Blockchain Consensus, Opinion Diffusion & Simple Games

Davide Grossi

Bernoulli Institute

university of groningen

www.ankemarijedamdesign.nl

Outline

□ **PART I**: The Consensus Problem

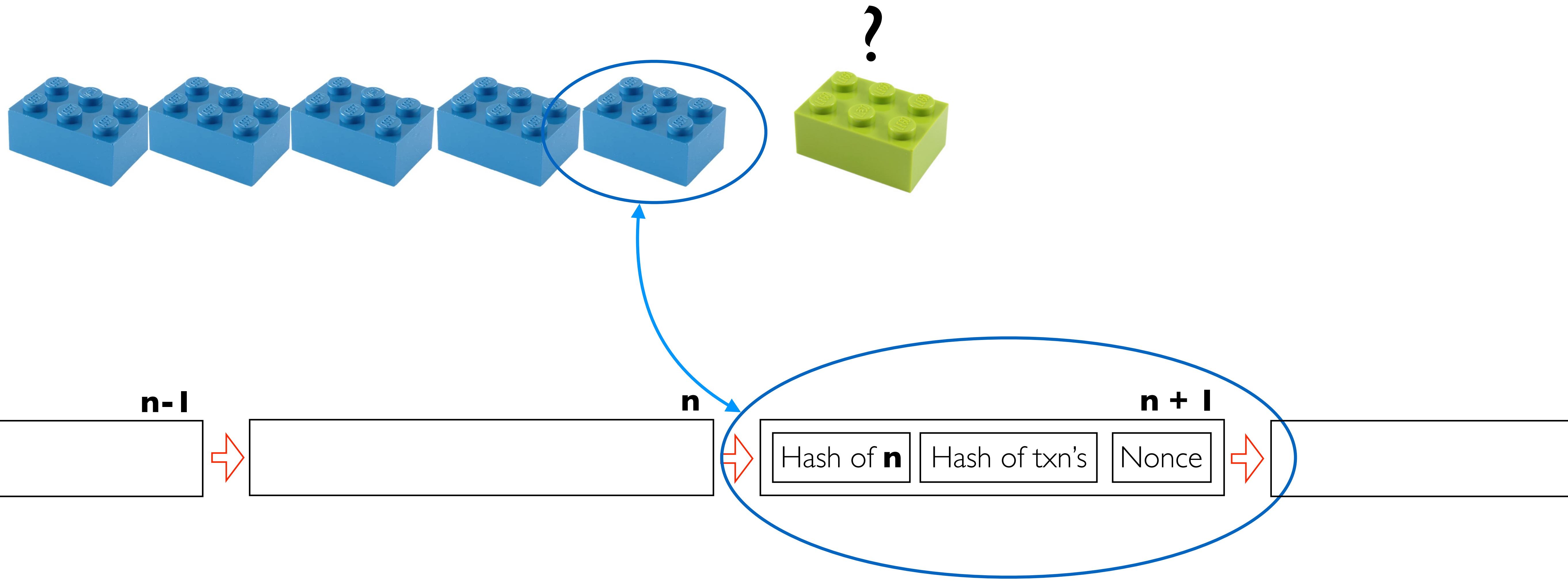
□ **PART II**: Nakamoto Consensus & beyond

□ **PART III**: A COMSOC analysis of Ripple & Stellar

PRELIMINARIES

$$\text{``Blockchain''} = \underbrace{\text{Blockchain}}_{\text{data structure}} + \text{Consensus Protocol}$$

Blockchain as data structure



?

n-1

n

n + 1

Hash of **n**

Hash of txn's

Nonce

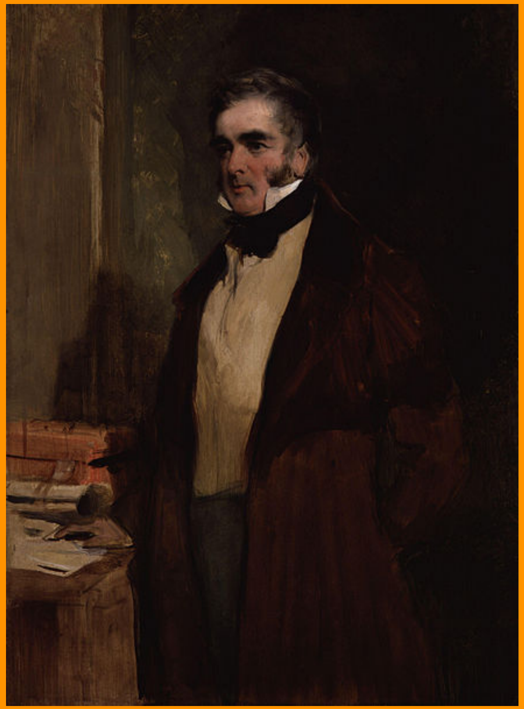
PART I

The problem of Consensus

(or: ***How to build a blockchain?***)

It is not much matter which we say, but mind, we must all say the same

Lord Melbourne (1830-1834)



The Byzantine Generals Problem

LESLIE LAMPORT, ROBERT SHOSTAK, and MARSHALL PEASE
SRI International

Daniel Z "DNL"

□ If they attack together they can win

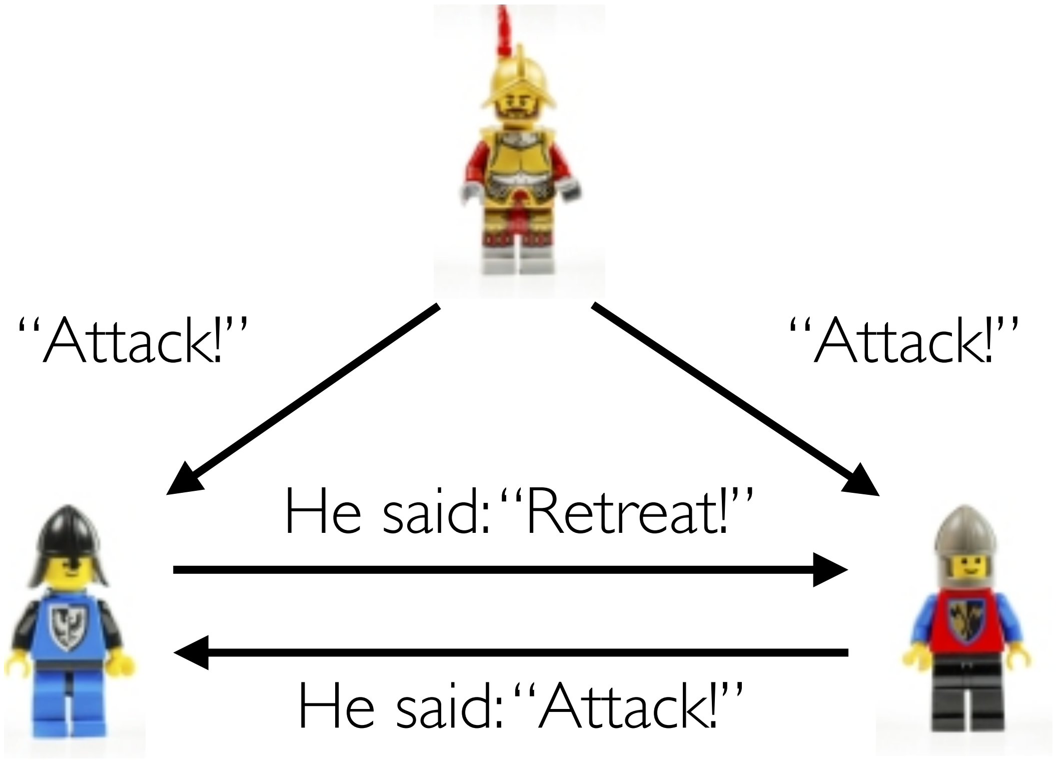
□ If they don't those attacking will be defeated

□ Some may be traitors (Byzantine)

□ Desideratum: *If the general is loyal*, then every *loyal lieutenant* obeys the same order

□ Solvable with private messages if:
|Loyals| > 3|Non-Loyals|

□ … *and if communication is synchronous*



	Attack	Wait
Attack	Win	Lose
Wait	Lose	Wait

Impossibility of Consensus

- □ **If** the system is
  - □ asynchronous (unbounded message delays)
  - □ and it is possible that one process is faulty (crashes)
- □ **then** there is no protocol that
  - □ Achieves consensus
  - □ And always terminates (never gets stuck)

Fischer, Lynch, Paterson. Impossibility of Distribured Consensus with One Faulty Process. Journal of the ACM, 1985

FLP impossibility

So what was the state-of-affairs pre-Bitcoin?

□ Protocols have been proposed and deployed (e.g. PAXOS, Practical Byzantine Fault-Tolerance)

□ They use randomisation or accept possibility of non-termination

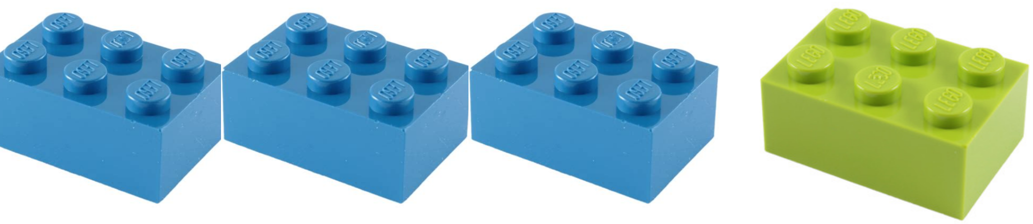
□ **BUT** they all rely on a 'closed' system (permissioned): the set of processes participating in consensus are known and fixed

□ Blockchains (typically) operate in an 'open' system (permissionless) where processes come and go

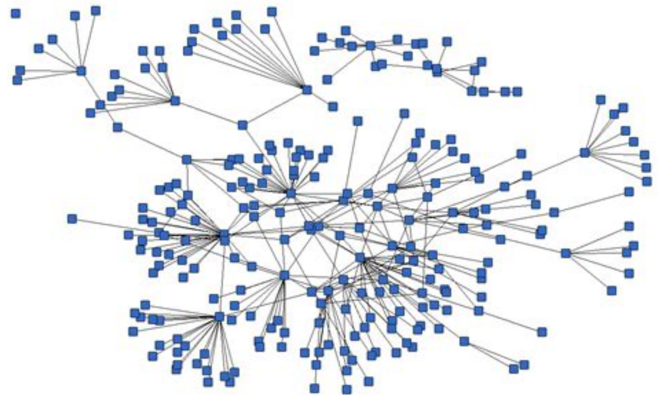
□ The breakthrough of Bitcoin was to show that (randomized) consensus is possible even in such settings

PART II

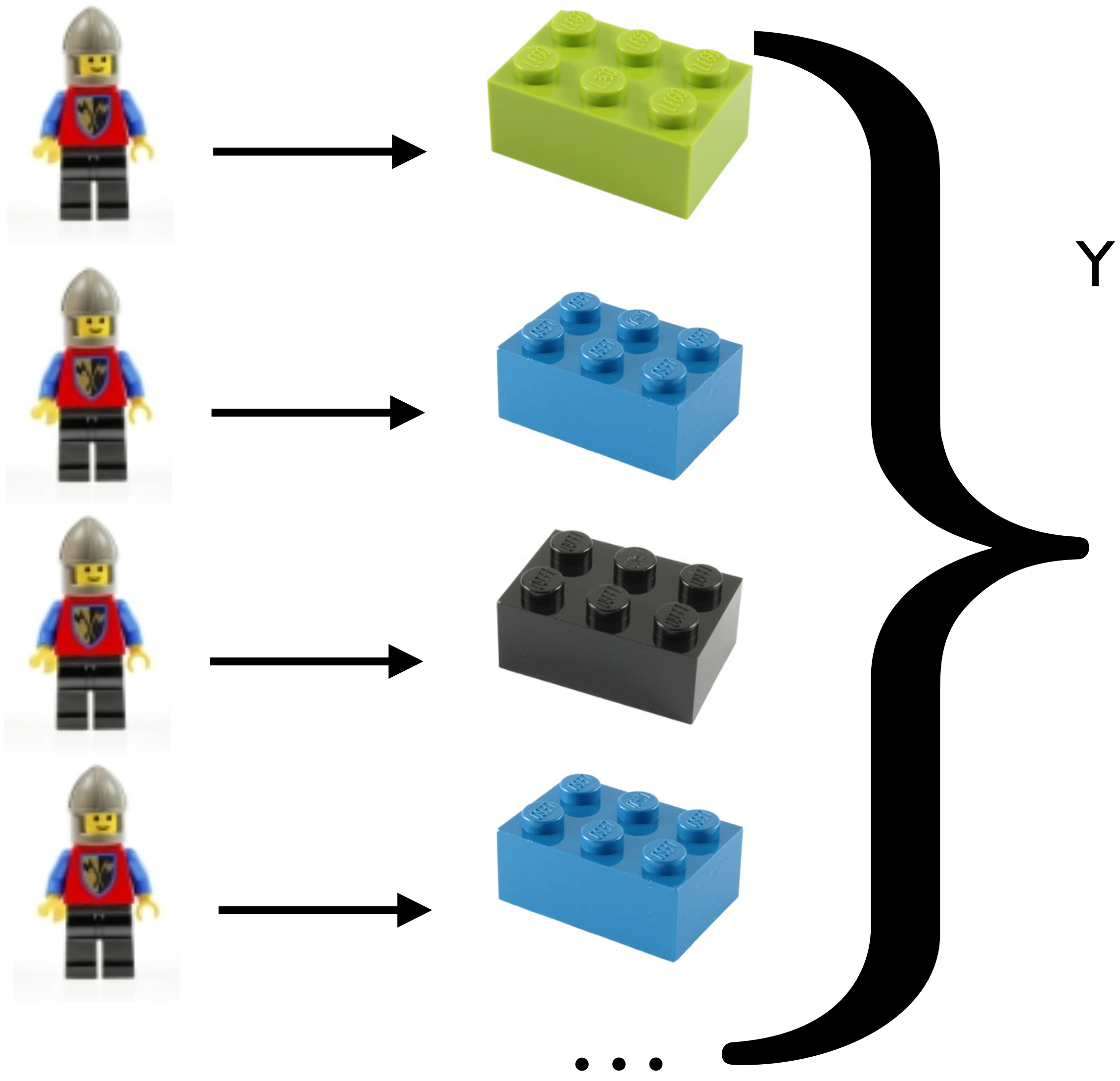
Nakamoto Consensus (& Beyond)



Which block should we add?

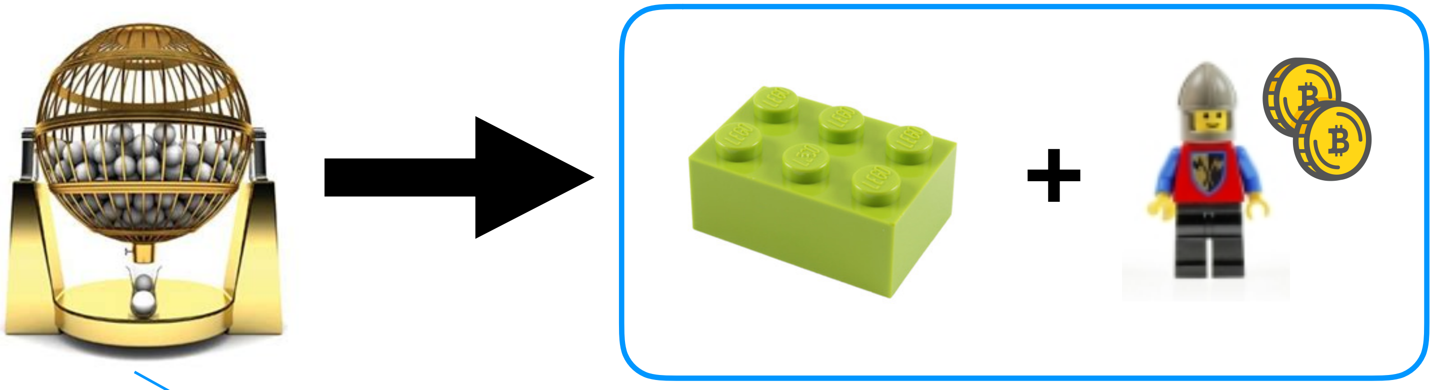


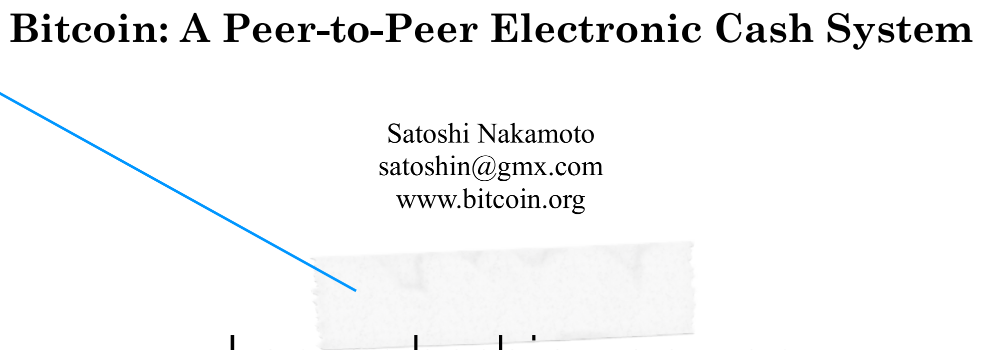
IDEA Let nodes propose blocks and select one at random



Problems?

YES Sybil attack!





Bitcoin: A Peer-to-Peer Electronic Cash System

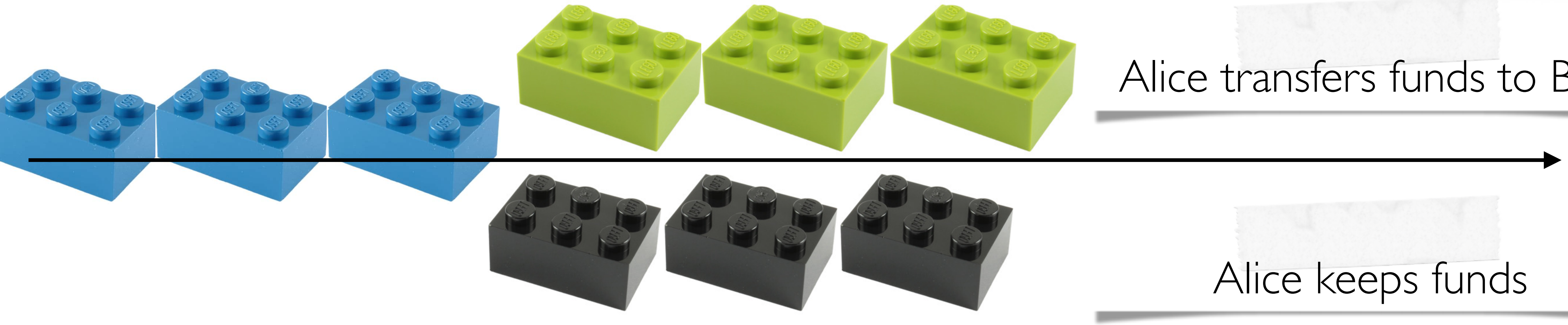
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Larger hashing power
Higher winning chances

What's consensus for (in Bitcoin)?

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org



Alice transfers funds to Bob

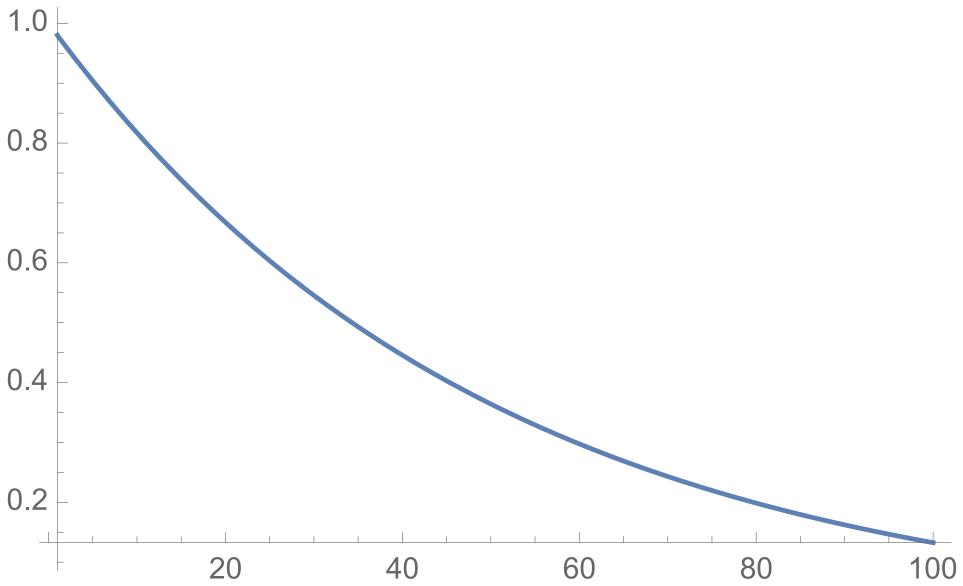
Alice keeps funds

- □ Consensus makes Double-Spending (**forks**) highly unlikely
- □ An attacker should 'catch up' on the honest chain

Probability a **honest** node mines next block

Number of blocks

$$\left(\frac{(1-p)}{p}\right)^{n}$$



‘Properties’ of Nakamoto consensus

This is how Bitcoin gets around the FLP impossibility!

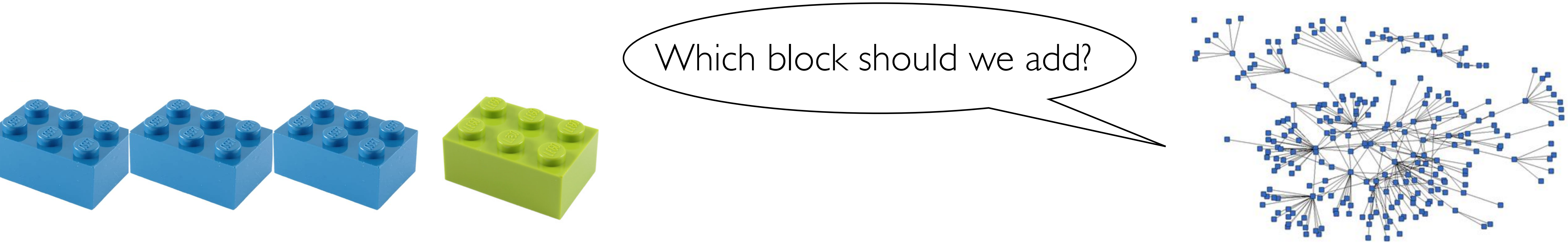
- □ **Eventual consensus**: at all times, all honest nodes will agree on a prefix of the blockchain which will become a prefix of the eventual blockchain
- □ **Exponential convergence**: the probability of a fork decreases exponentially with the length of the fork
- □ **Liveness**: new blocks will continue to be added
- □ **Correctness**: the longest chain will contain only valid transactions
- □ **Fairness**: In expectation, a miner with share p of the total hashing power will mine a p share of all blocks

Bonneau, Miller Clark, Narayanan, Kroll, Fekten. Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. 2015

A. Miller, J. LaViola. Anonymous Byzantine Consensus from Moderately-Hard Puzzles: A Model for Bitcoin, 2014

B. Biais, C. Bisiere, M. Bouvard, C. Casamatta. The Blockchain Folk Theorem. TSE Working Papers, 17-187, 2018

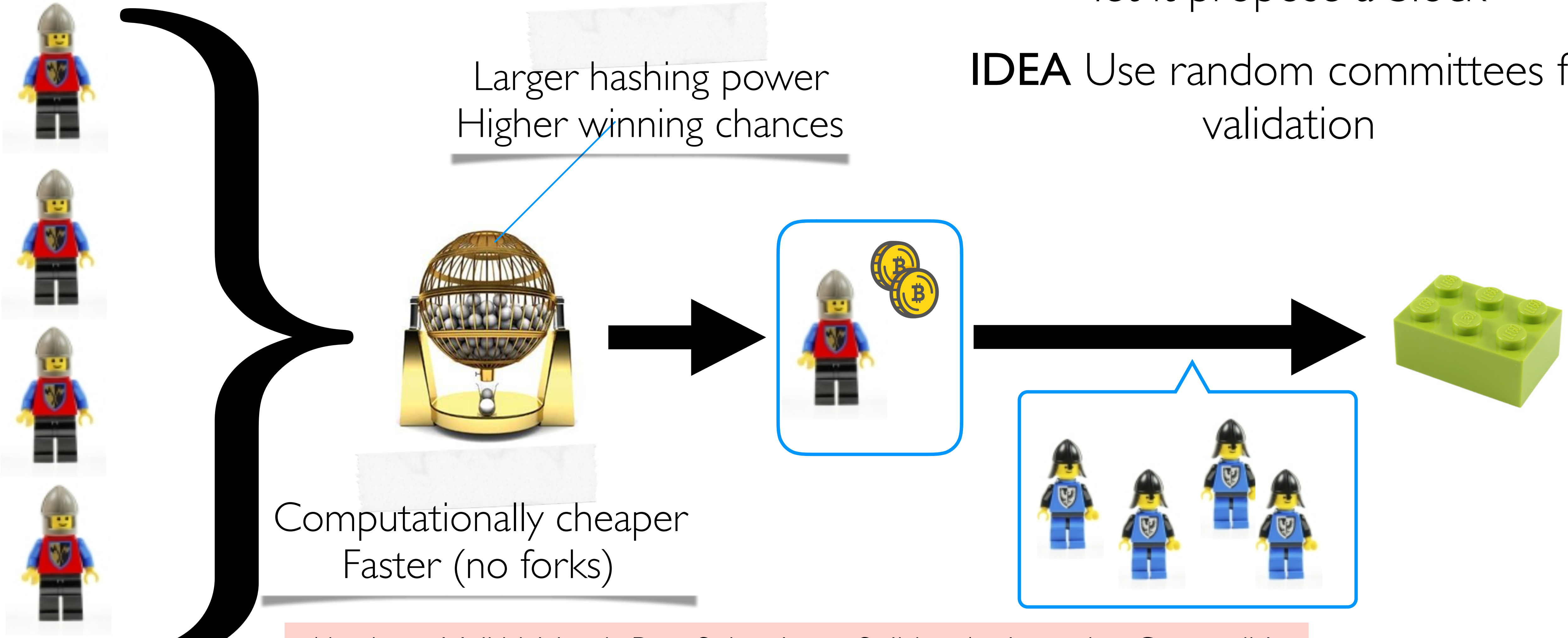
Stifter, Judmayer, Schindler, Zamayatin, Weippl. Agreement with Satosh: On the Formalisation of Nakamoto Consensus. 2017



Solidus

IDEA Select a node at random and let it propose a block

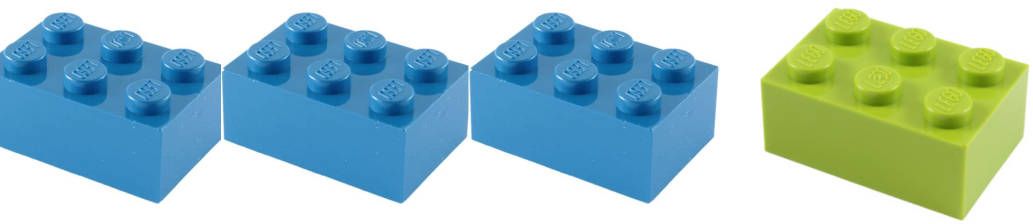
IDEA Use random committees for validation



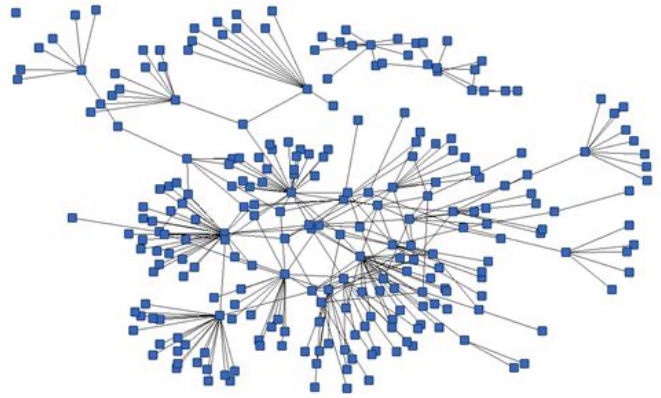
Larger hashing power
Higher winning chances

Computationally cheaper
Faster (no forks)

Abraham, Malkhi, Nayak, Ren, Spiegelman. Solidus: An Incentive-Compatible Cryptocurrency Based on Permissionless Byzantine Consensus, 2016



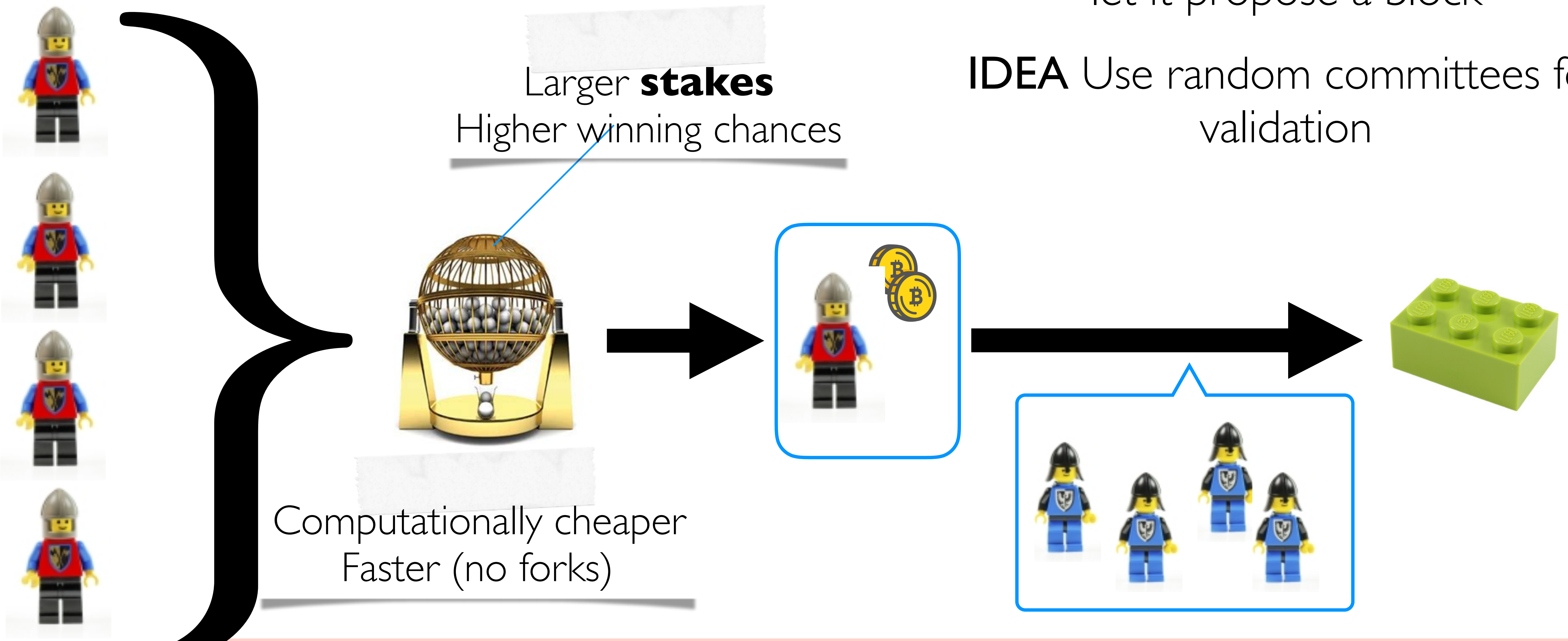
Which block should we add?



Algorand

IDEA Select a node at random and let it propose a block

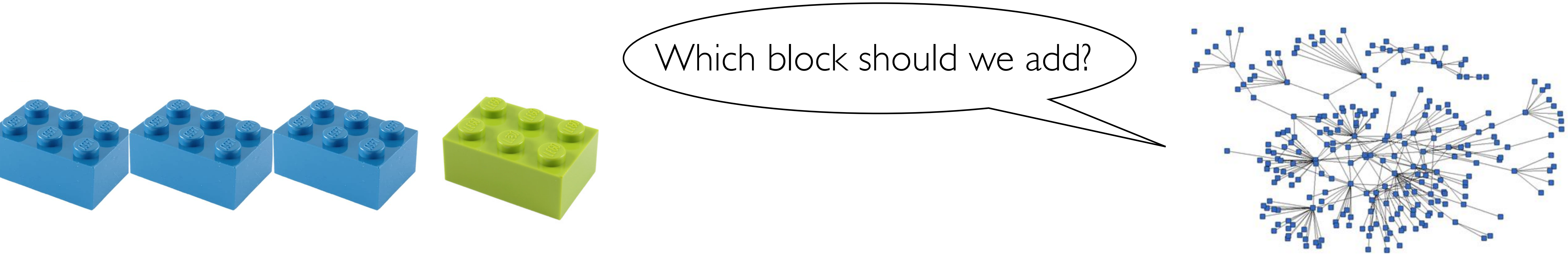
IDEA Use random committees for validation



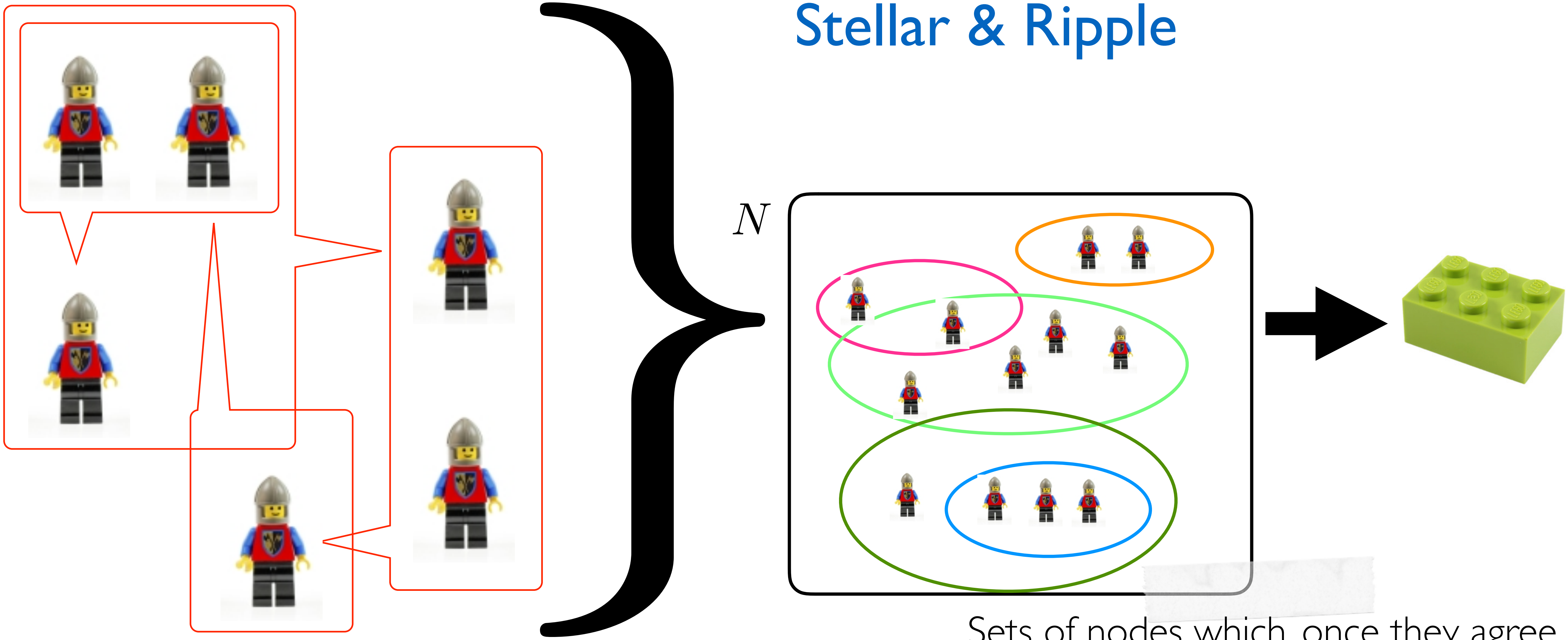
Larger **stakes**
Higher winning chances

Computationally cheaper
Faster (no forks)

Gilad, Hemo, Micali, Vlachos, Zeldovich. Algorand: Scaling byzantine agreements for cryptocurrencies. 2017



Stellar & Ripple



Sets of nodes which, once they agree on a value, they stabilise on that value

D. Mazyieres. The Stellar Consensus Protocol. Stellar Development Foundation 2015

PART III

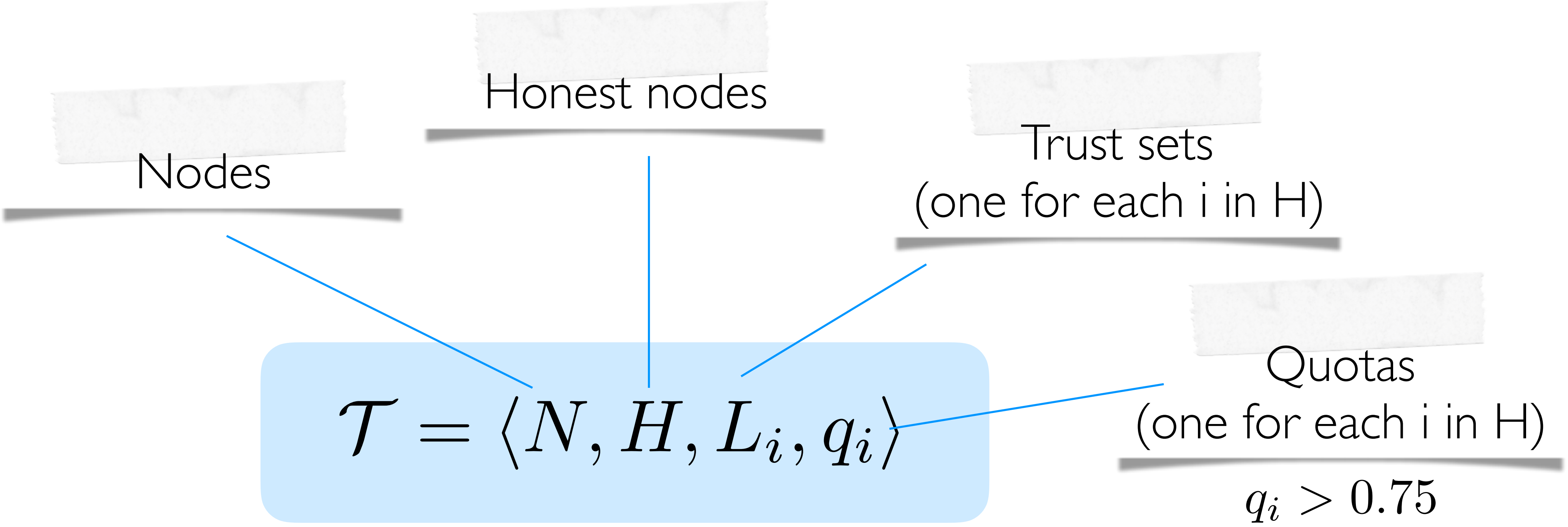
COMSOC of Ripple & Stellar

Andrea Bracciali

Ronald de Haan

UNIVERSITY of STIRLING

Byzantine Trust Networks (BTNs)



Nodes

Honest nodes

Trust sets
(one for each i in H)

Quotas
(one for each i in H)

$q_i > 0.75$

$$\mathcal{T} = \langle N, H, L_i, q_i \rangle$$

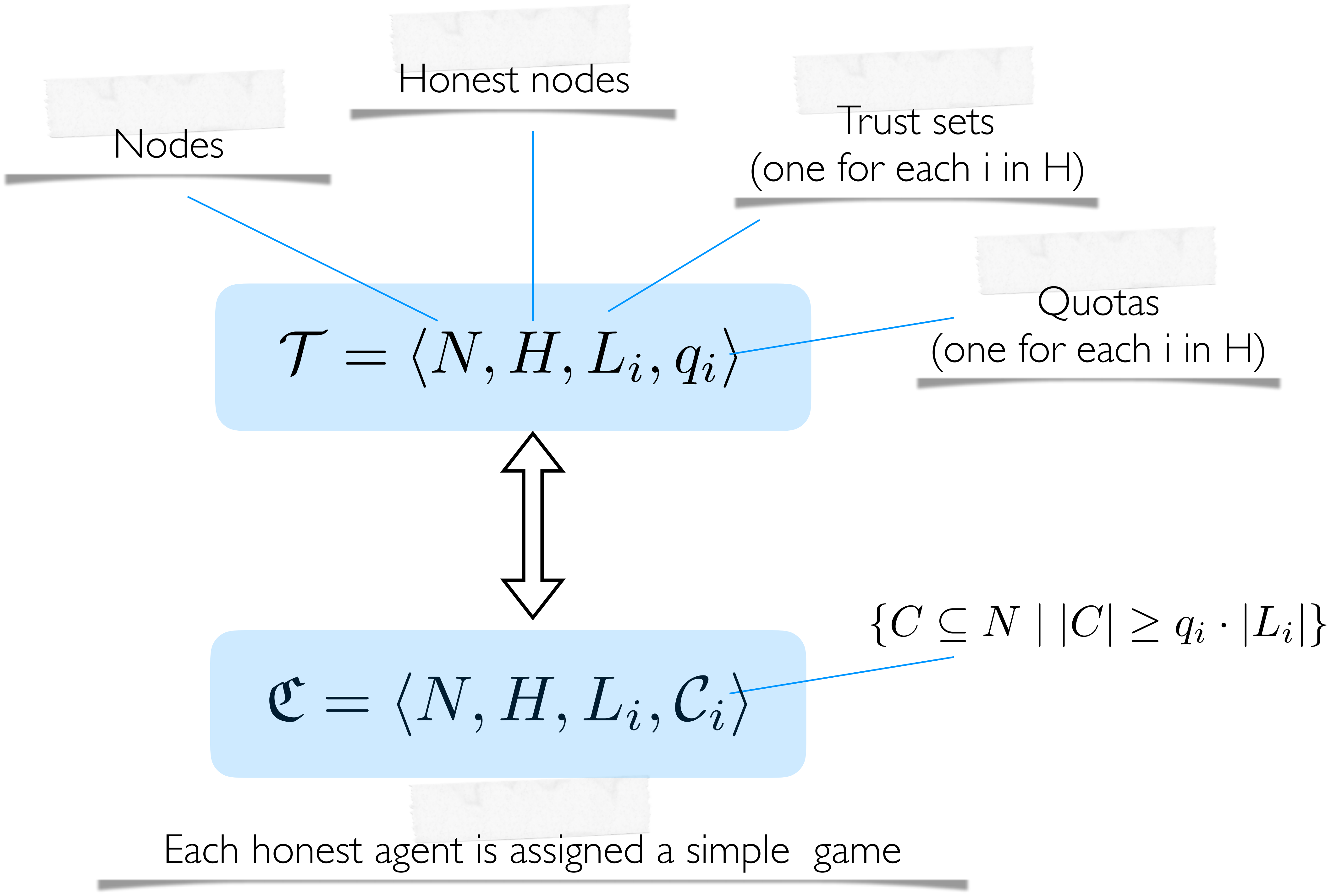
- □ Nodes make binary decisions
- □ … influenced by trusted nodes (if enough trusted nodes have opinion x then take up opinion x)
- □ Byzantine nodes can reveal any opinion to any honest node

$$\mathbf{o} : N \rightarrow \{0,1\} \cup \{0,1\}^H$$

$$\text{s.t. } \mathbf{o}(i) \in \{0,1\} \text{ if } I \in H \text{ and } \mathbf{o}(i) \in \{0,1\}^H \text{ if } I \in B.$$

university of
groningen

Command Games



Nodes

Honest nodes

Trust sets
(one for each i in H)

Quotas
(one for each i in H)

$$\mathcal{T} = \langle N, H, L_i, q_i \rangle$$

$$\Updownarrow$$

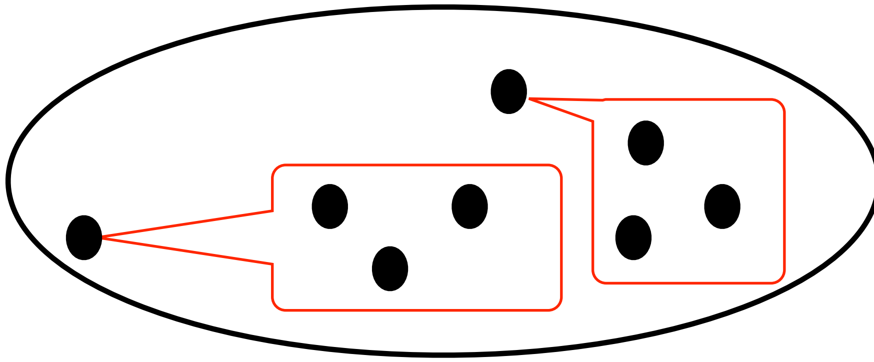
$$\{C \subseteq N \mid |C| \geq q_i \cdot |L_i|\}$$

$$\mathfrak{C} = \langle N, H, L_i, \mathcal{C}_i \rangle$$

Each honest agent is assigned a simple game

X. Hu and L. Shapley. On authority distributions in organizations: Controls. Games and Economic Behavior, 45:153–170, 2003.
X. Hu and L. Shapley. On authority distributions in organizations: Equilibrium. Games and Economic Behavior, 45:132–152, 2003.

Consensus in BTNs



An opinion profile $\mathbf{o}$ is a *consensus* profile (for $\mathcal{T}$) if, for all $i \in H$:

$$\mathbf{o}(i) = x \iff \forall j \in H, |L_j^{\mathbf{o}}(x) \cap H| > 0.5 \cdot |L_j|$$

$x \in \{0, 1\}$

Honest nodes cannot possibly hold a different opinion

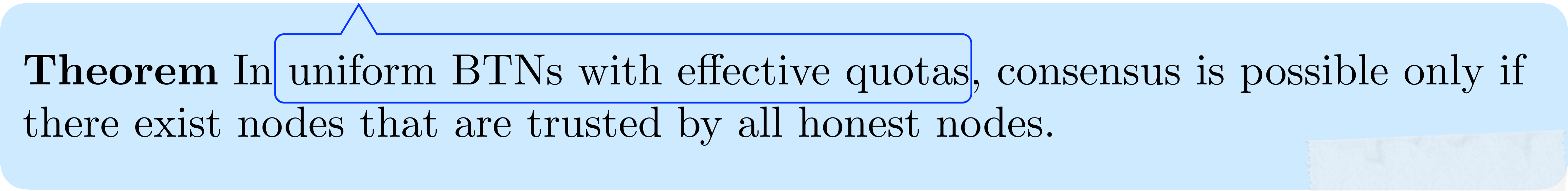
Questions:

□ What kind of implications does this notion of consensus have on the level of decentralisation BTNs?

□ … and on the relative influence of nodes on the consensus process?

Consensus & Decentralization in BTNs

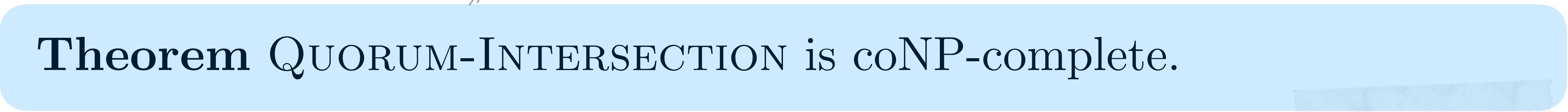
Ripple



Theorem In uniform BTNs with effective quotas, consensus is possible only if there exist nodes that are trusted by all honest nodes.

Fully decentralised consensus is impossible

Stellar



Theorem Quorum-Intersection is coNP-complete.

Maintaining the good-behaviour of the BTN is intractable

Influence

$$\mathfrak{C} = \langle N, H, \boxed{L_i, \mathcal{C}_i} \rangle$$

Influence matrix
(stochastic)

$$I = \begin{bmatrix} I_{11} & I_{12} & I_{13} & \dots & I_{1n} \\ I_{21} & I_{22} & I_{23} & \dots & I_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ I_{n1} & I_{n2} & I_{n3} & \dots & I_{nn} \end{bmatrix}$$

Penrose/Banzhaf index

$$\frac{1}{2^n} \sum_{C \subseteq N \setminus \{j\}} v(C \cup \{j\}) - v(C)$$

$$\boxed{I^* = \lim_{t \to \infty} I^t} \;?$$

Long-term influence

Theorem Let $\mathcal{T}$ be a uniform BTN with effective quotas. If $\mathcal{T}$ is consensus-enabling, then:

a) there exists a unique fixpoint $\boxed{\pi = \pi \cdot I}$, where I is the influence matrix induced by $\mathcal{T}$;

b) there are honest nodes with positive long-term influence iff $\bigcap_{I \in H} H_i$ does not contain byzantine nodes.

Byzantine node may determine
what the consensus is

Summary

□ Crash-course in blockchain consensus protocols

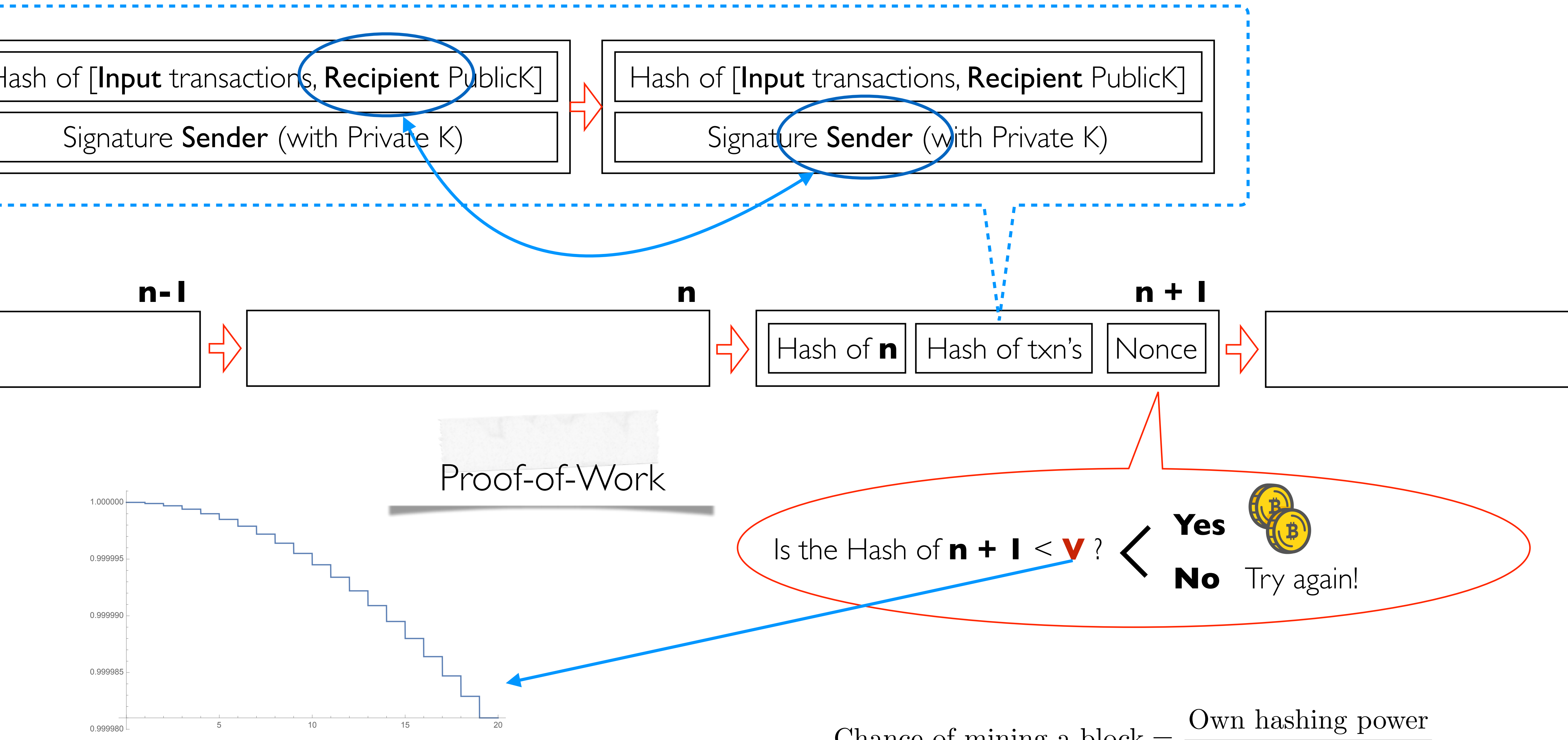
□ Relevance of COMSOC methods for their analysis

Bonus

Nakamoto Consensus

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org



Hash of [**Input** transactions, **Recipient** PublicK]
Signature **Sender** (with Private K)
Hash of [**Input** transactions, **Recipient** PublicK]
Signature **Sender** (with Private K)
n-1
n
n + 1
Hash of **n**
Hash of txn's
Nonce
Is the Hash of **n + 1** < **V** ?
Yes
No
Try again!
1.000000
0.999995
0.999990
0.999985
0.999980
5
10
15
20

Proof-of-Work

$$\text{Chance of mining a block} = \frac{\text{Own hashing power}}{\text{Total hashing power}}$$

Why mining?

□ All pay - one wins

□ R&D race

□ NE exists and is unique

i's hashing power

probability that **i** fails solving the puzzle first

$$u_i(\mathbf{h}) = (R - c_i h_i) \cdot \boxed{\frac{h_i}{\sum_{j\in N} h_j}} - c_i h_i \cdot \boxed{\frac{h_{-i}}{\sum_{j\in N} h_j}}$$

Investments in hashing power

Reward for solving puzzle

i's cost of hashing

probability that **i** solves the puzzle first

J. Ma, J. Gans, R. Tourky. Market Structure in Bitcoin Mining. NBER Working Paper, 2018

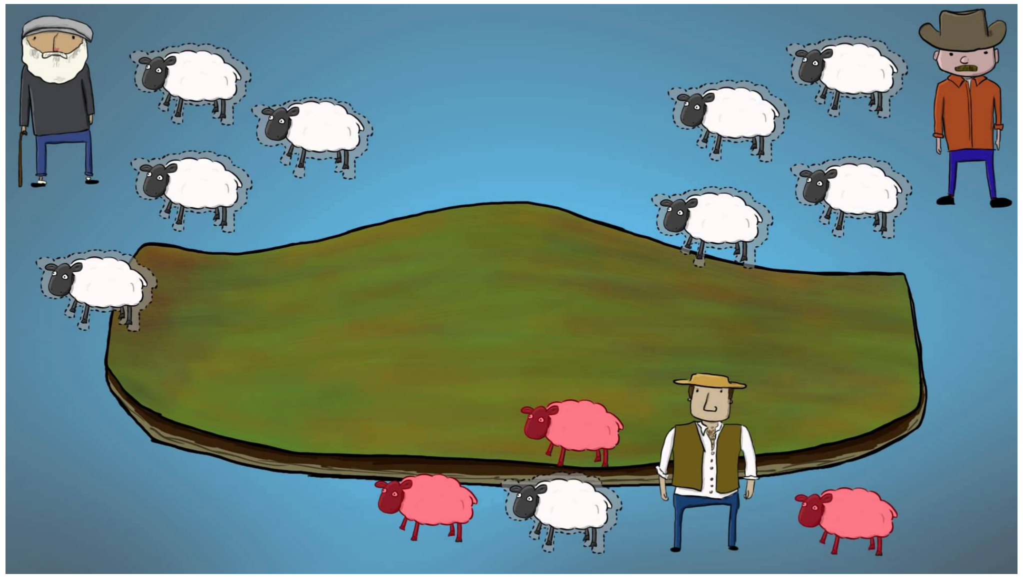
N. Dimitri. Bitcoin Mining as a Contest. Ledger, 2017

Why Verifying?

□ In Bitcoin verification work is negligible compared to mining, but that’s not the case in general (see Ethereum)

□ Miners are aware that non-valid transactions have the potential to decrease Bitcoin’s value

□ But this is ultimately a **public good** game and there is potential for 'tragedy of the commons’ scenario

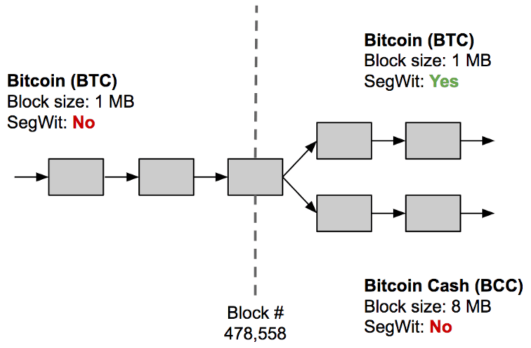


L. Luu, J. Teusch, R. Kulkarni, P. Saxena. Demistifying Incentives in the Consensus Computer, CCS’15, 2015

Blockchain Folk-Theorem

Nakamoto Consensus rules out the occurrence of forks

- □ True, at certain levels of abstraction
- □ But …



```
23:06   Luke Dashjr        so??? yay accidental hardfork? :x
23:06   Jouke Hofman       Holy crap


23:22   Gavin Andresen     the 0.8 fork is longer, yes? So majority hashpower is 0.8....
23:22   Luke Dashjr        Gavin Andresen: but 0.8 fork is not compatible earlier will be accepted by
all versions

23:23   Gavin Andresen     first rule of bitcoin: majority hashpower wins
23:23   Luke Dashjr        if we go with 0.8, we are hardforking


23:24   Luke Dashjr        so it's either 1) lose 6 blocks, or 2) hardfork for no benefit
23:25   BTC Guild      We'll lose more than 6

23:43   BTC Guild      I can single handedly put 0.7 back to the majority hash power I just need
confirmation

23:44   Pieter Wuille      BTC Guild: imho, that is was you should do, but we should have consensus
first
```

A. Narayanan. Analysing the 2013 Bitcoin Fork: Centralized Decision Making Saved the Day, 2015

A. Miller, J. LaViola. Anonymous Byzantine Consensus from Moderately-Hard Puzzles: A Model for Bitcoin, 2014

B. Biais, C. Bisiere, M. Bouvard, C. Casamatta. The Blockchain Folk Theorem. TSE Working Papers, 17-187, 2018

Blockchain Folk-Theorem

Nakamoto Consensus rules out the occurrence of forks

Keynes' Beauty Contest

- □ With no centralised solution:
  - □ Gradual consensus towards 0.8 branch (vs 0.7)
  - □ Coordination on which branch to mine harder/slower
  - □ Double spending attacks more possible
  - □ Fork would survive longer (than 8hrs), likely because of vested interest of miners on 0.7 fork

Shubik's dollar auction

A. Narayanan. Analysing the 2013 Bitcoin Fork: Centralized Decision Making Saved the Day, 2015

A. Miller, J. LaViola. Anonymous Byzantine Consensus from Moderately-Hard Puzzles: A Model for Bitcoin, 2014

B. Biais, C. Bisiere, M. Bouvard, C. Casamatta. The Blockchain Folk Theorem. TSE Working Papers, 17-187, 2018