Federal Reserve Bank of Philadelphia

Working Papers
Research Department

WP 18-07
February 2018
https://doi.org/10.21799/frbp.wp.2018.07

# On the Economics of Digital Currencies

**Jesús Fernández-Villaverde**
University of Pennsylvania, NBER, CEPR
Federal Reserve Bank of Philadelphia Visiting Scholar

**Daniel Sanches**
Federal Reserve Bank of Philadelphia Research Department

Consumer Finance Institute

**ISSN:** 1962-5361

# On the Economics of Digital Currencies[*†]

Jesús Fernández-Villaverde
University of Pennsylvania, NBER, and CEPR

Daniel Sanches
Federal Reserve Bank of Philadelphia

February 2018

**Abstract**

Can a monetary system in which privately issued cryptocurrencies circulate as media of exchange work? Is such a system stable? How should governments react to digital currencies? Can these currencies and government-issued money coexist? Are cryptocurrencies consistent with an efficient allocation? These are some of the important questions that the sudden rise of cryptocurrencies has brought to contemporary policy discussions. To answer these questions, we construct a model of competition among privately issued fiat currencies. We find that a purely private arrangement fails to implement an efficient allocation, even though it can deliver price stability under certain technological conditions. Currency competition creates problems for monetary policy implementation under conventional methods. However, it is possible to design a policy rule that uniquely implements an efficient allocation by driving private currencies out of the market. We also show that unique implementation of an efficient allocation can be achieved without government intervention if productive capital is introduced.

*Keywords*: Currency competition, cryptocurrencies, monetary policy
*JEL classification numbers*: E40, E42, E52

[*]Correspondence: jesusfv@econ.upenn.edu and Daniel.Sanches@phil.frb.org. Fernandez-Villaverde thanks the NSF for financial support.

# 1 Introduction

In 1976, F.A. Hayek published a short pamphlet, "The Denationalization of Money." Worried that the high inflation of the 1970s in Western countries could not be tackled by central banks because of political constraints, Hayek argued that money-issuing should be opened to market forces and that the government monopoly on the provision of means of exchange should be abolished. Hayek envisioned a system of private monies in which the forces of competition would induce banks to provide a stable means of exchange (Hayek, 1976). Despite some attention from a group of market-oriented economists, Hayek's proposal languished for decades, more as a curiosity than as a workable idea.

Technological developments over the last few years have made Hayek's proposal a reality, but as the result of many individual decisions and not as the outcome of a planned policy change (a process that Hayek would have appreciated). Nowadays it is straightforward to create a cryptocurrency, privately issued money. Thanks to fascinating advances in cryptography and computer science, cryptocurrencies are robust to over-issuing, the double-spending problem (i.e., the holder of the currency should not be able to spend the same token twice) and counterfeiting. These cryptocurrencies are different from the notes issued by financial institutions during the times of free banking for three reasons. First, most cryptocurrencies are fully fiduciary, while notes in the free banking era usually represented claims against deposits in gold or other assets. Second, cryptocurrencies are not directly related to credit but are issued by computer networks according to some predetermined criteria (such as a "proof-of-work," i.e., the solution of a complex mathematical problem). Third, cryptocurrencies such as Ethereum can also work as a sophisticated automatic escrow account.

Today, any person with internet access can use a bewildering array of cryptocurrencies as means of exchange. Everyone has heard about Bitcoin, whose market capitalization (the price per unit times the circulating supply), as of July 6, 2017, exceeded \$42 billion, only slightly below the market capitalization of Ford Motor Company. But six other cryptocurrencies (Ethereum, Ripple, Litecoin, Ethereum Classic, NEM, and Dash) have market capitalizations over \$1 billion. While it is true that cryptocurrencies represent only a trivial fraction of all payments in the world economy, it is not inconceivable that such shares may exponentially increase over the next few years and even become widespread in emerging economies with dysfunctional government monies.

This observation opens many positive and normative questions about how currency competition may work that Hayek did not address using modern economic theory (he admitted that his idea was more a springboard for further discussion than a thorough analysis). Among the positive questions: Will currency competition among private monies yield a stable price level? Will we have a "winner-takes-all" situation where one currency dominates the market? Or will we observe a landscape of several currencies each with a significant market share? How important are network effects? Can we have in the long run fully fiduciary private monies or will commodity-backed currencies dominate? Will we have the "right" amount of money in equilibrium? Can private monies and government-issued money coexist? Among the normative questions: How should governments react to private monies? Should governments have an "industrial policy" regarding private cryptocurrencies? Should they favor one cryptocurrency over the others? Or should they follow a policy of "benign neglect"? There are even questions relevant for would-be entrepreneurs: What is the best strategy for issuing currency? What are the competitive advantages that a new cryptocurrency requires to flourish? A formal theory of currency competition is surely needed.

In this paper, we take a first pass at this problem. We build a model of competition among privately issued fiduciary currencies by extending Lagos and Wright's (2005) environment, a workhorse of modern monetary economics. The standard Lagos-Wright model is augmented by including entrepreneurs who can issue their own currencies to maximize profits or by automata following a predetermined algorithm, as in Bitcoin. Otherwise, the model is standard. In our framework, competition is perfect: All private currencies have the same ability to settle payments and each entrepreneur behaves parametrically with respect to prices.

We highlight six of our results. First, we show that, in a perfectly competitive environment, the existence of a monetary equilibrium consistent with price stability crucially 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 exists only if the cost function associated with the production of private money is locally linear around the origin. If the cost function is strictly convex, then there is no equilibrium consistent with price stability. Thus, the argument developed in Hayek (1976) of a system of private monies competing among themselves to provide a stable means of exchange crucially relies on the properties of the available technologies.

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 is intriguing because it shows that the self-fulfilling inflationary episodes highlighted by Obstfeld and Rogoff (1983) and Lagos and Wright (2003) in economies with a government monopoly on the issuance of fiat money and a money-growth rule 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 purely private monetary system does not provide the socially optimum quantity of money. Private money does not solve the trading frictions at the core of the Lagos-Wright model and, more generally, of essential models of money, as those described in Wallace (2001). Furthermore, we show that private money creation can be a socially wasteful activity. In a well-defined sense, the market fails at providing the right amount of money in ways that it does not fail at providing 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 available 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 is strictly convex. As a result, 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. However, this allocation only partially vindicates Hayek's proposal since it does not deliver the first best.

Fifth, when we introduce a government competing with private monies, we show that currency competition creates problems for monetary policy implementation. For instance, if the supply of government money follows a money-growth rule, then it is impossible to implement a stationary 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 a deflationary process when the public is willing to hold private currencies in portfolio. To get around this problem, we study alternative policies that can simultaneously promote stability and efficiency. In particular, we study the properties of a policy rule that pegs the real value of government money. Under this alternative regime, we demonstrate that it is possible to implement an efficient allocation as the unique equilibrium outcome, which requires driving private money out of the economy. In addition, the proposed policy rule is robust to other forms of private monies, such as those issued by automata (i.e., non-profit-maximizing agents).

Our interpretation of these results is that the threat of competition from private entrepreneurs provides market discipline to any government agency involved in currency issuance. 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, it follows that unique implementation necessarily requires the provision of good government money.

Finally, we consider the implementation of an efficient allocation with automaton issuers in an economy with productive capital. This is an interesting institutional arrangement because it does not require the government's taxation power to support an efficient allocation. As we will see, an allocation that is arbitrarily close to an efficient allocation can be the *unique* equilibrium outcome provided that capital is sufficiently productive.

We are not the first to study private money. The literature is large and has approached the topic from many angles. At the risk of being highly selective, we build on the tradition of Cavalcanti, Erosa, Temzelides (1999), Cavalcanti and Wallace (1999), Williamson (1999), Berentsen (2006), and Monnet (2006). See, as well, from a very different methodological perspective, Selgin and White (1994). As previously mentioned, our emphasis is different from that in those 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. Our characterization captures the technical features of most cryptocurrencies, which are purely fiduciary (in fact, since the cryptocurrencies cannot be used to pay taxes in most sovereigns, their existence makes them more resilient than government-issued fiat monies that are usually granted the status of legal tender). 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.

# 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. In particular, 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 are able to produce, but do not want to consume. A seller is able to 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.

In addition to the previously described production technologies, there exists a technology to create tokens, which can take either a physical or an electronic form. 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 techniques) 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. In particular, an entrepreneur of type $i \in \{1, ..., N\}$ has the ability to use the technology to create type-$i$ tokens. Let $c : \mathbb{R}_+ \to \mathbb{R}_+$ denote the cost function associated with the minting of tokens. Assume that $c : \mathbb{R}_+ \to \mathbb{R}_+$ is strictly increasing and weakly convex, with $c(0) = 0$. This technology will permit 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 the utility function

$$U^b \left(x_t^b, q_t\right) = x_t^b + u(q_t).$$

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 the utility function

$$U^s(x_t^s, n_t) = x_t^s - w(n_t).$$

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 $i \in \{1, ..., N\}$. 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 the utility function

$$U^e \left(x_t^i, \Delta_t\right) = x_t^i - c\left(\Delta_t^i\right).$$

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 model of monetary exchange, a medium of exchange is supplied in the form of government-issued fiat money, with the government following a specific monetary policy rule (e.g., a money-growth rule). It is assumed that all agents in the economy can observe the money supply 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.

In this section, we consider the endogenous supply of outside money. In particular, we will study the properties of a monetary system in which profit-maximizing entrepreneurs have the ability to create intrinsically worthless tokens that can circulate as a medium of exchange. The fact that these tokens attain a strictly positive value in equilibrium allows us to safely refer to them as *currencies*, given their universal acceptability in trade. It is important to emphasize that these currencies are not associated with any promise to exchange them for goods or other assets at some future date. Finally, we assume that all agents in the economy can verify the total amount of each type of currency put into circulation.

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 in the currency market. These predictions about individual behavior allow agents to form beliefs regarding the exchange value of currencies, given the observability of individual issuances. In other words, profit maximization in a private money arrangement serves the same purpose as the monetary policy rule in the case of a government monopoly on currency issue. Thus, it is possible to conceive a system in which competing outside monies can attain a positive exchange value.

In the context of cryptocurrencies, we can reinterpret the entrepreneurs as "miners" and the index $i \in \{1, ..., N\}$ 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 (we will revisit later the case where the issuing of cryptocurrencies is pinned down by an automaton). Let $\phi_t^i \in \mathbb{R}_+$ denote the value of a unit of currency $i \in \{1, ..., N\}$ in terms of the CM good, and let $\boldsymbol{\phi}_t = \left(\phi_t^1, ..., \phi_t^N\right) \in \mathbb{R}_+^N$ denote the vector of real prices.

## 3.1 Buyer

We start by describing the portfolio problem of a typical buyer. Let $W^b\left(\mathbf{M}_{t-1}^b, t\right)$ 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 $V^b\left(\mathbf{M}_t^b, t\right)$ denote the value function in the DM. The Bellman equation can be written as

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

subject to the budget constraint

$$\boldsymbol{\phi}_t \cdot \mathbf{M}_t^b + x_t^b = \boldsymbol{\phi}_t \cdot \mathbf{M}_{t-1}^b.$$

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. With simple algebra, the value function $W^b\left(\mathbf{M}_{t-1}^b, t\right)$ can be written as

$$W^b\left(\mathbf{M}_{t-1}^b, t\right) = \boldsymbol{\phi}_t \cdot \mathbf{M}_{t-1}^b + W^b\left(\mathbf{0}, t\right),$$

with the intercept given by

$$W^b\left(\mathbf{0}, t\right) = \max_{\mathbf{M}_t^b \in \mathbb{R}_+^N} \left[-\boldsymbol{\phi}_t \cdot \mathbf{M}_t^b + V^b\left(\mathbf{M}_t^b, t\right)\right].$$

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

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

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

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

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

To determine the terms of trade in the decentralized market, we follow the standard approach in the search-theoretic literature and use the generalized Nash bargaining solution. Let $\theta \in [0,1]$ denote the buyer's bargaining power. Then the terms of trade $(q, \mathbf{d}) \in \mathbb{R}_{+}^{N+1}$ are determined by solving

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

subject to the participation constraints

$$u(q) - \beta \times \boldsymbol{\phi}_{t+1} \cdot \mathbf{d} \geq 0$$

and

$$-w(q) + \beta \times \boldsymbol{\phi}_{t+1} \cdot \mathbf{d} \geq 0,$$

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 given by

$$q\left(\mathbf{M}_t^b, t\right) = \begin{cases} m^{-1}\left(\beta \times \boldsymbol{\phi}_{t+1} \cdot \mathbf{M}_t^b\right) \text{ if } \boldsymbol{\phi}_{t+1} \cdot \mathbf{M}_t^b < \beta^{-1}\left[\theta w(q^*) + (1-\theta) u(q^*)\right] \\ q^* \text{ if } \boldsymbol{\phi}_{t+1} \cdot \mathbf{M}_t^b \geq \beta^{-1}\left[\theta w(q^*) + (1-\theta) u(q^*)\right] \end{cases}$$

and

$$\boldsymbol{\phi}_{t+1} \cdot \mathbf{d}\left(\mathbf{M}_t^b, t\right) = \begin{cases} \boldsymbol{\phi}_{t+1} \cdot \mathbf{M}_t^b \text{ if } \boldsymbol{\phi}_{t+1} \cdot \mathbf{M}_t^b < \beta^{-1}\left[\theta w(q^*) + (1-\theta) u(q^*)\right] \\ \beta^{-1}\left[\theta w(q^*) + (1-\theta) u(q^*)\right] \text{ if } \boldsymbol{\phi}_{t+1} \cdot \mathbf{M}_t^b \geq \beta^{-1}\left[\theta w(q^*) + (1-\theta) u(q^*)\right]. \end{cases}$$

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

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

One particular case of interest is when the buyer has all the bargaining power (i.e., when we take the limit $\theta \rightarrow 1$). In this case, the solution to the bargaining problem is given by

$$q\left(\mathbf{M}_t^b, t\right) = \begin{cases} w^{-1}\left(\beta \times \boldsymbol{\phi}_{t+1} \cdot \mathbf{M}_t^b\right) \text{ if } \boldsymbol{\phi}_{t+1} \cdot \mathbf{M}_t^b < \beta^{-1} w(q^*) \\ q^* \text{ if } \boldsymbol{\phi}_{t+1} \cdot \mathbf{M}_t^b \geq \beta^{-1} w(q^*) \end{cases}$$

and

$$\boldsymbol{\phi}_{t+1} \cdot \mathbf{d}\left(\mathbf{M}_t^b, t\right) = \begin{cases} \boldsymbol{\phi}_{t+1} \cdot \mathbf{M}_t^b \text{ if } \boldsymbol{\phi}_{t+1} \cdot \mathbf{M}_t^b < \beta^{-1} w\left(q^*\right) \\ \beta^{-1} w\left(q^*\right) \text{ if } \boldsymbol{\phi}_{t+1} \cdot \mathbf{M}_t^b \geq \beta^{-1} w\left(q^*\right). \end{cases}$$

Given the trading protocol, the solution to the bargaining problem allows us to characterize real expenditures in the DM, given by $\boldsymbol{\phi}_{t+1} \cdot \mathbf{d}\left(\mathbf{M}_t^b, t\right)$, 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 fiduciary currencies, given the absence of transaction costs when dealing with different currencies.

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

$$V^b\left(\mathbf{M}_t^b, t\right) = \sigma\left[u\left(m^{-1}\left(\beta \times \boldsymbol{\phi}_{t+1} \cdot \mathbf{M}_t^b\right)\right) - \beta \times \boldsymbol{\phi}_{t+1} \cdot \mathbf{M}_t^b\right] + \beta \times \boldsymbol{\phi}_{t+1} \cdot \mathbf{M}_t^b + \beta W^b\left(\mathbf{0}, t+1\right)$$

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

$$V^b\left(\mathbf{M}_t^b, t\right) = \sigma\left[u\left(q^*\right) - w\left(q^*\right)\right] + \beta \times \boldsymbol{\phi}_{t+1} \cdot \mathbf{M}_t^b + \beta W^b\left(\mathbf{0}, t+1\right)$$

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

The optimal portfolio problem can be defined as

$$\max_{\mathbf{M}_t^b \in \mathbb{R}_+^N} \left\{-\boldsymbol{\phi}_t \cdot \mathbf{M}_t^b + \sigma\left[u\left(q\left(\mathbf{M}_t^b, t\right)\right) - \beta \times \boldsymbol{\phi}_{t+1} \cdot \mathbf{d}\left(\mathbf{M}_t^b, t\right)\right] + \beta \times \boldsymbol{\phi}_{t+1} \cdot \mathbf{M}_t^b\right\}.$$

The optimal choice, then, satisfies

$$\phi_t^i = \beta \phi_{t+1}^i L_\theta\left(\boldsymbol{\phi}_{t+1} \cdot \mathbf{M}_t^b\right) \tag{1}$$

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

$$\lim_{t \to \infty} \beta^t \times \boldsymbol{\phi}_t \cdot \mathbf{M}_t^b = 0, \tag{2}$$

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

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

In the special case of take-it-or-leave-it offers by the buyer, we have

$$L_1(A) = \begin{cases} \sigma \frac{u'\left(w^{-1}(\beta A)\right)}{w'(w^{-1}(\beta A))} + 1 - \sigma \text{ if } A < \beta^{-1} w(q^*) \\ 1 \text{ if } A \geq \beta^{-1} w(q^*). \end{cases}$$

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

$$W^s\left(\mathbf{M}^s_{t-1}, t\right) = \max_{(x^s_t, \mathbf{M}^s_t) \in \mathbb{R} \times \mathbb{R}^N_+} \left[x^s_t + V^s\left(\mathbf{M}^s_t, t\right)\right]$$

subject to the budget constraint

$$\boldsymbol{\phi}_t \cdot \mathbf{M}^s_t + x^s_t = \boldsymbol{\phi}_t \cdot \mathbf{M}^s_{t-1}.$$

The value $V^s\left(\mathbf{M}^s_t, t\right)$ satisfies

$$V^s\left(\mathbf{M}^s_t, t\right) = \sigma\left[-w\left(q\left(\mathbf{M}^b_t, t\right)\right) + \beta W^s\left(\mathbf{M}^s_t + \mathbf{d}\left(\mathbf{M}^b_t, t\right), t+1\right)\right] + (1-\sigma)\beta W^s\left(\mathbf{M}^s_t, t+1\right).$$

Here the vector $\mathbf{M}^b_t \in \mathbb{R}^N_+$ denotes the portfolio of the buyer with whom the seller is matched in the DM. In the Lagos-Wright framework, the terms of trade in the decentralized market only depend on the real value of the buyer's portfolio, which implies that monetary 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 $\phi^i_{t+1}/\phi^i_t \leq \beta^{-1}$ holds for all $i \in \{1, ..., N\}$.

## 3.3 Entrepreneur

Now we describe the entrepreneur's problem to determine the money supply in the economy. We use $M_t^i \in \mathbb{R}_+$ to denote the per capita supply of currency $i$ in period $t$.[1] Let $\Delta_t^i \in \mathbb{R}$ denote the 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 $\Delta_t^i \geq 0$. Therefore, the entrepreneur's budget constraint can be written as

$$x_t^i + \sum\nolimits_{j \neq i} \phi_t^j M_t^{ij} = \phi_t^i \Delta_t^i + \sum\nolimits_{j \neq i} \phi_t^j M_{t-1}^{ij}$$

at each date $t \geq 0$. Here $M_t^{ij} \in \mathbb{R}_+$ denotes entrepreneur $i$'s holdings of type-$j$ currency, with $j \neq i$.

If $\phi_{t+1}^j / \phi_t^j \leq \beta^{-1}$ holds for all $j \in \{1, ..., N\}$, 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 just tells us that the entrepreneur's consumption in period $t$ is equal to the real value of the net circulation. Because $x_t^i \geq 0$, we must have, as previously mentioned, $\Delta_t^i \geq 0$. Given that an entrepreneur takes prices $\{\boldsymbol{\phi}_t\}_{t=0}^{\infty}$ as given, $\Delta_t^{*,i} \in \mathbb{R}_+$ solves the profit-maximization problem:

$$\Delta_t^{*,i} \in \arg\max_{\Delta \in \mathbb{R}_+} \left[ \phi_t^i \Delta - c(\Delta) \right]. \tag{3}$$

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

The solution to the entrepreneur's profit-maximization problem implies the law of motion

$$M_t^i = \Delta_t^{*,i} + M_{t-1}^i \tag{4}$$

at all dates $t \geq 0$.

[1] When we say *per capita* we really mean *per buyer*.

## 3.4 Equilibrium

The final step to construct an equilibrium is to impose the market-clearing condition

$$\mathbf{M}_t = \mathbf{M}_t^b + \mathbf{M}_t^s$$

at all dates. As we have seen, $\mathbf{M}_t^s = \mathbf{0}$ so that the market-clearing condition reduces to

$$\mathbf{M}_t = \mathbf{M}_t^b. \tag{5}$$

We can now provide a formal definition of equilibrium under a purely private monetary arrangement.

**Definition 1** *A perfect-foresight monetary equilibrium is an array* $\left\{\mathbf{M}_t, \mathbf{M}_t^b, \boldsymbol{\Delta}_t^*, \boldsymbol{\phi}_t\right\}_{t=0}^{\infty}$ *satisfying (1)-(5) for each* $i \in \{1, ..., N\}$ *at all dates* $t \geq 0$.

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 equilibrium allocations to investigate whether an efficient allocation can be the outcome of competition in the currency-issuing business. In what follows, it is helpful to provide a broad definition of price stability to evaluate the positive properties of private currencies.

**Definition 2** *We say that 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* $i \in \{1, ..., N\}$.

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

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

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 $\lim_{q \to 0} u'(q)/m'(q) = \infty$.

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 type-$i$ entrepreneurs when the cost function is strictly convex. The following result shows an important implication of this relation.

**Lemma 4** *Suppose that $c : \mathbb{R}_+ \to \mathbb{R}_+$ is strictly convex with $c'(0) = 0$. Then,*

$$\lim_{t\to\infty} \Delta_t^{*,i} = 0$$

*if and only if $\lim_{t\to\infty} \phi_t^i = 0$.*

**Proof.** ($\Leftarrow$) Suppose that $\lim_{t\to\infty} \phi_t^i = 0$. Because $c : \mathbb{R}_+ \to \mathbb{R}_+$ is strictly convex, the entrepreneur's profit-maximization problem has an interior solution characterized by the first-order condition

$$\phi_t^i = c'\left(\Delta_t^{*,i}\right)$$

when $\phi_t^i > 0$. Because $c'(0) = 0$, it follows that $\Delta_t^{*,i}$ converges to zero as $\phi_t^i$ approaches zero from above.

($\Rightarrow$) Suppose that $\lim_{t\to\infty} \Delta_t^{*,i} = 0$. Then we must have $\lim_{t\to\infty} \phi_t^i = 0$ to satisfy condition (3) at all dates. To verify this claim, suppose that $\lim_{t\to\infty} \phi_t^i = \bar{\phi} > 0$. Consider the neighborhood $\left(\bar{\phi} - \varepsilon, \bar{\phi} + \varepsilon\right)$ with $\varepsilon = \bar{\phi}/4$. There is a finite date $T$ such that $\phi_t^i \in \left(\bar{\phi} - \varepsilon, \bar{\phi} + \varepsilon\right)$ for all $t \geq T$. Because $\lim_{t\to\infty} \Delta_t^{*,i} = 0$, it follows that $\lim_{t\to\infty} c'\left(\Delta_t^{*,i}\right) = 0$, given that $c'(0) = 0$. Then there is a finite date $T'$ such that $c'\left(\Delta_t^{*,i}\right) \in (-\varepsilon, \varepsilon)$ for all $t \geq T'$. Finally, there is $T'' < \infty$ sufficiently large such that $\phi_t^i \in \left(\bar{\phi} - \varepsilon, \bar{\phi} + \varepsilon\right)$ and $c'\left(\Delta_t^{*,i}\right) \in (-\varepsilon, \varepsilon)$ for all $t \geq T''$. Because $(-\varepsilon, \varepsilon) \cup \left(\bar{\phi} - \varepsilon, \bar{\phi} + \varepsilon\right) = \emptyset$ when $\varepsilon = \bar{\phi}/4$, it follows that (3) does not hold at all dates. ■

We can now establish a central result of our positive analysis. The following proposition shows that price stability is inconsistent with a competitive supply of fiduciary currencies when the cost function is strictly convex.

**Proposition 1** *Suppose that $c : \mathbb{R}_+ \to \mathbb{R}_+$ is strictly convex. Then there is no monetary equilibrium consistent with price stability.*

**Proof.** Suppose, by way of contradiction, that $\lim_{t\to\infty} \phi_t^i = \bar{\phi}^i > 0$ for some currency $i$. Because $c : \mathbb{R}_+ \to \mathbb{R}_+$ is strictly convex, the entrepreneur's profit-maximization problem has an interior solution characterized by the first-order condition

$$\phi_t^i = c'\left(\Delta_t^{*,i}\right)$$

when $\phi_t^i > 0$. This solution implies the law of motion $M_t^i = (c')^{-1}\left(\phi_t^i\right) + M_{t-1}^i$.

Because $\lim_{t\to\infty} \phi_t^i = \bar{\phi}^i > 0$, there is a date $\hat{T} > 0$ such that $\phi_t^i > 0$ for all $t \geq \hat{T}$. As a result, the sequence $\{M_t^i\}_{t=0}^{\infty}$ is unbounded. Thus, there is a date $T > 0$ such that $\boldsymbol{\phi}_{t+1} \cdot \mathbf{M}_t > \beta^{-1}\left[\theta w(q^*) + (1-\theta)\, u(q^*)\right]$ for all $t \geq T$. To be consistent with an optimal portfolio choice, we must have $\phi_t^i = \beta \phi_{t+1}^i$ for all $t > T$. But this implies a violation of the transversality condition (2), given that $\{M_t^i\}_{t=0}^{\infty}$ is unbounded. ■

The previous proposition highlights that the main problem of a monetary system with competitive issuers is that the supply of each brand becomes unbounded when the cost function is strictly convex: Private entrepreneurs have an incentive to issue additional amounts of currencies when their value is strictly positive. As a result, 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 (1959) arrived at the same conclusion when arguing that a purely private system of fiduciary currencies would necessarily lead to instability in the price level. Thus, our formal analysis of currency competition confirms Friedman's conjecture.

This prediction of the model is in sharp contrast to the conclusions reached in Hayek (1976). Hayek argued that private agents through markets can achieve desirable outcomes, even in the field of money and banking. According to his view, government intervention is not necessary for the establishment of a monetary system consistent with price stability. The previous proposition formally shows that Hayek's conjecture does not hold in an environment with a strictly convex cost function.

Our next step is to verify whether other cost functions can be consistent with price stability. Precisely, we want to characterize *sufficient* conditions for price stability. We now establish that currency competition can deliver price stability when the cost function is weakly convex. In particular, the following result shows that Hayek's conjecture holds when the cost function is locally linear around the origin.

**Proposition 2** *Suppose that $c : \mathbb{R}_+ \to \mathbb{R}_+$ is locally linear in a neighborhood $[0, \Delta'] \subset \mathbb{R}_+$. Then there is a monetary equilibrium consistent with strong price stability provided the neighborhood $[0, \Delta']$ is sufficiently large.*

**Proof.** Because $c : \mathbb{R}_+ \to \mathbb{R}_+$ is locally linear with $c(0) = 0$, there is $k > 0$ such that $c(\Delta) = k\Delta$ for all $\Delta \in [0, \Delta']$, given some positive constant $\Delta' \in (0, \infty)$. Set $\phi_t^i = k$ at all dates $t \geq 0$. Consider a positive constant $\bar{\Delta}^i \leq \Delta'$ so that we can construct the candidate sequence $\left\{\Delta_t^{*,i}\right\}_{t=0}^{\infty}$ with $\Delta_0^{*,i} = \bar{\Delta}^i$ and $\Delta_t^{*,i} = 0$ for all $t \geq 1$. Given the real price $\phi_t^i = k$, the previously described sequence is consistent with profit maximization provided $\bar{\Delta}^i \leq \Delta'$. Then, we must have $M_t^i = \bar{\Delta}^i$ at each date $t \geq 0$.

Finally, it is possible to select a vector $\bar{\mathbf{\Delta}} = \left(\bar{\Delta}^1, ..., \bar{\Delta}^N\right)$ satisfying

$$\beta k \sum_{i=1}^{N} \bar{\Delta}^i = m\left(\hat{q}\right),$$

with the quantity $\hat{q}$ given by

$$1 = \beta \left[\sigma \frac{u'\left(\hat{q}\right)}{m'\left(\hat{q}\right)} + 1 - \sigma\right],$$

provided the neighborhood $[0, \Delta'] \subset \mathbb{R}_+$ is not too small. ■

The previous result shows how we can construct a monetary equilibrium consistent with our strong definition of price stability when the cost function is locally linear around the origin. In this equilibrium, agents do not expect monetary conditions to vary over time so that the real value of private currencies, as well as their expected return, remains constant. The previous result, therefore, provides a partial vindication of Hayek (1976). A purely private arrangement can deliver price stability for a strict subset of production technologies.

Our next result shows that, for the same subset of production technologies, other allocations with undesirable properties can also be consistent with the equilibrium conditions. These equilibria are 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 inflationary 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 $i \in \{1, ..., N\}$, the sequence $\left\{\phi_t^i\right\}_{t=0}^{\infty}$ converges monotonically to zero.*

**Proof.** Because $c : \mathbb{R}_+ \to \mathbb{R}_+$ is locally linear in a neighborhood $\left[0, \bar{\Delta}\right] \subset \mathbb{R}_+$, there is $k > 0$ such that $c\left(\Delta\right) = k\Delta$ for all $\Delta \in \left[0, \bar{\Delta}\right]$. Set $\phi_0^i = k$. Then, any value $\Delta^i \in \left[0, \bar{\Delta}\right]$ is consistent with profit maximization at date 0. The optimal portfolio choice implies $\phi_{t+1}^i = \gamma_{t+1}\phi_t^i$ at all dates $t \geq 0$, with $\gamma_{t+1} \in \mathbb{R}_+$ representing the common return across all valued currencies between dates $t$ and $t+1$. Given that $\phi_0^i = k$, we must have $\phi_t^i \leq k$ when $\gamma_t \leq 1$. As a result, the path $M_{t+1}^i = M_t^i = \Delta^i$ is consistent with profit maximization if $\gamma_{t+1} \leq 1$ at all dates $t \geq 0$.

Define $b_t^i \equiv \phi_t^i M_t^i$. Then, we have

$$1 = \beta\gamma_{t+1} L_\theta \left(\gamma_{t+1} \sum\nolimits_{i=1}^{N} b_t^i\right)$$

Because $\beta\gamma_{t+1}\sum_{i=1}^{N} b_t^i < \theta w(q^*) + (1-\theta)\, u(q^*)$, we can write

$$\sum\nolimits_{i=1}^{N} b_t^i = \frac{1}{\gamma_{t+1}} L_\theta^{-1}\left(\frac{1}{\beta\gamma_{t+1}}\right) \equiv z_\theta\left(\gamma_{t+1}\right).$$

Note that having $M_t^i = M_{t-1}^i = \Delta^i$ for each $i$ implies

$$z_\theta\left(\gamma_{t+1}\right) = \gamma_t z_\theta\left(\gamma_t\right) \tag{6}$$

provided that $\gamma_t \leq 1$. Since 0 is a fixed point of the implicitly defined mapping (6), it is possible to select a sufficiently small initial value $\gamma_1 < 1$ such that the price sequence $\left\{\phi_t^i\right\}_{t=0}^{\infty}$ satisfying $\phi_{t+1}^i = \gamma_{t+1}\phi_t^i$ converges monotonically to zero. ■

For any initial condition within a neighborhood of zero, there exists an associated equilibrium trajectory that is monotonically decreasing. Along this equilibrium path, 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 agent's optimization problem when the value of privately issued currencies persistently depreciates over time (i.e., the anticipated decline in the purchasing power of private money leads agents to reduce their real balances over time). As a result, trading activity in the decentralized market monotonically declines along the equilibrium trajectory. This property of equilibrium allocations with competitively issued currencies implies that 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 implies 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 and follows a money-growth rule. Lagos and Wright (2003) show that search-theoretic monetary models with fiat currency can also have self-fulfilling inflationary episodes under a money-growth rule. Our analysis of privately issued currencies shows that self-fulfilling inflationary equilibria can occur in the absence of government currency when private agents enter the currency-issuing business to maximize profits. Thus, replacing government monopoly under a money-growth rule with profit maximization does not overcome the fundamental fragility associated with fiduciary regimes, public or private.

To conclude this section, we want to show the existence of an asymmetric equilibrium with the property that a unique 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* $t \geq 0$*.*

**Proof.** The market-clearing condition implies

$$\sum_{i=1}^{N} b_t^i = z_\theta \left(\gamma_{t+1}\right),$$

with $\gamma_{t+1} \in \mathbb{R}_+$ representing the common return across all valued currencies between dates $t$ and $t+1$. Note that $b_t^j = 0$ implies either $\phi_t^j = 0$ or $M_t^j = 0$, or both. If we set $b_t^i = 0$ for all $i \geq 2$, then the market-clearing condition implies $b_t^1 = z_\theta \left(\gamma_{t+1}\right)$. Following the same steps as in the proof of the previous proposition, it is possible to show that there exists an equilibrium with $b_t^1 = z_\theta (1) > 0$ 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. In other words, 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 Properties

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. In our framework, 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.[2]

In this case, any solution to the social planner's problem is characterized by the surplus-maximizing quantity $q^*$ in the DM. Following the same steps as in Rocheteau (2012), it can be demonstrated 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 in an environment

[2] Alternatively, one can think of the social planner as minting a trivially small amount of currency at an epsilon cost: without money indivisibility, this is all that we need to achieve the role of money as memory.

with perfect record-keeping and full commitment) by systematically removing tokens from circulation.

In our equilibrium analysis, we used the generalized Nash bargaining solution to determine the terms of trade in the DM. Aruoba, Rocheteau, and Waller (2007) considered alternative axiomatic bargaining solutions and concluded that the properties of these solutions matter for the efficiency of monetary equilibrium. To avoid inefficiencies arising from the choice of the bargaining protocol, which may complicate the interpretation of the main results in the paper, we assume, in what follows, that the buyer makes a take-it-or-leave-it offer to the seller.[3]

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

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

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, it makes sense to restrict attention to 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 (i.e., increasing in the real return on money). In particular, it is helpful to make the following additional assumption.

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

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

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

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 important implication of the characterization of efficient allocations is that the persistent creation of tokens along the equilibrium path is a socially wasteful activity. Given an initial supply of tokens, the planner can implement an efficient allocation by systematically

[3] Lagos and Wright (2005) show that, with take-it-or-leave-it offers by the buyer, it is possible to achieve the socially efficient allocation provided the government implements the Friedman rule.

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 necessarily inefficient. Recall that entrepreneurs have an incentive to mint additional units of tokens when these objects are positively valued in equilibrium. From a social perspective, the planner wants to avoid the excessive creation of tokens so that there is scope for public policies that aim at preventing overissue. We will return to this issue later in the paper.

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 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.*

**Proof.** Note that the law of motion for currency $i \in \{1, ..., N\}$ implies

$$\phi_t^i M_t^i = \phi_t^i \Delta_t^{*,i} + \gamma_t \phi_{t-1}^i M_{t-1}^i,$$

where $\gamma_t \in \mathbb{R}_+$ represents the common real return across all valued currencies. Then, we can derive the following relation

$$\sum\nolimits_{i=1}^{N} \phi_t^i M_t^i = \sum\nolimits_{i=1}^{N} \phi_t^i \Delta_t^{*,i} + \gamma_t \sum\nolimits_{i=1}^{N} \phi_{t-1}^i M_{t-1}^i$$

at each date $t$. The market-clearing condition implies

$$\sum\nolimits_{i=1}^{N} \phi_t^i M_t^i = z\left(\gamma_{t+1}\right)$$

at all dates, where the function $z : \mathbb{R}_+ \to \mathbb{R}_+$ is given by

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

Given the previously derived equilibrium relations, we get the following condition:

$$z\left(\gamma_{t+1}\right) - \gamma_t z\left(\gamma_t\right) = \sum\nolimits_{i=1}^{N} \phi_t^i \Delta_t^{*,i}. \tag{7}$$

It is straightforward to show that the market-clearing condition is necessarily violated when (7) is violated and vice versa.

Suppose that there is a date $T \geq 0$ such that $\gamma_t > 1$ for all $t \geq T$. Because the right-hand side of (7) is nonnegative, we must have $\gamma_{t+1} > \gamma_t > 1$ for all $t \geq T$. In addition, there exists a lower bound $\bar{\gamma} > 1$ such that $\gamma_t \geq \bar{\gamma}$ for all $t \geq T$.

We claim that the sequence $\{\phi_t^i\}_{t=0}^{\infty}$ defined by $\phi_{t+1}^i = \gamma_{t+1}\phi_t^i$ is unbounded. To verify this claim, suppose that there is a finite scalar $\bar{B} > 0$ such that $\phi_t^i \leq \bar{B}$ for all $t \geq 0$. Because $\{\phi_t^i\}_{t=0}^{\infty}$ is strictly increasing and bounded, it must converge to a finite limit. Then, we must have

$$\lim_{t\to\infty} \frac{\phi_{t+1}^i}{\phi_t^i} = 1.$$

As a result, there is a date $\tilde{T} > 0$ such that $1 < \frac{\phi_{t+1}^i}{\phi_t^i} < \bar{\gamma}$ for all $t \geq \tilde{T}$. Because $\frac{\phi_{t+1}^i}{\phi_t^i} = \gamma_{t+1}$ is an equilibrium relation, we obtain a contradiction. Hence, we can conclude that the price sequence $\{\phi_t^i\}_{t=0}^{\infty}$ is unbounded.

Suppose the cost function $c : \mathbb{R}_+ \to \mathbb{R}_+$ is strictly convex. Then, we have an interior solution $\Delta_t^{*,i} > 0$ when $\phi_t^i > 0$. Define the value

$$\Gamma \equiv \max_{\gamma \in \mathbb{R}_+} z(\gamma),$$

where the maximization is subject to $\beta\gamma z(\gamma) \leq w(q^*)$.

Because $\gamma_{t+1} > \gamma_t > 1$ for all $t \geq T$, there is a finite date $\hat{T}$ such that

$$\Gamma < \sum\nolimits_{i=1}^{N} \phi_{\hat{T}}^i \Delta_{\hat{T}}^{*,i},$$

given that $\{\phi_t^i\}_{t=0}^{\infty}$ is strictly increasing and unbounded. But this implies that condition (7) is violated. As a result, we cannot have an equilibrium with the property that $\gamma_t > 1$ at all dates.

Suppose now that $c : \mathbb{R}_+ \to \mathbb{R}_+$ is locally linear around the origin. Given that $\{\phi_t^i\}_{t=0}^{\infty}$ is strictly increasing and unbounded, there exists a finite date $T'$ such that $\Delta_t^{*,i} > 0$ for all $t \geq T'$. Then, condition (7) is necessarily violated at a finite date.

Finally, assume that $c : \mathbb{R}_+ \to \mathbb{R}_+$ is linear. Because $c(0) = 0$, there is $k > 0$ such that $c(\Delta) = k\Delta$ for all $\Delta \geq 0$. Because $\gamma_{t+1} > \gamma_t > 1$ for all $t \geq T$, there is a finite date $T''$ such that $\phi_{T''}^i > k$. At that date, the entrepreneur's problem has no solution. ■

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). This result is central to our paper: Despite having entrepreneurs who 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. These pecuniary externalities mean that, 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.[4]

# 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 an upper bound on the supply of each brand. Motivated by this observation, 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 $i \in \{1, ..., N\}$. In this case, the entrepreneur's profit maximization problem can be described as

$$\Delta_t^{*,i} \in \arg \max_{0 \leq \Delta \leq \bar{\Delta}_t^i} \left[\phi_t^i \Delta - c\left(\Delta\right)\right]. \tag{8}$$

Then, we can define a monetary equilibrium in the same way as before by replacing (3) with (8).

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 is strictly convex.

**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 is shown to exist. These caps are such that $\bar{\Delta}_t^i > 0$ at dates $0 \leq t \leq T$ and $\bar{\Delta}_t^i = 0$ at all subsequent dates $t \geq T+1$, given a finite date $T > 0$.*

**Proof.** Consider a set of caps with the property that $\bar{\Delta}_t^i > 0$ at dates $0 \leq t \leq T$ and $\bar{\Delta}_t^i = 0$ at all subsequent dates $t \geq T+1$, given a finite date $T > 0$. For each $i$, set $\phi_t^i = \bar{\phi}$ at all dates $t \geq T+1$, with the constant $\bar{\phi} > 0$ satisfying

$$1 = \beta L_1 \left(\bar{\phi} \sum\nolimits_{i=1}^{N} \sum\nolimits_{\tau=0}^{T} \bar{\Delta}_\tau^i\right). \tag{9}$$

[4]If 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."

For any date $t \leq T$, the values $\{\phi_0, ..., \phi_T\}$ satisfy

$$\phi_t = \beta\phi_{t+1}L_1\left(\phi_{t+1}\sum\nolimits_{i=1}^{N} M_t^i\right), \tag{10}$$

where $M_0^i = \bar{\Delta}_0^i$ and $M_t^i = \bar{\Delta}_t^i + M_{t-1}^i$ at any date $1 \leq t \leq T$. We can rewrite (10) as

$$\phi_t = \beta\phi_{t+1}L_1\left(\phi_{t+1}\sum\nolimits_{i=1}^{N}\sum\nolimits_{\tau=0}^{t}\bar{\Delta}_\tau^i\right).$$

As a result, the partial sequence $\{\phi_0, ..., \phi_T\}$ can be constructed from (10), given the exogenous caps $\bar{\boldsymbol{\Delta}} = \left\{\bar{\Delta}_0^i, \bar{\Delta}_1^i, ..., \bar{\Delta}_T^i\right\}_{i=1}^N$.

The final step in the proof is to select each cap $\bar{\Delta}_t^i$ in such a way that it is consistent with profit maximization at the price $\phi_t$. Note that (9) implies $\partial\bar{\phi}/\partial\bar{\Delta}_t^i < 0$. Because $\phi_T = \bar{\phi}$, we have $\partial\phi_T/\partial\bar{\Delta}_t^i < 0$. At date $T-1$, we have

$$\phi_{T-1} = \beta\bar{\phi}L_1\left(\bar{\phi}\sum\nolimits_{i=1}^{N}\sum\nolimits_{\tau=0}^{T-1}\bar{\Delta}_\tau^i\right).$$

Because $\bar{\phi}\sum_{i=1}^{N}\sum_{\tau=0}^{T-1}\bar{\Delta}_\tau^i < \bar{\phi}\sum_{i=1}^{N}\sum_{\tau=0}^{T}\bar{\Delta}_\tau^i < \beta^{-1}w(q^*)$, the implicitly defined function $\phi_{T-1} = \phi_{T-1}\left(\bar{\boldsymbol{\Delta}}\right)$ is continuously differentiable in a sufficiently small neighborhood. In particular, we have

$$\begin{aligned}\frac{\partial\phi_{T-1}}{\partial\bar{\Delta}_t^i} &= \beta\frac{\partial\bar{\phi}}{\partial\bar{\Delta}_t^i}\left[L_1\left(\bar{\phi}\sum\nolimits_{i=1}^{N}\sum\nolimits_{\tau=0}^{T-1}\bar{\Delta}_\tau^i\right) + \left(\bar{\phi}\sum\nolimits_{i=1}^{N}\sum\nolimits_{\tau=0}^{T-1}\bar{\Delta}_\tau^i\right)L_1'\left(\bar{\phi}\sum\nolimits_{i=1}^{N}\sum\nolimits_{\tau=0}^{T-1}\bar{\Delta}_\tau^i\right)\right] \\ &\quad +\beta\bar{\phi}^2L_1'\left(\bar{\phi}\sum\nolimits_{i=1}^{N}\sum\nolimits_{\tau=0}^{T-1}\bar{\Delta}_\tau^i\right)\end{aligned}$$

for any $0 \leq t \leq T-1$ and

$$\frac{\partial\phi_{T-1}}{\partial\bar{\Delta}_T^i} = \beta\frac{\partial\bar{\phi}}{\partial\bar{\Delta}_T^i}\left[L_1\left(\bar{\phi}\sum\nolimits_{i=1}^{N}\sum\nolimits_{\tau=0}^{T-1}\bar{\Delta}_\tau^i\right) + \left(\bar{\phi}\sum\nolimits_{i=1}^{N}\sum\nolimits_{\tau=0}^{T-1}\bar{\Delta}_\tau^i\right)L_1'\left(\bar{\phi}\sum\nolimits_{i=1}^{N}\sum\nolimits_{\tau=0}^{T-1}\bar{\Delta}_\tau^i\right)\right].$$

Because $L_1(A) + AL_1'(A) > 0$ for all $A > 0$, we conclude that $\partial\phi_{T-1}/\partial\bar{\Delta}_t^i < 0$ for any $0 \leq t \leq T$. Following the same steps, one can show that every element in the sequence $\{\phi_0, ..., \phi_T\}$ satisfying (10) is strictly decreasing in $\bar{\Delta}_t^i$ for any $0 \leq t \leq T$. Then, it is possible to select a sufficiently low value for the caps $\left\{\bar{\Delta}_0^i, \bar{\Delta}_1^i, ..., \bar{\Delta}_T^i\right\}_{i=1}^N$ such that the constraint $\Delta \leq \bar{\Delta}_t^i$ in the optimization problem on the right-hand side of (8) is binding. In this case, we have $\Delta_t^{*,i} = \bar{\Delta}_t^i$ at all dates. ■

In the previously described allocation, the value of money and trading activity stabilize after date $T$. Thus, it is possible to have price stability with a strictly convex cost function 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.[5]

Although the existence of an upper bound on currency issuance can promote price stability in a competitive environment, it does not imply efficiency. The previously made arguments regarding the reasons for not achieving efficiency through a market arrangement continue to hold even if innovations in the field of computer science permit the implementation of exogenous bounds on the supply of cryptocurrencies. In view of the inefficiency of a private system, we turn to the study of the role of monetary policy in a competitive environment.

# 5 Monetary Policy

In this section, we study the role of monetary policy in the presence of privately issued currencies. As we have seen, a central result of our previous analysis is that there is no efficient equilibrium under a purely private arrangement. The competition process does not provide the incentives to deliver the socially optimal return on money and results in socially wasteful money creation. In what follows, we want to investigate whether it is possible to implement the socially optimal return on money by introducing government money and monetary policy. If so, we move on to provide sufficient conditions for efficiency.

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

$$\phi_t^{N+1}\Delta_t^{N+1} + \tau_t = c\left(\Delta_t^{N+1}\right), \tag{11}$$

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. Government money follows the law of motion

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

at all dates, given an initial condition $M_{-1}^{N+1} \in \mathbb{R}_+$.

[5] Our result resembles the existence result in Martin and Schreft (2006). These authors build an equilibrium in which 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 issuances will be worthless. That threshold works in similar ways as the bound of issuance in cryptocurrencies.

The definition of 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 determined by government policy. A formal definition is now provided.

**Definition 5** *A perfect-foresight monetary equilibrium is an array* $\left\{\mathbf{M}_t, \mathbf{M}_t^b, \boldsymbol{\phi}_t, \boldsymbol{\Delta}_t^*, \Delta_t^{N+1}, \tau_t\right\}_{t=0}^{\infty}$ *satisfying (1)-(5) and (11) for each* $i \in \{1, ..., N\}$ *at all dates* $t \geq 0$*.*

In any equilibrium with valued government money, we must have

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

at all dates $t \geq 0$. In the absence of portfolio restrictions, government money must yield the same rate of return as other monies 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 move on to 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.

**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.*

**Proof.** The law of motion for the supply of each currency $i \in \{1, ..., N\}$ implies the following relation

$$\sum\nolimits_{i=1}^{N} \phi_t^i M_t^i = \sum\nolimits_{i=1}^{N} \phi_t^i \Delta_t^{*,i} + \gamma_t \sum\nolimits_{i=1}^{N} \phi_{t-1}^i M_{t-1}^i,$$

where $\gamma_t \in \mathbb{R}_+$ represents the common real return across all valued currencies. The market-clearing condition implies

$$\phi_t^{N+1} M_t^{N+1} + \sum\nolimits_{i=1}^{N} \phi_t^i M_t^i = z\left(\gamma_{t+1}\right)$$

at all dates. Thus, we can derive the equilibrium relation

$$z\left(\gamma_{t+1}\right) - \gamma_t z\left(\gamma_t\right) = \sum\nolimits_{i=1}^{N} \phi_t^i \Delta_t^{*,i} + \phi_t^{N+1} \Delta_t^{N+1}. \tag{12}$$

Consider a money-growth rule with $\omega \geq 0$. Then, we have $\Delta_t^{N+1} \geq 0$ at all dates. Suppose that there is a date $T \geq 0$ such that $\gamma_t > 1$ for all $t \geq T$. Because the right-hand side of (12) is nonnegative, we have $\gamma_{t+1} > \gamma_t > 1$ for all $t \geq T$. In addition, there exists a lower bound $\bar{\gamma} > 1$ such that $\gamma_t \geq \bar{\gamma}$ for all $t \geq T$.

Suppose the cost function $c : \mathbb{R}_+ \to \mathbb{R}_+$ is strictly convex. Then, we have an interior solution $\Delta_t^{*,i} > 0$ when $\phi_t^i > 0$. Define the value

$$\Gamma \equiv \max_{\gamma \in \mathbb{R}_+} z\left(\gamma\right),$$

where the maximization is subject to $\beta \gamma z\left(\gamma\right) \leq w\left(q^*\right)$.

As previously shown, the sequence $\left\{\phi_t^i\right\}_{t=0}^{\infty}$ defined by $\phi_{t+1}^i = \gamma_{t+1} \phi_t^i$ is unbounded, given that $\gamma_{t+1} > \gamma_t > 1$ for all $t \geq T$. Then, there is a finite date $\hat{T}$ such that

$$\Gamma < \sum\nolimits_{i=1}^{N} \phi_{\hat{T}}^i \Delta_{\hat{T}}^{*,i} + \phi_{\hat{T}}^{N+1} \Delta_{\hat{T}}^{N+1},$$

given that $\Delta_t^{N+1} \geq 0$ holds at all dates. But this implies that condition (12) is violated. As previously mentioned, it is straightforward to show that the market-clearing condition is necessarily violated when condition (12) is violated and vice versa. As a result, we cannot have an equilibrium with the property that $\gamma_t > 1$ at all dates.

Suppose now that the cost function $c : \mathbb{R}_+ \to \mathbb{R}_+$ is locally linear around the origin. Given that $\left\{\phi_t^i\right\}_{t=0}^{\infty}$ is strictly increasing and unbounded, there exists a finite date $T'$ such that $\Delta_t^{*,i} > 0$ for all $t \geq T'$. Then, condition (12) is violated at some date.

Finally, assume that the cost function $c : \mathbb{R}_+ \to \mathbb{R}_+$ is linear. Then, there is $k > 0$ such that $c\left(\Delta\right) = k\Delta$ for all $\Delta \geq 0$. Because $\gamma_{t+1} > \gamma_t > 1$ for all $t \geq T$, there is a finite date $T''$ such that $\phi_{T''}^i > k$. At that date, the entrepreneur's problem has no solution.

Consider a money growth rate $\omega$ in the interval $(\beta - 1, 0)$. In this case, we have $\Delta_t^{N+1} < 0$ in every period. Suppose that there is a date $T \geq 0$ such that $\gamma_t > 1$ for all $t \geq T$. Then, $\gamma_{t+1} > \gamma_t > 1$ for all $t \geq T$.

Suppose the cost function $c : \mathbb{R}_+ \to \mathbb{R}_+$ is strictly convex. Then, the sequence $\left\{\Delta_t^{*,i}\right\}_{t=0}^{\infty}$ is strictly increasing and unbounded. In this case, a necessary condition for the existence of a stationary equilibrium is that $\phi_t^{N+1} M_t^{N+1}$ be strictly decreasing. Because $\left\{\phi_t^{N+1}\right\}_{t=0}^{\infty}$ is strictly increasing, the government money supply sequence $\left\{M_t^{N+1}\right\}_{t=0}^{\infty}$ must decrease at a faster rate so that the real value of government money, given by $\phi_t^{N+1} M_t^{N+1}$, is strictly decreasing. Because the real value of government money cannot fall below zero and the term $\sum_{i=1}^{N} \phi_t^i \Delta_t^{*,i}$ is unbounded, we cannot have an equilibrium with $\gamma_t > 1$ for all $t \geq T$ when $\omega \in (\beta - 1, 0)$.

When the cost function $c : \mathbb{R}_+ \to \mathbb{R}_+$ is locally linear around the origin, it is straightforward to show that $\sum_{i=1}^{N} \phi_t^i \Delta_t^{*,i}$ is unbounded. Finally, when the cost function is linear, one can easily show that the entrepreneur's problem has no solution at some finite date. ■

The intuition for the previous proposition 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 and systematic contraction of the money supply. The entrepreneurs are unwilling to shrink the private money supply by retiring previously issued currency. Thus, the only option left is to have the government systematically shrink the total supply to such an extent that the money stock declines in every period. The previous proposition shows that this strategy becomes unsustainable at some finite date because the entrepreneurs will create an ever-increasing amount of money when the government attempts to promote a deflationary process. Thus, it is impossible to have a stationary equilibrium with deflation and a positive real return on money when private money competes with government money (i.e., when private money is positively valued in equilibrium).

The main implication of the previous result is that the implementation of monetary policy through a money-growth rule is significantly impaired by the presence of competing currencies. Profit-maximizing entrepreneurs will frustrate the government's attempt to implement a positive real return on money through a deflationary process when the public is willing to hold private currencies.[6]

Note that the proposition does not rule out the existence of equilibria with a positive real return on money. It simply says that a stationary equilibrium with positive real returns on money *and* positively valued private currencies cannot exist under a money-growth rule in the presence of profit-maximizing entrepreneurs.

An immediate corollary of the previous proposition is that the socially optimal return on money can be implemented through a money-growth rule only if agents do not value privately

[6]We should emphasize 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 own currency).

issued currency. In particular, we can construct equilibria with the property $\phi_t^i = 0$ for all $i \in \{1, ..., N\}$ and $\phi_t^{N+1} > 0$ at all dates $t \geq 0$. In these equilibria, the sequence of returns satisfies, for all dates

$$z\left(\gamma_{t+1}\right) = (1+\omega)\, z\left(\gamma_t\right) \gamma_t. \tag{13}$$

The dynamic properties of the system (13) are exactly the same as those derived in Lagos and Wright (2003) when preferences and technologies imply a demand function for real balances that is strictly decreasing in the inflation rate.

A policy choice $\omega$ 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

$$\sigma \frac{u'\left(q\left(\omega\right)\right)}{w'\left(q\left(\omega\right)\right)} + 1 - \sigma = \frac{1+\omega}{\beta},$$

given that $\theta \to 1$.

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.

## 5.2 Pegging the real value of government money

In view of the previously described issues for monetary policy implementation, we develop an alternative policy rule that can *uniquely* implement the socially optimal return on money. As we will see, 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 the condition

$$\phi_t^{N+1} \bar{M}_t^{N+1} = m \tag{14}$$

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 (14) in every period, taking prices as given.

The following proposition establishes the main result of our analysis of currency competition under a hybrid system. It 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 8** *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.*

**Proof.** When the government pegs the real value of its own money, the market-clearing condition implies

$$m + \sum\nolimits_{i=1}^{N} \phi_t^i M_t^i = z\left(\gamma_{t+1}\right)$$

at all dates. The law of motion for the supply of each private currency implies the relation

$$\sum\nolimits_{i=1}^{N} \phi_t^i M_t^i = \sum\nolimits_{i=1}^{N} \Delta_t^{*,i} \phi_t^i + \gamma_t \sum\nolimits_{i=1}^{N} \phi_{t-1}^i M_{t-1}^i.$$

Then, we can rewrite the market-clearing condition as

$$z\left(\gamma_{t+1}\right) - m = \sum\nolimits_{i=1}^{N} \Delta_t^{*,i} \phi_t^i + \gamma_t \left[z\left(\gamma_t\right) - m\right].$$

In addition, we must have $z(\gamma_t) \geq m$ and $\beta \gamma_t z(\gamma_t) \leq w(q^*)$, given that $\phi_t^i \geq 0$ and $M_t^i \geq 0$.

Set the target value $m$ such that $z^{-1}(m) > 1$. Then, we must have

$$\gamma_t \geq z^{-1}(m) > 1$$

at all dates. Additionally, the real return on money must satisfy

$$z\left(\gamma_{t+1}\right) - m - \gamma_t \left[z\left(\gamma_t\right) - m\right] \geq 0$$

along the equilibrium trajectory because the term $\sum_{i=1}^{N} \Delta_t^{*,i} \phi_t^i$ is nonnegative. Define the value function

$$\Gamma(m) = \max_{\left(\gamma, \gamma_+\right) \in \mathbb{R}_+^2} \left\{z\left(\gamma_+\right) - m - \gamma\left[z(\gamma) - m\right]\right\},$$

with the maximization on the right-hand side subject to $z(\gamma) \geq m$, $z\left(\gamma_+\right) \geq m$, $\beta \gamma z(\gamma) \leq w(q^*)$, and $\beta \gamma_+ z\left(\gamma_+\right) \leq w(q^*)$. It is clear that $0 \leq \Gamma(m) < \infty$.

Because $\gamma_t > 1$ must hold at all dates, we have

$$\frac{\phi_{t+1}^i}{\phi_t^i} > 1$$

for any valued currency in every period. This means that the price sequence $\left\{\phi_t^i\right\}_{t=0}^{\infty}$ is strictly increasing. Following the same reasoning as that of Proposition 4, we can show that $\left\{\phi_t^i\right\}_{t=0}^{\infty}$ is an unbounded sequence.

Suppose the cost function $c : \mathbb{R}_+ \to \mathbb{R}_+$ is strictly convex. Then, the first-order condition for the profit maximization problem implies $\phi_t^i = c'\left(\Delta_t^{*,i}\right)$, which means that the profit-maximizing choice $\Delta_t^{*,i}$ is strictly increasing in $\phi_t^i$. As a result, there exists a finite date $T$ such that

$$\sum\nolimits_{i=1}^{N} \Delta_T^{*,i} c'\left(\Delta_T^{*,i}\right) > \Gamma\left(m\right),$$

which implies the violation of the market-clearing condition. Hence, we cannot have an equilibrium with valued privately issued currencies when the target value satisfies $z^{-1}\left(m\right) > 1$ and $\beta z^{-1}\left(m\right) m \leq w\left(q^*\right)$.

Suppose the cost function $c : \mathbb{R}_+ \to \mathbb{R}_+$ is locally linear around the origin. Because $c\left(0\right) = 0$, there exist scalars $\Delta' > 0$ and $k > 0$ such that $c\left(\Delta\right) = k\Delta$ for all $\Delta \in [0, \Delta']$. Then, there is a finite date $T'$ such that $\Delta_t^{*,i} > 0$ for all $t \geq T'$. Because $\left\{\phi_t^i\right\}_{t=0}^{\infty}$ is unbounded, the term $\sum_{i=1}^{N} \Delta_t^{*,i} \phi_t^i$ is unbounded, which leads to the violation of the market-clearing condition.

Finally, assume that the cost function $c : \mathbb{R}_+ \to \mathbb{R}_+$ is linear. Then, there is $k > 0$ such that $c\left(\Delta\right) = k\Delta$ for all $\Delta \geq 0$. Because $\left\{\phi_t^i\right\}_{t=0}^{\infty}$ is unbounded, there exists a finite date $T''$ such that $\phi_{T''}^i > k$. At that date, the profit-maximization problem has no solution.

Regardless of the properties of the cost function, we cannot have a monetary equilibrium with positively valued private currencies when the government sets a target value $m$ satisfying $z^{-1}\left(m\right) > 1$ and $\beta z^{-1}\left(m\right) m \leq w\left(q^*\right)$. When we set the value of private currencies to zero, we obtain the equilibrium trajectory $\gamma_t = z^{-1}\left(m\right)$ at all dates $t \geq 0$. This trajectory satisfies the other boundary condition because $\beta z^{-1}\left(m\right) m \leq w\left(q^*\right)$. ■

In Proposition 7, we have shown that, under a money-growth rule, there is no stationary equilibrium with a positive real return on money and positively valued private monies, which does not rule out the existence of equilibria with negative real returns on money and valued private monies. Proposition 8 provides a stronger result regarding the coexistence of private and public monies. 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 for real balances is sufficiently large.

The intuition behind this result is that, 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. Thus, by credibly guaranteeing the real value of money balances, the government is able to uniquely implement an allocation with a positive real return on money by driving private monies out of the economy.

Another way to interpret the previous result is to acknowledge that unique implementation requires the provision of "good" government money. The policy of pegging the real value of government money can be viewed as providing good money to support exchange in the economy. 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. 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, it follows that the real return on money must be strictly positive in any allocation that can be uniquely implemented under the previously described policy regime.

As we have seen, private money creation can be 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.

An important corollary from the previous proposition is that one can uniquely implement the socially optimal return on money by taking the limit

$$m \to z\left(\frac{1}{\beta}\right).$$

In this case, 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. To verify this claim, note that the government budget constraint can be written as

$$\tau_t = m(\gamma_t - 1)$$

in every period $t$. Because the unique equilibrium implies $\gamma_t = z^{-1}(m)$ for all $t \geq 0$, we must have

$$\tau_t = m\left[z^{-1}(m) - 1\right] > 0$$

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.

As previously mentioned, 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 $m \to z\left(\beta^{-1}\right)$ is socially efficient. As we have seen, 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 it is clear that the allocation associated with $m \to z\left(\beta^{-1}\right)$ 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. In addition, the lump-sum tax is neutral, given quasi-linear preferences.

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 a deflationary process. Here, we run into a classical 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 this section, we have demonstrated that the joint goal of monetary stability and efficiency can be achieved by public policy provided the government is able to tax private agents to guarantee a sufficiently large value of its money supply. The implementation of the socially optimal return on money requires government money to drive private money out of the economy, which also avoids the socially wasteful production of tokens in the private sector.

# 6 Automata

In the previous section, we have shown that the government is able to drive private money out of the economy by pegging the real value of its own currency brand. As we have seen, the entrepreneurs' profit-maximizing behavior plays a central role in the construction of the results. In this section, we want to show that the previously described policy rule is robust to other forms of private money, such as those issued by automata.

Consider the benchmark economy described in Section 3 without profit-maximizing entrepreneurs. 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 $j \in \{1, ..., J\}$ 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, then we must have

$$\frac{\phi_{t+1}^{j}}{\phi_{t}^{j}}=\gamma_{t+1} \tag{15}$$

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 (15) implies

$$h_{t}^{j}=h_{t-1}^{j}\gamma_{t} \tag{16}$$

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

$$m+\sum_{j=1}^{J}h_{t}^{j}=z\left(\gamma_{t+1}\right). \tag{17}$$

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

**Definition 6** *A perfect-foresight monetary equilibrium is a sequence* $\left\{\mathbf{h}_{t},\gamma_{t},\Delta_{t}^{N+1},\tau_{t}\right\}_{t=0}^{\infty}$ *satisfying (11), (14), (16), (17),* $h_{t}^{j}\geq 0$, $z\left(\gamma_{t}\right)\geq m$, *and* $\beta\gamma_{t}z\left(\gamma_{t}\right)\leq w\left(q^{*}\right)$ *for all* $t\geq 0$ *and* $j\in\{1,...,J\}$.

It is possible to demonstrate that the result derived in Proposition 8 holds when private monies are issued by automata.

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

**Proof.** Condition (16) implies the relation

$$\sum_{j=1}^{J}h_{t}^{j}=\gamma_{t}\sum_{j=1}^{J}h_{t-1}^{j}.$$

Using the market-clearing condition (17), we find that the dynamic system governing the evolution of the real return on money is given by

$$z\left(\gamma_{t+1}\right)-m=\gamma_{t}z\left(\gamma_{t}\right)-m\gamma_{t}.$$

In addition, we must have the boundary conditions $z\left(\gamma_{t}\right)\geq m$ and $\beta\gamma_{t}z\left(\gamma_{t}\right)\leq w\left(q^{*}\right)$ at all dates.

Note that $\gamma_t = 1$ for all $t \geq 0$ is a stationary solution to the dynamic system. Because $z^{-1}(m) > 1$, it violates the boundary condition $z(\gamma_t) \geq m$, so it cannot be an equilibrium. There exits another stationary solution: $\gamma_t = z^{-1}(m)$ at all dates $t \geq 0$. This solution satisfies the boundary conditions provided $\beta z^{-1}(m)\, m \leq w(q^*)$. Because any nonstationary solution necessarily violates at least one boundary condition, the previously described dynamic system has a unique solution satisfying both boundary conditions, which is necessarily stationary. ■

The previous proposition shows that an equilibrium can be described by a sequence $\{\gamma_t\}_{t=0}^{\infty}$ satisfying the dynamic system

$$z\left(\gamma_{t+1}\right) - m = \gamma_t \left[z\left(\gamma_t\right) - m\right],$$

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*.[7] To illustrate this property, it is helpful to 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 the conditions

$$\frac{\sigma^{\frac{1+\alpha}{\eta+\alpha}} \left(\beta\gamma_{t+1}\right)^{\frac{1+\alpha}{\eta+\alpha}-1}}{\left[1-(1-\sigma)\beta\gamma_{t+1}\right]^{\frac{1+\alpha}{\eta+\alpha}}} = \frac{\beta^{\frac{1+\alpha}{\eta+\alpha}-1} \left(\sigma\gamma_t\right)^{\frac{1+\alpha}{\eta+\alpha}}}{\left[1-(1-\sigma)\beta\gamma_t\right]^{\frac{1+\alpha}{\eta+\alpha}}} - m\gamma_t + m \tag{18}$$

with

$$\frac{\left(\beta\gamma_t\right)^{\frac{1+\alpha}{\eta+\alpha}-1}}{1+\alpha} \left[\frac{\sigma}{1-(1-\sigma)\beta\gamma_t}\right]^{\frac{1+\alpha}{\eta+\alpha}} \geq m \tag{19}$$

at all dates $t \geq T$. Condition (19) imposes a lower bound on the equilibrium return on money, which can result in the existence of a steady state at the lower bound.

It is helpful to 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 $\gamma_t$ satisfies the law of motion

$$\gamma_{t+1} = \gamma_t^2 - \frac{m}{\beta}\gamma_t + \frac{m}{\beta} \tag{20}$$

[7] In bifurcation theory, a transcritical bifurcation is one in which a fixed point exists for all values of a parameter and is never destroyed. Both before and after the bifurcation, there is one unstable and one stable fixed point. However, their stability is exchanged when they collide, so the unstable fixed point becomes stable and vice versa.

and the boundary condition

$$\frac{m}{\beta} \leq \gamma_t \leq \frac{1}{\beta}. \tag{21}$$

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

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

If $m \neq \beta$, the roots are 1 and $\beta^{-1}m$. If $m = \beta$, the unique solution is 1. As we will see, the properties of the 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 $\gamma_0 \in \left(\beta^{-1}m, 1\right)$ 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 (20) at the point $(1, 1)$, so the dynamic system remains above the 45-degree line. When we introduce the boundary restriction (21), 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 sustained deflation to ensure that the real return on money remains above one. To implement sustained deflation, the government must contract its money supply, a policy financed through taxation.

# 7 Productive Capital

The goal of this section is to investigate whether it is possible to implement an efficient allocation in the absence of government intervention if we introduce productive capital into the economy. 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, we will demonstrate that, with automaton issuers, it is possible to implement an allocation that is arbitrarily close to an efficient allocation 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. Then, the entrepreneur's budget constraint is given by

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

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 $j \in \{1, ..., N\}$. 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

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

It is clear that the set of solutions for the previous problem is the same as that of (3). 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 $\{f_t^j\}_{t=0}^{\infty}$ 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 $j \in \{1, ..., J\}$, we have the budget constraint

$$\phi_t^j \Delta_t^j + \frac{\kappa}{J} = f_t^j, \tag{22}$$

together with the law of motion

$$H_t^j = \Delta_t^j + H_{t-1}^j.$$

In addition, assume that $H_{-1}^j > 0$ for some $j \in \{1, ..., J\}$. In other words, the economy starts with a strictly positive amount of tokens.

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 $j \in \{1, ..., J\}$ and let $\mathbf{h}_t \in \mathbb{R}_+^J$ denote the vector of real values. Also, let $\mathbf{f}_t \in \mathbb{R}_+^J$ denote the vector of real dividends. The market-clearing condition in the money market is given by

$$\sum_{j=1}^{J} h_t^j = z\left(\gamma_{t+1}\right) \tag{23}$$

for all $t \geq 0$. For each automaton $j$, we can rewrite the budget constraint (22) as

$$h_t^j - \gamma_t h_{t-1}^j + \frac{\kappa}{J} = f_t^j. \tag{24}$$

Given these changes in the environment, we can now provide a formal definition of equilibrium under an institutional arrangement with the property that automaton issuers have access to productive capital.

**Definition 7** *Given a predetermined dividend plan $\{\mathbf{f}_t\}_{t=0}^{\infty}$, a perfect-foresight monetary equilibrium is a sequence $\{\mathbf{h}_t, \gamma_t\}_{t=0}^{\infty}$ satisfying (23), (24), $h_t^j \geq 0$, $z(\gamma_t) \geq 0$, and $\beta\gamma_t z(\gamma_t) \leq w(q^*)$ for all $t \geq 0$ and $j \in \{1, ..., J\}$.*

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 $j \in \{1, ..., J\}$ at all dates $t \geq 0$, with $0 \leq f \leq \kappa$. In this case, we obtain the dynamic system:

$$z\left(\gamma_{t+1}\right) - \gamma_t z\left(\gamma_t\right) + \kappa - f = 0 \tag{25}$$

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 10** *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* $1 < \gamma^s \leq \beta^{-1}$*.*

**Proof.** Given 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 $\alpha \geq 0$, the dynamic system (25) reduces to

$$\frac{\sigma^{\frac{1+\alpha}{\eta+\alpha}} \left(\beta\gamma_{t+1}\right)^{\frac{1+\alpha}{\eta+\alpha}-1}}{\left[1-(1-\sigma)\beta\gamma_{t+1}\right]^{\frac{1+\alpha}{\eta+\alpha}}} + \hat{\kappa} = \frac{\beta^{\frac{1+\alpha}{\eta+\alpha}-1} \left(\sigma\gamma_t\right)^{\frac{1+\alpha}{\eta+\alpha}}}{\left[1-(1-\sigma)\beta\gamma_t\right]^{\frac{1+\alpha}{\eta+\alpha}}},$$

where $\hat{\kappa} \equiv \kappa - f$.

It can be easily shown that $d\gamma_{t+1}/d\gamma_t > 0$ for all $\gamma_t > 0$. When $\gamma_{t+1} = 0$, we have

$$\gamma_t = \frac{\hat{\kappa}^{\frac{\eta+\alpha}{1+\alpha}}}{\sigma\beta^{\frac{1-\eta}{1+\alpha}} + \hat{\kappa}^{\frac{\eta+\alpha}{1+\alpha}} (1-\sigma)\beta}.$$

Because $\gamma_t \in \left[0, \beta^{-1}\right]$ for all $t \geq 0$, a nonstationary solution would violate the boundary condition. Thus, the unique solution is necessarily stationary, $\gamma_t = \gamma^s$ for all $t \geq 0$, and satisfies

$$\sigma^{\frac{1+\alpha}{\eta+\alpha}} \left(\beta\gamma^s\right)^{\frac{1+\alpha}{\eta+\alpha}-1} + \hat{\kappa}\left[1-(1-\sigma)\beta\gamma^s\right]^{\frac{1+\alpha}{\eta+\alpha}} = \beta^{\frac{1+\alpha}{\eta+\alpha}-1} \left(\sigma\gamma^s\right)^{\frac{1+\alpha}{\eta+\alpha}}$$

and

$$\frac{\hat{\kappa}^{\frac{\eta+\alpha}{1+\alpha}}}{\sigma\beta^{\frac{1-\eta}{1+\alpha}} + \hat{\kappa}^{\frac{\eta+\alpha}{1+\alpha}} (1-\sigma)\beta} \leq \gamma^s \leq \frac{1}{\beta}.$$

■

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, it is helpful to further simplify the dynamic system by assuming that $\eta = \frac{1}{2}$ and $\alpha = 0$. In addition, take the limit $\sigma \to 1$. In this case, the dynamic system reduces to

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

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

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

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 bear some resemblance to those of Andolfatto, Berentsen, and Waller (2016), who study the properties of a monetary arrangement in which an institution with the 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

Our analysis has shown that a system of competing privately issued monies can work only for a strict subset of production technologies (i.e., the technology used to issue digital currencies). Despite the possibility of having an equilibrium consistent with price stability for a strict subset of production technologies, we have demonstrated that a purely private arrangement does not deliver an efficient allocation. In addition, the presence of privately issued currencies can create problems for monetary policy implementation under 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.

In view of 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 to support exchange in the economy.

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 allocation that is arbitrarily close to an efficient allocation can be the unique equilibrium outcome provided that capital is sufficiently productive.

# References

[1] D. Andolfatto, A. Berentsen, C. Waller. "Monetary policy with asset-backed money," *Journal of Economic Theory* 164 (2016), pp. 166-186.

[2] B. Aruoba, G. Rocheteau, C. Waller. "Bargaining and the value of money," *Journal of Monetary Economics* 54 (2007), pp. 2636-55.

[3] A. Berentsen. "On the private provision of fiat currency," *European Economic Review* 50 (2006), pp. 1683-1698.

[4] R. Cavalcanti, A. Erosa, T. Temzelides. "Private money and reserve management in a random-matching model," *Journal of Political Economy* 107 (1999), pp. 929-945.

[5] R. Cavalcanti, N. Wallace. "A model of private bank-note issue." *Review of Economic Dynamics* 2 (1999), pp. 104-36.

[6] M. Friedman. *A Program for Monetary Stability*, New York: Fordham University Press (1959).

[7] M. Friedman. "The optimum quantity of money," in *The Optimum Quantity of Money and Other Essays*, 1969, Aldine Publishing Company.

[8] H. Halaburda, M. Sarvary. *Beyond Bitcoin: The Economics of Digital Currencies*, 2015. Palgrave Macmillan.

[9] F. Hayek. *Denationalisation of Money*, Hobart Papers 70, 2nd ed., The Institute of Economic Affairs, London (1976).

[10] R. Lagos, R. Wright. "Dynamics, cycles and sunspot equilibria in 'genuinely dynamic, fundamentally disaggregative' models of money," *Journal of Economic Theory* 109 (2003), pp. 156-171.

[11] R. Lagos, R. Wright. "A unified framework for monetary theory and policy analysis," *Journal of Political Economy* 113 (2005), pp. 463-84.

[12] A. Martin, S. Schreft. "Currency competition: A partial vindication of Hayek," *Journal of Monetary Economics* 53 (2006), pp. 2085-2111.

[13] C. Monnet. "Private versus public money." *International Economic Review 47* (2006), pp. 951-60.

[14] M. Obstfeld, K. Rogoff. "Speculative hyperinflations in maximizing models: Can we rule them out?" *Journal of Political Economy* 91 (1983), pp. 675-87.

[15] G. Rocheteau. "The cost of inflation: A mechanism design approach," *Journal of Economic Theory* 147 (2012), pp. 1261-1279.

[16] G. Selgin, L.H. White. "How would the invisible hand handle money?" *Journal of Economic Literature* 32 (1994), pp. 1718-49.

[17] N. Wallace. "Whither monetary economics?" *International Economic Review* 42 (2001), pp. 847-69.

[18] S. Williamson."Private money," *Journal of Money, Credit and Banking* 31 (1999), pp. 469-491.