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:

<table>
<thead>
<tr>
<th></th>
<th>Traditional currencies</th>
<th>Cryptocurrencies</th>
<th>Currency Community</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design</td>
<td>Centralized</td>
<td>Decentralized</td>
<td>Decentralized</td>
</tr>
<tr>
<td>Control</td>
<td>Central bank</td>
<td>Miners</td>
<td>Participants</td>
</tr>
<tr>
<td># Entities in actual control</td>
<td>1</td>
<td>&lt;5</td>
<td># Participants</td>
</tr>
</tbody>
</table>

https://bitcoinera.app/arewedecentralizedyet/

A Currency Community:
- Agents
- Coins
- Configuration function $h: C \rightarrow V$.
- 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.

Figure:
Each point in the bounded area will converge to 1:1 exchange rates.
$|V^1| = m_1$, $|V^2| = m_2$. 