

Can Currency Competition Work?*

Jesús Fernández-Villaverde

University of Pennsylvania, NBER, and CEPR

Daniel Sanches

Federal Reserve Bank of Philadelphia

December 14, 2018

Abstract

Can competition among privately-issued fiat currencies work? Only sometimes and partially. To show this, we build a model of competition among privately-issued fiat currencies. We modify a workhorse of monetary economics, the Lagos-Wright environment, by including entrepreneurs who can issue their own fiat currencies to maximize their utility. Otherwise, the model is standard. A purely private arrangement fails to implement an efficient allocation, even though it can deliver price stability under certain technological conditions. Although currency competition creates problems for monetary policy implementation under conventional methods, it is possible to design a policy rule that uniquely implements an efficient allocation. We also show that unique implementation of an efficient allocation can be achieved without government intervention if productive capital is introduced. Finally, we investigate the properties of bounds on money issuing and the role of network effects.

Keywords: Private money, currency competition, cryptocurrencies, monetary policy

JEL classification numbers: E40, E42, E52

*Correspondence: jesusfv@econ.upenn.edu (Fernández-Villaverde) and Daniel.Sanches@phil.frb.org (Sanches). Sean Myers provided us with a much more powerful way to state one of our main results, and we are deeply in his debt. We also thank Ed Green, Todd Keister, Ed Nelson, Guillermo Ordoñez, Rob Reed, George Selgin, Shouyong Shi, Neil Wallace, Steve Williamson, Randy Wright, Cathy M. Zhang, and participants at several seminars for useful comments. The views expressed in this paper are those of the authors and do not necessarily reflect those of the Federal Reserve Bank of Philadelphia or the Federal Reserve System.

1 Introduction

Can competition among privately-issued fiduciary currencies work? The sudden appearance of Bitcoin, Ethereum, and other cryptocurrencies has triggered a wave of interest in privately-issued monies.¹ A similar interest in the topic has not been seen since the vivid polemics associated with the demise of free banking in the English-speaking world in the middle of the 19th century (White, 1995). Somewhat surprisingly, this interest has not translated, so far, into much research within monetary economics. Most papers analyzing the cryptocurrency phenomenon have either been descriptive (Böhme, Christin, Edelman, and Moore, 2015) or have dealt with governance and regulatory concerns from a legal perspective (Chuen, 2015).² In comparison, there has been much research related to the computer science aspects of the phenomenon (Narayanan, Bonneau, Felten, Miller, and Goldfeder, 2016).

This situation is unfortunate. Without a theoretical understanding of how currency competition works, we cannot answer a long list of positive and normative questions. Among the positive questions: Will a system of private money deliver price stability? Will one currency drive all others from the market? Or will several of these currencies coexist along the equilibrium path? Do private monies require a commodity backing? Will the market provide the socially optimum amount of money? Can private monies and a government-issued money compete? Can a unit of account be separated from a medium of exchange? Among the normative questions: Should governments prevent the circulation of private monies? Should governments treat private monies as currencies or as any other regular property? Should the private monies be taxed? Even more radically, now that cryptocurrencies are technically feasible, should we revisit Friedman and Schwartz's (1986) celebrated arguments justifying the role of governments as money issuers? There are even questions relevant for entrepreneurs: What is the best strategy to jump start the circulation of a currency? How do you maximize the seigniorage that comes from it?

To address some of these questions, we build a model of competition among privately-issued fiduciary currencies. We modify a workhorse of monetary economics, the Lagos and Wright (2005) (LW) environment, by including entrepreneurs who can issue their own currencies to maximize their utility. Otherwise, the model is standard. Following LW has two important advantages. First, since the model is particularly amenable to analysis, we can derive many insights about currency competition. Second, the use of the LW framework

¹As of October 28, 2017, besides Bitcoin, 11 other cryptocurrencies have market capitalizations over \$1 billion and another 49 between \$100 and \$999.99 million. Updated numbers are reported by <https://coinmarketcap.com/>. Following convention, we will use Bitcoin, with a capital B, to refer to the whole payment environment, and bitcoin, with a lower case b, to denote the currency units of the payment system. See Antonopoulos (2015) for a technical introduction to Bitcoin.

²Some exceptions are Chiu and Wong (2014) and Hendrickson, Hogan, and Luther (2016).

makes our new results easy to compare with previous findings in the literature.³

We highlight six of our results. First, we show that, in a 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 can exist only if the cost function associated with the production of private money is strictly increasing and locally linear around the origin. If the cost function has a positive derivative at zero, then there is no equilibrium consistent with price stability. Thus, [Hayek's \(1999\)](#) vision of a system of private monies competing among themselves to provide a stable means of exchange 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 shows that the self-fulfilling inflationary episodes highlighted by [Obstfeld and Rogoff \(1983\)](#) and [Lagos and Wright \(2003\)](#) in economies with government-issued 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.⁴

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

Fourth, we show that the main features of cryptocurrencies, such as the existence of an upper bound on the 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 has positive derivative at zero. A purely private system can deliver price stability under a wide array of preferences and technologies, provided that some limit on the total circulation of private currencies is enforced by an immutable protocol. However, this

³An alternative tractable framework that also creates a role for a medium of exchange is the large household model in [Shi \(1997\)](#).

⁴[Tullock \(1975\)](#) argued that competition among monies could stop inflation (although he dismissed this possibility due to the short planning horizon of governments, which prevents them from valuing the future income streams from maintaining a stable currency). Our analysis is a counterexample to Tullock's suggestion.

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, 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 an allocation with the property that the real return on money equals the rate of time preference if agents are willing to hold privately-issued monies. Profit-maximizing entrepreneurs will frustrate the government’s attempt to implement a positive real return on money through deflation when the public is willing to hold private currencies. To get around this problem, we study alternative policies that can simultaneously promote stability and efficiency. In particular, we analyze the properties of a policy rule that pegs the real value of government money. Under this regime, it is possible to implement an efficient allocation as the unique equilibrium outcome, which requires driving private money out of the economy. Also, the proposed policy rule is robust to other forms of private monies, such as those issued by automata (i.e., non-profit-maximizing agents).

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

We also 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. An efficient allocation can be the *unique* equilibrium outcome provided that capital is sufficiently productive.

Finally, we illustrate the implications of network effects for competition in the currency-issuing business. In particular, we show that the presence of network effects can be relevant for the welfare properties of equilibrium allocations in a competitive environment.

The astute reader might have noticed that we have used the word “entrepreneur” and not the more common “banker” to denote the issuers of private money. This linguistic turn is important. Our model highlights how the issuing of a private currency is logically separated from banking. Both tasks were historically linked for logistical reasons: banks had a central location in the network of payments that made it easy for them to introduce currency into

circulation.⁵ The internet has broken the logistical barrier. The issuing of bitcoins, for instance, is done through a proof-of-work system that is independent of any banking activity (or at least of banking understood as the issuing and handling of deposits and credit).⁶

This previous explanation also addresses a second concern: What are the differences between private monies issued in the past by banks (such as during the Scottish free banking experience between 1716 and 1845) and modern cryptocurrencies? As we mentioned, a first difference is the distribution process, which is now much wider and dispersed than before. A second difference is the possibility, through the protocols embodied in the software, of having quasi-commitment devices regarding how much money will be issued. The most famous of these devices is the 21 million bitcoins that will eventually be released.⁷ We will discuss how to incorporate an automaton issuer of private money into our model to analyze this property of cryptocurrencies. Third, cryptographic techniques, such as those described in [von zur Gathen \(2015\)](#), make it harder to counterfeit digital currencies than traditional physical monies, minimizing a historical obstacle that private monies faced ([Gorton, 1989](#)). Fourth, most (but not all) historical cases of private money were of commodity-backed currencies, while most cryptocurrencies are fully fiduciary.

At the same time, we ignore all issues related to the payment structure of cryptocurrencies, such as the blockchain, the emergence of consensus on a network, or the possibilities of Goldfinger attacks (see [Narayanan, Bonneau, Felten, Miller, and Goldfeder 2016](#)). While these topics are of foremost importance, they require a specific modeling strategy that falls far from the one we follow in this paper and that we feel is more suited to the macroeconomic questions we focus on.

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, and Temzelides \(1999, 2005\)](#), [Cavalcanti and Wallace \(1999\)](#), [Williamson \(1999\)](#), [Berentsen \(2006\)](#), and [Monnet \(2006\)](#). See, from another perspective, [Selgin and White \(1994\)](#). Our emphasis is different from that in these previous papers, as we depart from modeling banks and their reserve management problem. Our entrepreneurs issue fiduciary money that cannot be redeemed for any other asset. Our characterization captures the purely fiduciary features of most cryptocurrencies (in fact, since cryptocurrencies cannot be used to

⁵In this respect, our analysis can be viewed as also belonging to the literature on the provision of liquidity by productive firms ([Holmström and Tirole, 2011](#); [Dang, Gorton, Holmström, and Ordoñez, 2014](#); and [Geromichalos and Herrenbrueck, 2016](#)).

⁶Similarly, some of the community currencies that have achieved a degree of success do not depend on banks backing or issuing them (see [Greco, 2001](#)).

⁷We use the term “quasi-commitment” because the software code can be changed by sufficient consensus in the network. This possibility is not appreciated enough in the discussion about open-source cryptocurrencies. For the importance of commitment, see [Araujo and Camargo \(2008\)](#).

pay taxes in most sovereigns, their existence is more interesting, for an economist, than government-issued fiat monies with legal tender status). Our partial vindication of Hayek shares many commonalities with [Martin and Schreft \(2006\)](#), who were the first to prove the existence of equilibria for environments in which outside money is issued competitively. Lastly, we cannot forget [Klein \(1974\)](#) and his application of industrial organization insights to competition among monies.

The rest of the paper is organized as follows. Section 2 presents our basic model. Section 3 characterizes the properties of a purely private arrangement. Motivated by institutional features of cryptocurrencies, we investigate, in Section 4, the implications of an exogenous bound on the supply of private currencies. Section 5 studies the interaction between private and government monies and defines the role of monetary policy in a competitive environment. Section 6 considers money issued by automata. In Section 7, we explore the welfare properties of an economy with productive capital. Section 8 illustrates the implications of network effects for currency competition. Section 9 concludes.

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 can produce, but do not want to consume. A seller can produce a perishable good, referred to as the DM good, using a divisible technology that delivers one unit of the good for each unit of effort he exerts. An entrepreneur is neither a producer nor a consumer of the DM good.

In addition to the 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. Specifically, an entrepreneur of type

$i \in \{1, \dots, N\}$ has the ability to use the technology to create type- i tokens. Let $c : \mathbb{R}_+ \rightarrow \mathbb{R}_+$ denote the cost function (in terms of the utility of the entrepreneur) that depends on the tokens minted in the period. We will assume throughout the paper that $c : \mathbb{R}_+ \rightarrow \mathbb{R}_+$ is strictly increasing and weakly convex, with $\infty > c(0) \geq 0$ (when explicitly mentioned, we will add further structure to the cost function to either derive a concrete result or to simplify the proofs). 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

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

Assume that $u : \mathbb{R}_+ \rightarrow \mathbb{R}$ 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 $w : \mathbb{R}_+ \rightarrow \mathbb{R}_+$ is continuously differentiable, increasing, and weakly convex, with $w(0) = 0$.

There is a $[0, 1]$ -continuum of entrepreneurs of each type $i \in \{1, \dots, N\}$. 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

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

Finally, let $\beta \in (0, 1)$ denote the discount factor, which is common across all types.

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

3 Competitive Money Supply

Because the meetings in the DM are anonymous, there is no scope for trading future

promises in this market. As a result, a medium of exchange is essential to achieve allocations that we could not achieve without it. In a typical monetary model, a medium of exchange is supplied in the form of a government-issued fiat money, with the government following a monetary policy rule (e.g., a money-growth rule). In this section, we consider, instead, the endogenous supply of outside fiduciary money. In particular, we study a monetary system in which profit-maximizing entrepreneurs have the ability to create intrinsically worthless tokens that can circulate as a medium of exchange. These currencies are not associated with any promise to exchange them for goods or other assets at some future date. Also, it is assumed that all agents in the economy can observe the total supply of each currency put into circulation at each date. These features allow agents to form beliefs about the exchange value of money in the current and future periods, so that fiat money can attain a positive value in equilibrium. The fact that these tokens attain a strictly positive value in equilibrium allows us to refer to them as *currencies*.

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

In the context of cryptocurrencies (an important, but not necessarily the only case of currency competition), we can re-interpret the entrepreneurs as “miners” and the index $i \in \{1, \dots, N\}$ 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 in which 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 $i \in \{1, \dots, N\}$ in terms of the CM good, and let $\phi_t = (\phi_t^1, \dots, \phi_t^N) \in \mathbb{R}_+^N$ denote the vector of real prices.

3.1 Buyer

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

Bellman equation can be written as

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

subject to the budget constraint

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

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 $W^b(\mathbf{M}_{t-1}^b, t)$ can be written as

$$W^b(\mathbf{M}_{t-1}^b, t) = \phi_t \cdot \mathbf{M}_{t-1}^b + W^b(\mathbf{0}, t),$$

with the intercept given by

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

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

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

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

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

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

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

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

subject to the participation constraints

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

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

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

and

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

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

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

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

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

and

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

Given the trading protocol, the solution to the bargaining problem allows us to characterize real expenditures in the DM, given by $\boldsymbol{\phi}_{t+1} \cdot \mathbf{d}(\mathbf{M}_t^b, t)$, 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 ab-

sence of portfolio restrictions and barriers to trade, the exchange rate between two currencies is indeterminate in a flexible-price economy. In our framework, a similar result holds with respect to privately-issued currencies, given the absence of transaction costs when dealing with different currencies. Buyers and sellers do not “prefer” any currency over another and there is a sense in which we can talk about perfect competition among currencies.

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

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

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

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

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

The optimal portfolio problem can be defined as

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

The optimal choice, then, satisfies

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

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

$$\lim_{t \rightarrow \infty} \beta^t \times \phi_t \cdot \mathbf{M}_t^b = 0, \quad (2)$$

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

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

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

3.2 Seller

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

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

subject to the budget constraint

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

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

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

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

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 (i.e., *per buyer*) supply of currency i in period t . Let $\Delta_t^i \in \mathbb{R}$ denote entrepreneur i 's net circulation of newly minted tokens in period t (or the mining of new cryptocurrency). If we anticipate that all type- i entrepreneurs behave identically, given that they solve the same decision problem, then we can write the law of motion for type- i tokens as

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

where $M_{-1}^i \in \mathbb{R}_+$ denotes the initial stock.

We will show momentarily that $\Delta_t^i \geq 0$. Therefore, the entrepreneur's budget constraint can be written as

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

at each date $t \geq 0$. Here $M_t^{ij} \in \mathbb{R}_+$ denotes entrepreneur i 's holdings of currency issued by entrepreneur $j \neq i$. This budget constraint highlights that privately-issued currencies are not

associated with an explicit promise by the issuers to exchange them for goods or assets at a future date.

If $\phi_{t+1}^j/\phi_t^j \leq \beta^{-1}$ for all $j \in \{1, \dots, N\}$, then entrepreneur i chooses not to hold other currencies across periods, so that $M_t^{ij} = 0$ for all $j \neq i$. Thus, we can rewrite the budget constraint as

$$x_t^i = \phi_t^i \Delta_t^i,$$

which tells us that the entrepreneur's consumption in period t is equal to the real value of the net circulation. Because $x_t^i \geq 0$, we must have, as previously mentioned, $\Delta_t^i \geq 0$, i.e., an entrepreneur does not retire currency from circulation (see Section 7 for a more general case). Given that an entrepreneur takes prices $\{\phi_t\}_{t=0}^\infty$ as given, $\Delta_t^{*,i} \in \mathbb{R}_+$ solves the profit-maximization problem:

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

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

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

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

at all dates $t \geq 0$.

3.4 Equilibrium

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

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

at all dates. Since $\mathbf{M}_t^s = \mathbf{0}$, the market-clearing condition reduces to

$$\mathbf{M}_t = \mathbf{M}_t^b. \quad (5)$$

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 $\{\mathbf{M}_t, \mathbf{M}_t^b, \mathbf{\Delta}_t^*, \phi_t\}_{t=0}^\infty$ satisfying (1)-(5) for each $i \in \{1, \dots, N\}$ 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 assess 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.

Definition 2 *We say that a monetary equilibrium is consistent with price stability if*

$$\lim_{t \rightarrow \infty} \phi_t^i = \bar{\phi}^i > 0$$

for at least one currency $i \in \{1, \dots, N\}$.

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 $i \in \{1, \dots, N\}$ 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 $\lim_{q \rightarrow 0} u'(q)/m'(q) = \infty$.

A key property of equilibrium allocations under a competitive regime is that profit maximization establishes a positive relationship between the real price of currency i and the additional amount put into circulation by entrepreneur i when the cost function satisfies some basic properties. The following result shows an important implication of this relation.⁸

Lemma 4 *Suppose that $c'(0) = 0$. Then, we have*

$$\Delta_t^{*,i} > 0.$$

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

⁸Sean Myers helped us in reshaping the following lemma and its proof from our original, less general, result.

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

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

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

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

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

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

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

This prediction of the model is in sharp contrast to [Hayek \(1999\)](#), who argued that 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 fails in our environment with $c'(0) = 0$.⁹

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

Proposition 2 *Suppose that $c : \mathbb{R}_+ \rightarrow \mathbb{R}_+$ 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 not too small.*

Proof. Because $c : \mathbb{R}_+ \rightarrow \mathbb{R}_+$ 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 $\{\Delta_t^{*,i}\}_{t=0}^\infty$ 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 $\bar{\Delta} = (\bar{\Delta}^1, \dots, \bar{\Delta}^N)$ satisfying

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

with the quantity \hat{q} given by

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

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. In the context of cryptocurrencies, a cost function that is locally linear around the origin implies that the difficulty of the puzzle associated with the mining of new units does not change initially. The previous result provides a partial vindication of [Hayek \(1999\)](#): A purely private arrangement can deliver price stability for a strict subset of production technologies.

⁹It is straightforward to add, for instance, shocks to the cost function to make the evolution of the price level random. Furthermore, as we will argue later, a private money system is subject to self-fulfilling inflationary episodes, which means that such a system is plagued by an inherent lack of predictability. These two considerations show that the shortcomings of private money arrangements go well beyond the perhaps smaller problem of price changes under perfect foresight highlighted by [Proposition 1](#).

However, our next result shows that, for the same subset of production technologies, other allocations are also 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 different equilibria.

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

Proof. Because $c : \mathbb{R}_+ \rightarrow \mathbb{R}_+$ is locally linear in a neighborhood $[0, \bar{\Delta}] \subset \mathbb{R}_+$, there is $k > 0$ such that $c(\Delta) = k\Delta$ for all $\Delta \in [0, \bar{\Delta}]$. Set $\phi_0^i = k$. Then, any value $\Delta^i \in [0, \bar{\Delta}]$ 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

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

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

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

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

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

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 $\{\phi_t^i\}_{t=0}^\infty$ 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 $t \rightarrow \infty$. 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. Therefore, private money is inherently unstable in that changes in beliefs can lead to undesirable self-fulfilling inflationary episodes.

The existence of these inflationary equilibrium trajectories in a purely private monetary arrangement also means that hyperinflationary episodes are not an exclusive property of government-issued money. [Obstfeld and Rogoff \(1983\)](#) build economies that can display self-fulfilling inflationary episodes when the government is the sole issuer of currency and follows a money-growth rule. [Lagos and Wright \(2003\)](#) show the same result in search-theoretic monetary models with government-supplied currency. Our analysis illustrates that replacing government monopoly under a money-growth rule with private currencies does not overcome the fundamental fragility associated with fiduciary regimes, public or private.

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

Proposition 4 *Suppose that $c : \mathbb{R}_+ \rightarrow \mathbb{R}_+$ 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

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

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 $b_t^1 = z_\theta(\gamma_{t+1})$. 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. Market participants understand the discipline imposed by competition, summarized in the rate-of-return equality equilibrium condition, even though they see a single brand circulating in the economy. As in the previous case, an equilibrium with a stable value of money is as likely to occur as an equilibrium with a declining value of money.

3.5 Welfare

To simplify our welfare analysis, we consider the solution to the planner’s problem when the economy is initially endowed with a strictly positive amount of tokens. These durable objects serve as a record-keeping device that allows the planner to implement allocations with positive trade in the DM, even though the actions in each bilateral meeting are privately observable and agents cannot commit to their promises. Thanks to the existence of an initial positive amount of tokens, the planner does not need to use the costly technology to mint additional tokens to serve as a record-keeping device in decentralized transactions.¹⁰

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

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

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

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

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.

¹⁰Alternatively, one can think about the social planner as minting a trivially small amount of currency at an epsilon cost. Without the indivisibility of money, this is all we need to achieve the role of money as memory.

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

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

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

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 socially wasteful. Given an initial supply of tokens, the planner can implement an efficient allocation by systematically removing tokens from circulation so that the production of additional tokens is unnecessary. Because the creation of tokens is socially costly, any allocation involving a production plan that implies a growing supply of tokens is inefficient. Recall that entrepreneurs have an incentive to mint additional units of tokens when these objects are positively valued in equilibrium. The planner wants to avoid the excessive creation of tokens so that there is scope for public policies that aim to prevent 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 efficient 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 $i \in \{1, \dots, N\}$ 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

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

at each date t . The market-clearing condition implies

$$\sum_{i=1}^N \phi_t^i M_t^i = z(\gamma_{t+1})$$

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

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

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

$$z(\gamma_{t+1}) - \gamma_t z(\gamma_t) = \sum_{i=1}^N \phi_t^i \Delta_t^{*,i}. \quad (7)$$

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

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

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 $c : \mathbb{R}_+ \rightarrow \mathbb{R}_+$ is strictly convex with $c'(0) = 0$. 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

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

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 $\gamma_t > 1$ at all dates.

Suppose now that $c : \mathbb{R}_+ \rightarrow \mathbb{R}_+$ 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 $c : \mathbb{R}_+ \rightarrow \mathbb{R}_+$ 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 that take prices parametrically, competition cannot provide an optimal outcome because entrepreneurs do not internalize the pecuniary externalities they create in the decentralized market by minting additional tokens. 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.¹¹

4 Limited Supply

In the previous section, entrepreneurs could mint as much new currency as they wanted in each period subject to the cost function. However, in reality, the protocol behind most cryptocurrencies sets up an upper bound on the supply of each brand. 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 $i \in \{1, \dots, N\}$. In this case, the miner's profit-maximization problem is given by

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

Then, we can define a monetary equilibrium 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 has a zero derivative at the origin.

¹¹If the productivity in the CM and DM markets grew over time, we could have deflation with a constant supply of private money and, under a peculiar combination of parameters, achieve efficiency. However, this would only be the product of a "divine coincidence."

Proposition 6 Suppose $L_1(A) + AL'_1(A) > 0$ for all $A > 0$. Then, there is a class of caps $\{\bar{\Delta}_t\}_{t=0}^\infty$ 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

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

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

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

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

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

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

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 ϕ_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

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

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 $\phi_{T-1} = \phi_{T-1}(\bar{\Delta})$ is continuously differentiable in a sufficiently small neighborhood. In particular, we have

$$\begin{aligned} \frac{\partial \phi_{T-1}}{\partial \bar{\Delta}_t^i} &= \beta \frac{\partial \bar{\phi}}{\partial \bar{\Delta}_t^i} \left[L_1 \left(\bar{\phi} \sum_{i=1}^N \sum_{\tau=0}^{T-1} \bar{\Delta}_\tau^i \right) + \left(\bar{\phi} \sum_{i=1}^N \sum_{\tau=0}^{T-1} \bar{\Delta}_\tau^i \right) L'_1 \left(\bar{\phi} \sum_{i=1}^N \sum_{\tau=0}^{T-1} \bar{\Delta}_\tau^i \right) \right] \\ &\quad + \beta \bar{\phi}^2 L'_1 \left(\bar{\phi} \sum_{i=1}^N \sum_{\tau=0}^{T-1} \bar{\Delta}_\tau^i \right) \end{aligned}$$

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

$$\frac{\partial \phi_{T-1}}{\partial \bar{\Delta}_T^i} = \beta \frac{\partial \bar{\phi}}{\partial \bar{\Delta}_T^i} \left[L_1 \left(\bar{\phi} \sum_{i=1}^N \sum_{\tau=0}^{T-1} \bar{\Delta}_\tau^i \right) + \left(\bar{\phi} \sum_{i=1}^N \sum_{\tau=0}^{T-1} \bar{\Delta}_\tau^i \right) L'_1 \left(\bar{\phi} \sum_{i=1}^N \sum_{\tau=0}^{T-1} \bar{\Delta}_\tau^i \right) \right].$$

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 $\{\phi_0, \dots, \phi_T\}$ 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 $\{\bar{\Delta}_0^i, \bar{\Delta}_1^i, \dots, \bar{\Delta}_T^i\}_{i=1}^N$ 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 described allocation, the value of money and trading activity stabilize after date T . Thus, it is possible to have price stability with $c'(0) = 0$ when the protocol behind cryptocurrencies limits the amount of each privately-issued currency. In this respect, the innovations associated with cryptocurrencies and their immutable protocols can provide an effective mechanism to make a purely private arrangement consistent with price stability in the absence of government intervention.¹²

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

5 Monetary Policy

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

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

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

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.

¹²Our result resembles the existence result in [Martin and Schreft \(2006\)](#). These authors build an equilibrium where agents believe that if an issuer mints more than some threshold amount of currency, then only the currency issued up to the threshold will be valued and additional issuance will be worthless. That threshold works in similar ways to the bound on the issuance of cryptocurrencies.

Given an initial condition $M_{-1}^{N+1} \in \mathbb{R}_+$, government money follows at all dates the law of motion

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

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 ϕ_t are now elements in \mathbb{R}_+^{N+1} and the scalar sequence $\{\Delta_t^{N+1}\}_{t=0}^\infty$ is exogenously given. A formal definition follows.

Definition 5 *A perfect-foresight monetary equilibrium is an array $\{\mathbf{M}_t, \mathbf{M}_t^b, \phi_t, \Delta_t^*, \Delta_t^{N+1}, \tau_t\}_{t=0}^\infty$ satisfying (1)-(5) and (11) for each $i \in \{1, \dots, N\}$ 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 $t \geq 0$, where $\gamma_t \in \mathbb{R}_+$ represents the common real return across all valued currencies. In the absence of portfolio restrictions, government money must yield the same rate of return as other monetary assets for it to be valued in equilibrium.

5.1 Money-growth rule

We start our analysis of a hybrid arrangement by assuming that the government follows a money-growth rule of the form

$$M_t^{N+1} = (1 + \omega) M_{t-1}^{N+1},$$

with the money growth rate satisfying $\omega \geq \beta - 1$ (otherwise, we would not have an equilibrium). Given this policy rule, we derive a crucial property of the hybrid monetary system. As we have seen, a necessary condition for efficient 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 $i \in \{1, \dots, N\}$ implies

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

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

$$\phi_t^{N+1} M_t^{N+1} + \sum_{i=1}^N \phi_t^i M_t^i = z(\gamma_{t+1})$$

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

$$z(\gamma_{t+1}) - \gamma_t z(\gamma_t) = \sum_{i=1}^N \phi_t^i \Delta_t^{*,i} + \phi_t^{N+1} \Delta_t^{N+1}. \quad (12)$$

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 $c : \mathbb{R}_+ \rightarrow \mathbb{R}_+$ is strictly convex with $c'(0) = 0$. 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 $\beta\gamma z(\gamma) \leq w(q^*)$.

As previously shown, the sequence $\{\phi_t^i\}_{t=0}^\infty$ 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

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

given that $\Delta_t^{N+1} \geq 0$ holds at all dates. But this implies that condition (12) is violated. 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 $c : \mathbb{R}_+ \rightarrow \mathbb{R}_+$ 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 (12) is violated at some date.

Finally, assume that the cost function $c : \mathbb{R}_+ \rightarrow \mathbb{R}_+$ is linear. Then, 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.

Consider a money growth rate ω 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 $c : \mathbb{R}_+ \rightarrow \mathbb{R}_+$ is strictly convex with $c'(0) = 0$. Then, the sequence $\{\Delta_t^{*,i}\}_{t=0}^\infty$ 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 $\{\phi_t^{N+1}\}_{t=0}^\infty$ is strictly increasing, the government money supply sequence $\{M_t^{N+1}\}_{t=0}^\infty$ 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 $c : \mathbb{R}_+ \rightarrow \mathbb{R}_+$ 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 result is as follows. An equilibrium with a positive real return on money requires deflation. A deflationary process can occur along the equilibrium path only if there is a persistent contraction of the money supply. The entrepreneurs are unwilling to shrink the private money supply by retiring previously issued currency. The only option left is to have the government systematically shrinking the supply of its brand to such an extent that the total money supply declines in every period. The proposition shows that this strategy becomes unsustainable at some finite date because the entrepreneurs will take advantage of the deflation engineered by monetary policy to create an ever increasing amount of money. The main implication of this 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 deflation process when the public is willing to hold private currencies. Recall that there is nothing intrinsically superior about government money from the perspective of the agents. For example, we are not assuming that the government forces agents to pay their taxes in its own currency.

The proposition does not rule out the existence of equilibria with a positive real return on money. It simply says that an equilibrium with a positive real return on money *and* positively valued private currencies cannot exist under a money-growth rule in the presence of profit-maximizing entrepreneurs. A corollary of Proposition 7 is that the socially optimal return on money can be implemented through a money-growth rule only if agents do not value privately-issued currency. In particular, we can construct equilibria with the property $\phi_t^i = 0$ for all $i \in \{1, \dots, N\}$ and $\phi_t^{N+1} > 0$ at all dates $t \geq 0$. In these equilibria, the sequence

of returns satisfies, for all dates

$$z(\gamma_{t+1}) = (1 + \omega) z(\gamma_t) \gamma_t. \quad (13)$$

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

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

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

If we let $\omega \rightarrow \beta - 1$, the associated steady state delivers an efficient allocation (i.e., $q(\omega) \rightarrow q^*$ as $\omega \rightarrow \beta - 1$). 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 previous results, we develop an alternative policy rule that can *uniquely* implement the socially optimal return on money. This outcome will require government money to drive private money out of the economy.

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

$$\phi_t^{N+1} \bar{M}_t^{N+1} = m \quad (14)$$

at all dates for some target value $m > 0$. This means that the government adjusts the sequence $\{\Delta_t^{N+1}\}_{t=0}^{\infty}$ to satisfy (14) in every period.

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

$$m + \sum_{i=1}^N \phi_t^i M_t^i = z(\gamma_{t+1})$$

at all dates. The law of motion for the supply of each private currency gives us

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

Then, we can rewrite the market-clearing condition as

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

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. In addition, the real return on money must satisfy

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

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

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

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

Because $\gamma_t > 1$ must hold at all dates, we get, for any valued currency in every period:

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

This means that the price sequence $\{\phi_t^i\}_{t=0}^\infty$ is strictly increasing. Following the same reason-

ing as in previous propositions, we can show that $\{\phi_t^i\}_{t=0}^\infty$ is an unbounded sequence.

Suppose the cost function $c : \mathbb{R}_+ \rightarrow \mathbb{R}_+$ is strictly convex with $c'(0) = 0$. Then, the first-order condition for the profit-maximization problem implies $\phi_t^i = c'(\Delta_t^{*,i})$, which means that the profit-maximizing choice $\Delta_t^{*,i}$ is strictly increasing in ϕ_t^i . As a result, there exists a finite date such that

$$\sum_{i=1}^N \Delta_T^{*,i} c'(\Delta_T^{*,i}) > \Gamma(m),$$

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

Suppose the cost function $c : \mathbb{R}_+ \rightarrow \mathbb{R}_+$ is locally linear around the origin. Because $c(0) = 0$, there exist scalars $\Delta' > 0$ and $k > 0$ such that $c(\Delta) = k\Delta$ 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 $\{\phi_t^i\}_{t=0}^\infty$ 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 $c : \mathbb{R}_+ \rightarrow \mathbb{R}_+$ is linear. Then, there is $k > 0$ such that $c(\Delta) = k\Delta$ for all $\Delta \geq 0$. Because $\{\phi_t^i\}_{t=0}^\infty$ 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 $z^{-1}(m) > 1$ and $\beta z^{-1}(m)m \leq w(q^*)$. When we set the value of private currencies to zero, we obtain the equilibrium trajectory $\gamma_t = z^{-1}(m)$ at all dates $t \geq 0$. This trajectory satisfies the other boundary condition because $\beta z^{-1}(m)m \leq w(q^*)$. ■

Proposition 7 shows that, under a money-growth rule, there is no equilibrium with a positive real return on money and positively valued private monies. But this result does not rule out the existence of equilibria with a negative real return on money and valued private monies. Proposition 8 provides a stronger result. Specifically, it shows that an equilibrium with valued private monies does not exist when the government follows a policy rule that pegs the real value of government money, provided that the target value is sufficiently large.

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. By credibly guaranteeing the real value of money balances, the government can uniquely implement an allocation with a positive real return on money by driving private monies out of the economy.

Another interpretation of Proposition 8 is that unique implementation requires the provision of “good” government money. Pegging the real value of government money can be viewed as providing good money to support exchange in the economy. 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, the real return on money must be strictly positive in any allocation that can be uniquely implemented under the previously described policy regime. Furthermore, private money creation is a socially wasteful activity. Thus, an immediate societal benefit of a policy that drives private money out of the economy is to prevent the wasteful creation of tokens in the private sector.

An important corollary from Proposition 8 is that one can uniquely implement the socially optimal return on money by taking the limit

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

Hence, the surplus-maximizing quantity q^* is traded in each bilateral meeting in the DM.

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

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

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

If the initial endowment of government money is zero, then the government needs to mint an initial amount of tokens so that it can systematically shrink the available supply

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

In conclusion: the joint goal of monetary stability and efficiency can be achieved by public policy provided the government can tax private agents to guarantee a sufficiently large value of its money supply. 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 can drive private money out of the economy by pegging the real value of its currency brand. The entrepreneurs' profit-maximizing behavior played a central role in the construction of the results. In this section, we show that this policy rule is, nevertheless, robust to other forms of private money, such as those issued by automata, a closer description of the protocols behind some cryptocurrencies.

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 $j \in \{1, \dots, J\}$ and let $\mathbf{h}_t \in \mathbb{R}_+^J$ denote the vector of real values. If the units issued by automaton j are valued in equilibrium, we must have

$$\frac{\phi_{t+1}^j}{\phi_t^j} = \gamma_{t+1} \quad (15)$$

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

$$h_t^j = h_{t-1}^j \gamma_t \quad (16)$$

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

$$m + \sum_{j=1}^J h_t^j = z(\gamma_{t+1}). \quad (17)$$

for all $t \geq 0$. Given these conditions, we can 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 $\{\mathbf{h}_t, \gamma_t, \Delta_t^{N+1}, \tau_t\}_{t=0}^{\infty}$ satisfying (11), (14), (16), (17), $h_t^j \geq 0$, $z(\gamma_t) \geq m$, and $\beta\gamma_t z(\gamma_t) \leq w(q^*)$ for all $t \geq 0$ and $j \in \{1, \dots, J\}$.*

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 $z^{-1}(m) > 1$ and $\beta z^{-1}(m)m \leq w(q^*)$. In this equilibrium, government money drives private money out of the economy.*

Proof. Condition (16) implies $\sum_{j=1}^J h_t^j = \gamma_t \sum_{j=1}^J h_{t-1}^j$. Using the market-clearing condition (17), we find that the dynamic system governing the evolution of the real return on money is given by

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

with boundary conditions $z(\gamma_t) \geq m$ and $\beta\gamma_t z(\gamma_t) \leq w(q^*)$ 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 exists 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 $z(\gamma_{t+1}) - m = \gamma_t [z(\gamma_t) - m]$, together with the boundary conditions $z(\gamma_t) \geq m$ and $\beta\gamma_t z(\gamma_t) \leq w(q^*)$.

We want to show that the properties of the dynamic system depend on the value of the policy parameter m . Precisely, the previously described system is a *transcritical bifurcation*.¹³ To illustrate this property, it is helpful to consider the functional forms $u(q) = (1 - \eta)^{-1} q^{1-\eta}$

¹³In 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 $w(q) = (1 + \alpha)^{-1} q^{1+\alpha}$, with $0 < \eta < 1$ and $\alpha \geq 0$. In this case, the equilibrium evolution of the real return on money satisfies the conditions

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

with

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

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.

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

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

and the boundary condition

$$\frac{m}{\beta} \leq \gamma_t \leq \frac{1}{\beta}. \quad (21)$$

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.

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

value of money declines monotonically to the lower bound m and government money drives private money out of the economy.

If $m = \beta$, the unique steady state is $\gamma_t = 1$ for all $t \geq 0$. In this case, the 45-degree line is the tangent line to the graph of (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 a sustained deflation to ensure that the real return on money remains above one. To implement a sustained deflation, the government must contract its money supply, a policy financed through taxation.

7 Productive Capital

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

7.1 Profit-maximizing entrepreneurs

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

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

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 $j \in \{1, \dots, N\}$. 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 $j \in \{1, \dots, J\}$, we have the budget constraint

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

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

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

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

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

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

Given these changes in the environment, we must 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 $j \in \{1, \dots, J\}$.*

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

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

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

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

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 $\gamma_t \in [0, \beta^{-1}]$ 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 must satisfy

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

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, we further simplify the dynamic system by assuming that $\eta = \frac{1}{2}$ and $\alpha = 0$. In addition, we take the limit $\sigma \rightarrow 1$. 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 $[0, \beta^{-1}]$ 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 $0 = g(\sqrt{\beta^{-1}\hat{\kappa}})$, 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 $\hat{\kappa} \rightarrow \frac{1-\beta}{\beta}$, 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 Network Effects

Many discussions of currency competition highlight the importance of network effects in the use of currencies. See, for example, [Halaburda and Sarvary \(2015\)](#). To evaluate these network effects, let us consider a version of the baseline model in which the economy consists of a countable infinity of identical locations indexed by $j \in \{\dots, -2, -1, 0, 1, 2, \dots\}$. Each location contains a $[0, 1]$ -continuum of buyers and a $[0, 1]$ -continuum of sellers. For simplicity, we remove the entrepreneurs from the model and assume that in each location j there is a fixed supply of N types of tokens, as in the previous section. All agents have the same preferences and technologies as previously described. In addition, we take the limit $\sigma \rightarrow 1$ so that each buyer is randomly matched with a seller with probability one and vice versa.

The main change from the baseline model is that sellers move randomly across locations. Suppose that a fraction $1 - \delta$ of sellers in each location j is randomly selected to move to location $j + 1$ at each date $t \geq 0$. Assume that the seller's relocation status is publicly revealed at the beginning of the decentralized market and that the actual relocation occurs after the decentralized market closes.

Suppose that each location j starts with $M^i > 0$ units of "locally issued" currency $i \in$

$\{1, \dots, N\}$. We start by showing the existence of a symmetric and stationary equilibrium with the property that currency issued by an entrepreneur in location j circulates only in that location. In this equilibrium, a seller who finds out he is going to be relocated from location j to $j + 1$ does not produce the DM good for the buyer in exchange for local currency because he believes that currency issued in location j will not be valued in location $j + 1$. This belief can be self-fulfilling so that currency issued in location j circulates only in that location. In this case, the optimal portfolio choice implies the first-order condition

$$\delta \frac{u'(q(\mathbf{M}_t, t))}{w'(q(\mathbf{M}_t, t))} + 1 - \delta = \frac{1}{\beta \gamma_{t+1}^i}$$

for each currency i . Note that we have suppressed any superscript or subscript indicating the agent's location, given that we restrict attention to symmetric equilibria. Define $L_\delta : \mathbb{R}_+ \rightarrow \mathbb{R}_+$ by

$$L_\delta(A) = \begin{cases} \delta \frac{u'(w^{-1}(\beta A))}{w'(w^{-1}(\beta A))} + 1 - \delta & \text{if } A < \beta^{-1}w(q^*) \\ 1 & \text{if } A \geq \beta^{-1}w(q^*). \end{cases}$$

Then, the demand for real balances in each location is given by

$$z(\gamma_{t+1}; \delta) \equiv \frac{1}{\gamma_{t+1}} L_\delta^{-1} \left(\frac{1}{\beta \gamma_{t+1}} \right),$$

where γ_{t+1} denotes the common rate of return on money in a given location. Because the market-clearing condition implies

$$\sum_{i=1}^N \phi_t^i M^i = z(\gamma_{t+1}; \delta),$$

the equilibrium sequence $\{\gamma_t\}_{t=0}^\infty$ satisfies the law of motion

$$z(\gamma_{t+1}; \delta) = \gamma_t z(\gamma_t; \delta)$$

and the boundary condition $\beta \gamma_t z(\gamma_t; \delta) \leq w(q^*)$.

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, the dynamic system describing the equilibrium evolution of γ_t is given by

$$\frac{\gamma_{t+1}^{\frac{1+\alpha}{\eta+\alpha}-1}}{[1 - (1 - \delta) \beta \gamma_{t+1}]^{\frac{1+\alpha}{\eta+\alpha}}} = \frac{\gamma_t^{\frac{1+\alpha}{\eta+\alpha}}}{[1 - (1 - \delta) \beta \gamma_t]^{\frac{1+\alpha}{\eta+\alpha}}}. \quad (26)$$

The following proposition establishes the existence of a stationary equilibrium with the prop-

erty that privately-issued currencies circulate locally.

Proposition 11 *Suppose $u(q) = (1 - \eta)^{-1} q^{1-\eta}$ and $w(q) = (1 + \alpha)^{-1} q^{1+\alpha}$, with $0 < \eta < 1$ and $\alpha \geq 0$. There exists a stationary equilibrium with the property that the quantity traded in the DM is given by $\hat{q}(\delta) \in (0, q^*)$ satisfying*

$$\delta \frac{u'(\hat{q}(\delta))}{w'(\hat{q}(\delta))} + 1 - \delta = \beta^{-1}. \quad (27)$$

In addition, $\hat{q}(\delta)$ is strictly increasing in δ .

Proof. It is easy to show that the sequence $\gamma_t = 1$ for all $t \geq 0$ satisfies (26). Then, the solution to the optimal portfolio problem implies that the DM output must satisfy (27). Because the term $u'(q)/w'(q)$ is strictly decreasing in q , it follows that the solution $\hat{q}(\delta)$ to (27) must be strictly increasing in δ . ■

This stationary allocation is associated with price stability across all locations, but production in the DM occurs only in a fraction $\delta \in (0, 1)$ of all bilateral meetings. Only a seller who is not going to be relocated is willing to produce the DM good in exchange for locally issued currency. A seller who finds out he is going to be relocated does not produce in the DM because the buyer can only offer him currencies that are not valued in other locations.

Now we construct an equilibrium in which the currency initially issued by an entrepreneur in location j circulates in other locations. In a symmetric equilibrium, the same amount of type- i currency that flowed from location j to $j+1$ in the previous period flowed into location j as relocated sellers moved across locations. As a result, we can construct an equilibrium with the property that all sellers in a given location accept locally issued currency because they believe that these currencies will be valued in other locations.

The optimal portfolio choice implies the first-order condition

$$\frac{u'(q(\mathbf{M}_t, t))}{w'(q(\mathbf{M}_t, t))} = \frac{1}{\beta\gamma_{t+1}^i}$$

for each currency i . Then, the demand for real balances in each location is given by

$$z(\gamma_{t+1}; 1) = \frac{1}{\gamma_{t+1}} L_1^{-1} \left(\frac{1}{\beta\gamma_{t+1}} \right).$$

Because the market-clearing condition implies

$$\sum_{i=1}^N \phi_t^i M^i = z(\gamma_{t+1}; 1),$$

the equilibrium sequence $\{\gamma_t\}_{t=0}^\infty$ satisfies the law of motion

$$z(\gamma_{t+1}; 1) = \gamma_t z(\gamma_t; 1)$$

and the boundary condition $\beta \gamma_t z(\gamma_t; 1) \leq w(q^*)$.

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, the dynamic system describing the equilibrium evolution of γ_t is

$$\gamma_{t+1}^{\frac{1+\alpha}{\eta+\alpha}-1} = \gamma_t^{\frac{1+\alpha}{\eta+\alpha}}. \quad (28)$$

The following proposition establishes the existence of a stationary equilibrium with the property that locally issued currencies circulate in several locations.

Proposition 12 *Suppose $u(q) = (1 - \eta)^{-1} q^{1-\eta}$ and $w(q) = (1 + \alpha)^{-1} q^{1+\alpha}$, with $0 < \eta < 1$ and $\alpha \geq 0$. There exists a stationary equilibrium with the property that the quantity traded in the DM is given by $\hat{q}(1) \in (\hat{q}(\delta), q^*)$ satisfying*

$$\frac{u'(\hat{q}(1))}{w'(\hat{q}(1))} = \beta^{-1}. \quad (29)$$

Proof. It is easy to see that the sequence $\gamma_t = 1$ for all $t \geq 0$ satisfies (28). Then, the solution to the optimal portfolio problem implies that the DM output must satisfy (29). The quantities \bar{q} and $\hat{q}(\delta)$ satisfy

$$\frac{u'(\hat{q}(1))}{w'(\hat{q}(1))} = \delta \frac{u'(\hat{q}(\delta))}{w'(\hat{q}(\delta))} + 1 - \delta.$$

Because $\delta \in (0, 1)$, we must have $\hat{q}(1) > \hat{q}(\delta)$ as claimed. ■

Because $\hat{q}(1) > \hat{q}(\delta)$, the allocation associated with the global circulation of private currencies Pareto dominates the allocation associated with the local circulation of private currencies. Therefore, network effects can be relevant for the welfare properties of equilibrium allocations in the presence of competing monies.

9 Conclusions

In this paper, we have shown how a system of competing private currencies can work. Our evaluation of such a system is nuanced. While we offer glimpses of hope for it by proving the existence of stationary equilibria that deliver price stability, there are plenty of other less desirable equilibria. And even the best equilibrium does not deliver the socially optimum

amount of money. At this stage, we do not have any argument to forecast the empirical likelihood of each of these equilibria. Furthermore, we have shown that currency competition can be a socially wasteful activity.

Our analysis has also shown that the presence of privately-issued currencies can create problems for 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.

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

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

References

- ANDOLFATTO, D., A. BERENTSEN, AND C. WALLER (2016): “Monetary policy with asset-backed money,” *Journal of Economic Theory*, 164, 166–186.
- ANTONOPOULOS, A. M. (2015): *Mastering Bitcoin*. O’Reilly.
- ARAUJO, L., AND B. CAMARGO (2008): “Endogenous supply of fiat money,” *Journal of Economic Theory*, 142(1), 48–72.
- ARUOBA, S., G. ROCHETEAU, AND C. WALLER (2007): “Bargaining and the value of money,” *Journal of Monetary Economics*, 54(8), 2636–2655.
- BERENTSEN, A. (2006): “On the private provision of fiat currency,” *European Economic Review*, 50(7), 1683–1698.
- BÖHME, R., N. CHRISTIN, B. EDELMAN, AND T. MOORE (2015): “Bitcoin: economics, technology, and governance,” *Journal of Economic Perspectives*, 29(2), 213–38.
- CAVALCANTI, R. D. O., A. EROSA, AND T. TEMZELIDES (1999): “Private money and reserve management in a random-matching model,” *Journal of Political Economy*, 107(5), 929–945.
- (2005): “Liquidity, money creation and destruction, and the returns to banking,” *International Economic Review*, 46(2), 675–706.
- CAVALCANTI, R. D. O., AND N. WALLACE (1999): “Inside and outside money as alternative media of exchange,” *Journal of Money, Credit and Banking*, 31(3), 443–57.
- CHIU, J., AND T.-N. WONG (2014): “E-Money: efficiency, stability and optimal policy,” Staff Working Papers 14-16, Bank of Canada.
- CHUEN, D. L. K. (2015): *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*. Elsevier.
- DANG, T. V., G. GORTON, B. HOLMSTRÖM, AND G. ORDOÑEZ (2014): “Banks as secret keepers,” Working Paper 20255, National Bureau of Economic Research.
- FRIEDMAN, M. (1960): *A Program for Monetary Stability*. Fordham University Press.
- (1969): “The optimum quantity of money,” in *The Optimum Quantity of Money and Other Essays*. Aldine Publishing Company.

- FRIEDMAN, M., AND A. J. SCHWARTZ (1986): “Has government any role in money?,” *Journal of Monetary Economics*, 17(1), 37–62.
- GEROMICHALOS, A., AND L. HERRENBRUECK (2016): “The strategic determination of the supply of liquid assets,” MPRA Working Papers 71454.
- GORTON, G. (1989): “An Introduction to Van Court’s Bank Note Reporter and Counterfeit Detector,” Working paper, University of Pennsylvania.
- GRECO, T. H. (2001): *Money: Understanding and Creating Alternatives to Legal Tender*. Chelsea Green Publishing.
- HALABURDA, H., AND M. SARVARY (2015): *Beyond Bitcoin: The Economics of Digital Currencies*. Palgrave Macmillan.
- HAYEK, F. (1999): “The denationalization of money: An analysis of the theory and practice of concurrent currencies,” in *The Collected Works of F.A. Hayek, Good Money, Part 2*, ed. by S. Kresge. The University of Chicago Press.
- HENDRICKSON, J. R., T. L. HOGAN, AND W. J. LUTHER (2016): “The political economy of Bitcoin,” *Economic Inquiry*, 54(2), 925–939.
- HOLMSTRÖM, B., AND J. TIROLE (2011): *Inside and Outside Liquidity*. The MIT Press.
- KAREKEN, J., AND N. WALLACE (1981): “On the indeterminacy of equilibrium exchange rates,” *The Quarterly Journal of Economics*, 96(2), 207–222.
- KLEIN, B. (1974): “The competitive supply of money,” *Journal of Money, Credit and Banking*, 6(4), 423–53.
- LAGOS, R., AND R. WRIGHT (2003): “Dynamics, cycles, and sunspot equilibria in ‘genuinely dynamic, fundamentally disaggregative’ models of money,” *Journal of Economic Theory*, 109(2), 156–171.
- (2005): “A unified framework for monetary theory and policy analysis,” *Journal of Political Economy*, 113(3), 463–484.
- MARTIN, A., AND S. L. SCHREFT (2006): “Currency competition: A partial vindication of Hayek,” *Journal of Monetary Economics*, 53(8), 2085–2111.
- MONNET, C. (2006): “Private versus public money,” *International Economic Review*, 47(3), 951–960.

- NARAYANAN, A., J. BONNEAU, E. FELTEN, A. MILLER, AND S. GOLDFEDER (2016): *Bitcoin and Cryptocurrency Technologies*. Princeton University Press.
- OBSTFELD, M., AND K. ROGOFF (1983): “Speculative hyperinflations in maximizing models: Can we rule them out?,” *Journal of Political Economy*, 91(4), 675–87.
- ROCHETEAU, G. (2012): “The cost of inflation: A mechanism design approach,” *Journal of Economic Theory*, 147(3), 1261–1279.
- SELGIN, G. A., AND L. H. WHITE (1994): “How would the invisible hand handle money?,” *Journal of Economic Literature*, 32(4), 1718–1749.
- SHI, S. (1997): “A divisible search model of fiat money,” *Econometrica*, 65(1), 75–102.
- TULLOCK, G. (1975): “Competing monies,” *Journal of Money, Credit and Banking*, 7(4), 491–97.
- VON ZUR GATHEN, J. (2015): *CryptoSchool*. Springer.
- WALLACE, N. (2001): “Whither monetary economics?,” *International Economic Review*, 42(4), 847–69.
- WHITE, L. H. (1995): *Free Banking in Britain: Theory, Experience and Debate, 1800-1845*. Institute of Economic Affairs, second (revised and extended) edn.
- WILLIAMSON, S. D. (1999): “Private money,” *Journal of Money, Credit and Banking*, 31(3), 469–91.