Egalitarian and Just Digital Currency Networks*

Extended Abstract

Gal Shahaf
Weizmann Institute of Science
gal.shahaf@weizmann.ac.il

Ehud Shapiro
Weizmann Institute of Science
ehud.shapiro@weizmann.ac.il

Nimrod Talmon
Ben-Gurion University
talmonn@bgu.ac.il

ABSTRACT

We explore the possibility of an alternative cryptocurrency that is egalitarian in control, just in the distribution of its created wealth, and forms and grows in a grassroots way; we analyze it via a mathematical entity called a *currency network*. Our main result states sufficient conditions for the establishment of 1:1 exchange rates and distributive justice in a currency network.

KEYWORDS

Cryptocurrencies; Universal Basic Income; Distributive Justice

ACM Reference Format:
Gal Shahaf, Ehud Shapiro, and Nimrod Talmon. 2021. Egalitarian and Just Digital Currency Networks: Extended Abstract. In *Proc. of the 20th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2021), Online, May 3–7, 2021*, IFAAMAS, 3 pages.

1 INTRODUCTION

We explore the possibility of an egalitarian and just digital currency that may form currency networks in a grassroots manner. Our goal here is the design of a digital currency that may be issued by all, where both control and benefit are equally distributed among the people participating in the creation and use of the currency. Such a currency implements distributive justice in the sense that each person enjoys an equal share of its created value. Furthermore, as we wish our medium to be scalable, our further goal is to build this digital currency in a grassroots way. In particular, our paper may be viewed as means for a joint, safe scale-up of such communities, concentrating on the aspect of distributive justice as we rely on the infrastructure of digital social contracts [1] for equality in execution.

Our main contributions are as follows:

- We develop a formal model of currency networks that generalizes the model of credit networks. Our model allows for a rigorous study of economic properties of interoperable currency communities.
- We show circumstances under which it is possible to achieve global distributive justice in such currency networks, through a process we term *joint egalitarian minting* that results, in the limit and under certain assumptions, in a 1-1 exchange rates between the currencies used in the network.

We view the current paper as providing the theoretical foundations for an egalitarian and just digital currency networks. To be used in practice, certain aspects of our modeling shall be refined and extended.

2 CURRENCY NETWORKS

We begin with formal definitions of currency communities, payments and community histories.

Definition 2.1 (Currency Community). A *Currency Community* is a tuple $\mathcal{A} = (V, C, h)$, where V is a set of agents, C is a set of fungible coins, and $h : C \rightarrow V$ is a configuration function that indicates the *holder* of each coin $h(c) \in V$.

A *payment* from u to v is a transfer from u to v of a coin $c \in C$, initially held by u. The result of such a payment, denoted by $\mathcal{A} \xrightarrow{pay(c,u,v)} \mathcal{A}'$, is the currency community $\mathcal{A}' = (V, C, h')$, in which: $h'(x) := \begin{cases} v & \text{if } x = c\,, \\ h(x) & otherwise \end{cases}$.

A *currency network history* is a sequence of currency communities $\mathcal{A}_0, \mathcal{A}_1, \mathcal{A}_2, \ldots$, with the following monotonic attributes:
(1) *Agent growth*: $V_t \subseteq V_{t+1}$ for all $t \geq 0$.
(2) *Coin growth*: $C_t \subseteq C_{t+1}$ for all $t \geq 0$.

As we envision that currency communities would emerge independently, we define the notion of a *currency network*, in which several currency communities may operate simultaneously.

Definition 2.2 (Currency Network). A *currency network* is a tuple of currency communities $\mathcal{CN} = \{\mathcal{A}^1, ..., \mathcal{A}^k\}$, $\mathcal{A}^i = (V^i, C^i, h^i)$, with disjoint sets of coins, $C^i \cap C^j = \emptyset$ for every $i, j \in [k]$. The currency network has agents $V = \bigcup_i V^i$, coins $C = \bigcup_i C^i$, and a *network configuration function* $h : C \rightarrow V$ defined by $h|_{C^i} := h^i$.

A *currency network history* is a sequence of currency networks $\mathcal{CN}_0, \mathcal{CN}_1, \mathcal{CN}_2, \ldots$, such that $\mathcal{A}^i_0, \mathcal{A}^i_1, \mathcal{A}^i_2, \ldots$, is a currency community history for all $1 \leq i \leq k$.

In essence, a currency network is a tuple of communities that employ independent currencies. The network structure arises from chain payments via agents that are members in multiple communities simultaneously. This model is a direct generalization of *credit networks* [2–4, 8, 10]. See Figure 1 for a visual example.

3 TOWARDS DISTRIBUTIVE JUSTICE

The key property we aim to study in this context is distributive justice among the members of the network. Namely, we wish that each agent in the network would enjoy an equal share of the value created by the network, while being able to freely trade his assets with other agents. For a formal definition of this property we refer the reader to [9].

Joint Egalitarian Coin Minting. Achieving distributive justice within a currency network is far from trivial, and requires collaboration among the communities within the network. In order to refrain

*A full version of this paper is available [9].

Proc. of the 20th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2021), U. Endriss, A. Nowé, F. Dignum, A. Lomuscio (eds.), May 3–7, 2021, Online.

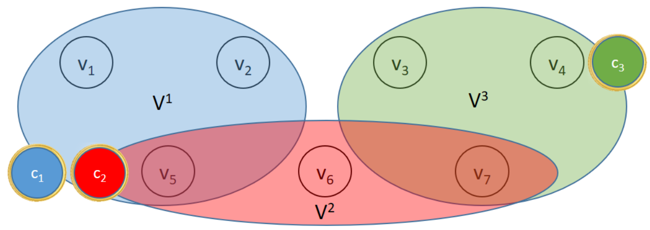

Figure 1: A currency network with 7 vertices v_i, $i \in [7]$ and 3 communities. The blue (red, green) hyperedge on the left (resp., bottom, right) represents the vertices V^1 (resp., V^2, V^3) of community C^1 (resp., C^2, C^3). The agent corresponding to v_5 holds the coin c_1 of C^1 and the coin c_2 of C^2, and the agent of v_4 holds the coin c_3 of C^3.

from harsh interventions (say, in the form of reallocation of coins), we rely on the distribution of newly minted coins as mechanism that may be agreeable to all communities in the network.

Definition 3.1 (Joint Egalitarian Minting). A currency network history is said to employ *joint egalitarian minting* if, at every time step, every agent mints exactly one coin among all currencies in the network.

Exchange Rates. The interactions among currencies within a network are inherent to our model. We reason that whenever agents may freely trade with each other, any relation among independent currencies is based upon what the currencies represent, namely actual commodities (e.g., goods and services) that may be purchased from agents that accept these currencies as payment. So, our analysis focuses on the exchange rates that emerge at equilibrium, wrt. individual preferences over these underlying commodities.

We follow standard practice and assume that in this setting, generally known as *pure exchange economy* [5, 6, 11], an equilibrium establishes not only an allocation (reflected by the function h), but also *marginal rates of substitution* among currencies [7]: A matrix $MRS \in \mathbb{R}^{k \times k}$ where MRS_{ij} denotes the quantity of the currency $\mathcal{A}^j$ that an agent can exchange for one (infinitesimal) unit of currency $\mathcal{A}^i$ while maintaining the same level of utility.

The normalization of the marginal rates of substitution among currencies by the currency volumes, naturally gives rise to exchange rates among coins within these currencies. As these rates are induced by individual preferences, we term them *preferences-based* exchange rates:

Definition 3.2 (Preferences-based rates). Let $\mathcal{CN}^*$ be a currency network which forms an equilibrium under agents' preferences over the currencies. The preferences-based rates between coins in $\mathcal{A}^i$ and $\mathcal{A}^j$ is given by

$$EX_{ij} := MRS_{ij} \cdot \frac{|C^j|}{|C^i|} \,. \tag{1}$$

Myopic Agents. Under a joint minting regime, the natural question that each agent shall ask at each timestep is: *Which coin should I mint next?* Indeed, there are many possibilities. Here we consider a simple answer: *Always mint the highest-valued coin.* The next definition formalizes the notion of myopic behaviour under egalitarian minting in a network.

Definition 3.3 (Myopic Agents). Let $\mathcal{CN}_1, \mathcal{CN}_2, \ldots$ be a network history that employs joint egalitarian minting. We say that the agents in the network are *myopic* if in every time step t, every agent $v \in V_t$ mints a most valued v-coin (ties are broken arbitrarily).

Sufficient conditions for Asymptotic Justice. With the above notions at hand, we can now state our main theorem:

Theorem 3.4. *Let $\mathcal{CN}_0, \mathcal{CN}_1, \mathcal{CN}_2, \ldots$ be a currency network history with 2 communities $\mathcal{CN}_t = (\mathcal{A}^1_t, \mathcal{A}^2_t)$ that employs joint egalitarian coin minting. Assume:*

- *Fixed agents' preferences over the currencies.*
- *Preference-based coin exchange rates.*
- *An efficient network history.*
- *Myopic agents.*

Then, if it holds that $\frac{|V^1 \setminus V^2|}{|V^2|} \leq \lim_t \mathrm{MRS}_{12}(\mathcal{CN}_t) \leq \frac{|V^1|}{|V^2 \setminus V^1|}$, then the network history is asymptotically just. It also follows that $\lim_t \mathrm{EX}_{12}(\mathcal{CN}_t) = 1$.

The proof of this theorem follows the observation that only the agents in the intersection $V^1 \cap V^2$ can choose which coin to mint, and, with myopic minting, they would choose the more valuable coin; thus, if there are relatively enough agents in the intersection, then, together, they would mint enough coins to set the coin exchange rate right, and asymptotic justice then follows.

4 OUTLOOK

Here we analyzed the possibility of a digital currency that realizes *equality* – there is not a single entity controlling the currency but all genuine agents equally control the system; *distributive justice* – every agent is granted an equal share of the created value of the digital currency; and *grassroots* – several independent communities may freely trade while satisfying joint distributive justice.

Our main result specify sufficient conditions that give rise to 1:1 coin exchange rates and distributive justice among independent communities that adhere to a joint egalitarian minting regime. Specifically, we show that free trade among myopic agents within two communities with sufficiently large intersection results with the same coin values and distributive justice among their members. Indeed, as we envision bottom-up growth of communities, our analysis, modeled via currency networks, paves the way for interoperability and offers the possibility of equality and justice at scale, as iterative adjustment of the coin exchange rates among two communities at a time, potentially results in asymptotic global distributive justice. We leave the analysis of this iterative process, as well as the natural extension of Theorem 3.4 to multiple communities for future work.

ACKNOWLEDGEMENTS

Ehud Shapiro is the Incumbent of The Harry Weinrebe Professorial Chair of Computer Science and Biology. We thank the generous support of the Braginsky Center for the Interface between Science and the Humanities. Nimrod Talmon was supported by the Israel Science Foundation (ISF; Grant No. 630/19).

REFERENCES

[1] Luca Cardelli, Gal Shahaf, Ehud Shapiro, and Nimrod Talmon. 2020. Digital Social Contracts: A Foundation for an Egalitarian and Just Digital Society. arXiv:2005.06261 [cs.CY]

[2] Pranav Dandekar, Ashish Goel, Ramesh Govindan, and Ian Post. 2011. Liquidity in credit networks: A little trust goes a long way. In *Proceedings of EC '11*. ACM, 147–156.

[3] Pranav Dandekar, Ashish Goel, Michael P Wellman, and Bryce Wiedenbeck. 2015. Strategic formation of credit networks. *ACM Transactions on Internet Technology (TOIT)* 15, 1 (2015), 1–41.

[4] Arpita Ghosh, Mohammad Mahdian, Daniel M Reeves, David M Pennock, and Ryan Fugger. 2007. Mechanism design on trust networks. In *Proceedings of WINE '07*. Springer, 257–268.

[5] Robert E Lucas Jr. 1978. Asset prices in an exchange economy. *Econometrica: Journal of the Econometric Society* (1978), 1429–1445.

[6] James C. Moore. 2007. Pure Exchange Economies. *General Equilibrium and Welfare Economics: An Introduction* (2007), 131–153.

[7] Robert S Pindyck and Daniel L Rubinfeld. 2005. Microeconomics, 6. *Auflage, New Jersey* (2005), 613–640.

[8] Geoffrey Ramseyer, Ashish Goel, and David Mazieres. 2019. Constrained Credit Networks. *arXiv preprint arXiv:1910.02194* (2019).

[9] Gal Shahaf, Ehud Shapiro, and Nimrod Talmon. 2020. Egalitarian and Just Digital Currency Networks. *arXiv preprint arXiv:2005.14631* (2020).

[10] Sten Thore. 1969. Credit networks. *Economica* 36, 141 (1969), 42–57.

[11] Hal R Varian. 1992. *Microeconomic analysis*. Vol. 3. Norton New York.