Egalitarian and Just Currency Networks

Gal Shahaf • Ehud Shapiro • Nimrod Talmon

We aim to design a monetary system that is:

1. Egalitarian – in terms of control over its execution.
2. Just – value is distributed equally among the participants.

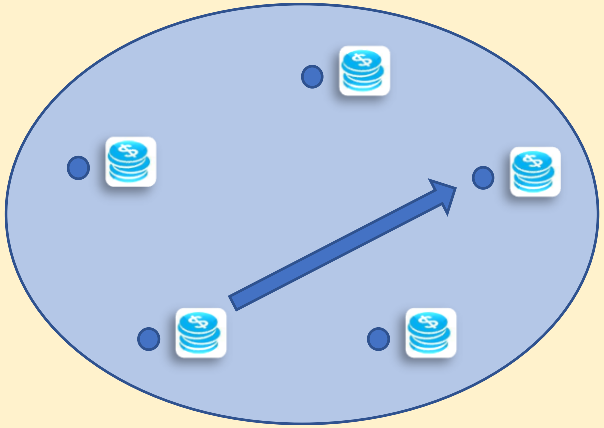
Current systems:

	Traditional currencies	Cryptocurrencies	Currency Community
Design	Centralized	Decentralized	Decentralized
Control	Central bank	Miners	Participants
# Entities in actual control	1	<5	# Participants

https://bitcoinera.app/arewedecentralizedyet/

A Currency Community:

- Agents
- Coins
- Configuration function $h: C \to V$.
- Payment correspond to the transfer of coins between the agents.



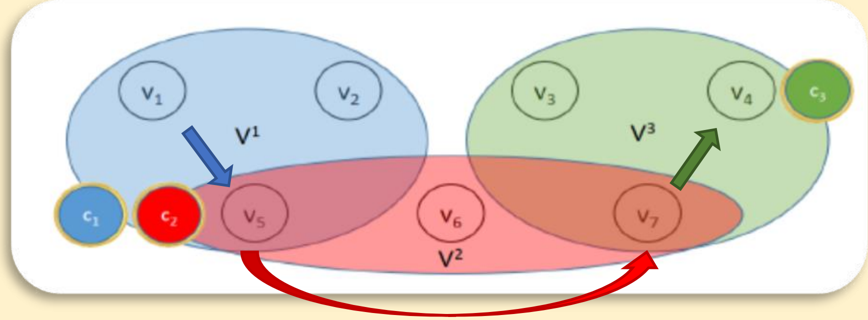
Standard distributed computation satisfies:

- Equality.
- Distributive justice.
- Fault tolerance up to 1/3 byzantine agents.

Main Question: How can the community safely scale-up?

Currency network:

Communities may inter-operate via chain-payments.



Joint egalitarian minting:

Every agent mints one coin in only one community at each timestep.

THEOREM 4.6. *Assuming:*

- *Joint egalitarian employed by two currency communities.*
- *Fixed agents' preferences over the currencies.*
- *Preference-based coin exchange rates.*
- *An efficient network history.*
- *Myopic agents.*

Then, if it holds that $\frac{|V^1 \setminus V^2|}{|V^2|} \le \lim_t \mathrm{MRS}_{12}(CN_t) \le \frac{|V^1|}{|V^2 \setminus V^1|}$, *then the network history is asymptotically just, and* $\lim_t \mathrm{EX}_{12}(CN_t) = 1$.

Figure:

Each point in the bounded area will converge to 1:1 exchange rates.

$|V^1| = m_1, |V^2| = m_2$.