Can currency competition work?☆

Jesús Fernández-Villaverde [a,*], Daniel Sanches [b]

[a] *Department of Economics, TheRonald O. Perelman Center for Political Science and Economics, University of Pennsylvania, NBER, and CEPR, 133 South 36th Street, Suite 150, Philadelphia, PA 19104, USA*
[b] *Federal Reserve Bank of Philadelphia USA*

A B S T R A C T

Can competition among privately-issued fiat currencies work? Only sometimes and partially. To show this, we build a model of competition among privately-issued fiat currencies. A purely private arrangement fails to implement an efficient allocation, even though it can deliver price stability under certain technological conditions. Although currency competition creates problems for monetary policy, it is possible to design a policy rule that uniquely implements an efficient allocation.

© 2019 Elsevier B.V. All rights reserved.

1. Introduction

Can competition among privately-issued fiduciary currencies work? The appearance of Bitcoin, Ethereum, Libra, and other cryptocurrencies has triggered a wave of interest in privately-issued monies. A similar interest in the topic has not been seen since the polemics associated with the demise of free banking in the English-speaking world in the middle of the 19th century. Somewhat surprisingly, this interest has not translated, so far, into much research within monetary economics.

This situation is unfortunate. Without a theoretical understanding of how currency competition works, we cannot answer a long list of positive and normative questions. Among the positive questions: Will a system of private money deliver price stability? Will one currency drive all others from the market? Or will several of these currencies coexist along the equilibrium path? Do private monies require a commodity backing? Will the market provide the socially optimum amount of money? Can private monies and a government-issued money compete? Can a unit of account be separated from a medium of exchange? Among the normative questions: Should governments prevent the circulation of private monies? Should governments treat private monies as currencies or as any other regular property? Should the private monies be taxed? Even

more radically, should we revisit the celebrated arguments by Friedman and Schwartz (1986) justifying the role of governments as money issuers?

To address some of these questions, we build a model of competition among privately-issued fiduciary currencies. We modify a workhorse of monetary economics, the (Lagos and Wright, 2005) (LW) environment, by including entrepreneurs who can issue their currencies to maximize their utility. Otherwise, the model is standard. Since the LW model is particularly amenable to analysis, we can derive many insights about currency competition. Besides, the use of the LW framework makes our new results easy to compare with previous findings in the literature.

We highlight six results. First, we show that, in a competitive environment, the existence of a monetary equilibrium consistent with price stability depends on the properties of the available technologies. More concretely, the shape of the cost function determines the relationship between equilibrium prices and the entrepreneur's incentive to increase his money supply. An equilibrium with stable prices can exist only if the cost function associated with the production of private money is strictly increasing and locally linear around the origin. If the cost function has a positive derivative at zero, then there is no equilibrium consistent with price stability. Thus, Hayek's vision of a system of private monies competing among themselves to provide stable means of exchange is not general (Hayek, 1999).

Second, there exists a continuum of equilibrium trajectories with the property that the value of private monies monotonically converges to zero, even if the environment admits the existence of an equilibrium with stable prices. This result shows that the self-fulfilling inflationary episodes highlighted by Obstfeld and Rogoff (1983) and Lagos and Wright (2003) are not an inherent feature of public monies. Private monies are also subject to self-fulfilling inflationary episodes, even when they are issued by profit-maximizing, long-lived entrepreneurs who care about the future value of their monies.

Third, we show that although the equilibrium with stable prices Pareto dominates all other equilibria in which the value of private monies declines over time, a private monetary system does not provide the socially optimum quantity of money. Private money does not solve the trading frictions at the core of LW and, more generally, of essential models of money (Wallace, 2001). Furthermore, in our environment, private money creation can be socially wasteful. In a well-defined sense, the market fails to provide the right amount of money in ways that it does not fail to provide the right amount of other goods.

Fourth, we show that the main features of cryptocurrencies, such as the existence of an upper bound on the supply of each brand, make privately-issued money in the form of cryptocurrencies consistent with price stability in a competitive environment, even if the cost function has a positive derivative at zero. A purely private system can deliver price stability under a wide array of preferences and technologies, provided that some limit on the total circulation of private currencies is enforced by an immutable protocol. This allocation only partially vindicates Hayek's proposal since it does not deliver the first best allocation.

Fifth, when we introduce a government competing with private monies, currency competition creates limits for monetary policy. For instance, if the supply of government money follows a money-growth rule, then it is impossible to implement an allocation with the property that the real return on money equals the rate of time preference if agents are willing to hold privately-issued monies. Profit-maximizing entrepreneurs will frustrate the government's attempt to implement a positive real return on money through deflation when the public is willing to hold private currencies. To get around this problem, we analyze the properties of a policy rule that pegs the real value of government money. Under this regime, it is possible to implement an efficient allocation as the unique equilibrium outcome, which requires driving private money out of the economy. Also, the proposed policy rule is robust to other forms of private monies, such as those issued by automata.

In other words: the threat of competition from private entrepreneurs provides market discipline to any government involved in currency-issuing. If the government does not provide a sufficiently "good" money, then it will have difficulties in the implementation of allocations. Even if the government is not interested in maximizing social welfare, but values the ability to select a plan of action that induces a unique equilibrium outcome, the set of equilibrium allocations satisfying unique implementation is such that any element in that set Pareto dominates any equilibrium allocation in the purely private arrangement. Because unique implementation requires driving private money out of the economy, unique implementation asks for the provision of "good" government money.

Last, and motivated by recent exercises by companies to issue their own cryptocurrencies, we study the implementation of an efficient allocation with automaton issuers in an economy with productive capital. This institutional arrangement can provide an efficient allocation as the *unique* equilibrium outcome if capital is sufficiently productive. In this respect, our analysis can be viewed as also belonging to the literature on the provision of liquidity by productive firms, such as the Libra currency recently launched by Facebook (Holmström and Tirole, 2011 and Dang et al., 2014).

In an Online Appendix, we show how the presence of network effects can be relevant for the welfare properties of equilibrium allocations in a competitive money environment.

We have used the word "entrepreneur" and not the more common "banker" to denote the issuers of private money. Our model highlights how the issuing of a private currency is logically separated from banking. Both tasks were historically linked for logistical reasons: banks had a central location in the network of payments that made it easy for them to introduce currency into circulation. The internet has broken the logistical barrier. The issuing of bitcoins, for instance, is done through a proof-of-work system that is independent of any issuing and handling of deposits and credit.[1]

---

[1] Similarly, some of the community currencies that have achieved a degree of success do not depend on banks backing or issuing them (see Greco, 2001).

This previous explanation also addresses a second concern: What are the differences between private monies issued in the past by banks (such as during the Scottish free banking experience between 1716 and 1845) and modern cryptocurrencies? A first difference is the distribution process, which is now much wider and more dispersed than before. A second difference is the possibility, through software protocols, of having quasi-commitment devices regarding how much money will be issued. The most famous of these devices is the 21 million bitcoins that will eventually be released.[2] We will discuss how to incorporate an automaton issuer of private money into our model to analyze this property of cryptocurrencies. Third, cryptographic techniques make it harder to counterfeit digital currencies than traditional physical monies, minimizing a historical obstacle that private monies faced. Fourth, most (but not all) historical cases of private money were of commodity-backed currencies, while most cryptocurrencies are fully fiduciary.

At the same time, we ignore all issues related to the payment structure of cryptocurrencies, such as the blockchain, the emergence of consensus on a network, or the possibilities of Goldfinger attacks. While these topics are of foremost importance, they require a specific modeling strategy that falls far from the one we follow, which is more suited to the macroeconomic questions we focus on.

We are not the first to study private money. At the risk of being highly selective, we build on the tradition of Cavalcanti et al. (1999), Cavalcanti and Wallace (1999), Cavalcanti et al. (2005), Williamson (1999), Berentsen (2006) and Monnet (2006). See, from another perspective, Selgin and White (1994). Our emphasis is different from that in these previous papers, as we depart from modeling banks and their reserve management problem. Our entrepreneurs issue fiduciary money that cannot be redeemed for any other asset. Since cryptocurrencies cannot be used to pay taxes in most sovereigns, their existence is more interesting, for an economist, than government-issued fiat monies with legal tender status. Our partial vindication of Hayek shares many commonalities with Martin and Schreft (2006), who were the first to prove the existence of equilibria for environments in which outside money is issued competitively. Lastly, we cannot forget (Klein, 1974) and his application of industrial organization insights to competition among monies.

2. Model

The economy consists of a large number of three types of agents, referred to as buyers, sellers, and entrepreneurs. All agents are infinitely lived. Each period contains two distinct subperiods in which economic activity will differ. In the first subperiod, all types interact in a centralized market (CM) where a perishable good, referred to as the CM good, is produced and consumed. Buyers and sellers can produce the CM good by using a linear technology that requires effort as input. All agents want to consume the CM good.

In the second subperiod, buyers and sellers interact in a decentralized market (DM) characterized by pairwise meetings, with entrepreneurs remaining idle. A buyer is randomly matched with a seller with probability $\sigma \in (0, 1)$ and vice versa. In the DM, buyers want to consume, but cannot produce, whereas sellers can produce, but do not want to consume. A seller can produce a perishable good, referred to as the DM good, using a divisible technology that delivers one unit of the good for each unit of effort he exerts. An entrepreneur is neither a producer nor a consumer of the DM good.

Besides, there exists a technology to create tokens, which can be either physical or electronic. The essential feature of the tokens is that their authenticity can be publicly verified at zero cost (for example, thanks to the application of cryptography) so that counterfeiting will not be an issue. Precisely, there exist $N \in \mathbb{N}$ distinct types of tokens with identical production functions. Only entrepreneurs have the expertise to use the technology to create tokens. Specifically, an entrepreneur of type $i \in \{1, \ldots, N\}$ has the ability to use the technology to create type-i tokens. Let $c : \mathbb{R}_+ \to \mathbb{R}_+$ denote the cost function (in terms of the utility of the entrepreneur) that depends on the tokens minted in the period. We will assume throughout the paper that $c : \mathbb{R}_+ \to \mathbb{R}_+$ is strictly increasing and weakly convex, with $\infty > c(0) \geq 0$ (when explicitly mentioned, we will add further structure to the cost function to either derive a concrete result or simplify the proofs). This technology allows entrepreneurs to issue tokens that can circulate as a medium of exchange.

There is a $[0, 1]$-continuum of buyers. Let $x_t^b \in \mathbb{R}$ denote the buyer's net consumption of the CM good, and let $q_t \in \mathbb{R}_+$ denote consumption of the DM good. The buyer's preferences are represented by $U^b(x_t^b, q_t) = x_t^b + u(q_t)$. Assume that $u : \mathbb{R}_+ \to \mathbb{R}$ is continuously differentiable, increasing, and strictly concave, with $u'(0) = \infty$ and $u(0) = 0$.

There is a $[0, 1]$-continuum of sellers. Let $x_t^s \in \mathbb{R}$ denote the seller's net consumption of the CM good, and let $n_t \in \mathbb{R}_+$ denote the seller's effort level to produce the DM good. The seller's preferences are represented by $U^s(x_t^s, n_t) = x_t^s - w(n_t)$. Assume that $w : \mathbb{R}_+ \to \mathbb{R}_+$ is continuously differentiable, increasing, and weakly convex, with $w(0) = 0$.

There is a $[0, 1]$-continuum of entrepreneurs of each type $i \in \{1, \ldots, N\}$. Let $x_t^i \in \mathbb{R}_+$ denote an entrepreneur's consumption of the CM good, and let $\Delta_t^i \in \mathbb{R}_+$ denote the production of type-i tokens. Entrepreneur i has preferences represented by $U^e(x_t^i, \Delta_t) = x_t^i - c(\Delta_t^i)$. Finally, let $\beta \in (0, 1)$ denote the discount factor, which is common across all types.

Throughout the analysis, we assume that buyers and sellers are anonymous (i.e., their identities are unknown and their trading histories are privately observable), which precludes credit in the decentralized market.

---

3. Competitive money supply

Because the meetings in the DM are anonymous, there is no scope for trading future promises in this market. As a result, a medium of exchange is essential to achieve allocations that we could not achieve without it. In a typical monetary model, a medium of exchange is supplied in the form of a government-issued fiat money. In this section, instead, we study a monetary system in which profit-maximizing entrepreneurs can create intrinsically worthless tokens that can circulate as a medium of exchange. These currencies are not associated with any promise to exchange them for goods or other assets at some future date. Also, it is assumed that all agents in the economy can observe the total supply of each currency put into circulation at each date. These features allow agents to form beliefs about the exchange value of money in the current and future periods, so that fiat money can attain a positive value in equilibrium. The fact that these tokens attain a strictly positive value in equilibrium allows us to refer to them as *currencies*.

Profit maximization will determine the money supply in the economy. Since all agents know that an entrepreneur enters the currency-issuing business to maximize profits, one can describe individual behavior by solving the entrepreneur's optimization problem. These predictions about individual behavior allow agents to form beliefs regarding the exchange value of currencies, given the observability of individual issuances.

In the context of cryptocurrencies, we can re-interpret the entrepreneurs as "miners" and the index $i \in \{1, \ldots, N\}$ as the name of each cryptocurrency. The miners are willing to solve a complicated problem that requires real inputs, such as computational resources, programming effort, and electricity, to get the new electronic tokens as specified by the protocol of each cryptocurrency. Let $\phi_t^i \in \mathbb{R}_+$ denote the value of a unit of currency $i \in \{1, \ldots, N\}$ in terms of the CM good, and let $\phi_t = (\phi_t^1, \ldots, \phi_t^N) \in \mathbb{R}_+^N$ denote the vector of real prices.

3.1. Buyer

We start by describing the portfolio problem of a typical buyer. Let $W^b(\mathbf{M}_{t-1}^b, t)$ denote the value function for a buyer who starts period t holding a portfolio $\mathbf{M}_{t-1}^b \in \mathbb{R}_+^N$ of privately-issued currencies in the CM, and let $V^b(\mathbf{M}_t^b, t)$ denote the value function in the DM. The Bellman equation can be written as:

$$W^b(\mathbf{M}_{t-1}^b, t) = \max_{(x_t^b, \mathbf{M}_t^b) \in \mathbb{R} \times \mathbb{R}_+^N} \left[x_t^b + V^b(\mathbf{M}_t^b, t) \right] \tag{1}$$

subject to the budget constraint

$$\phi_t \cdot \mathbf{M}_t^b + x_t^b = \phi_t \cdot \mathbf{M}_{t-1}^b. \tag{2}$$

The vector $\mathbf{M}_t^b \in \mathbb{R}_+^N$ describes the buyer's portfolio after trading in the CM, and $x_t^b \in \mathbb{R}$ denotes net consumption of the CM good.

The value for a buyer holding a portfolio $\mathbf{M}_t^b$ in the DM is

$$V^b(\mathbf{M}_t^b, t) = \sigma \left[u(q(\mathbf{M}_t^b, t)) + \beta W^b(\mathbf{M}_t^b - \mathbf{d}(\mathbf{M}_t^b, t), t+1) \right] + (1 - \sigma) \beta W^b(\mathbf{M}_t^b, t+1), \tag{3}$$

with $\{q(\mathbf{M}_t^b, t), \mathbf{d}(\mathbf{M}_t^b, t)\}$ being the terms of trade. Specifically, $q(\mathbf{M}_t^b, t) \in \mathbb{R}_+$ is the production of the DM good and the vector of currencies the buyer transfers to the seller is $\mathbf{d}(\mathbf{M}_t^b, t) = (d^1(\mathbf{M}_t^b, t), \ldots, d^N(\mathbf{M}_t^b, t)) \in \mathbb{R}_+^N$. Because $W^b(\mathbf{M}_t^b, t+1) = \phi_{t+1} \cdot \mathbf{M}_t^b + W^b(\mathbf{0}, t+1)$, we rewrite the value function as

$$V^b(\mathbf{M}_t^b, t) = \sigma \left[u(q(\mathbf{M}_t^b, t)) - \beta \times \phi_{t+1} \cdot \mathbf{d}(\mathbf{M}_t^b, t) \right] + \beta \times \phi_{t+1} \cdot \mathbf{M}_t^b + \beta W^b(\mathbf{0}, t+1). \tag{4}$$

Buyers and sellers can use any currency they want without any restriction beyond respecting the terms of trade.

These terms of trade are determined through the generalized Nash solution. Let $\theta \in [0, 1]$ denote the buyer's bargaining power. Then, the terms of trade $(q, \mathbf{d}) \in \mathbb{R}_+^{N+1}$ solve

$$\max_{(q, \mathbf{d}) \in \mathbb{R}_+^{N+1}} \left[u(q) - \beta \times \phi_{t+1} \cdot \mathbf{d} \right]^\theta \left[-w(q) + \beta \times \phi_{t+1} \cdot \mathbf{d} \right]^{1-\theta} \tag{5}$$

subject to the participation constraints:

$$u(q) - \beta \times \phi_{t+1} \cdot \mathbf{d} \geq 0 \tag{6}$$

$$-w(q) + \beta \times \phi_{t+1} \cdot \mathbf{d} \geq 0, \tag{7}$$

and the buyer's liquidity constraint $\mathbf{d} \leq \mathbf{M}_t^b$.

Let $q^* \in \mathbb{R}_+$ denote the quantity satisfying $u'(q^*) = w'(q^*)$ so that q^* gives the surplus-maximizing quantity, determining the efficient level of production in the DM. The solution to the bargaining problem is:

$$q(\mathbf{M}_t^b, t) = \begin{cases} m^{-1}(\beta \times \phi_{t+1} \cdot \mathbf{M}_t^b) & \text{if } \phi_{t+1} \cdot \mathbf{M}_t^b < \beta^{-1}[\theta w(q^*) + (1 - \theta)u(q^*)] \\ q^* & \text{otherwise} \end{cases} \tag{8}$$

and

$$\phi_{t+1} \cdot \mathbf{d}\big(\mathbf{M}_t^b, t\big) = \begin{cases} \phi_{t+1} \cdot \mathbf{M}_t^b \text{ if } \phi_{t+1} \cdot \mathbf{M}_t^b < \beta^{-1}[\theta w(q^*) + (1-\theta)u(q^*)] \\ \beta^{-1}[\theta w(q^*) + (1-\theta)u(q^*)] \text{ otherwise.} \end{cases} \quad (9)$$

The function $m : \mathbb{R}_+ \to \mathbb{R}_+$ is defined as

$$m(q) \equiv \frac{(1-\theta)u(q)w'(q) + \theta w(q)u'(q)}{\theta u'(q) + (1-\theta)w'(q)}. \quad (10)$$

A case of interest is when the buyer has all the bargaining power (i.e., when we take the limit $\theta \to 1$). In this situation, the solution to the bargaining problem is:

$$q\big(\mathbf{M}_t^b, t\big) = \begin{cases} w^{-1}\big(\beta \times \phi_{t+1} \cdot \mathbf{M}_t^b\big) \text{ if } \phi_{t+1} \cdot \mathbf{M}_t^b < \beta^{-1}w(q^*) \\ q^* \text{ if } \phi_{t+1} \cdot \mathbf{M}_t^b \geq \beta^{-1}w(q^*) \end{cases} \quad (11)$$

and

$$\phi_{t+1} \cdot \mathbf{d}\big(\mathbf{M}_t^b, t\big) = \begin{cases} \phi_{t+1} \cdot \mathbf{M}_t^b \text{ if } \phi_{t+1} \cdot \mathbf{M}_t^b < \beta^{-1}w(q^*) \\ \beta^{-1}w(q^*) \text{ if } \phi_{t+1} \cdot \mathbf{M}_t^b \geq \beta^{-1}w(q^*). \end{cases} \quad (12)$$

Given the trading protocol, the solution to the bargaining problem characterizes the real expenditures in the DM, given by $\phi_{t+1} \cdot \mathbf{d}\big(\mathbf{M}_t^b, t\big)$, as a function of the real value of the buyer's portfolio, with the composition of the basket of currencies transferred to the seller remaining indeterminate.

The indeterminacy of the portfolio of currencies transferred to the seller in the DM is reminiscent of Kareken and Wallace (1981). These authors have established that, in the absence of portfolio restrictions and barriers to trade, the exchange rate between two currencies is indeterminate in a flexible-price economy. In our framework, a similar result holds with respect to privately-issued currencies, given the absence of transaction costs when dealing with different currencies. Buyers and sellers do not "prefer" any currency over another and there is a sense in which we can talk about perfect competition among currencies.

Given the solution to the bargaining problem, the value function $V\big(\mathbf{M}_t^b, t\big)$ takes the form:

$$V^b\big(\mathbf{M}_t^b, t\big) = \sigma \big[u\big(m^{-1}\big(\beta \times \phi_{t+1} \cdot \mathbf{M}_t^b\big)\big) - \beta \times \phi_{t+1} \cdot \mathbf{M}_t^b\big] + \beta \times \phi_{t+1} \cdot \mathbf{M}_t^b + \beta W^b(\mathbf{0}, t+1) \quad (13)$$

if $\phi_{t+1} \cdot \mathbf{M}_t^b < \beta^{-1}[\theta w(q^*) + (1-\theta)u(q^*)]$ and the form:

$$V^b\big(\mathbf{M}_t^b, t\big) = \sigma \theta[u(q^*) - w(q^*)] + \beta \times \phi_{t+1} \cdot \mathbf{M}_t^b + \beta W^b(\mathbf{0}, t+1) \quad (14)$$

if $\phi_{t+1} \cdot \mathbf{M}_t^b \geq \beta^{-1}[\theta w(q^*) + (1-\theta)u(q^*)]$.

The optimal portfolio problem can be defined as

$$\max_{\mathbf{M}_t^b \in \mathbb{R}_+^N} \big\{-\phi_t \cdot \mathbf{M}_t^b + \sigma\big[u\big(q\big(\mathbf{M}_t^b, t\big)\big) - \beta \times \phi_{t+1} \cdot \mathbf{d}\big(\mathbf{M}_t^b, t\big)\big] + \beta \times \phi_{t+1} \cdot \mathbf{M}_t^b\big\}. \quad (15)$$

The optimal choice, then, satisfies

$$\phi_t^i = \beta \phi_{t+1}^i L_\theta\big(\phi_{t+1} \cdot \mathbf{M}_t^b\big) \quad (16)$$

for every type $i \in \{1, \dots, N\}$, together with the transversality condition

$$\lim_{t \to \infty} \beta^t \times \phi_t \cdot \mathbf{M}_t^b = 0, \quad (17)$$

where $L_\theta : \mathbb{R}_+ \to \mathbb{R}_+$ is given by

$$L_\theta(A) = \begin{cases} \sigma \dfrac{u'\big(m^{-1}(\beta A)\big)}{m'\big(m^{-1}(\beta A)\big)} + 1 - \sigma \text{ if } A < \beta^{-1}[\theta w(q^*) + (1-\theta)u(q^*)] \\ 1 \text{ if } A \geq \beta^{-1}[\theta w(q^*) + (1-\theta)u(q^*)]. \end{cases} \quad (18)$$

In other words: in an equilibrium with multiple currencies, the expected return on money must be equalized across all valued currencies. In the absence of portfolio restrictions, an agent is willing to hold in portfolio two alternative currencies only if they yield the same rate of return, given that these assets are equally useful in facilitating exchange in the DM.

3.2. Seller

Let $W^s\big(\mathbf{M}_{t-1}^s, t\big)$ denote the value function for a seller who enters period t holding a portfolio $\mathbf{M}_{t-1}^s \in \mathbb{R}_+^N$ of privately-issued currencies in the CM, and let $V^s\big(\mathbf{M}_t^s, t\big)$ denote the value function in the DM. The Bellman equation can be written as:

$$W^s\big(\mathbf{M}_{t-1}^s, t\big) = \max_{(x_t^s, \mathbf{M}_t^s) \in \mathbb{R} \times \mathbb{R}_+^N} [x_t^s + V^s(\mathbf{M}_t^s, t)] \quad (19)$$

subject to the budget constraint $\phi_t \cdot \mathbf{M}_t^s + x_t^s = \phi_t \cdot \mathbf{M}_{t-1}^s$.

The value $V^s\big(\mathbf{M}_t^s, t\big)$ satisfies:

$$V^s(\mathbf{M}_t^s, t) = \sigma\Big[-w\big(q\big(\mathbf{M}_t^b, t\big)\big) + \beta W^s\big(\mathbf{M}_t^s + \mathbf{d}\big(\mathbf{M}_t^b, t\big), t+1\big)\Big] + (1-\sigma)\beta W^s(\mathbf{M}_t^s, t+1). \tag{20}$$

Here the vector $\mathbf{M}_t^b \in \mathbb{R}_+^N$ denotes the portfolio of the buyer with whom the seller is matched in the DM. In the LW framework, the terms of trade in the decentralized market only depend on the real value of the buyer's portfolio, which implies that assets do not bring any additional benefit to the seller in the decentralized market. Consequently, the seller optimally chooses not to hold monetary assets across periods when $\phi_{t+1}^i/\phi_t^i \le \beta^{-1}$ for all $i \in \{1, \ldots, N\}$.

3.3. Entrepreneur

Now we describe the entrepreneur's problem. We use $M_t^i \in \mathbb{R}_+$ to denote the per buyer supply of currency i in period t. Let $\Delta_t^i \in \mathbb{R}$ denote entrepreneur i's net circulation of newly minted tokens in period t (or the mining of new cryptocurrency). If we anticipate that all type-i entrepreneurs behave identically, given that they solve the same decision problem, then we can write the law of motion for type-i tokens as $M_t^i = \Delta_t^i + M_{t-1}^i$, where $M_{-1}^i \in \mathbb{R}_+$ denotes the initial stock.

We will show momentarily that $\Delta_t^i \ge 0$. Thus, the entrepreneur's budget constraint becomes $x_t^i + \sum_{j\neq i}\phi_t^j M_t^{ij} = \phi_t^i \Delta_t^i + \sum_{j\neq i}\phi_t^j M_{t-1}^{ij}$ at each date $t \ge 0$. Here $M_t^{ij} \in \mathbb{R}_+$ denotes entrepreneur i's holdings of currency issued by entrepreneur $j\neq i$. This budget constraint highlights that privately-issued currencies are not associated with an explicit promise by the issuers to exchange them for goods or assets at a future date.

If $\phi_{t+1}^j/\phi_t^j \le \beta^{-1}$ for all $j \in \{1, \ldots, N\}$, then entrepreneur i chooses not to hold other currencies across periods, so that $M_t^{ij} = 0$ for all $j\neq i$. Thus, we can rewrite the budget constraint as $x_t^i = \phi_t^i \Delta_t^i$, which tells us that the entrepreneur's consumption in period t is equal to the real value of the net circulation. Because $x_t^i \ge 0$, we must have $\Delta_t^i \ge 0$. Given that an entrepreneur takes prices $\{\phi_t\}_{t=0}^\infty$ as given, $\Delta_t^{*,i} \in \mathbb{R}_+$ maximizes profits:

$$\Delta_t^{*,i} \in \arg\max_{\Delta \in \mathbb{R}_+}\big[\phi_t^i \Delta - c(\Delta)\big]. \tag{21}$$

Thus, profit maximization establishes a relation between net circulation $\Delta_t^{*,i}$ and the real price ϕ_t^i. Let $\boldsymbol{\Delta}_t^* \in \mathbb{R}_+^N$ denote the vector describing the optimal net circulation in period t for all currencies.

The solution to the entrepreneur's profit-maximization problem implies, at all dates $t \ge 0$:

$$M_t^i = \Delta_t^{*,i} + M_{t-1}^i. \tag{22}$$

3.4. Equilibrium

The final step in constructing an equilibrium is to impose the market-clearing condition $\mathbf{M}_t = \mathbf{M}_t^b + \mathbf{M}_t^s$ at all dates. Since $\mathbf{M}_t^s = \mathbf{0}$, the market-clearing condition reduces to

$$\mathbf{M}_t = \mathbf{M}_t^b. \tag{23}$$

We can now provide a formal definition of a (perfect-foresight) equilibrium under a purely private monetary arrangement.

Definition 1. An equilibrium is an array $\big\{\mathbf{M}_t, \mathbf{M}_t^b, \boldsymbol{\Delta}_t^*, \phi_t\big\}_{t=0}^\infty$ satisfying (16)–(23) for each $i \in \{1, \ldots, N\}$ at all dates $t \ge 0$.

We start our analysis by investigating whether a monetary equilibrium consistent with price stability exists in the presence of currency competition. Subsequently, we turn to the welfare properties of the equilibrium allocations. In what follows, it is helpful to provide a broad definition of price stability.

Definition 2. A monetary equilibrium is consistent with price stability if $\lim_{t\to\infty}\phi_t^i = \bar{\phi}^i > 0$ for at least one currency $i \in \{1, \ldots, N\}$.

We also provide a stronger definition of price stability that requires the price level to stabilize after a finite date.

Definition 3. A monetary equilibrium is consistent with *strong* price stability if there is a finite date $T \ge 0$ such that $\phi_t^i = \bar{\phi}^i > 0$ for each $i \in \{1, \ldots, N\}$ at all dates $t \ge T$.

Throughout the paper, we make the following assumption to guarantee a well-defined demand schedule for real balances.

Assumption 1. $u'(q)/m'(q)$ is strictly decreasing for all $q < q^*$ and we have $\lim_{q\to 0} u'(q)/m'(q) = \infty$.

A key property of equilibrium allocations under a competitive regime is that profit maximization establishes a positive relationship between the real price of currency i and the additional amount put into circulation by entrepreneur i when the cost function satisfies some basic properties. The following result shows an important implication of this relation.

Lemma 4. Suppose that $c'(0) = 0$. Then, we have $\Delta_t^{*,i} > 0$.

Proof. Suppose that $\Delta_t^{*,i} = 0$. Because the cost function is differentiable at 0, it must be right differentiable at 0. Thus, we have $\lim_{\Delta \to 0^+} \frac{c(\Delta) - c(0)}{\Delta} = c'(0) = 0$. This means there must exist some $\Delta' > 0$ such that $\frac{c(\Delta') - c(0)}{\Delta'} < \phi_t^i$.

Note that $\Delta_t^{*,i} = 0$ implies $\phi_t^i \Delta_t^{*,i} - c(\Delta_t^{*,i}) = -c(0)$. Then, we have $\phi_t^i \Delta \leq c(\Delta) - c(0)$ for all $\Delta > 0$. Rearranging this expression, we get $\frac{c(\Delta) - c(0)}{\Delta} \geq \phi_t^i$ for all $\Delta > 0$, which implies a contradiction. □

We can now establish a central result of our positive analysis: price stability is inconsistent with a competitive supply of fiduciary currencies for a class of cost functions satisfying the previous assumptions.

Proposition 1. *If $c'(0) = 0$, then there is no monetary equilibrium consistent with price stability.*

Proof. Proof by contradiction. Suppose that $\left\{ \mathbf{M}_t, \mathbf{M}_t^b, \boldsymbol{\Delta}_t^*, \phi_t \right\}_{t=0}^{\infty}$ is a monetary equilibrium with price stability. Then, $\lim_{t \to \infty} \phi_t^i = \bar{\phi}^i > 0$ for some i. Given any $\varepsilon \in \left(0, \bar{\phi}^i\right)$, there exists T such that $\phi_t^i \in \left(\bar{\phi}^i - \varepsilon, \bar{\phi}^i + \varepsilon\right)$ for all $t \geq T$. From Lemma 1, we have $\delta \equiv \arg\max_{\Delta \geq 0} \left\{ \left(\bar{\phi}^i - \varepsilon\right)\Delta - c(\Delta) \right\} > 0$. Because $\Delta_t^{*,i}$ is weakly increasing in ϕ_t^i, we have $\Delta_t^{*,i} \geq \delta$ for all $t \geq T$.

Because there is a positive lower bound on new minting of coins after time T, we know that M_t^i will be unbounded and that $\phi_{t+1}^i M_t^i$ will similarly be unbounded since there is a lower bound on the price, $\phi_t^i \geq \bar{\phi}^i - \varepsilon$, after time T. This means that there is some time T' such that $L_\theta(\phi_{t+1} \cdot \mathbf{M}_t) = 1$ for all $t \geq T'$.

Choose $\varepsilon > 0$ small enough such that $\frac{\bar{\phi}^i - \varepsilon}{\bar{\phi}^i + \varepsilon} > \beta$ and find the corresponding T such that $\phi_t^i \in \left(\bar{\phi}^i - \varepsilon, \bar{\phi}^i + \varepsilon\right)$ for all $t \geq T$. Then, for any time $t > \max\{T, T'\}$, we know that $L_\theta(\phi_{t+1} \cdot \mathbf{M}_t) = 1$ and $\phi_t^i / \phi_{t+1}^i > \beta$. But this implies that the buyer's first-order condition is not satisfied, a contradiction. □

The previous proposition emphasizes that the main problem of a monetary system with competitive issuers is that the supply of each brand becomes unbounded when the marginal cost goes to zero as new minting goes to zero: Private entrepreneurs always have an incentive to mint just a little bit more of the currency. But then one cannot have a stable value of privately-issued currencies, given that such stability would eventually lead to the violation of the transversality condition. Friedman (1960) arrived at the same conclusion when arguing that a purely private system of fiduciary currencies would necessarily lead to instability in the price level. Our formal analysis confirms Friedman's conjecture.

This prediction of the model is in sharp contrast to Hayek (1999), who argued that government intervention is not necessary for the establishment of a monetary system consistent with price stability. The previous proposition shows that Hayek's conjecture fails in our environment with $c'(0) = 0$.[3]

Our next step is to verify whether other cost functions can be consistent with price stability. More concretely, we want to characterize *sufficient* conditions for price stability. We now establish that currency competition can deliver Hayek's conjecture of price stability when the cost function is locally linear around the origin.[4]

Proposition 2. *Suppose that $c : \mathbb{R}_+ \to \mathbb{R}_+$ is locally linear in a neighborhood $\left[0, \Delta'\right] \subset \mathbb{R}_+$. Then, there is a monetary equilibrium consistent with strong price stability provided the neighborhood $[0, \Delta']$ is not too small.*

In this equilibrium, the real value of private currencies, as well as their expected return, remains constant. In the context of cryptocurrencies, a cost function that is locally linear around the origin implies that the difficulty of mining new units does not change. The previous result provides a partial vindication of Hayek (1999): a purely private arrangement can deliver price stability for a strict subset of production technologies.

However, our next result shows that, for the same subset of production technologies, we have other equilibria characterized by the persistently declining purchasing power of private money and falling trading activity. There is no reason to forecast that the equilibrium with stable value will prevail over these different equilibria.

Proposition 3. *Suppose that $c : \mathbb{R}_+ \to \mathbb{R}_+$ is locally linear in a neighborhood $\left[0, \bar{\Delta}\right] \subset \mathbb{R}_+$. Then, there exists a continuum of equilibria with the property that, for each $i \in \{1, \ldots, N\}$, the sequence $\left\{\phi_t^i\right\}_{t=0}^{\infty}$ converges monotonically to zero.*

For any initial condition within a neighborhood of zero, there exists an associated equilibrium trajectory that is monotonically decreasing. In this equilibrium, real money balances decrease monotonically over time and converge to zero, so the equilibrium allocation approaches autarky as $t \to \infty$. The decline in the desired amount of real balances follows from the anticipated decline in the purchasing power of private money. As a result, trading activity in the decentralized market monotonically declines along the equilibrium trajectory. Therefore, private money is inherently unstable in that changes in beliefs can lead to undesirable self-fulfilling inflationary episodes.

The existence of these inflationary equilibrium trajectories in a purely private monetary arrangement also means that hyperinflationary episodes are not an exclusive property of government-issued money. Obstfeld and Rogoff (1983) build economies that can display self-fulfilling inflationary episodes when the government is the sole issuer of currency.

---

[3] It is straightforward to add, for instance, shocks to the cost function to make the evolution of the price level random. Furthermore, as we will argue later, a private money system is subject to self-fulfilling inflationary episodes. These two considerations show that the shortcomings of private money arrangements go well beyond the perhaps smaller problem of price changes under perfect foresight highlighted by Proposition 1.

[4] All the omitted proofs are included in the Online Appendix.

Lagos and Wright (2003) show the same result in search-theoretic monetary models with government-supplied currency. Our analysis illustrates that replacing government monopoly with private currencies does not overcome the fundamental fragility associated with fiduciary regimes, public or private.

To conclude this section, we show the existence of an asymmetric equilibrium with the property that a single private currency circulates in the economy. This occurs because the market share across different types of money is indeterminate.

Proposition 4. *Suppose that $c : \mathbb{R}_+ \to \mathbb{R}_+$ is locally linear in a neighborhood $[0, \Delta'] \subset \mathbb{R}_+$. Let $b_t^i \equiv \phi_t^i M_t^i$ denote real balances for currency i. Then, there exists a monetary equilibrium satisfying $b_t^1 = b > 0$ and $b_t^i = 0$ for all $i \geq 2$ at all dates $t \geq 0$.*

In these equilibria, a single currency brand becomes the sole means of payment in the economy. Competition constrains individual behavior in the market for private currencies. Market participants understand the discipline imposed by competition, summarized in the rate-of-return equality equilibrium condition, even though they see a single brand circulating in the economy. As in the previous case, an equilibrium with a stable value of money is as likely to occur as an equilibrium with a declining value of money.

3.5. Welfare

To simplify our welfare analysis, we consider the solution to the planner's problem when the economy is initially endowed with a strictly positive amount of tokens. These durable objects serve as a record-keeping device that allows the planner to implement allocations with positive trade in the DM, even though the actions in each bilateral meeting are privately observable and agents cannot commit to their promises. Thanks to the existence of an initial positive amount of tokens, the planner does not need to use the costly technology to mint additional tokens to serve as a record-keeping device in decentralized transactions.[5]

In this case, any solution to the social planner's problem is characterized by the surplus-maximizing quantity q^* in the DM. Following Rocheteau (2012), it can be shown that a social planner with access to lump-sum taxes in the CM can implement the first-best allocation (i.e., the allocation the planner would choose with perfect record-keeping and full commitment) by systematically removing tokens from circulation.

In our analysis above, we used the generalized Nash bargaining solution to determine the terms of trade in the DM. Lagos and Wright (2005) demonstrate that Nash bargaining can result in a holdup problem and inefficient trading activity in the DM. Aruoba et al. (2007) show that alternative bargaining solutions matter for the efficiency of monetary equilibria. Thus, we will restrict our attention to an "efficient" bargaining protocol where the buyer makes a take-it-or-leave-it offer to the seller. In that way, it will be transparent how private currencies generate their own inefficiencies that are different from the more general inefficiencies discussed in Lagos and Wright (2005).

Given Assumption 1, $L_1 : \mathbb{R}_+ \to \mathbb{R}_+$ is invertible in the range $\left(0, \beta^{-1} w(q^*)\right)$ so that we can define

$$z(\gamma) \equiv \frac{1}{\gamma} L_1^{-1} \left(\frac{1}{\beta \gamma} \right), \tag{24}$$

where $\gamma \in \mathbb{R}_+$ represents the common real return across all valued currencies. The previous relation describes the demand for real balances as a function of the real return on money.

At this point, we focus on preferences and technologies that imply an empirically plausible money demand function satisfying the property that the demand for real balances is decreasing in the inflation rate.

Assumption 2. *Suppose $z : \mathbb{R}_+ \to \mathbb{R}_+$ is strictly increasing.*

An implication of this result is that the equilibrium with stable prices is not socially efficient. In this equilibrium, the quantity traded in the DM $\hat{q}$ satisfies

$$\sigma \frac{u'(\hat{q})}{w'(\hat{q})} + 1 - \sigma = \frac{1}{\beta}, \tag{25}$$

which is below the socially efficient quantity (i.e., $\hat{q} < q^*$). Although the allocation associated with the equilibrium with stable prices is not efficient, it Pareto dominates the nonstationary equilibria described in Proposition 3. To verify this claim, note that the quantity traded in the DM starts from a value below $\hat{q}$ and decreases monotonically in an inflationary equilibrium.

Another implication is that the persistent creation of tokens along the equilibrium path is socially wasteful. Given an initial supply of tokens, the planner can implement an efficient allocation by systematically removing tokens from circulation so that the production of additional tokens is unnecessary. Because the creation of tokens is socially costly, any allocation involving a production plan that implies a growing supply of tokens is inefficient.

In equilibrium, a necessary condition for efficiency is to have the real rate of return on money equal to the rate of time preference. In this case, there is no opportunity cost of holding money balances for transaction purposes so that the socially

---

[5] Alternatively, one can think about the social planner as minting a trivially small amount of perfectly divisible currency at an epsilon cost.

efficient quantity q^* is traded in every bilateral match in the DM. Because a necessary condition for efficiency involves a strictly positive real return on money in equilibrium, the following result implies that a socially efficient allocation cannot be implemented as an equilibrium outcome in a purely private arrangement.

Proposition 5. *There is no stationary monetary equilibrium with a strictly positive real return on money.*

An immediate corollary from the previous proposition is that a purely private monetary system does not provide the socially optimum quantity of money, as defined in Friedman (1969). Despite having entrepreneurs that take prices parametrically, competition cannot provide an optimal outcome because entrepreneurs do not internalize the pecuniary externalities they create in the decentralized market by minting additional tokens. At a fundamental level, the market for currencies is very different from the market for goods such as wheat, and the forces that drive optimal outcomes under perfect competition in the latter fail in the former. If the productivity in the CM and DM markets grew over time, we could have deflation with a constant supply of private money and, under a peculiar combination of parameters, achieve efficiency. However, this would only be the product of a "divine coincidence."

4. Limited supply

In the previous section, entrepreneurs could mint as much new currency as they wanted in each period subject to the cost function. However, in reality, the protocol behind most cryptocurrencies sets up an upper bound on the supply of each brand. Thus, we extend our model to investigate the positive implications of such bounds.

Assume that there is a cap on the amount of each cryptocurrency that can be mined at each date. Formally, let $\bar{\Delta}_t^i \in \mathbb{R}_+$ denote the date-t cap on cryptocurrency $i \in \{1, \ldots, N\}$. In this case, the miner's profit-maximization problem is:

$$\Delta_t^{*,i} \in \arg \max_{0 \le \Delta \le \bar{\Delta}_t^i} \left[\phi_t^i \Delta - c(\Delta) \right]. \tag{26}$$

Then, we can define a monetary equilibrium by replacing (21) with (26).

The following result establishes that it is possible to have a monetary equilibrium consistent with our stronger definition of price stability when the protocol behind each cryptocurrency imposes an upper bound on total circulation, even if the cost function has a zero derivative at the origin.

Proposition 6. *Suppose $L_1(A) + AL_1'(A) > 0$ for all $A > 0$. Then, there is a class of caps $\left\{ \bar{\mathbf{\Delta}}_t \right\}_{t=0}^{\infty}$ such that a monetary equilibrium consistent with strong price stability exists. These caps are such that $\bar{\Delta}_t^i > 0$ at dates $0 \le t \le T$ and $\bar{\Delta}_t^i = 0$ at all subsequent dates $t \ge T + 1$, given a finite date $T > 0$.*

In the described allocation, the value of money and trading activity stabilize after date T. Thus, it is possible to have price stability with $c'(0) = 0$ when the protocol behind cryptocurrencies limits the amount of each privately-issued currency. In this respect, the innovations associated with cryptocurrencies and their immutable protocols can provide an effective mechanism to make a purely private arrangement consistent with price stability in the absence of government intervention. Our result resembles the existence result in Martin and Schreft (2006). These authors build an equilibrium where agents believe that if an issuer mints more than some threshold amount of currency, then only the currency issued up to the threshold will be valued and additional issuance will be worthless.

Although the existence of an upper bound on currency issue can promote price stability in a competitive environment, it does not imply efficiency. The arguments in Section 3.5 regarding why a market arrangement in currencies does not achieve efficiency continue to hold even if innovations in computer science permit the implementation of exogenous bounds on the supply of cryptocurrencies.

5. Monetary policy

We now study monetary policy in the presence of privately-issued currencies and its role in mitigating the undesirable properties of the competitive equilibrium. Is it possible to implement the socially optimal return on money by introducing government money?

Suppose the government enters the currency-issuing business by creating its own brand, referred to as currency $N + 1$. In this case, the government budget constraint is given by

$$\phi_t^{N+1} \Delta_t^{N+1} + \tau_t = c\left(\Delta_t^{N+1}\right), \tag{27}$$

where $\tau_t \in \mathbb{R}$ is the real value of lump-sum taxes, $\phi_t^{N+1} \in \mathbb{R}_+$ is the real value of government-issued currency, and $\Delta_t^{N+1} \in \mathbb{R}$ is the amount of the government brand issued at date t. What makes government money fundamentally different from private money is that, behind the government brand, there is a fiscal authority with the power to tax agents in the economy. Given an initial condition $M_{-1}^{N+1} \in \mathbb{R}_+$, government money follows, at all dates:

$$\bar{M}_t^{N+1} = \Delta_t^{N+1} + \bar{M}_{t-1}^{N+1}. \tag{28}$$

The definition of a perfect-foresight equilibrium in the presence of government money is the same as before except that the vectors $\mathbf{M}_t$, $\mathbf{M}_t^b$, and $\boldsymbol{\phi}_t$ are now elements in $\mathbb{R}_+^{N+1}$ and the scalar sequence $\left\{\Delta_t^{N+1}\right\}_{t=0}^{\infty}$ is exogenously given.

Definition 5. A monetary equilibrium with government money is an array $\left\{ \mathbf{M}_t, \mathbf{M}_t^b, \phi_t, \mathbf{\Delta}_t^*, \Delta_t^{N+1}, \tau_t \right\}_{t=0}^{\infty}$ satisfying (16)–(23) and (27) for each $i \in \{1, \ldots, N\}$ at all dates $t \geq 0$.

In any equilibrium with valued government money, we must have

$$\frac{\phi_{t+1}^{N+1}}{\phi_t^{N+1}} = \gamma_{t+1} \tag{29}$$

at all dates $t \geq 0$, where $\gamma_t \in \mathbb{R}_+$ represents the common real return across all valued currencies. In the absence of portfolio restrictions, government money must yield the same rate of return as other monetary assets for it to be valued in equilibrium.

5.1. Money-growth rule

We start our analysis of a hybrid arrangement by assuming that the government follows a money-growth rule of the form $M_t^{N+1} = (1 + \omega)M_{t-1}^{N+1}$, with the money growth rate satisfying $\omega \geq \beta - 1$ (otherwise, we would not have an equilibrium). Given this policy rule, we derive a crucial property of the hybrid monetary system. As we have seen, a necessary condition for efficiency is to have the real return on money equal to the rate of time preference. Thus, the socially optimal return on money is necessarily positive. The following proposition shows that it is impossible to have a monetary equilibrium with a positive real return on money *and* positively valued privately-issued money when there is no exogenous upper bound on the supply of each brand.

Proposition 7. *There is no stationary equilibrium with the properties that (i) at least one private currency is valued and (ii) the real return on money is strictly positive.*

The intuition for the result is as follows. An equilibrium with a positive real return on money requires deflation. A deflationary process can occur along the equilibrium path only if there is a persistent contraction of the money supply. The entrepreneurs are unwilling to shrink the private money supply by retiring previously issued currency. The only option left is to have the government systematically shrinking the supply of its brand to such an extent that the total money supply declines in every period. The proposition shows that this strategy becomes unsustainable at some finite date because the entrepreneurs will take advantage of the deflation engineered by monetary policy to create an ever-increasing amount of money. In other words: the implementation of monetary policy through a money-growth rule is impaired by competing currencies. Profit-maximizing entrepreneurs will frustrate the government's attempt to implement a positive real return on money through a deflation process when the public is willing to hold private currencies. Recall that there is nothing intrinsically superior about government money from the perspective of the agents. For example, we are not assuming that the government forces agents to pay their taxes in its currency.

A corollary of Proposition 7 is that the socially optimal return on money can be implemented through a money-growth rule only if agents do not value privately-issued currency. In particular, we can construct equilibria with the property $\phi_t^i = 0$ for all $i \in \{1, \ldots, N\}$ and $\phi_t^{N+1} > 0$ at all dates $t \geq 0$. In these equilibria, the sequence of returns satisfies, for all dates

$$z(\gamma_{t+1}) = (1 + \omega)z(\gamma_t)\gamma_t. \tag{30}$$

A policy choice ω in the range $(\beta - 1, 0)$ is associated with a steady state characterized by deflation and a strictly positive real return on money. In particular, we have $\gamma_t = (1 + \omega)^{-1}$ for all $t \geq 0$. In this stationary equilibrium, the quantity traded in the DM, represented by $q(\omega)$, satisfies

$$\sigma \frac{u'(q(\omega))}{w'(q(\omega))} + 1 - \sigma = \frac{1 + \omega}{\beta}. \tag{31}$$

If we let $\omega \to \beta - 1$, the associated steady state delivers an efficient allocation (i.e., $q(\omega) \to q^*$ as $\omega \to \beta - 1$). This policy prescription is the celebrated Friedman rule, which eliminates the opportunity cost of holding money balances for transaction purposes. The problem with this arrangement is that the Friedman rule is not *uniquely* associated with an efficient allocation. In addition to the equilibrium allocations characterized by the coexistence of private and government monies, there exists a continuum of inflationary trajectories that are also associated with the Friedman rule. These trajectories are suboptimal because they involve a persistently declining value of money.

The result in the previous proposition does not necessarily hold if we allow for the existence of exogenous upper bounds on the supply of each brand of currency. The following proposition shows that it is possible to construct an equilibrium with valued private money and a strictly positive real return on money after some finite date provided the upper bounds are selected in the same way as in Proposition 6.

Proposition 8. *Suppose $L_1(A) + AL_1'(A) > 0$ for all $A > 0$. Then, there is a set of caps $\left\{ \bar{\mathbf{\Delta}}_t \right\}_{t=0}^{\infty}$ such that a monetary equilibrium with valued private money and a strictly positive real return on money exists.*

An immediate corollary of the previous proposition is that an efficient allocation can be implemented after some finite date if the government follows a version of the Friedman rule. Although the existence of upper bounds can lead to an equilibrium consistent with efficiency after a finite date, the implementation of policy is not unique.

5.2. Pegging the real value of government money

In view of the previous results, we develop an alternative policy rule that can *uniquely* implement the socially optimal return on money. This outcome will require government money to drive private money out of the economy.

Consider a policy rule that pegs the real value of government money. Specifically, assume the government issues currency to satisfy:

$$\phi_t^{N+1} \bar{M}_t^{N+1} = m \tag{32}$$

at all dates for some target value $m > 0$. This means that the government adjusts the sequence $\left\{ \Delta_t^{N+1} \right\}_{t=0}^{\infty}$ to satisfy (32) in every period.

The following proposition shows that it is possible to select a target value m for government policy that *uniquely* implements a stationary equilibrium with a strictly positive real return on money.

Proposition 9. *There exists a unique stationary monetary equilibrium characterized by a constant positive real return on money provided the target value m satisfies $z^{-1}(m) > 1$ and $\beta z^{-1}(m)m \leq w(q^*)$. In this equilibrium, government money drives private money out of the economy.*

Proposition 7 shows that, under a money-growth rule, there is no equilibrium with a positive real return on money and positively valued private monies. But this result does not rule out the existence of equilibria with a negative real return on money and valued private monies. Proposition 9 provides a stronger result. Specifically, it shows that an equilibrium with valued private monies does not exist when the government follows a policy rule that pegs the real value of government money, provided that the target value is sufficiently large. Given the government's commitment to peg the purchasing power of money balances, a private entrepreneur needs to be willing to shrink the supply of his own brand to maintain a constant purchasing power of money balances when the value of money increases at a constant rate along the equilibrium trajectory. But profit maximization implies that an entrepreneur wants to expand his supply, not contract it. As a result, an equilibrium with valued private money cannot exist when the government pegs the purchasing power of money at a sufficiently high level.

Another interpretation of Proposition 9 is that unique implementation requires the provision of "good" government money. Pegging the real value of government money can be viewed as providing good money to support exchange in the economy. To verify this claim, note that unique implementation requires $z^{-1}(m) > 1$. Because $\gamma_t \geq z^{-1}(m)$ must hold at all dates, the real return on money must be strictly positive in any allocation that can be uniquely implemented under the previously described policy regime. Furthermore, private money creation is a socially wasteful activity. Thus, an immediate societal benefit of a policy that drives private money out of the economy is to prevent the wasteful creation of tokens in the private sector.

A corollary from Proposition 9 is that we can uniquely implement the socially optimal return on money by taking the limit $m \to z\left(\frac{1}{\beta}\right)$. Hence, the surplus-maximizing quantity q^* is traded in each bilateral meeting in the DM.

To implement a target value with $z^{-1}(m) > 1$, the government must tax private agents in the CM. The government budget constraint can be written, in every period t, as $\tau_t = m(\gamma_t - 1)$. Because the unique equilibrium implies $\gamma_t = z^{-1}(m)$ for all $t \geq 0$, we must have $\tau_t = m\left[z^{-1}(m) - 1\right] > 0$, also at all dates $t \geq 0$. To implement its target value m, the government needs to persistently contract the money supply by making purchases that exceed its sales in the CM, with the shortfall financed by taxes.

We already saw that a necessary condition for efficiency is to have the real return on money equal to the rate of time preference. It remains to characterize sufficient conditions for efficiency. In particular, we want to verify whether the unique allocation associated with the policy choice $m \to z(\beta^{-1})$ is socially efficient. The nontrivial element of the environment that makes the welfare analysis more complicated is the presence of a costly technology to manufacture durable tokens that circulate as a medium of exchange.

If the initial endowment of government money across agents is strictly positive, then the allocation associated with $m \to z(\beta^{-1})$ is socially efficient, given that the entrepreneurs are driven out of the market and the government does not use the costly technology to create additional tokens. Also, given a quasi-linear preference, the lump-sum tax is neutral.

If the initial endowment of government money is zero, then the government needs to mint an initial amount of tokens so that it can systematically shrink the available supply in subsequent periods to induce deflation. Here, we run into a classic issue in monetary economics: how much money to issue initially in an environment where it is costly to mint additional units? The government would like to issue as little as possible at the initial date, given that tokens are costly to produce. In fact, the problem of determining the socially optimal initial amount has no solution in the presence of divisible money. Despite this issue, it is clear that, after the initial date, the equilibrium allocation is socially efficient.

In conclusion: the joint goal of monetary stability and efficiency can be achieved by public policy provided the government can tax private agents to guarantee a sufficiently large value of its money supply.

6. Automata

Consider the benchmark economy described in Section 3 without profit-maximizing entrepreneurs. Instead, private money is issued by automata, a closer description of the protocols behind some cryptocurrencies.

To so so, we add to that economy J automata, each programmed to maintain a constant amount $H^j \in \mathbb{R}_+$ of tokens. Let $h_t^j \equiv \phi_t^j H^j$ denote the real value of the tokens issued by automaton $j \in \{1, \ldots, J\}$ and let $\mathbf{h}_t \in \mathbb{R}_+^J$ denote the vector of real values. If the units issued by automaton j are valued in equilibrium, we must have

$$\frac{\phi_{t+1}^j}{\phi_t^j} = \gamma_{t+1} \tag{33}$$

at all dates $t \geq 0$. Here $\gamma_{t+1} \in \mathbb{R}_+$ continues to represent the common real return across all valued currencies in equilibrium. Thus, condition (33) implies

$$h_t^j = h_{t-1}^j \gamma_t \tag{34}$$

for each j at all dates. The market-clearing condition in the money market becomes

$$m + \sum_{j=1}^{J} h_t^j = z(\gamma_{t+1}). \tag{35}$$

for all $t \geq 0$. Given these conditions, we can provide a definition of a (perfect-foresight) equilibrium in the presence of automata under the policy of pegging the real value of government money.

Definition 6. A monetary equilibrium is a sequence $\left\{\mathbf{h}_t, \gamma_t, \Delta_t^{N+1}, \tau_t\right\}_{t=0}^{\infty}$ satisfying (27), (32), (34), (35), $h_t^j \geq 0$, $z(\gamma_t) \geq m$, and $\beta \gamma_t z(\gamma_t) \leq w(q^*)$ for all $t \geq 0$ and $j \in \{1, \ldots, J\}$.

The result derived in Proposition 9 holds when private monies are issued by automata.

Proposition 10. *There exists a unique monetary equilibrium characterized by a constant positive real return on money provided the target value m satisfies $z^{-1}(m) > 1$ and $\beta z^{-1}(m)m \leq w(q^*)$. In this equilibrium, government money drives private money out of the economy.*

The previous proposition shows that an equilibrium can be described by a sequence $\{\gamma_t\}_{t=0}^{\infty}$ satisfying the dynamic system $z(\gamma_{t+1}) - m = \gamma_t[z(\gamma_t) - m]$, together with the boundary conditions $z(\gamma_t) \geq m$ and $\beta \gamma_t z(\gamma_t) \leq w(q^*)$.

We want to show that the properties of the dynamic system depend on the value of the policy parameter m. Precisely, the previously described system is a transcritical bifurcation. Consider the functional forms $u(q) = (1 - \eta)^{-1} q^{1-\eta}$ and $w(q) = (1 + \alpha)^{-1} q^{1+\alpha}$, with $0 < \eta < 1$ and $\alpha \geq 0$. In this case, the equilibrium evolution of the real return on money satisfies

$$\frac{\sigma^{\frac{1+\alpha}{\eta+\alpha}} (\beta \gamma_{t+1})^{\frac{1+\alpha}{\eta+\alpha} - 1}}{[1 - (1-\sigma)\beta\gamma_{t+1}]^{\frac{1+\alpha}{\eta+\alpha}}} = \frac{\beta^{\frac{1+\alpha}{\eta+\alpha} - 1} (\sigma\gamma_t)^{\frac{1+\alpha}{\eta+\alpha}}}{[1 - (1-\sigma)\beta\gamma_t]^{\frac{1+\alpha}{\eta+\alpha}}} - m\gamma_t + m \tag{36}$$

with

$$\frac{(\beta\gamma_t)^{\frac{1+\alpha}{\eta+\alpha} - 1}}{1+\alpha} \left[\frac{\sigma}{1 - (1-\sigma)\beta\gamma_t}\right]^{\frac{1+\alpha}{\eta+\alpha}} \geq m \tag{37}$$

at all dates $t \geq T$. Condition (37) imposes a lower bound on the equilibrium return on money, which can result in the existence of a steady state at the lower bound.

We further simplify the dynamic system by assuming that $\alpha = 0$ (linear disutility of production) and $\sigma \to 1$ (no matching friction in the decentralized market). In this case, the equilibrium evolution of the return on money γ_t satisfies:

$$\gamma_{t+1} = \gamma_t^2 - \frac{m}{\beta}\gamma_t + \frac{m}{\beta} \tag{38}$$

and the boundary condition

$$\frac{m}{\beta} \leq \gamma_t \leq \frac{1}{\beta}. \tag{39}$$

The policy parameter can take on any value in the interval $0 \leq m \leq 1$. Also, the real value of the money supply remains above the lower bound m at all dates. Given that the government provides a credible lower bound for the real value of the money supply due to its taxation power, the return on money is bounded below by a strictly positive constant $\beta^{-1}m$ along the equilibrium path.

We can obtain a steady state by solving the polynomial equation

$$\gamma^2 - \left(\frac{m}{\beta} + 1\right)\gamma + \frac{m}{\beta} = 0. \tag{40}$$

If $m \neq \beta$, the roots are 1 and $\beta^{-1}m$. If $m = \beta$, the unique solution is 1.

The properties of this dynamic system differ considerably depending on the value of the policy parameter m. If $0 < m < \beta$, then there exist two steady states: $\gamma_t = \beta^{-1}m$ and $\gamma_t = 1$ for all $t \geq 0$. The steady state $\gamma_t = 1$ for all $t \geq 0$ corresponds to the previously described stationary equilibrium with constant prices. The steady state $\gamma_t = \beta^{-1}m$ for all $t \geq 0$ is an equilibrium with the property that only government money is valued, which is globally stable. There exists a continuum of equilibrium trajectories starting from any point $\gamma_0 \in (\beta^{-1}m, 1)$ with the property that the return on money converges to $\beta^{-1}m$. Along these trajectories, the value of money declines monotonically to the lower bound m and government money drives private money out of the economy.

If $m = \beta$, the unique steady state is $\gamma_t = 1$ for all $t \geq 0$. In this case, the 45-degree line is the tangent line to the graph of (38) at the point $(1, 1)$, so the dynamic system remains above the 45-degree line. When we introduce the boundary restriction (39), we find that $\gamma_t = 1$ for all $t \geq 0$ is the unique equilibrium trajectory. Thus, the policy choice $m = \beta$ results in global determinacy, with the unique equilibrium outcome characterized by price stability.

If $\beta < m < 1$, the unique steady state is $\gamma_t = \beta^{-1}m$ for all $t \geq 0$. Setting the target for the value of government money in the interval $\beta < m < 1$ results in a sustained deflation to ensure that the real return on money remains above one. To implement a sustained deflation, the government must contract its money supply, a policy financed through taxation.

7. Productive capital

How does our analysis change if we introduce productive capital into the economy? For example, what happens if the entrepreneurs can use the proceeds from minting their coins to buy capital and use it to implement another currency minting strategy? In what follows, we show that productive capital does not change the set of implementable allocations in the economy with profit-maximizing entrepreneurs, a direct consequence of the entrepreneur's linear utility function. On the other hand, with automaton issuers, it is possible to implement an efficient allocation in the absence of government intervention provided that the automaton issuers have access to sufficiently productive capital.

7.1. Profit-maximizing entrepreneurs

Suppose that there is a real asset that yields a constant stream of dividends $\kappa > 0$ in terms of the CM good (i.e., a Lucas tree). Let us assume that each entrepreneur is endowed with an equal claim on the real asset. The entrepreneur's budget constraint is given by

$$x_t^i + \sum_{j \neq i} \phi_t^j M_t^{ij} = \frac{\kappa}{N} + \phi_t^i \Delta_t^i + \sum_{j \neq i} \phi_t^j M_{t-1}^{ij}. \tag{41}$$

As we have seen, it follows that $M_t^{ij} = 0$ for all $j \neq i$ if $\phi_{t+1}^j/\phi_t^j \leq \beta^{-1}$ holds for all $j \in \{1, \ldots, N\}$. Then, the budget constraint reduces to $x_t^i = \frac{\kappa}{N} + \phi_t^i \Delta_t^i$. Finally, the profit-maximization problem can be written as

$$\max_{\Delta \in \mathbb{R}_+} \left[\frac{\kappa}{N} + \phi_t^i \Delta - c(\Delta) \right]. \tag{42}$$

It is clear that the set of solutions for the previous problem is the same as that of (21). Thus, the presence of productive capital does not change the previously derived properties of the purely private arrangement.

7.2. Automata

Suppose that there exist J automata, each programmed to follow a predetermined plan. Consider an arrangement with the property that each automaton has an equal claim on the real asset and that automaton j is programmed to manage the supply of currency j to yield a predetermined dividend plan $\left\{ f_t^j \right\}_{t=0}^{\infty}$ satisfying $f_t^j \geq 0$ at all dates $t \geq 0$. The nonnegativity of the real dividends f_t^j reflects the fact that an automaton issuer has no taxation power. Finally, all dividends are rebated to households, the ultimate owners of the stock of real assets, who had "rented" these assets to "firms."

Formally, for each automaton $j \in \{1, \ldots, J\}$, we have the budget constraint

$$\phi_t^j \Delta_t^j + \frac{\kappa}{J} = f_t^j, \tag{43}$$

together with the law of motion $H_t^j = \Delta_t^j + H_{t-1}^j$. Also, assume that $H_{-1}^j > 0$ for some $j \in \{1, \ldots, J\}$.

As in the previous section, let $h_t^j \equiv \phi_t^j H^j$ denote the real value of the tokens issued by automaton $j \in \{1, \ldots, J\}$ and let $\mathbf{h}_t \in \mathbb{R}_+^J$ denote the vector of real values. Let $\mathbf{f}_t \in \mathbb{R}_+^J$ denote the vector of real dividends. Market clearing in the money market is given by

$$\sum_{j=1}^{J} h_t^j = z(\gamma_{t+1}) \tag{44}$$

for all $t \geq 0$. For each automaton j, we can rewrite the budget constraint (43) as

$$h_t^j - \gamma_t h_{t-1}^j + \frac{\kappa}{J} = f_t^j. \tag{45}$$

Given these changes in the environment, we must now provide a formal definition of a perfect-foresight equilibrium when automaton issuers have access to productive capital.

Definition 7. Given a predetermined dividend plan $\{\mathbf{f}_t\}_{t=0}^{\infty}$, a monetary equilibrium is a sequence $\{\mathbf{h}_t, \gamma_t\}_{t=0}^{\infty}$ satisfying (44), (45), $h_t^j \geq 0$, $z(\gamma_t) \geq 0$, and $\beta \gamma_t z(\gamma_t) \leq w(q^*)$ for all $t \geq 0$ and $j \in \{1, \ldots, J\}$.

It remains to verify whether a particular set of dividend plans can be consistent with an efficient allocation. An obvious candidate for an efficient dividend plan is the constant sequence $f_t^j = \frac{f}{J}$ for all $j \in \{1, \ldots, J\}$ at all dates $t \geq 0$, with $0 \leq f \leq \kappa$. In this case, we obtain the dynamic system:

$$z(\gamma_{t+1}) - \gamma_t z(\gamma_t) + \kappa - f = 0 \tag{46}$$

with $z(\gamma_t) \geq 0$ and $\beta \gamma_t z(\gamma_t) \leq w(q^*)$. The following proposition establishes the existence of a unique equilibrium allocation with the property that the real return on money is strictly positive.

Proposition 11. *Suppose $u(q) = (1 - \eta)^{-1} q^{1-\eta}$ and $w(q) = (1 + \alpha)^{-1} q^{1+\alpha}$, with $0 < \eta < 1$ and $\alpha \geq 0$. Then, there exists a unique equilibrium allocation with the property $\gamma_t = \gamma^s$ for all $t \geq 0$ and $1 < \gamma^s \leq \beta^{-1}$.*

Our next step is to show that the unique equilibrium is socially efficient if the real dividend $\kappa > 0$ is sufficiently large. To demonstrate this result, we further simplify the dynamic system by assuming that $\eta = \frac{1}{2}$ and $\alpha = 0$. In addition, we take the limit $\sigma \to 1$. In this case, the dynamic system reduces to

$$\gamma_{t+1} = \gamma_t^2 - \beta^{-1} \hat{\kappa} \equiv g(\gamma_t), \tag{47}$$

where $\hat{\kappa} \equiv \kappa - f$. The unique fixed point in the range $\left[0, \beta^{-1}\right]$ is

$$\gamma^s \equiv \frac{1 + \sqrt{1 + 4\beta^{-1}\hat{\kappa}}}{2} \tag{48}$$

provided $\hat{\kappa} \leq \frac{1-\beta}{\beta}$. Because $g'(\gamma) > 0$ for all $\gamma > 0$ and $0 = g\left(\sqrt{\beta^{-1}\hat{\kappa}}\right)$, it follows that $\gamma_t = \gamma^s$ for all $t \geq 0$ is the unique equilibrium trajectory. As we can see, the real return on money is strictly positive. If we take the limit $\hat{\kappa} \to \frac{1-\beta}{\beta}$, we find that the unique equilibrium approaches the socially efficient allocation. Thus, it is possible to uniquely implement an allocation that is arbitrarily close to an efficient allocation if the stock of real assets is sufficiently productive to finance the deflationary process associated with the Friedman rule.

The results derived in this subsection resemble those of Andolfatto et al. (2016), who study the properties of a monetary arrangement in which an institution with monopoly rights on the economy's physical capital issues claims that circulate as a medium of exchange. Both analyses confirm that the implementation of an efficient allocation does not necessarily rely on the government's taxation power if private agents have access to productive assets.

8. Conclusions

In this paper, we have shown how a system of competing private currencies can work. Our evaluation of such a system is nuanced. While we offer glimpses of hope for it by proving the existence of stationary equilibria that deliver price stability, there are plenty of other less desirable equilibria. And even the best equilibrium does not deliver the socially optimum amount of money. At this stage, we do not have any argument to forecast the empirical likelihood of each of these equilibria. Furthermore, we have shown that currency competition can be a socially wasteful activity.

Our analysis has also shown that the presence of privately-issued currencies can create problems for a money-growth rule. As we have seen, profit-maximizing entrepreneurs will frustrate the government's attempt to implement a positive real return on money when the public is willing to hold in portfolio privately-issued currencies.

Given these difficulties, we have characterized an alternative monetary policy rule that uniquely implements a socially efficient allocation by driving private monies out of the economy. We have shown that this policy rule is robust to other forms of private monies, such as those issued by automata. In addition, we have argued that, in a well-defined sense, currency competition provides market discipline to monetary policy implementation by inducing the government to provide "good" money.

Finally, we have considered the possibility of implementing an efficient allocation with automaton issuers in an economy with productive capital. As we have seen, an efficient allocation can be the unique equilibrium outcome provided that capital is sufficiently productive.

We have, nevertheless, just scratched the surface of the study of private currency competition. Many other topics, such as introducing random shocks and trends to productivity, the analysis of the different degrees of moneyness of private currencies (including interest-bearing assets and redeemable instruments), the role of positive transaction costs among different currencies, the entry and exit of entrepreneurs, the possibility of market power by currency issuers, and the consequences of the lack of enforceability of contracts, are some of the avenues for future research.

Supplementary material

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.jmoneco.2019.07.003.

References

Andolfatto, D., Berentsen, A., Waller, C., 2016. Monetary policy with asset-backed money. J. Econ. Theory 164, 166–186.

Araujo, L., Camargo, B., 2008. Endogenous supply of fiat money. J. Econ. Theory 142 (1), 48–72.

Aruoba, S., Rocheteau, G., Waller, C., 2007. Bargaining and the value of money. J. Monet. Econ. 54 (8), 2636–2655.

Berentsen, A., 2006. On the private provision of fiat currency. Eur. Econ. Rev. 50 (7), 1683–1698.

Cavalcanti, R.d. O., Erosa, A., Temzelides, T., 1999. Private money and reserve management in a random-matching model. J. Polit. Econ. 107 (5), 929–945.

Cavalcanti, R.d. O., Erosa, A., Temzelides, T., 2005. Liquidity, money creation and destruction, and the returns to banking. Int. Econ. Rev. 46 (2), 675–706.

Cavalcanti, R.d. O., Wallace, N., 1999. Inside and outside money as alternative media of exchange. J. Money Credit Bank. 31 (3). 443–57

Dang, T.V., Gorton, G., Holmström, B., Ordoñez, G., 2014. Banks as Secret Keepers. Working Paper. National Bureau of Economic Research.

Friedman, M., 1960. A Program for Monetary Stability. Fordham University Press.

Friedman, M., 1969. The optimum quantity of money. The Optimum Quantity of Money and Other Essays. Aldine Publishing Company.

Friedman, M., Schwartz, A.J., 1986. Has government any role in money? J. Monet. Econ. 17 (1), 37–62.

Greco, T.H., 2001. Money: Understanding and Creating Alternatives to Legal Tender. Chelsea Green Publishing.

Hayek, F., 1999. The denationalization of money: an analysis of the theory and practice of concurrent currencies. In: Kresge, S. (Ed.), The Collected Works of F.A. Hayek, Good Money, Part 2. The University of Chicago Press.

Holmström, B., Tirole, J., 2011. Inside and Outside Liquidity. The MIT Press.

Kareken, J., Wallace, N., 1981. On the indeterminacy of equilibrium exchange rates. Q. J. Econ. 96 (2), 207–222.

Klein, B., 1974. The competitive supply of money. J. Money Credit Bank. 6 (4), 423–453.

Lagos, R., Wright, R., 2003. Dynamics, cycles, and sunspot equilibria in 'genuinely dynamic, fundamentally disaggregative' models of money. J. Econ. Theory 109 (2), 156–171.

Lagos, R., Wright, R., 2005. A unified framework for monetary theory and policy analysis. J. Polit. Econ. 113 (3), 463–484.

Martin, A., Schreft, S.L., 2006. Currency competition: a partial vindication of Hayek. J. Monet. Econ. 53 (8), 2085–2111.

Monnet, C., 2006. Private versus public money. Int. Econ. Rev. 47 (3), 951–960.

Obstfeld, M., Rogoff, K., 1983. Speculative hyperinflations in maximizing models: can we rule them out? J. Polit. Econ. 91 (4), 675–687.

Rocheteau, G., 2012. The cost of inflation: a mechanism design approach. J. Econ. Theory 147 (3), 1261–1279.

Selgin, G.A., White, L.H., 1994. How would the invisible hand handle money? J. Econ. Lit. 32 (4), 1718–1749.

Wallace, N., 2001. Whither monetary economics? Int. Econ. Rev. 42 (4), 847–869.

Williamson, S.D., 1999. Private money. J. Money Credit Bank. 31 (3), 469–491.