Andrea Bracciali

UNIVERSITY of STIRLING

Ronald de Haan

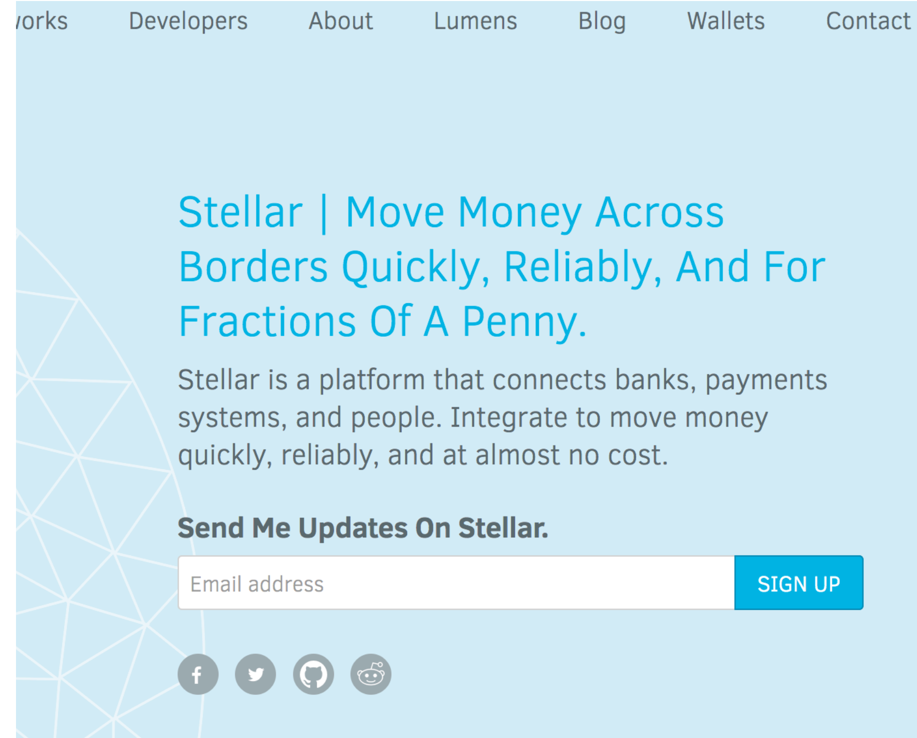
Decentralization in Open Quorum Systems

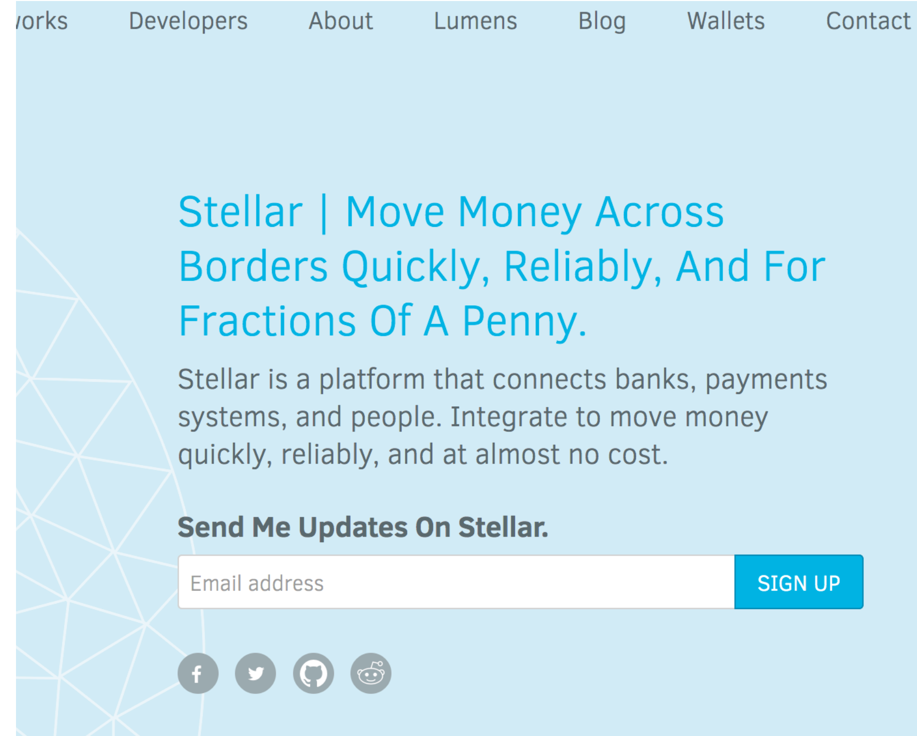
Davide Grossi

university of groningen

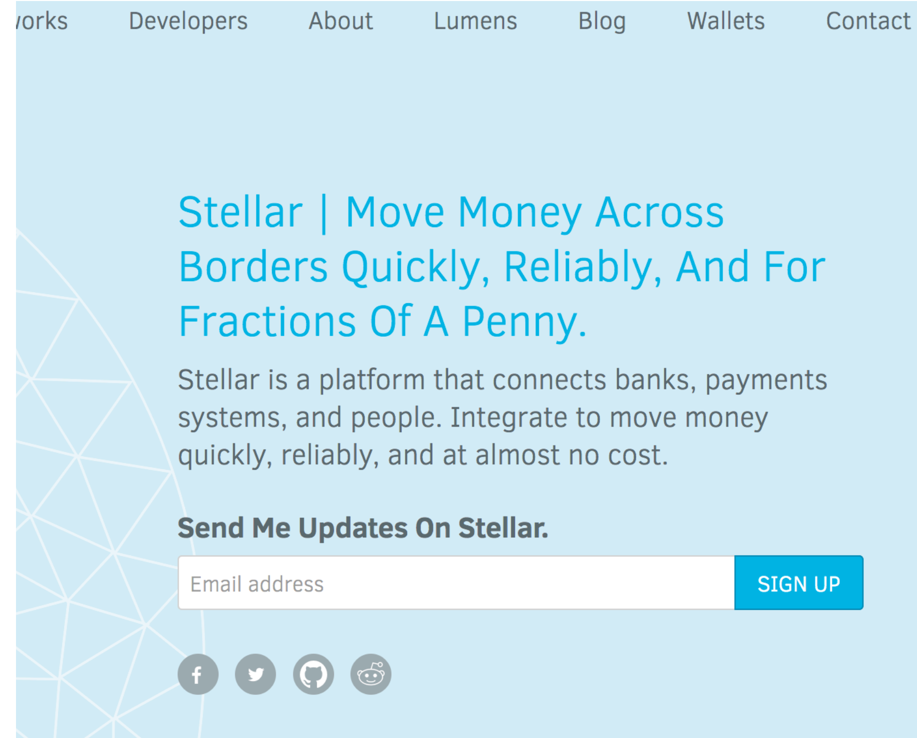
UNIVERSITY OF AMSTERDAM


ripple
RippleNet
Join RippleNet
One frictionless experience to send money globally
How RippleNet Works

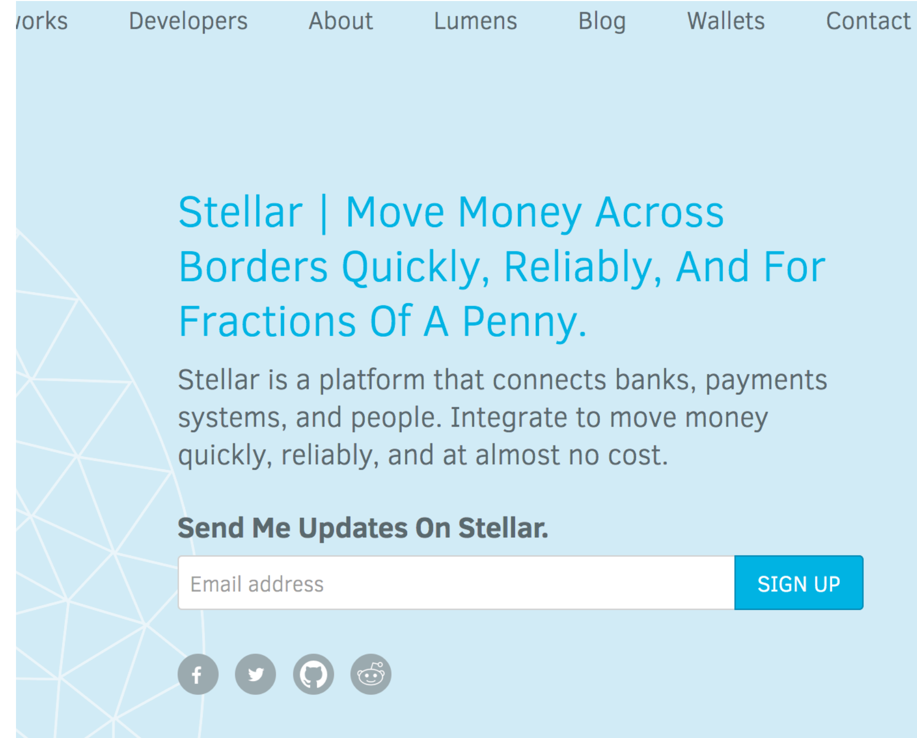

orks
Developers
About
Lumens
Blog
Wallets
Contact
Stellar | Move Money Across Borders Quickly, Reliably, And For Fractions Of A Penny.
Stellar is a platform that connects banks, payments systems, and people. Integrate to move money quickly, reliably, and at almost no cost.
Send Me Updates On Stellar.
Email address
SIGN UP



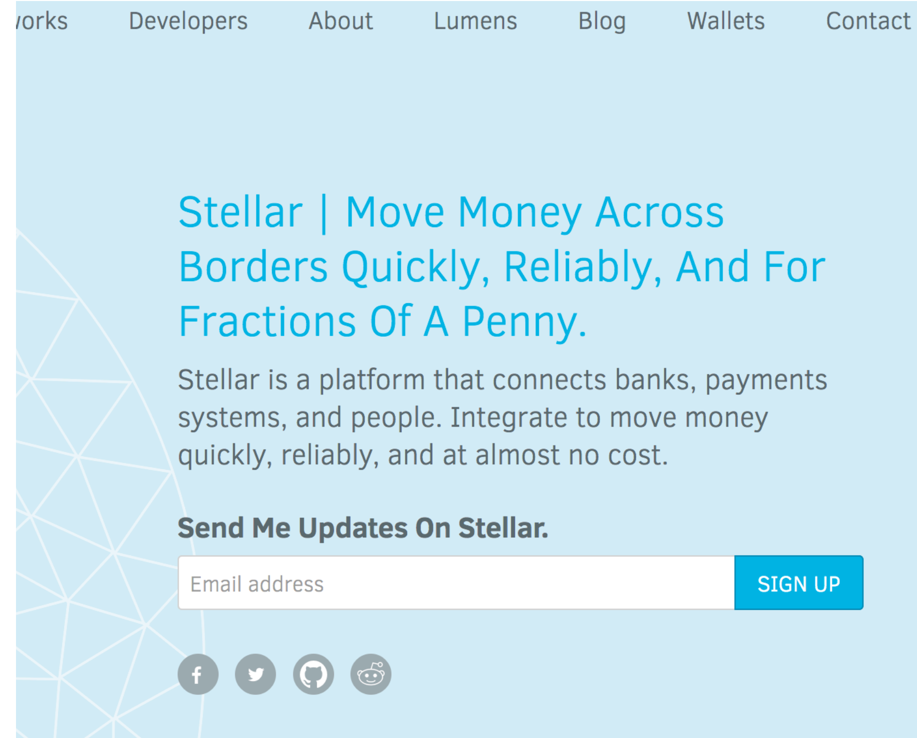
- Ripple & Stellar



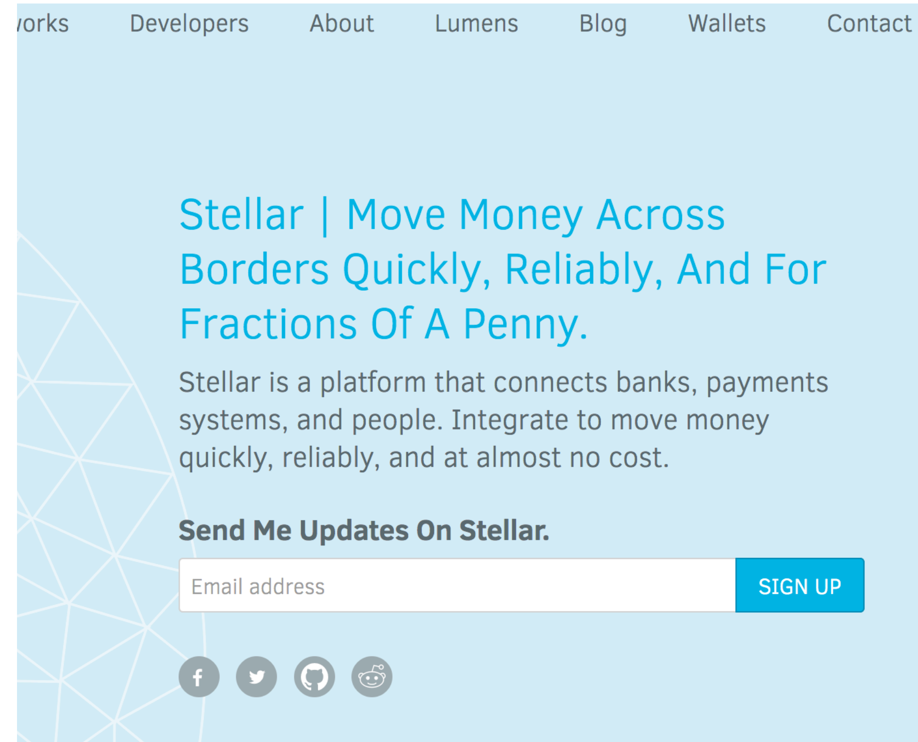
- Ripple & Stellar
- Respectively 4th and 17th largest blockchain companies by market capitalisation



- Ripple & Stellar
- Respectively 4th and 17th largest blockchain companies by market capitalisation
- Relatively few academic research



- Ripple & Stellar
- Respectively 4th and 17th largest blockchain companies by market capitalisation
- Relatively few academic research
- Criticisms to their level of decentralisation (permissioned)

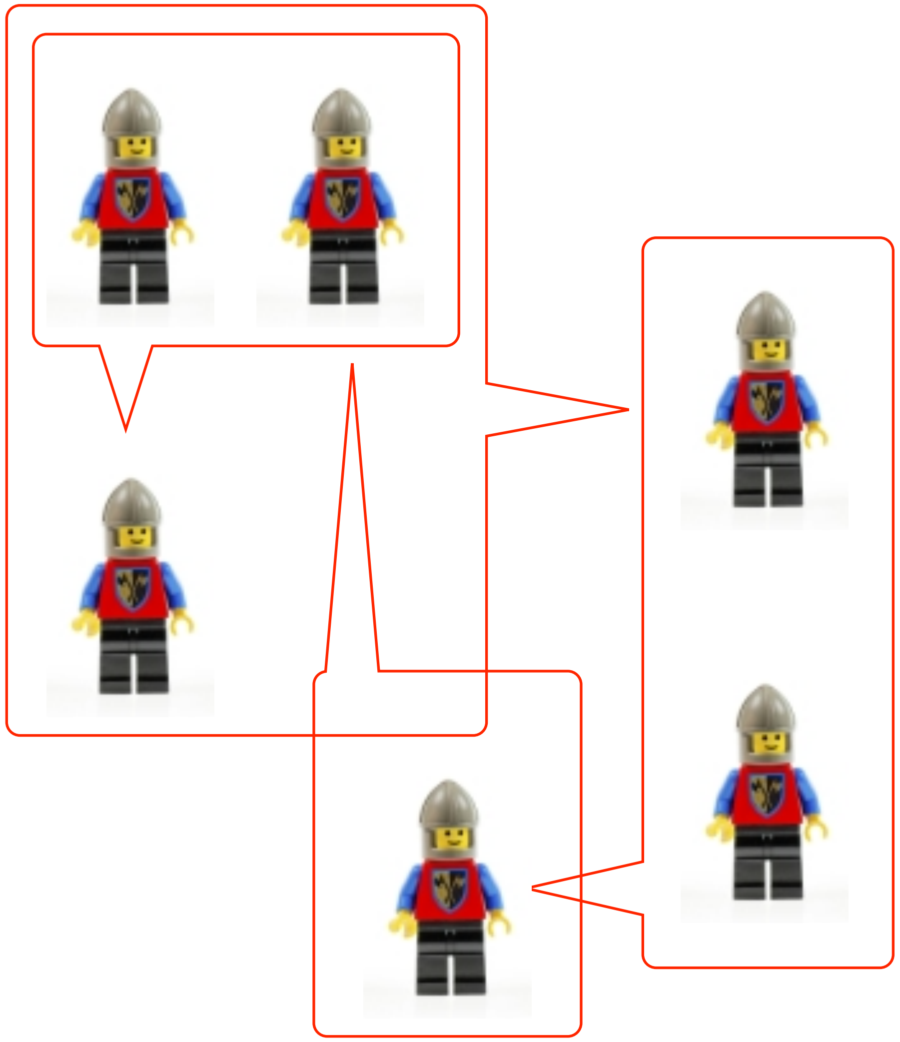


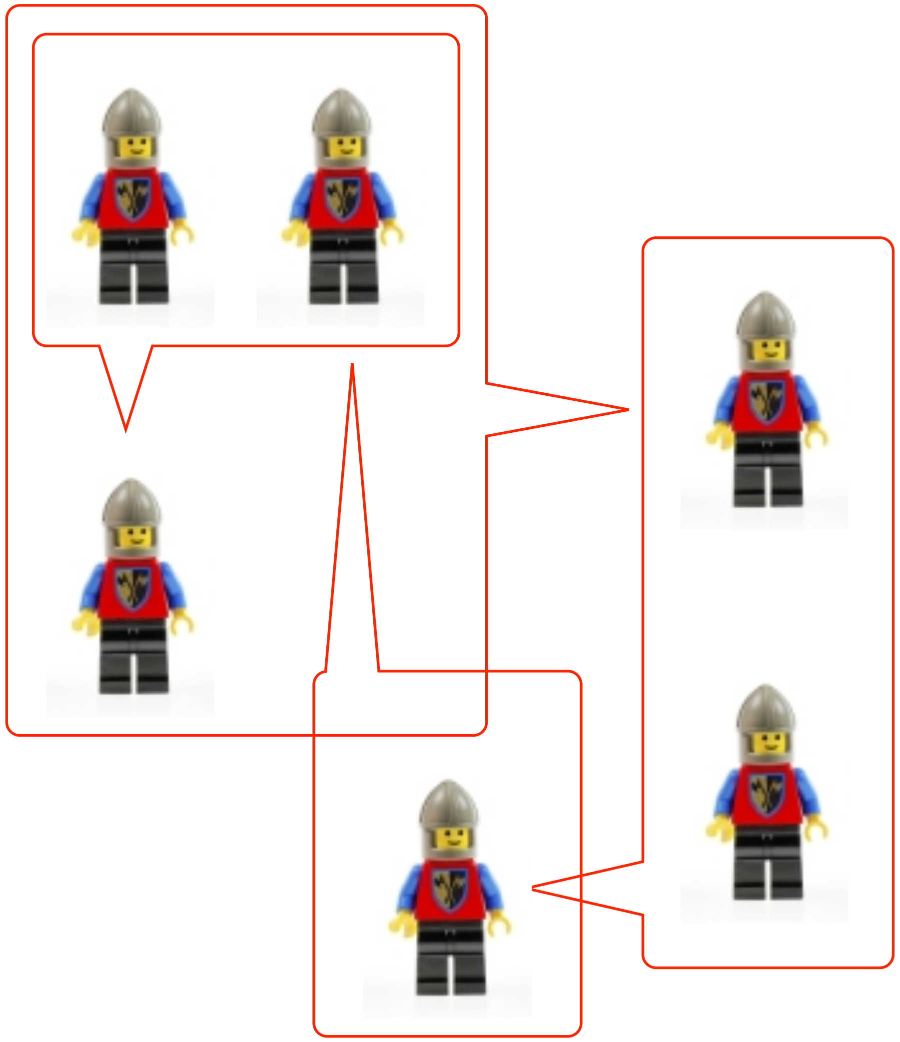
- Ripple & Stellar
- Respectively 4th and 17th largest blockchain companies by market capitalisation
- Relatively few academic research
- Criticisms to their level of decentralisation (permissioned)

Are there inherent limitations to decentralisation in this form of consensus?

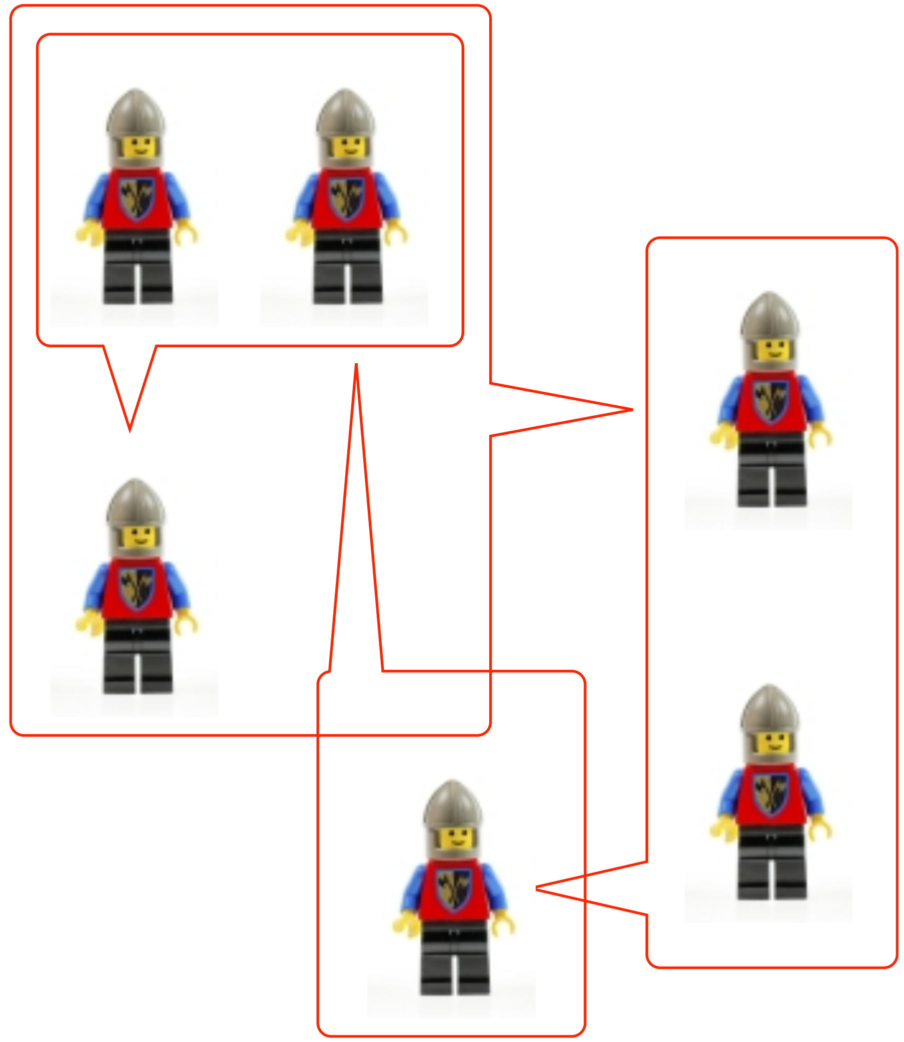
PART I

P2P Trust Networks

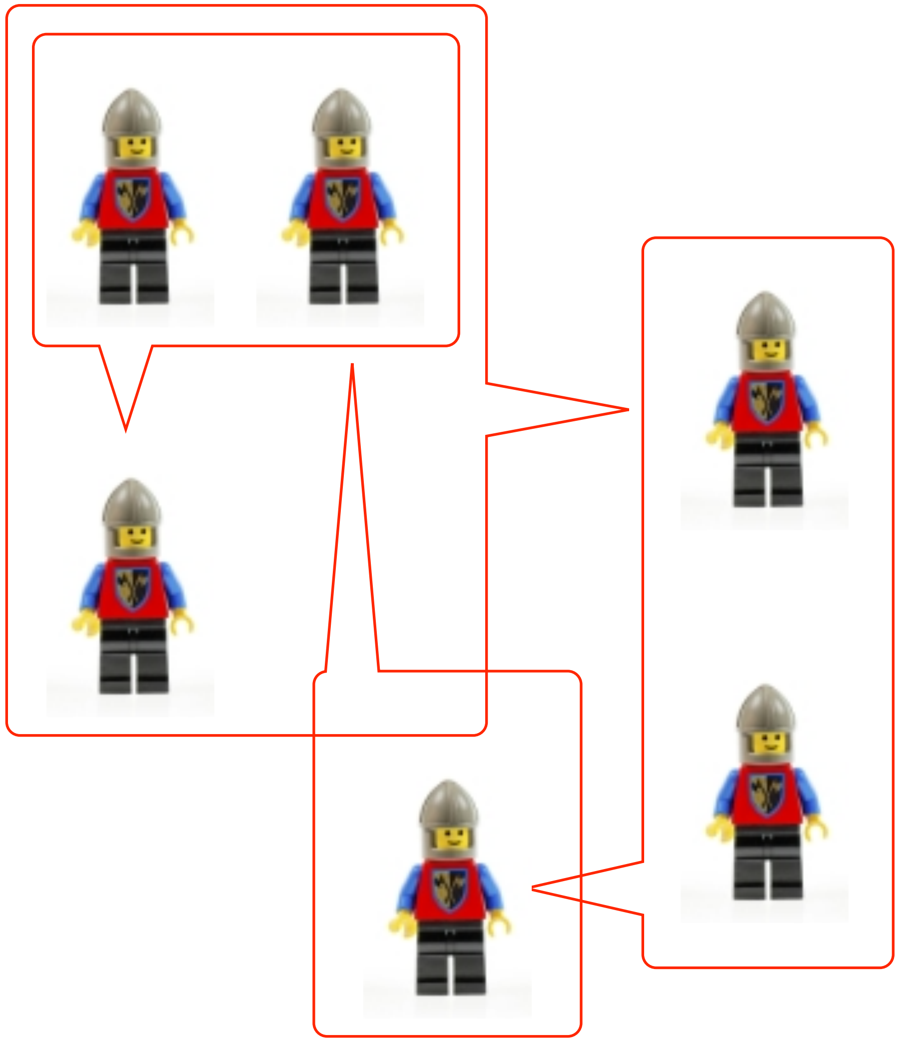




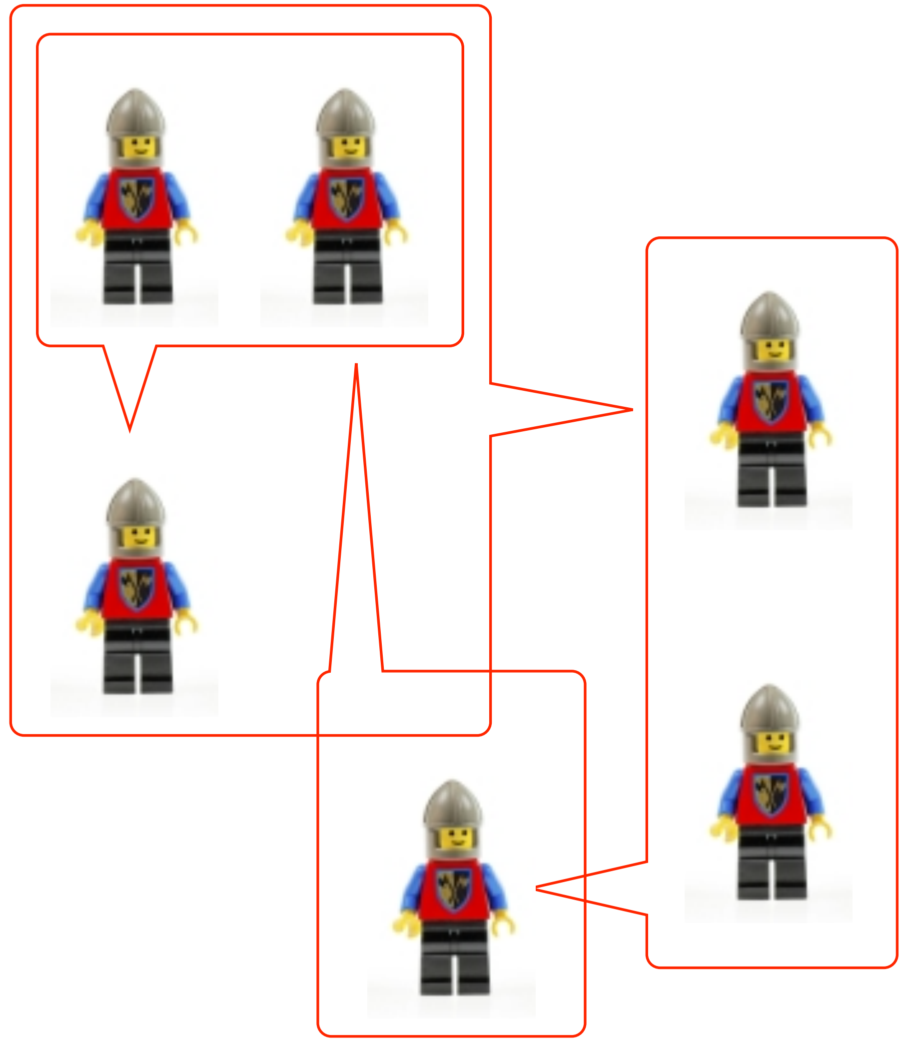
- Nodes select which other nodes to trust (Sybil-proofness)



- ☐ Nodes select which other nodes to trust (Sybil-proofness)
- ☐ … and a quota/threshold to settle their own opinion:



- Nodes select which other nodes to trust (Sybil-proofness)
- … and a quota/threshold to settle their own opinion:
- when a quota of trusted nodes agree (on whether to record a transaction or not) the node settles its value on that agreement



- ☐ Nodes select which other nodes to trust (Sybil-proofness)
- ☐ … and a quota/threshold to settle their own opinion:
- ☐ when a quota of trusted nodes agree (on whether to record a transaction or not) the node settles its value on that agreement
- ☐ CONSENSUS = all honest nodes ***agree stably***

Byzantine Trust Networks (BTNs)

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

Byzantine Trust Networks (BTNs)

Nodes

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

Byzantine Trust Networks (BTNs)

Nodes

Honest nodes

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

Byzantine Trust Networks (BTNs)

Nodes

Honest nodes

Trust sets
(one for each i in H)

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

Byzantine Trust Networks (BTNs)

Nodes

Honest nodes

Trust sets
(one for each i in H)

Quotas
(one for each i in H)

$q \geq 0.75$

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

Byzantine Trust Networks (BTNs)

Nodes

Honest nodes

Trust sets
(one for each i in H)

Quotas
(one for each i in H)

$q \geq 0.75$

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

- ☐ Nodes make binary decisions ("should a transaction be included?")

Byzantine Trust Networks (BTNs)

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

- Nodes: N
- Honest nodes: H
- Trust sets (one for each i in H): L_i
- Quotas (one for each i in H): q_i

$q \geq 0.75$

- Nodes make binary decisions ("should a transaction be included?")
- … influenced by trusted nodes (if enough trusted nodes have opinion x then take up opinion x, i.e. **validate x**)

Byzantine Trust Networks (BTNs)

Nodes

Honest nodes

Trust sets
(one for each i in H)

Quotas
(one for each i in H)

$q \geq 0.75$

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

- Nodes make binary decisions ("should a transaction be included?")
- … influenced by trusted nodes (if enough trusted nodes have opinion x then take up opinion x, i.e. **validate x**)
- Byzantine nodes can reveal any opinion to any honest node

Command Games

Nodes

Honest nodes

Trust sets
(one for each i in H)

Quotas
(one for each i in H)

$q_i > 0.75$

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

$$\Updownarrow$$

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

Command Games

Nodes

Honest nodes

Trust sets
(one for each i in H)

Quotas
(one for each i in H)

$q_i > 0.75$

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

$$\Updownarrow$$

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

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

Command Games

Nodes

Honest nodes

Trust sets
(one for each i in H)

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

Quotas
(one for each i in H)

$q_i > 0.75$

$$\Updownarrow$$

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

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

Each honest agent is assigned a **simple game**

Command Games

Nodes

Honest nodes

Trust sets
(one for each i in H)

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

Quotas
(one for each i in H)

$q_i > 0.75$

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

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

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.

Command Games

Nodes

Honest nodes

Trust sets
(one for each i in H)

Quotas
(one for each i in H)

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

$q_i > 0.75$

$\Updownarrow$

FBAS in Stellar

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

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

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.

Safety of BTNs

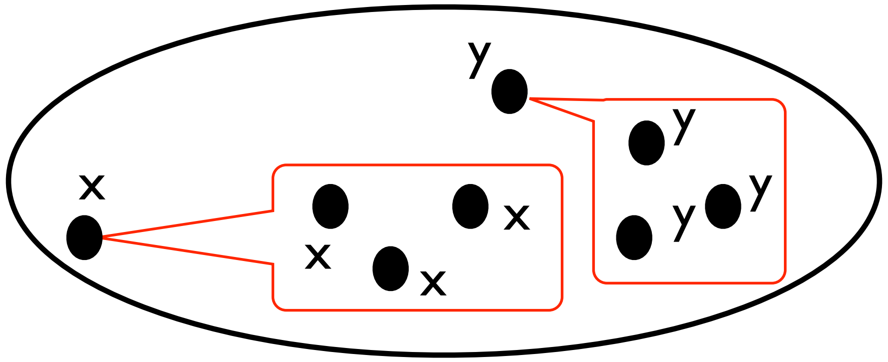
Safety of BTNs

- An opinion profile is **forked** if there are two honest nodes validating opposite values (i.e., stable opinions on opposite values)

Safety of BTNs

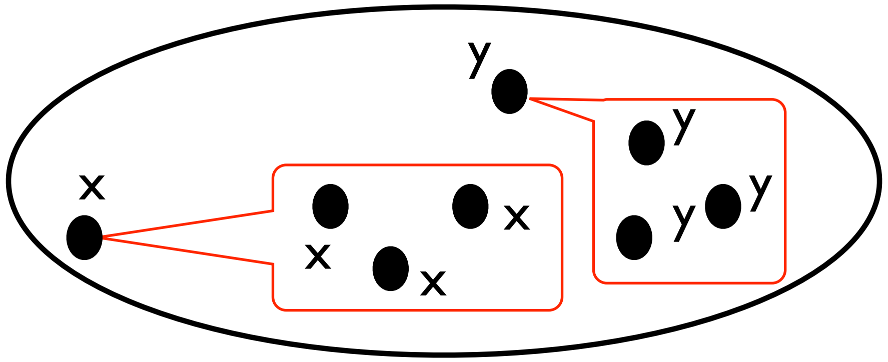
- An opinion profile is **forked** if there are two honest nodes validating opposite values (i.e., stable opinions on opposite values)
- A BTN is **safe** iff there exist no forked profiles for it

Safety of BTNs



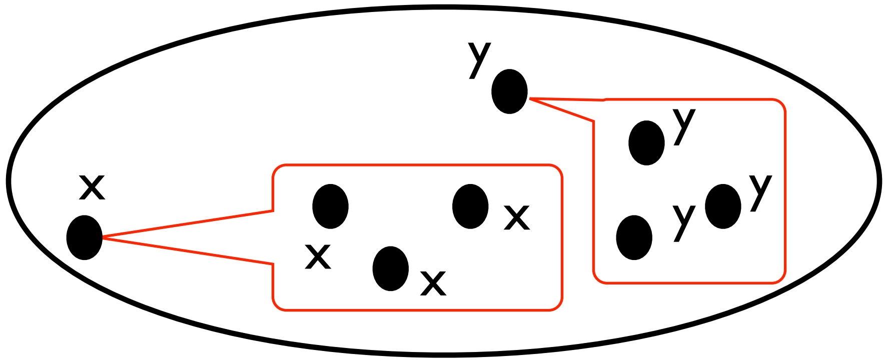
- An opinion profile is **forked** if there are two honest nodes validating opposite values (i.e., stable opinions on opposite values)
- A BTN is **safe** iff there exist no forked profiles for it

Safety of BTNs



- An opinion profile is **forked** if there are two honest nodes validating opposite values (i.e., stable opinions on opposite values)
- A BTN is **safe** iff there exist no forked profiles for it
- NOTE: safety is protocol-independent

Safety of BTNs



- An opinion profile is **forked** if there are two honest nodes validating opposite values (i.e., stable opinions on opposite values)
- A BTN is **safe** iff there exist no forked profiles for it
- NOTE: safety is protocol-independent
- **QUESTION**: what are necessary structural conditions for safety?

PART II

Decentralization

Safety & Decentralization in uniform BTNs

Theorem In uniform BTNs with quotas in $[0.75, 0.8]$, safety implies the existence of nodes that are trusted by all honest nodes.

Safety & Decentralization in uniform BTNs

Ripple

Theorem In uniform BTNs with quotas in $[0.75, 0.8]$, safety implies the existence of nodes that are trusted by all honest nodes.

Safety & Decentralization in uniform BTNs

Ripple

Theorem In uniform BTNs with quotas in $[0.75, 0.8]$, safety implies the existence of nodes that are trusted by all honest nodes.

- Safety implies any two trust sets should overlap for at least (1-q)/q of their combined size
- If all pairs of trust sets overlap for at least 0.25 of their combined size, then the intersection of all trust sets is non-empty (i.e., there are nodes trusted by all nodes)
- This is the case for quotas in [0.75,0.8]

Safety & Decentralization in uniform BTNs

Ripple

Theorem In uniform BTNs with quotas in $[0.75, 0.8]$, safety implies the existence of nodes that are trusted by all honest nodes.

Theoretical justification for current implementation of Ripple

- Safety implies any two trust sets should overlap for at least (1-q)/q of their combined size
- If all pairs of trust sets overlap for at least 0.25 of their combined size, then the intersection of all trust sets is non-empty (i.e., there are nodes trusted by all nodes)
- This is the case for quotas in [0.75,0.8]

Safety & Decentralization in uniform BTNs

Ripple

BTNs with quotas in $[0.75, 0.8]$,

Theorem In uniform BTNs with quotas in $[0.75, 0.8]$, safety implies the existence of nodes that are trusted by all honest nodes.

Theoretical justification for current implementation of Ripple

Fully decentralised consensus is impossible

- Safety implies any two trust sets should overlap for at least (1-q)/q of their combined size
- If all pairs of trust sets overlap for at least 0.25 of their combined size, then the intersection of all trust sets is non-empty (i.e., there are nodes trusted by all nodes)
- This is the case for quotas in [0.75,0.8]

Safety & Decentralization in (non-uniform) BTNs

Safety & Decentralization in (non-uniform) BTNs

- The BTN of Stellar is not uniform (more freedom to nodes)

Safety & Decentralization in (non-uniform) BTNs

- The BTN of Stellar is not uniform (more freedom to nodes)
- A necessary condition for safety is that any two ‘self-sufficient’ sets of nodes (called **quora**) intersect:

Safety & Decentralization in (non-uniform) BTNs

Theorem QUORUM-INTERSECTION is coNP-complete.

- The BTN of Stellar is not uniform (more freedom to nodes)
- A necessary condition for safety is that any two 'self-sufficient' sets of nodes (called **quora**) intersect:

Safety & Decentralization in (non-uniform) BTNs

Theorem QUORUM-INTERSECTION is coNP-complete.

Maintaining the good-behaviour of the BTN is intractable

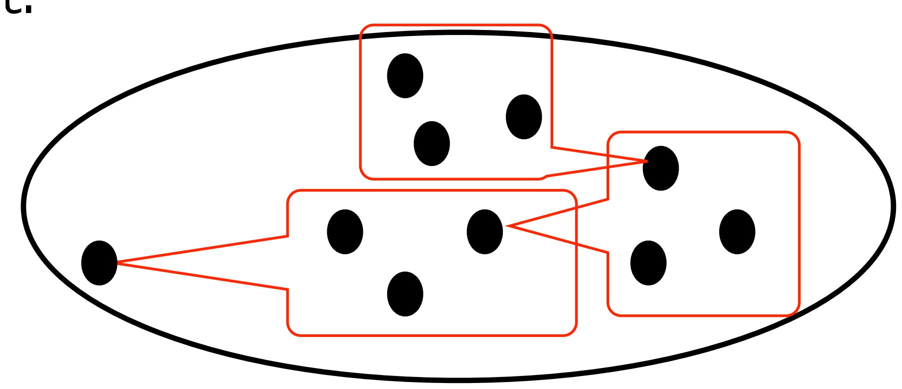
- The BTN of Stellar is not uniform (more freedom to nodes)
- A necessary condition for safety is that any two ‘self-sufficient’ sets of nodes (called **quora**) intersect:

Safety & Decentralization in (non-uniform) BTNs

Theorem QUORUM-INTERSECTION is coNP-complete.

Maintaining the good-behaviour of the BTN is intractable

- ☐ The BTN of Stellar is not uniform (more freedom to nodes)
- ☐ A necessary condition for safety is that any two 'self-sufficient' sets of nodes (called **quora**) intersect:



PART III

Influence

Influence in uniform safe BTNs

Influence in uniform safe BTNs

- Theorem 1: safety implies existence of all-trusted nodes

Influence in uniform safe BTNs

- Theorem 1: safety implies existence of all-trusted nodes
- What does this mean concretely in terms of the influence that nodes have on consensus?

Influence in uniform safe BTNs

- Theorem 1: safety implies existence of all-trusted nodes
- What does this mean concretely in terms of the influence that nodes have on consensus?
- In PoW/PoS it is relatively easy to understand a node's influence/power on consensus

Influence in uniform safe BTNs

- Theorem 1: safety implies existence of all-trusted nodes
- What does this mean concretely in terms of the influence that nodes have on consensus?
- In PoW/PoS it is relatively easy to understand a node's influence/power on consensus
- It is trickier for consensus based on trust networks

Influence in uniform safe BTNs

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

Influence in uniform safe BTNs

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

Power index
e.g.: Penrose/Banzhaf

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

Influence in uniform safe BTNs

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

Influence matrix (stochastic)

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

Power index
e.g.: Penrose/Banzhaf

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

Influence in uniform safe BTNs

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

Influence matrix
(stochastic)

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

Power index
e.g.: Penrose/Banzhaf

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

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

Long-term influence

Influence in uniform safe BTNs

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

Influence matrix (stochastic)

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

Power index e.g.: Penrose/Banzhaf

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

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

Long-term influence

Theorem The influence matrix of a safe uniform BTN is regular. It is fully regular if there exists at most one Byzantine node.

Influence in uniform safe BTNs

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

Influence matrix (stochastic)

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

Power index e.g.: Penrose/Banzhaf

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

Long-term influence

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

Theorem The influence matrix of a safe uniform BTN is regular. It is fully regular if there exists at most one Byzantine node.

Influence in uniform safe BTNs

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

Influence matrix (stochastic)

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

Power index e.g.: Penrose/Banzhaf

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

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

Long-term influence

Theorem The influence matrix of a safe uniform BTN is regular. It is fully regular if there exists at most one Byzantine node.

If no Byzantine nodes exist, then the all-trusted nodes are the only ones with positive long-term influence

Influence in uniform safe BTNs

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

Influence matrix (stochastic)

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

Power index e.g.: Penrose/Banzhaf

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

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

Long-term influence

Theorem The influence matrix of a safe uniform BTN is regular. It is fully regular if there exists at most one Byzantine node.

If no Byzantine nodes exist, then the all-trusted nodes are the only ones with positive long-term influence

If they exist they are the only ones with positive long-term influence

Summary

Summary

A. An analysis of inherent limitations of consensus based on trust networks: decentralisation & influence

B. Relevance of economic methods (game theory and social choice) for the analysis of consensus protocols

Summary

A. An analysis of inherent limitations of consensus based on trust networks: decentralisation & influence

B. Relevance of economic methods (game theory and social choice) for the analysis of consensus protocols