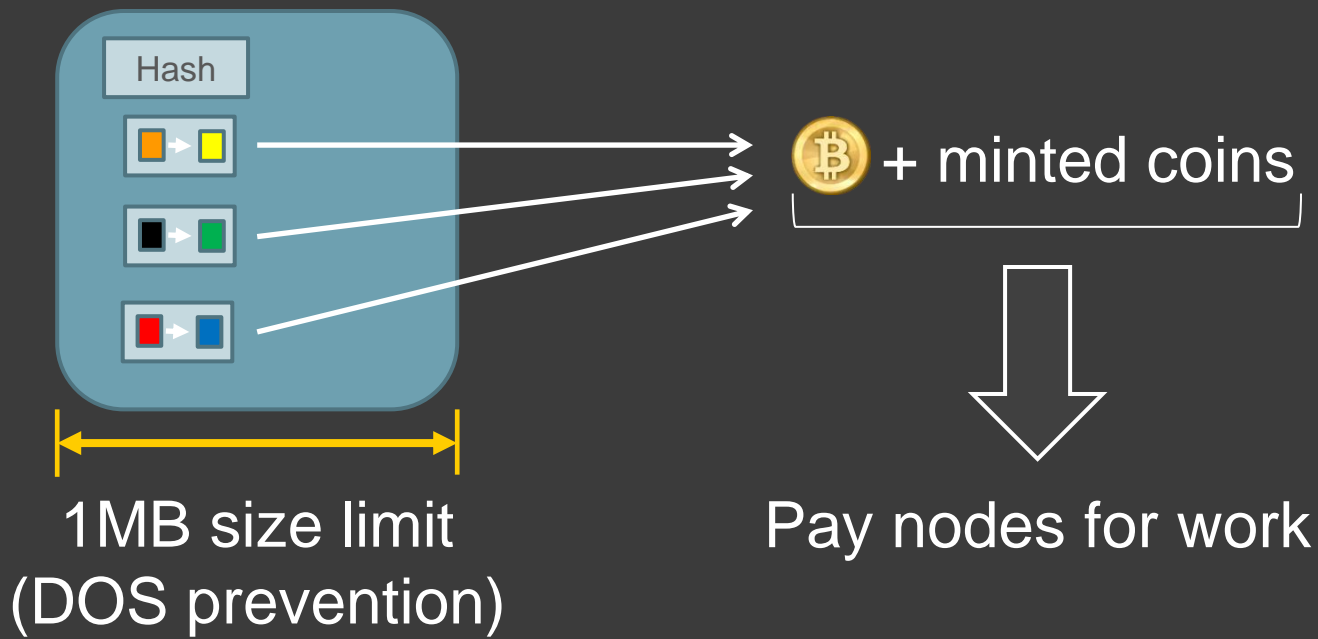
The Double-Spend Attack



Main theorem [Satoshi Nakamoto]

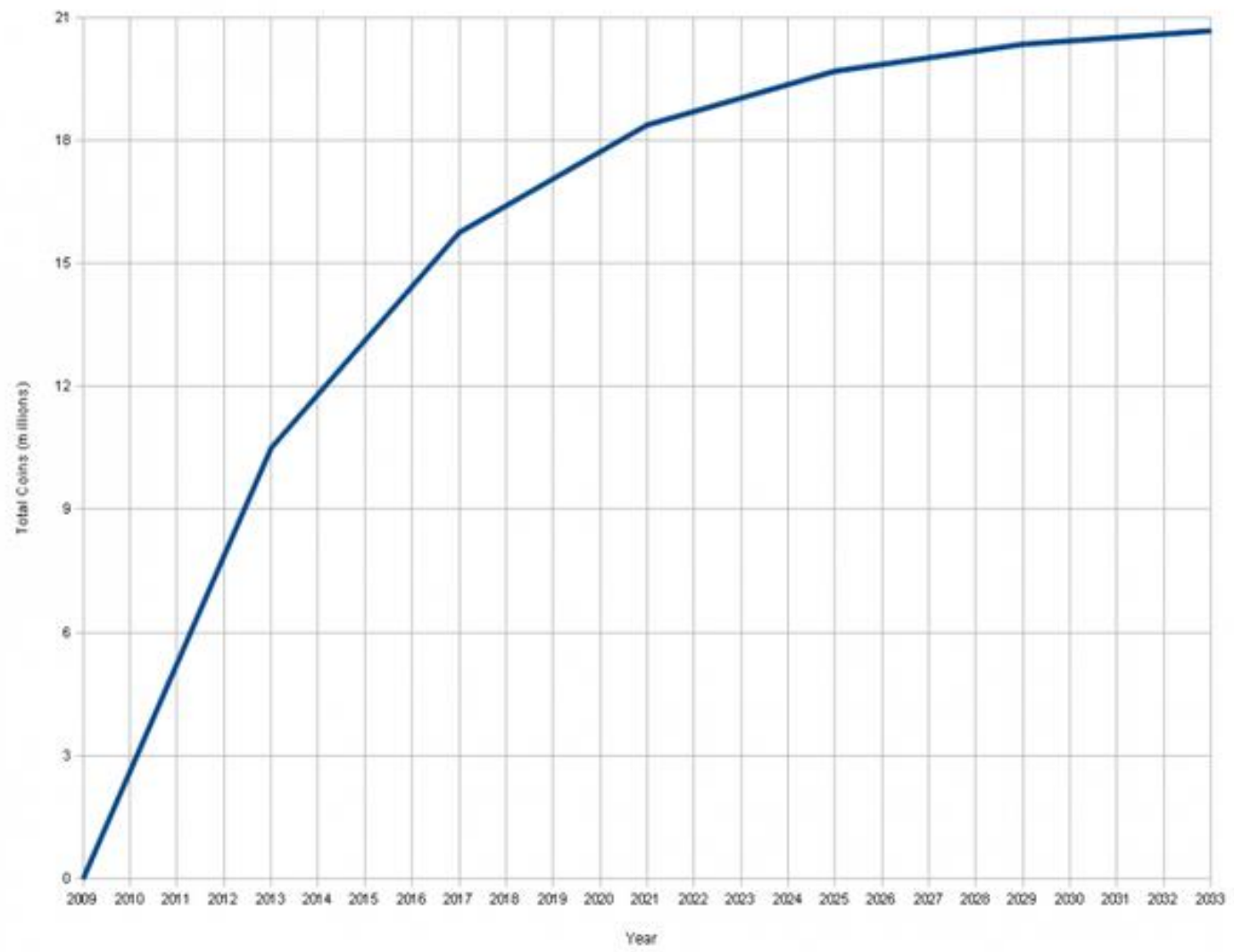


Incentives




“Mining”

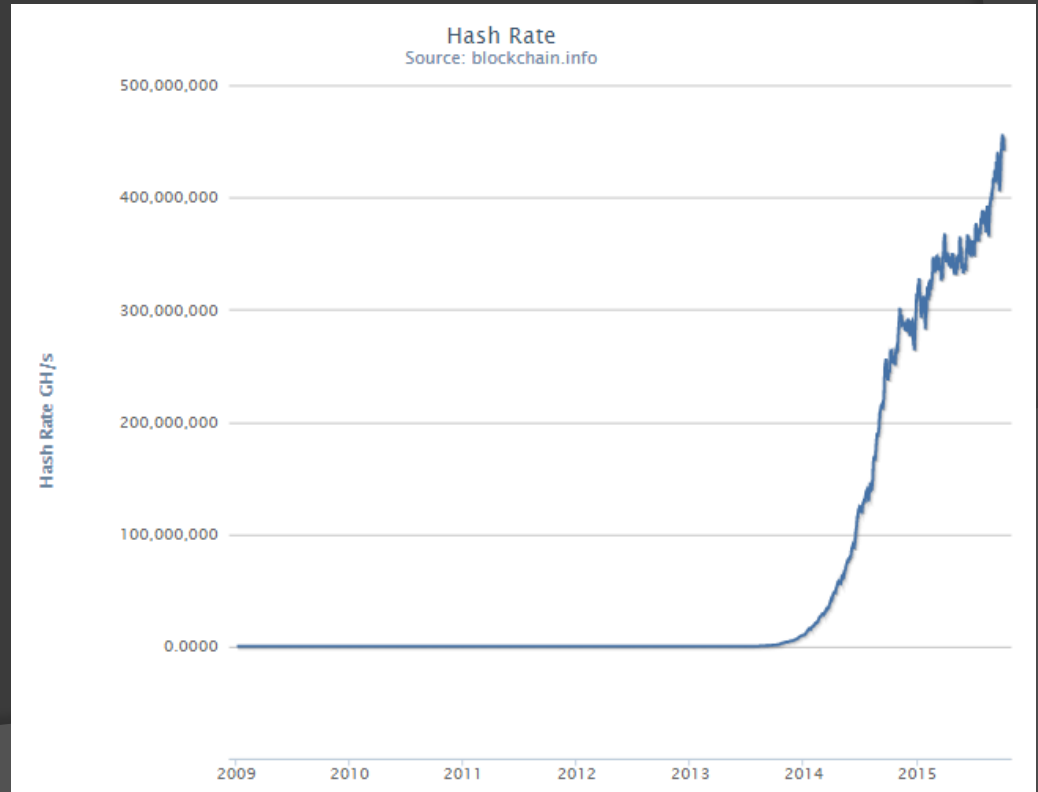
Total Bitcoins over time



**TURN YOUR
COMPUTER
INTO A
MONEY
MACHINE**



**WORK FROM HOME. BE YOUR OWN
BOSS. CREATE THE LIFE YOU WANT**
avery-brayner



Number Of transactions Per Day

Source: blockchain.info



Where incentives break down

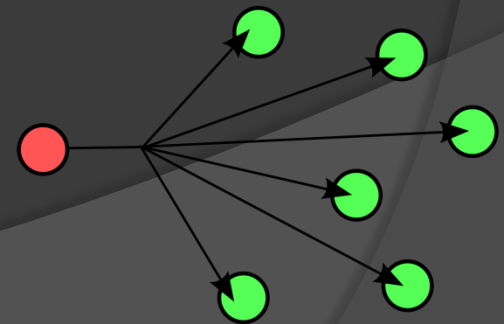
Incentives to send messages

Competition is important

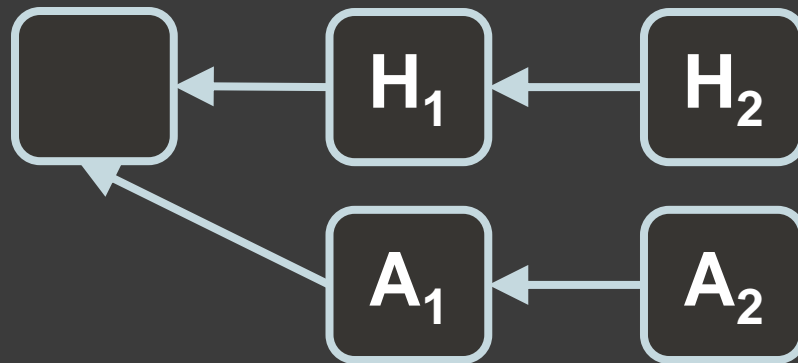
In order to compete nodes need access to

- Transactions
- recent blocks
- ⦿ No proper incentives to share either one

“On Bitcoin and Red Balloons”
[Babaioff, Dobzinsky, Oren, Zohar]



Selfish Mining

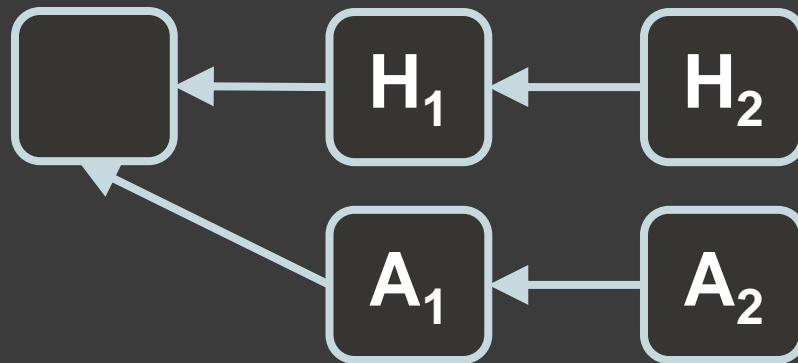


First demonstrated
by [Eyal & Sirer]

- ⦿ Attacker knocks out more blocks than he loses
- ⦿ Works if attacker has “enough” comp. power (e.g., over 1/3), or communicates fast.
- ⦿ How do we fix this?
- ⦿ First step: how do we find a best-response?

Optimal Selfish Mining

[Sapirshtein, Sompolinsky, Zohar]



What should we do?

$$REV := \mathbb{E} \left[\liminf_{T \rightarrow \infty} \frac{\sum_{t=1}^T r_t^1(\pi)}{\sum_{t=1}^T (r_t^1(\pi) + r_t^2(\pi))} \right].$$

- State: length of each chain after the fork
- Actions: wait, adopt, override...

We know how to find the optimal deviation
(using a reduction to MDPs)

Table 3: Optimal actions for an attacker with $\alpha = 0.35, \gamma = 0$, in states (a, h) with $a, h \leq 7$.

$a \backslash h$	0	1	2	3	4	5	6	7
0	*	a	*	*	*	*	*	*
1	w	w	w	a	*	*	*	*
2	w	o	w	w	a	*	*	*
3	w	w	o	w	w	a	*	*
4	w	w	w	o	w	w	w	a
5	w	w	w	w	o	w	w	w
6	w	w	w	w	w	o	w	w
7	w	w	w	w	w	w	o	w

Results

- ⦿ Smaller miners can in fact profit from these attacks
- ⦿ Some suggested fixes *slightly* worse than expected (e.g., 50-50 fix by E&S) others **much** worse than prev. thought.

The really bad news:

- ⦿ In networks with delays
all miners profit from deviation.

Many more incentive problems and connections

- ⦿ Fee markets need to replace minting
- ⦿ Externalities that are not reflected in prices
 - every transaction accepted consumes resources from all
 - Every block helps all previous blocks be a bit more secure.





“Breaking the chains” of blockchain protocols [Lewenberg, Sompolinsky, Zohar]

Hidden links to social choice?

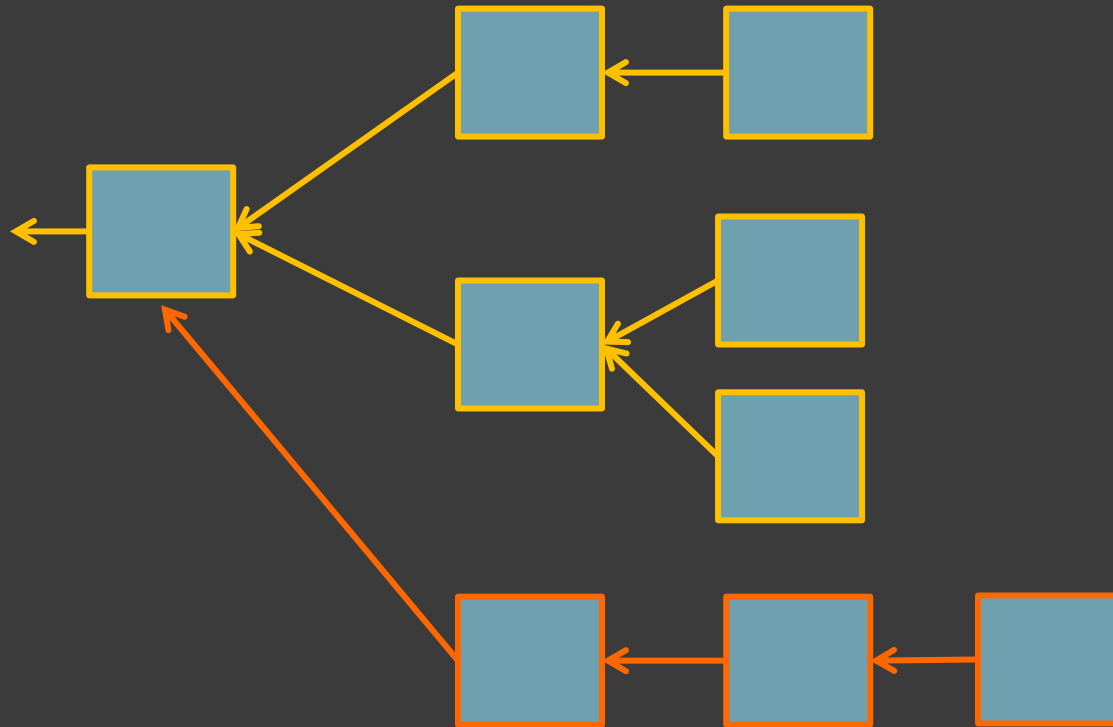
Intuitions...

Bigger & Faster

- Bitcoin 3.3 transactions per sec
- Visa > 2000 tps

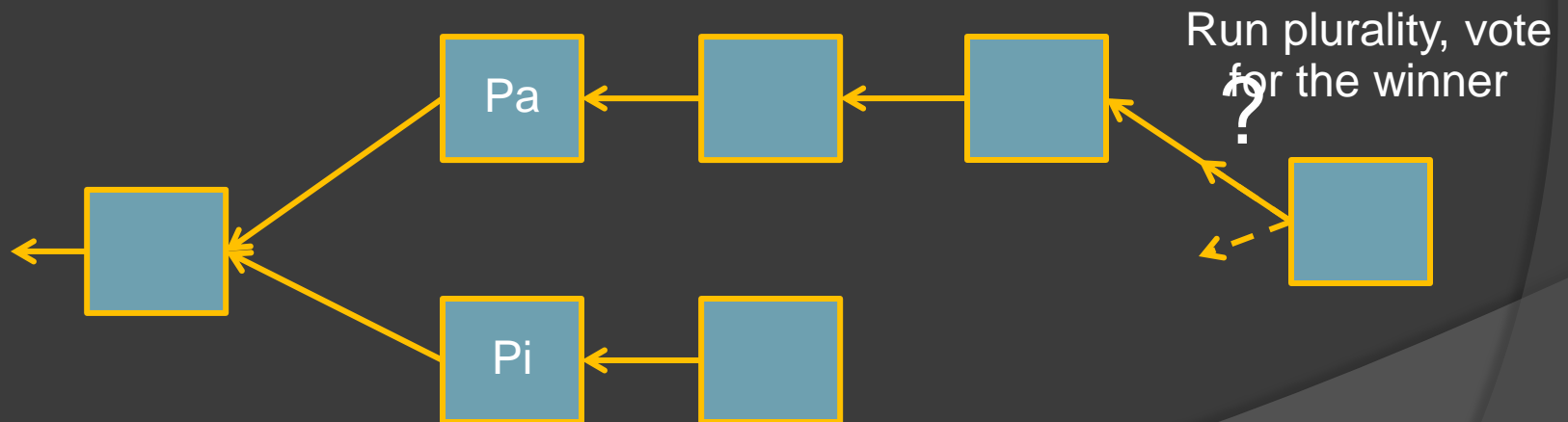
- Bitcoin blocks: every 10 minutes
- Need faster confirmation times!

Speeding up is problematic



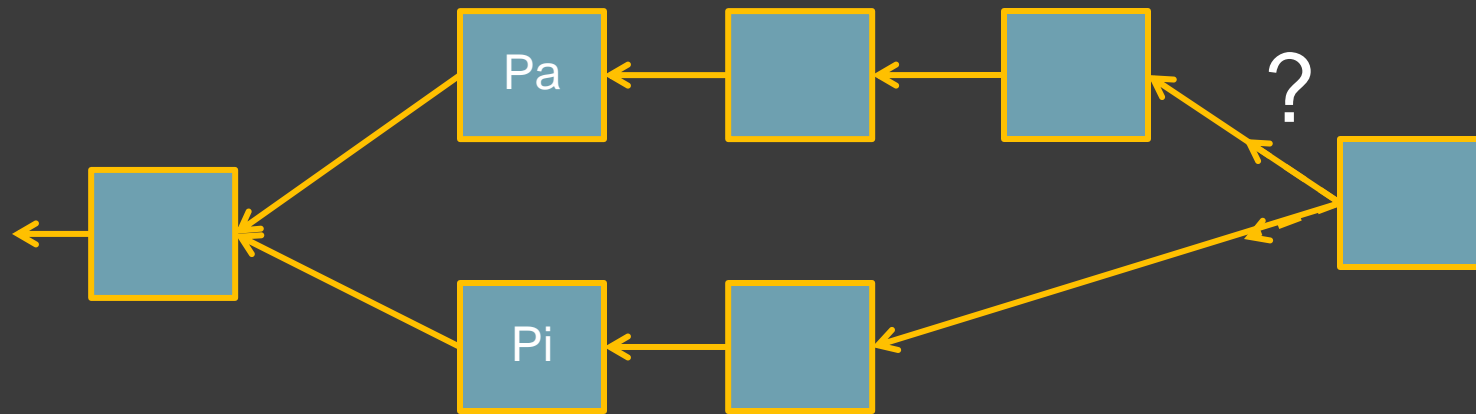
Need new protocol that will be more tolerant to delay, but still secure.

Hidden links to social choice?

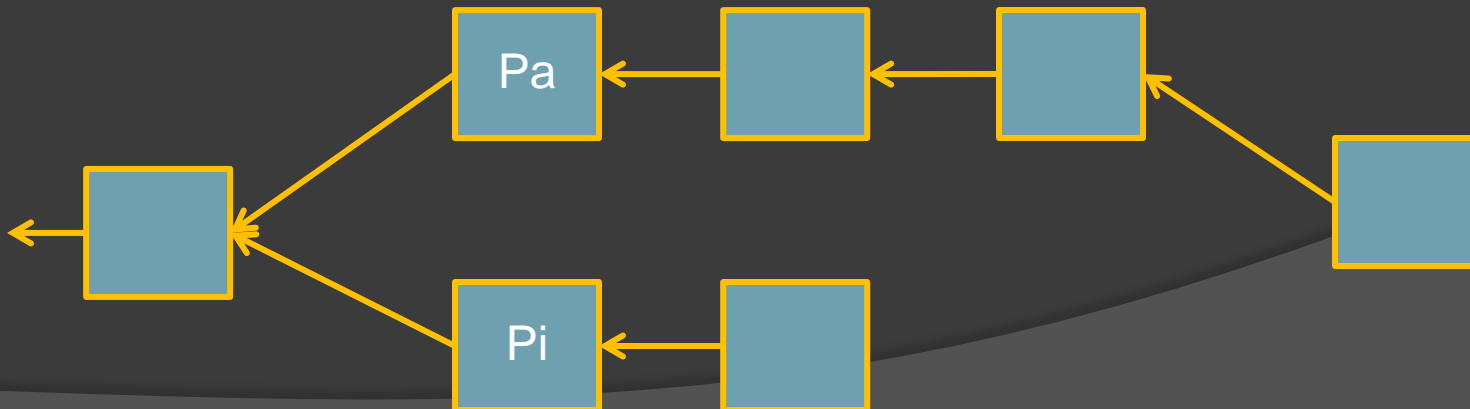


The revelation principle

Tell us about all blocks you saw.

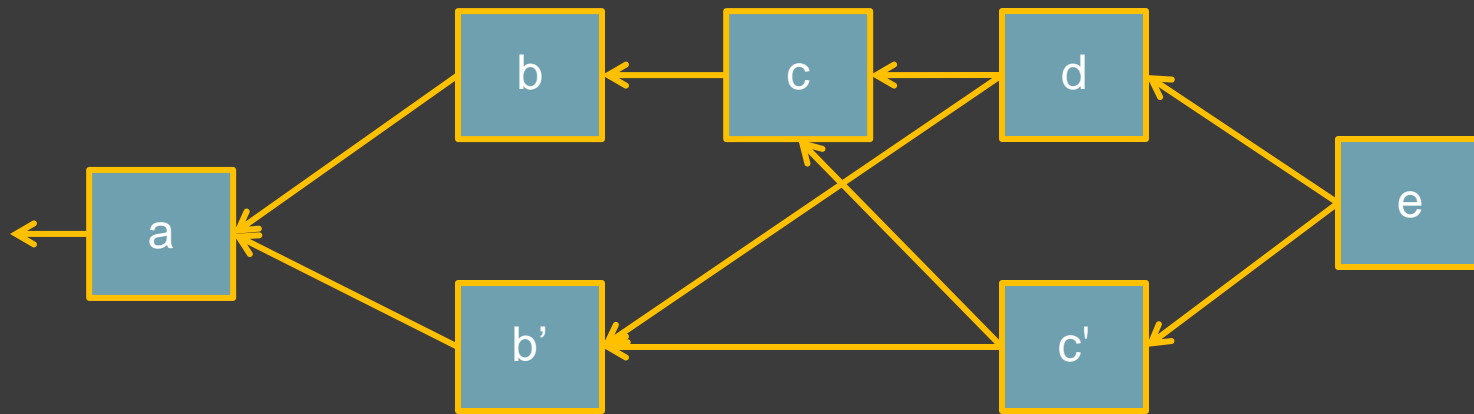


This is now different:



Chainless protocols

Given a DAG

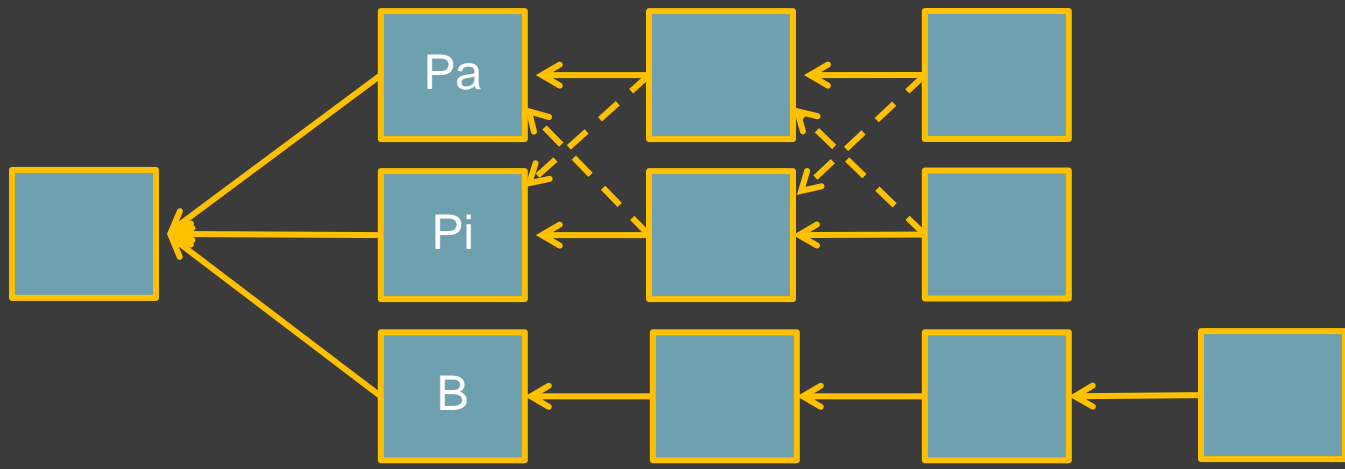
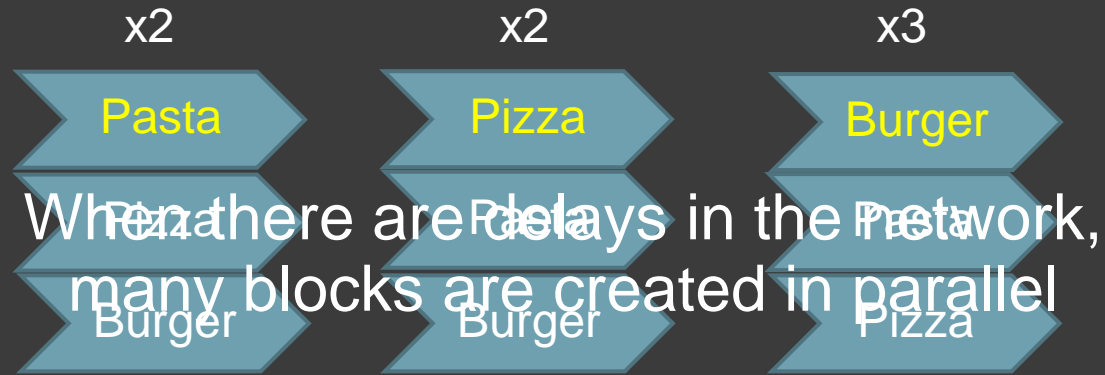


Output a linear order of the blocks (topological sort)



Accept transactions in order of appearance (toss out illegal ones)

Insight from social choice



Blocks Pa, Pi have no conflicting transactions.
Can we consider them “accepted”?

Our result: a new protocol (on ArXiv soon)

◎ Chainless

- we pick an order over all blocks



◎ Resilience in the presence of delays.

- Double spending attacks
- Confirmation delay attacks
(unless it is for a visible double-spend)

◎ Based on voting with “ranked pairs”

◎ Blocks have “preferences”

- prefer blocks that they see over ones they do not.

◎ (Unfortunately, much more complicated)

Conclusion



Simple



Complex

- Bitcoin already “exceeds expectations”

Incentives are needed!

- I am optimistic!



- More insights from social choice?

Thank You!

email: avivz@cs.huji.ac.il