Can Currency Competition Work?*

Jesús Fernández-Villaverde

University of Pennsylvania, NBER, and CEPR

Daniel Sanches

Federal Reserve Bank of Philadelphia

June 27, 2016

Abstract

Can competition among privately issued fiat currencies such as Bitcoin or Ethereum work? Only sometimes. To show this, we build a model of competition among privately issued fiat currencies. We modify the current 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 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). We thank Ed Green, Todd Keister, Guillermo Ordoñez, George Selgin, Neil Wallace, Randy Wright, 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. Lastly, we also thank the NSF for financial support.

1 Introduction

Can competition among privately issued fiat currencies work? The sudden appearance of Bitcoin, Ethereum, and other cryptocurrencies has triggered a wave of public interest in privately issued monies.[1] A similar interest in the topic has not been seen, perhaps, 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? Will the market provide the socially optimum amount of money? Can private monies and a government-issued money compete? Do private monies require a commodity backing? 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 fiat currencies. We modify the workhorse of monetary economics, the Lagos and Wright (2005) (LW) environment, by including entrepreneurs who can issue their own fiat 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

[1] As of June 29, 2016, besides Bitcoin, three other cryptocurrencies (Etherum, Litecoin, and Ripple) have market capitalizations over $100 million and another fifteen between $10 and $100 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.

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

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

We highlight five of our results. First, we show that, under perfect competition, the existence of a monetary equilibrium consistent with price stability crucially depends on the available technologies. In particular, an equilibrium with stable prices exists only if the cost function associated with the production of private money is locally linear around the origin. If the cost function is strictly convex, then there is no equilibrium consistent with price stability. Thus, Hayek's (1999) vision of a system of private monies competing among themselves to provide a stable means of exchange does not hold in an environment with a strictly convex cost function.

Second, there exists a continuum of equilibrium trajectories with the property that the value of private currencies monotonically converges to zero. This result is intriguing because it shows that the self-fulfilling inflationary episodes highlighted by Obstfeld and Rogoff (1983) and Lagos and Wright (2003) in economies with 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.[3]

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

Fourth, we show that the main features of cryptocurrencies, such as the existence of an upper bound on the available supply, make privately issued money in the form of cryptocurrencies consistent with price stability in a competitive environment, even if the cost function is strictly convex. As a result, a purely private system can deliver price stability under a wide array of preferences and technologies, provided that some limit on the total circulation of private currencies is enforced by an immutable protocol determining the available supply of each currency. This allocation vindicates Hayek's proposal, even though we show that it does not deliver the first best. It also links our research to the literature on the provision of liquidity by productive firms (Holmström and Tirole, 2011, and Dang, Gorton, Holmström, and Ordoñez, 2014).

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

Fifth, when we introduce a government competing with private money, we show that it is impossible for the government to implement an efficient allocation through a money-growth rule if agents value privately issued currencies by holding them in portfolio. Thus, currency competition creates problems for monetary policy implementation under conventional methods. Because the problem of achieving a unique efficient equilibrium remains unresolved under a money-growth rule, we investigate the extent to which the presence of government money can simultaneously promote stability and efficiency under an alternative policy rule. In particular, we study the properties of a policy rule that pegs the real value of government money. Under this alternative regime, we show that it is possible to implement an efficient allocation as the unique global equilibrium, but this requires driving private money out of the economy.

The careful reader might have noticed that we have used the word "entrepreneur" and not the more common "banker" to denote the issuers of private money. We believe 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 in circulation. We will argue that 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).[4]

This previous explanation may also address a second concern of this enlightened reader: 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 more 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.[5] 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

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

[5]We 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).

were of commodity-backed currencies, while most cryptocurrencies are fully fiduciary.

Note that 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 for more details). 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 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).[6] As we mentioned above, our emphasis is different from that in these previous papers, as we depart from modeling banks and their reserve management problem. Our entrepreneurs issue fiat money that cannot be redeemed for any other asset. Our characterization captures the technical features of most cryptocurrencies, which are purely fiat (in fact, since the cryptocurrencies cannot be used to pay taxes in most sovereigns, they are more "fiat" than public monies).

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, Section 4 studies the implications of an exogenous bound on the supply of private currencies. Section 5 studies the interaction between private and government monies and characterizes optimal monetary policy in a competitive environment. Section 6 considers network effects. Section 7 concludes.

[6] See, as well, from a very different methodological perspective, Selgin and White (1994).

2 Model

The economy consists of a large number of buyers and sellers, with a $[0,1]$-continuum of each type, and a finite number of entrepreneurs. Each period is divided into two subperiods. In the first subperiod, all types interact in a centralized market (CM) where a perishable good, referred to as the CM good, is produced and consumed. Buyers and sellers can produce the CM good by using a linear technology that requires effort as input. All agents want to consume the CM good.

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

Entrepreneurs are endowed with a technology to create differentiated tokens, which can take either a physical or an electronic form. Even if the tokens are differentiated (for example, each has a different "seal" or "digital signature"), all of them are intrinsically worthless. Let $c : \mathbb{R}_+ \to \mathbb{R}_+$ denote the cost function associated with minting tokens. Assume that $c : \mathbb{R}_+ \to \mathbb{R}_+$ is strictly increasing and weakly convex, with $c(0) = 0$. 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. This technology will permit entrepreneurs to issue tokens that can circulate as a medium of exchange.

Let us now explicitly describe preferences. Start with a typical buyer. Let $x_t^b \in \mathbb{R}$ denote net consumption of the CM good, and let $q_t \in \mathbb{R}_+$ denote consumption of the DM good. A buyer's preferences are represented by

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

The utility function $u : \mathbb{R}_+ \to \mathbb{R}$ is continuously differentiable, increasing, and strictly concave, with $u'(0) = \infty$ and $u(0) = 0$. Consider now a typical seller. Let $x_t^s \in \mathbb{R}$ denote net consumption of the CM good, and let $n_t \in \mathbb{R}_+$ denote the seller's effort level to produce the DM good. A seller's preferences are represented by

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

Assume that $w : \mathbb{R}_+ \to \mathbb{R}_+$ is continuously differentiable, increasing, and weakly convex, with $w(0) = 0$. Finally, let $x_t^i \in \mathbb{R}_+$ denote entrepreneur i's consumption of the CM good, with $i \in \{1, ..., N\}$. Entrepreneur i has preferences represented by

$$\sum_{t=0}^{\infty} \beta^t x_t^i.$$

The discount factor $\beta \in (0, 1)$ 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. In contrast, an entrepreneur's trading history is publicly observable (i.e., an entrepreneur is endowed with a record-keeping technology that permits him to reveal costlessly his trading history). As we will argue below, public knowledge of an entrepreneur's trading history will permit the circulation of private currencies.

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 currency, with the government following a monetary policy rule (e.g., a money-growth rule). Also, all agents in the economy can observe the money supply at each date. These features allow agents to form beliefs about the exchange value of money in the current and future periods.

We start our analysis by considering the possibility of a purely private monetary arrangement. In particular, we focus on a system in which entrepreneurs issue intrinsically worthless tokens that circulate as a medium of exchange, attaining a strictly positive value. These privately issued currencies are not associated with any promise to exchange them for goods or other assets at some future date. Because the currency issued by an entrepreneur is non-falsifiable and an entrepreneur's trading history is publicly observable, all agents can verify the total amount put into circulation by any individual issuer.

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

individual issuances. In other words, profit maximization in a private money arrangement serves the same purpose as the monetary policy rule in the case of a government monopoly on currency issue. Thus, it is possible to conceive a system in which privately issued currencies can attain a positive exchange value.

We can think of each entrepreneur as issuing a monetary unit with its own brand ("ducats," "florins," ...). In the context of cryptocurrencies, we can re-interpret the entrepreneurs as "miners" and the index $i \in \{1, ..., N\}$ as the name of each cryptocurrency. In that interpretation, and for simplicity, we assume that there is only one miner per cryptocurrency and, hence, entrepreneur i means a miner of cryptocurrency i. 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 tokens as specified by the protocol of each cryptocurrency (we will revisit later the case where the issuing of cryptocurrencies is pinned down by an automaton). But, regardless of the interpretation we give to our framework, let $\phi_t^i \in \mathbb{R}_+$ denote the value of a unit of currency $i \in \{1, ..., N\}$ in terms of the CM good and let $\boldsymbol{\phi}_t = \left(\phi_t^1, ..., \phi_t^N\right) \in \mathbb{R}_+^N$ denote the vector of real prices.

3.1 Buyer

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

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

subject to the budget constraint

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

The vector $\mathbf{M}_t^b \in \mathbb{R}_+^N$ describes the buyer's monetary portfolio after trading in the CM, and $x_t^b \in \mathbb{R}$ denotes net consumption of the CM good. With simple algebra, the value function $W^b\left(\mathbf{M}_{t-1}^b, t\right)$ can be written as

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

with the intercept given by

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

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

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

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

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

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

The standard approach in the search-theoretic literature determines the terms of trade by using Nash bargaining. Lagos and Wright (2005) demonstrate that Nash bargaining can result in a holdup problem, leading to inefficient trading activity in the DM. Aruoba, Rocheteau, and Waller (2007) consider alternative axiomatic bargaining solutions and conclude that the properties of these solutions matter for the efficiency of monetary equilibrium. To avoid inefficiencies arising from the choice of the bargaining protocol, which may complicate the interpretation of the main results in the paper, we assume the buyer makes a take-it-or-leave-it offer to the seller.[7]

With take-it-or-leave-it offers, the buyer chooses the amount of the DM good, represented by $q\in\mathbb{R}_+$, the seller is supposed to produce and the vector of currencies, represented by $\mathbf{d}\in\mathbb{R}_+^N$, to be transferred to the seller to maximize expected surplus in the DM. Formally, the terms of trade $(q,\mathbf{d})$ are determined by solving

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

subject to the seller's participation constraint

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

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

and the buyer's liquidity constraint

$$\mathbf{d} \leq \mathbf{M}_t^b. \tag{1}$$

Let $q^* \in \mathbb{R}_+$ denote the quantity satisfying $u'(q^*) = w'(q^*)$. Note that q^* is the surplus-maximizing quantity determining the efficient level of production in the DM. The solution to the buyer's problem is given by

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

and

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

Note that the solution to the bargaining problem allows us to characterize real expenditures in the DM, given by $\boldsymbol{\phi}_{t+1} \cdot \mathbf{d}\left(\mathbf{M}_t^b, t\right)$, as a function of the buyer's portfolio, with the composition of the basket of currencies transferred to the seller remaining indeterminate.

The indeterminacy of the portfolio of currencies transferred to the seller in the DM is reminiscent of Kareken and Wallace (1981). These authors have established that, in the absence of portfolio restrictions and barriers to trade, the exchange rate between two currencies is indeterminate in a flexible-price economy. In our framework, a similar result holds with respect to privately issued currencies, given the absence of transaction costs when dealing with different currencies. Buyers and sellers do not "prefer" any currency over another and there is a sense in which we can talk about perfect competition among currencies. This allows us to assume that all agents behave parametrically with respect to the sequence of prices $\{\boldsymbol{\phi}_t\}_{t=0}^{\infty}$.[8]

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

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

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

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

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

[8] At the cost of much heavier notation and additional technical conditions, we could redo our analysis with a continuum of entrepreneurs.

The optimal portfolio problem can be defined as

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

The optimal choice, then, satisfies

$$\phi_t^i = \beta \phi_{t+1}^i L\left(\boldsymbol{\phi}_{t+1} \cdot \mathbf{M}_t^b \right) \tag{2}$$

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

$$\lim_{t \to \infty} \beta^t \times \boldsymbol{\phi}_t \cdot \mathbf{M}_t^b = 0, \tag{3}$$

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

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

In 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 $W^s\left(\mathbf{M}_{t-1}^s, t \right)$ 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 $V^s\left(\mathbf{M}_t^s, t \right)$ denote the value function in the DM. The Bellman equation can be written as

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

subject to the budget constraint

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

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

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

Here the vector $\mathbf{M}_t^b \in \mathbb{R}_+^N$ denotes the monetary 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 monetary portfolio, which implies that monetary assets do not bring any additional benefit to the seller in the decentralized market. Consequently, the seller optimally chooses not to hold monetary assets across periods when $\phi_{t+1}^i/\phi_t^i \leq \beta^{-1}$ for all i.

3.3 Entrepreneur

Now we describe the entrepreneur's problem to determine the money supply in the economy. Let us use $M_t^i \in \mathbb{R}_+$ to denote the per-capita supply of currency i in period t. Next, define $\Delta_t^i \in \mathbb{R}$, the entrepreneur i's net circulation of newly issued currency in period t (or the mining of new cryptocurrency), as:

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

except for the initial period where

$$\Delta_0^i = M_0^i.$$

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

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

at each date $t \geq 0$. Here $M_t^{ij} \in \mathbb{R}_+$ denotes entrepreneur i's holdings of currency issued by entrepreneur $j \neq i$. This budget constraint indicates 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 $j \in \{1, ..., N\}$, 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

$$x_t^i = \phi_t^i \Delta_t^i - c\left(\Delta_t^i\right),$$

which just tells us that the entrepreneur's consumption in period t is equal to the real value of the net circulation ($\phi_t^i \Delta_t^i$) minus the cost of minting additional units. Because $x_t^i \geq 0$, we must have, as previously mentioned, $\Delta_t^i \geq 0$. Given that an entrepreneur takes prices $\{\boldsymbol{\phi}_t\}_{t=0}^{\infty}$ as given, $\Delta_t^{*,i} \in \mathbb{R}_+$ solves the profit-maximization problem:

$$\Delta_t^{*,i} \in \arg\max_{\Delta \in \mathbb{R}_+} \left[\phi_t^i \Delta - c\left(\Delta\right)\right]. \tag{4}$$

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 optimal net circulation in period t for all currencies.

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

$$M_0^i = \Delta_0^{*,i} \tag{5}$$

and

$$M_t^i = \Delta_t^{*,i} + M_{t-1}^i \tag{6}$$

at all dates $t \geq 1$.

3.4 Equilibrium

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

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

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

$$\mathbf{M}_t = \mathbf{M}_t^b. \tag{7}$$

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

Definition 1 *A perfect-foresight monetary equilibrium is an array* $\left\{\mathbf{M}_t, \mathbf{M}_t^b, \mathbf{\Delta}_t^*, \boldsymbol{\phi}_t\right\}_{t=0}^{\infty}$ *satisfying (2)-(7) for each* $i \in \{1, ..., N\}$ *at all dates* $t \geq 0$.

In what follows, it is helpful to provide a broad definition of price stability to evaluate the properties of private currencies. We start our analysis by investigating whether a monetary equilibrium consistent with price stability exists in the presence of currency competition. Then, we turn to the welfare properties of equilibrium allocations to investigate whether an efficient allocation can be the outcome of perfect competition in the currency-issuing business.

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

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

for at least one currency i.

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 date $T \geq 0$ such that $\phi_t^i = \bar{\phi}^i > 0$ for each currency i at all dates $t \geq T$.*

A 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 is strictly convex. The following result shows an important implication of this relation.

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

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

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

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

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

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

($\Rightarrow$) Suppose that $\lim_{t\to\infty} \Delta_t^{*,i} = 0$. Then, we must have $\lim_{t\to\infty} \phi_t^i = 0$ to satisfy condition (4) at all dates. ■

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

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

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

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

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

Because $\lim_{t\to\infty} \phi_t^i = \bar{\phi}^i > 0$, there is a date $\hat{T} > 0$ such that $\phi_t^i > 0$ for all $t \geq \hat{T}$. As a result, the sequence $\{M_t^i\}_{t=0}^{\infty}$ is unbounded. Thus, there is a date $T > 0$ such that $\boldsymbol{\phi}_{t+1} \cdot \mathbf{M}_t > \beta^{-1} w(q^*)$ for all $t \geq T$. To be consistent with an optimal portfolio choice, we must have $\phi_t^i = \beta \phi_{t+1}^i$ for all $t > T$. But this implies that the transversality condition (3) is necessarily violated, given that $\{M_t^i\}_{t=0}^{\infty}$ is unbounded. ■

The previous proposition highlights that the main problem of a monetary system with perfectly competitive issuers is that the supply of each brand becomes unbounded when the cost function is strictly convex: 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.

This prediction of the model is in sharp contrast to the conclusions reached in Hayek (1999). Hayek argued that private agents through markets can achieve desirable outcomes, even in the field of money and banking. According to his view, government intervention is not necessary for the establishment of a stable monetary system. The previous proposition formally shows that Hayek's conjecture does not hold in an environment with a strictly convex cost function.

However, it is possible to obtain a stable monetary system when the cost function is weakly convex. In particular, the following result shows that Hayek's conjecture holds when the cost function is locally linear around the origin.

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

Proof. Because $c : \mathbb{R}_+ \to \mathbb{R}_+$ is locally linear with $c(0) = 0$, there is $k > 0$ such that $c(\Delta) = k\Delta$ for all $\Delta \in [0, \Delta']$. Set $\phi_t^i = k$ at all dates $t \geq 0$. Consider the sequence $\left\{\Delta_t^{*,i}\right\}_{t=0}^{\infty}$ with $\Delta_0^{*,i} = \bar{\Delta}^i > 0$ 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 $\bar{\boldsymbol{\Delta}} = \left(\bar{\Delta}^1, ..., \bar{\Delta}^N\right)$ satisfying

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

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

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

provided the neighborhood $[0, \Delta'] \subset \mathbb{R}_+$ is sufficiently large. ■

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. 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. Our analysis finds, therefore, that the type of purely private arrangement initially envisaged by Hayek (1999) can be feasible under certain conditions on technologies.

However, we will show momentarily that other allocations with undesirable properties can also be consistent with the same equilibrium conditions. These equilibria are characterized by the persistently declining purchasing power of private currencies and falling trading activity. There is no reason to forecast that the equilibrium with stable value will prevail over these different equilibria.

Furthermore, even the equilibrium with a stable value of currencies is socially inefficient. 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 equilibrium with stable currencies Pareto dominates all other equilibria in which the value of private currencies declines over time, a purely private monetary system does not provide the socially optimum quantity of money, as defined in Friedman (1969). This insight 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 currency. 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.[9]

Our next step is to characterize nonstationary equilibria with the property that the value of privately issued currencies collapses along the equilibrium path. The following proposition shows that hyperinflationary episodes can be consistent with the equilibrium conditions even

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

if the environment admits an equilibrium with stable prices.

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

Proof. Because $c : \mathbb{R}_+ \to \mathbb{R}_+$ is locally linear in a neighborhood $\left[0, \bar{\Delta}\right] \subset \mathbb{R}_+$, there is $k > 0$ such that $c(\Delta) = k\Delta$ for all $\Delta \in \left[0, \bar{\Delta}\right]$. Set $\phi_0^i = k$. Then, any value $\Delta^i \in \left[0, \bar{\Delta}\right]$ is consistent with profit maximization at date 0. The optimal portfolio choice implies $\phi_{t+1}^i = \gamma_{t+1}\phi_t^i$ at all dates $t \geq 0$, with $\gamma_{t+1} \in \mathbb{R}_+$ representing the common return across all valued monetary assets 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

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

so that

$$\sum\nolimits_{i=1}^{N} b_t^i = \frac{1}{\gamma_{t+1}} L^{-1}\left(\frac{1}{\beta\gamma_{t+1}}\right) \equiv z\left(\gamma_{t+1}\right)$$

provided $\beta\gamma_{t+1}\sum_{i=1}^{N} b_t^i < w(q^*)$. Note that $M_t^i = M_{t-1}^i = \Delta^i$ for each i implies

$$z\left(\gamma_{t+1}\right) = \gamma_t z\left(\gamma_t\right) \tag{8}$$

provided $\beta\gamma_t z(\gamma_t) < w(q^*)$ and $\gamma_t \leq 1$. Since 0 is a fixed point of the implicitly defined mapping (8), it is possible to select an arbitrary initial value $\gamma_1 < 1$ sufficiently small such that the price sequence $\left\{\phi_t^i\right\}_{t=0}^{\infty}$ satisfying $\phi_{t+1}^i = \gamma_{t+1}\phi_t^i$ converges monotonically to zero. ■

For any initial condition within a neighborhood of zero, there exists an associated equilibrium trajectory that is monotonically decreasing. Along this equilibrium path, real money balances decrease monotonically over time and converge to zero, so the equilibrium allocation approaches autarky as $t \to \infty$. The decline in the desired amount of real balances follows from the agent's optimization problem when the value of privately issued currencies persistently depreciates over time (i.e., the anticipated decline in the purchasing power of private money leads agents to reduce their real money balances over time). As a result, trading activity in the decentralized market monotonically declines along the equilibrium trajectory. This property of equilibrium allocations with privately issued currencies implies that private money is inherently unstable in that changes in beliefs can lead to undesirable self-fulfilling inflationary episodes.

The existence of these inflationary equilibrium trajectories in a purely private monetary arrangement implies that hyperinflationary episodes are not an exclusive property of government-issued money. Obstfeld and Rogoff (1983) build economies that can display self-fulfilling inflationary episodes when the government is the sole issuer of currency and follows a money-growth rule. Lagos and Wright (2003) show that search-theoretic monetary models with government-supplied currency can also have self-fulfilling inflationary episodes under a money-growth rule. Our analysis of privately issued currencies shows that self-fulfilling inflationary equilibria can occur in the absence of government currency when private agents enter the currency-issuing business to maximize profits. Thus, replacing government monopoly under a money-growth rule with profit maximization does not overcome the fundamental fragility associated with fiduciary regimes, public or private.

As previously mentioned, the stationary equilibrium with a stable value of private currencies Pareto dominates any nonstationary equilibria, even though that equilibrium does not achieve the first best. To verify this claim, note that the quantity traded in the DM starts from a value below $\hat{q}$ and decreases monotonically in a nonstationary equilibrium. As a result, the allocation in the equilibrium with a stable value of money Pareto dominates the allocation associated with any inflationary equilibrium.

In a later section, we introduce government currency and study the possibility of stabilization policies. As we will see, the set of equilibrium allocations characterized by LW arises as a special case in our analysis. In addition, we will characterize optimal monetary policy in a competitive environment.

4 Limited Supply

In the previous section, entrepreneurs (or "miners") could mint as much new currency as they wanted in each period. However, in reality, the protocol behind most cryptocurrencies sets up an upper bound on the supply of each brand. Motivated by this observation, we extent our model to investigate the consequences of such bounds. In particular, we assume that there is a cap on the amount of each currency that can be mined at each date. Formally, let $\bar{\Delta}_t^i \in \mathbb{R}_+$ denote the date-t cap on currency $i \in \{1, ..., N\}$. In this case, the entrepreneur's profit maximization problem is given by

$$\Delta_t^{*,i} \in \arg \max_{0 \leq \Delta \leq \bar{\Delta}_t^i} \left[\phi_t^i \Delta - c\left(\Delta\right) \right]. \tag{9}$$

Then, we can define a monetary equilibrium in the same way as before by replacing (4) with (9).

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 private currency imposes an upper bound on total circulation, even if the cost function is strictly convex.

Proposition 4 *Suppose* $L(A) + AL'(A) > 0$ *for all* $A > 0$. *Then, there is a class of caps* $\left\{\bar{\mathbf{\Delta}}_t\right\}_{t=0}^{\infty}$ *such that a monetary equilibrium consistent with strong price stability is shown to exist. These caps are such that* $\bar{\Delta}_t^i > 0$ *at dates* $0 \leq t \leq T$ *and* $\bar{\Delta}_t^i = 0$ *at all subsequent dates* $t \geq T+1$, *given a finite date* $T > 0$.

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

$$1 = \beta L\left(\bar{\phi}\sum\nolimits_{i=1}^{N}\sum\nolimits_{\tau=0}^{T}\bar{\Delta}_{\tau}^{i}\right). \tag{10}$$

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

$$\phi_t = \beta\phi_{t+1}L\left(\phi_{t+1}\sum\nolimits_{i=1}^{N}M_t^i\right), \tag{11}$$

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 (11) as

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

As a result, the partial sequence $\{\phi_0, ..., \phi_T\}$ can be obtained from (11), given the exogenous caps $\bar{\mathbf{\Delta}} = \left\{\bar{\Delta}_0^i, \bar{\Delta}_1^i, ..., \bar{\Delta}_T^i\right\}_{i=1}^{N}$.

The final step in the proof is to select each cap $\bar{\Delta}_t^i$ in such a way that it is consistent with profit maximization at the price ϕ_t. Note that (10) 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

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

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

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

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

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

Because $L(A) + AL'(A) > 0$ 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, we conclude that every element in the sequence $\{\phi_0, ..., \phi_T\}$ satisfying (11) is strictly decreasing in $\bar{\Delta}_t^i$ for any $0 \leq t \leq T$. Then, it is possible to select a sufficiently low value for the caps $\left\{\bar{\Delta}_0^i, \bar{\Delta}_1^i, ..., \bar{\Delta}_T^i\right\}_{i=1}^N$ such that the constraint $\Delta \leq \bar{\Delta}_t^i$ in the optimization problem on the right-hand side of (9) is binding. In this case, we have $\Delta_t^{*,i} = \bar{\Delta}_t^i$ at all dates. ■

In the previously described allocation, the value of money and trading activity stabilize after date T. Thus, it is possible to have price stability with a strictly convex cost function when the protocol behind cryptocurrencies limits the amount of each privately issued currency. In this respect, the innovations associated with cryptocurrencies and their immutable protocols provide an effective mechanism to make a purely private arrangement consistent with price stability in the absence of government intervention.[10]

Although the existence of an upper bound on currency issue promotes price stability in a competitive environment, it does not imply efficiency. The previously made arguments regarding the reasons for not achieving efficiency through a market arrangement continue to hold even if innovations in the field of computer sciences permit the creation of exogenous bounds on the supply of private currencies. Motivated by this observation, we turn to the study of optimal monetary policy in a competitive environment.

5 Monetary Policy

In this section, we characterize optimal monetary policy by the government in the presence of privately issued currencies. Recall that a central result that we derived above was that there is no efficient equilibrium under a purely private arrangement. In our framework, an efficient allocation is implemented when the real rate of return on money is equal to the rate of time preference and the competition process did not provide the incentives to deliver such real rate of return. In what follows, we want to investigate whether it is possible to implement the socially efficient real return on money by introducing government money.

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

Suppose the government enters the currency-issuing business by creating its own brand, referred to as currency $N+1$. Without loss of generality, we assume that there is no cost to issue additional units of government currency. In this case, the government budget constraint is given by

$$\phi_t^{N+1}\Delta_t^{N+1} + \tau_t = 0, \tag{12}$$

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.[11] What makes government money fundamentally different from private money is that behind the government brand there is a fiscal authority with the power to tax agents in the economy. Government money follows the law of motion

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

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

The definition of equilibrium in the presence of government money is the same as before except that now the vectors $\mathbf{M}_t$, $\mathbf{M}_t^b$, and $\boldsymbol{\phi}_t$ are elements in $\mathbb{R}_+^{N+1}$ and the scalar sequence $\left\{\Delta_t^{N+1}\right\}_{t=0}^{\infty}$ is exogenously given. In addition, we need to include the sequence of lump-sum taxes $\{\tau_t\}_{t=0}^{\infty}$ and require that (12) holds at all dates.

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 assumption.

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

Given this assumption, $L(A)$ is invertible in the range $\left(0, \beta^{-1}w(q^*)\right)$ so that we can define

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

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

In any equilibrium with valued government money, we must have

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

[11] With positive minting costs, we could think about these lump-sum taxes as being net of these costs. Given the results that we will derive below, nothing is lost by ignoring these costs. In particular, we will *not* argue that a goverment money derives any its possible advantages from the absence of minting costs.

at all dates $t \geq 0$. 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 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 studied in this section. The following proposition shows that it is impossible to have a monetary equilibrium with a constant positive real return on money and positively valued privately issued money.

Proposition 5 *Suppose that $c : \mathbb{R}_+ \to \mathbb{R}_+$ is strictly convex. There is no equilibrium with the properties that (i) at least one private currency is valued and (ii) the real return on money is positive and constant.*

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

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

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

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

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

$$z\left(\gamma_{t+1}\right) - \gamma_t z\left(\gamma_t\right) = \sum\nolimits_{i=1}^{N} \Delta_t^{*,i} c'\left(\Delta_t^{*,i}\right) + \phi_t^{N+1} \Delta_t^{N+1}. \tag{13}$$

Consider a policy rule $\omega \geq 0$. Then, we have $\Delta_t^{N+1} \geq 0$ at all dates. As we have seen, $\Delta_t^{*,i} > 0$ when $\phi_t^i > 0$, given that the cost function is strictly convex. Suppose that $\gamma_t = \bar{\gamma} > 1$ at all dates. Then, the left-hand side of (13) is strictly negative. Because $\Delta_t^{*,i} > 0$ for each $i \in \{1, ..., N\}$ and $\Delta_t^{N+1} \geq 0$, (13) is violated when $\gamma_t = \bar{\gamma} > 1$ at all dates. Thus, we cannot have an equilibrium with a positive real return on money when $\omega > 0$.

Consider a policy rule ω in the interval $(\beta - 1, 0)$. Then, we have $\Delta_t^{N+1} < 0$ in every period. Suppose that $\gamma_t = \bar{\gamma} > 1$ at all dates. In this case, any valued currency must satisfy $\phi_{t+1}^i = \bar{\gamma}\phi_t^i$ at all dates. Because $\bar{\gamma} > 1$, the sequence $\left\{\Delta_t^{*,i}\right\}_{t=0}^{\infty}$ is strictly increasing and unbounded. A monetary equilibrium with $\gamma_t = \bar{\gamma} > 1$ at all dates can exist only if $\phi_t^{N+1} M_t^{N+1}$ is strictly decreasing. Because the sequence $\left\{\phi_t^{N+1}\right\}_{t=0}^{\infty}$ grows at the constant rate $\bar{\gamma} > 1$, the government money supply sequence $\left\{M_t^{N+1}\right\}_{t=0}^{\infty}$ must decrease at a faster rate so that the real value of government money $\phi_t^{N+1} M_t^{N+1}$ is strictly decreasing. Because the real value of government money is bounded below by zero and the real value of all privately issued currencies is unbounded, we cannot have an equilibrium with a positive real return on money when $\omega \in (\beta - 1, 0)$. ■

The intuition for this result is straightforward. A positive and constant real rate of return of money is not compatible with (weakly) positive issuance of private monies. Entrepreneurs would need to retire currency from circulation, which is unfeasible for them, in order to generate that positive and constant real rate of return. This result is a close relative of the idea that competition cannot deliver the socially optimum amount of money (which requires a positive and constant real rate of return of money), but with three important strengthenings. First, the lack of equilibrium with positively value private currencies is for *any* positive and constant real rate of return of money (regardless of whether this rate induces the optimal allocation). Second, the proposition allows for the existence of equilibria with positive and constant real rate of return of money, just not equilibria with positively valued private currencies. Third, the proposition does not rule out equilibria where private money is valued, but government money is not. 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).

In fact, the previous proposition implies that an efficient allocation, where the real return on money to be equal to the rate of time preference, 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 $i \in \{1, ..., N\}$ and $\phi_t^{N+1} > 0$ at all dates $t \geq 0$. In these equilibria, the sequence of returns satisfies, for all dates

$$z\left(\gamma_{t+1}\right) = (1 + \omega)\, z\left(\gamma_t\right) \gamma_t. \tag{14}$$

The dynamic properties of the system (14) are exactly the same as those derived in Lagos and Wright (2003) when preferences and technologies imply a demand function for real balances that is strictly decreasing in the inflation rate.

A policy choice 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 $\omega \to \beta - 1$, the associated steady state delivers an efficient allocation (i.e., $q(\omega) \to q^*$ as $\omega \to \beta - 1$). This policy prescription is the celebrated Friedman rule, which eliminates the opportunity cost of holding money balances in private portfolios 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 allocations characterized by the coexistence of private and government monies, there exists a continuum of suboptimal equilibrium trajectories that are also associated with the Friedman rule. These trajectories involve a persistently declining value of money.

5.2 Pegging the real value of government money

In this section, we develop an alternative monetary policy rule that can implement a *unique* efficient equilibrium allocation. This outcome will be feasible only if the government can tax private agents to finance policy implementation. Also, it will require government money to drive private money out of the economy.

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

$$\phi_t^{N+1} \bar{M}_t^{N+1} = m \tag{15}$$

at all dates for some target value $m > 0$. This means that the government adjusts the sequence $\left\{\Delta_t^{N+1}\right\}_{t=0}^{\infty}$ to satisfy (15) in each period.

The following proposition establishes a central result of our normative analysis of currency competition. It shows that it is possible to select a target value m for government policy that *uniquely* implements an equilibrium with a strictly positive real return on money.

Proposition 6 *Suppose that $c : \mathbb{R}_+ \to \mathbb{R}_+$ is strictly convex. There exists a unique monetary equilibrium characterized by a constant positive real return on money provided the target value m satisfies $z^{-1}(m) > 1$. In this equilibrium, government money drives private money out of the economy*

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

condition implies

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

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

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

Then, we can rewrite the market-clearing condition as

$$z\left(\gamma_{t+1}\right) - m = \sum\nolimits_{i=1}^{N} \Delta_t^{*,i} c'\left(\Delta_t^{*,i}\right) + \gamma_t z\left(\gamma_t\right) - m\gamma_t.$$

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

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

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

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

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

along the equilibrium trajectory because the term $\sum_{i=1}^{N} \Delta_t^{*,i} c'\left(\Delta_t^{*,i}\right)$ is nonnegative. Define the value

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

with the maximization on the right-hand side subject to $z\left(\gamma\right) \geq m$, $z\left(\gamma_+\right) \geq m$, $\beta\gamma z\left(\gamma\right) \leq w\left(q^*\right)$, and $\beta\gamma_+ z\left(\gamma_+\right) \leq w\left(q^*\right)$.

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

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

for any valued currency in every period. This means that the price sequence $\left\{\phi_t^i\right\}_{t=0}^{\infty}$ is strictly increasing and unbounded. As we have seen, the profit-maximizing choice $\Delta_t^{*,i}$ is strictly increasing in ϕ_t^i when the cost function is strictly convex. As a result, there exists a date $T \geq 0$ such that

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

which implies a contradiction. Thus, we cannot have a monetary equilibrium in which privately issued currencies are positively valued when the government sets a target value m such

that $z^{-1}(m) > 1$.

When we set the value of privately issued currencies to zero, we obtain the dynamic system

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

governing the evolution of the real return on government money. In addition, we must have the 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 exits another stationary solution: $\gamma_t = z^{-1}(m)$ at all dates $t \geq 0$. This solution satisfies the boundary conditions provided $\beta z^{-1}(m)\, m \leq w(q^*)$. Because any nonstationary solution necessarily violates at least one boundary condition, the previously described dynamic system has a unique solution satisfying both boundary conditions. ■

An immediate corollary from the previous proposition is that one can uniquely implement an efficient allocation by taking the limit

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

In this case, the surplus-maximizing quantity q^* is traded in each bilateral meeting in the DM. Because the target for the real value of government money has to be sufficiently large to implement the socially optimal real return on money, it follows that government money drives private money out of the economy.

To implement a target value with $z^{-1}(m) > 1$, the government must tax private agents in the CM. To verify this claim, note that the government budget constraint can be written as

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

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

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

at all dates $t \geq 0$. To implement its target value m, the government needs to persistently shrink the money supply by making purchases that exceed its sales in the CM, with the shortfall financed by taxes.

In this section, we have demonstrated that the joint goal of monetary stability and efficiency can be achieved by government policy provided the government is able to tax private agents to guarantee a sufficiently large value of its own money. The only caveat is that the

implementation of an efficient allocation requires government money to drive private money out of the economy.

6 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 $j \in \{..., -2, -1, 0, 1, 2, ...\}$. 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. All agents have the same preferences and technologies as previously described. In addition, we take the limit $\sigma \to 1$ 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. 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

$$\delta \frac{u'\left(q\left(\mathbf{M}_t, t\right)\right)}{w'\left(q\left(\mathbf{M}_t, t\right)\right)} + 1 - \delta = \frac{1}{\beta \gamma^i_{t+1}}$$

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 $L_\delta : \mathbb{R}_+ \to \mathbb{R}_+$ by

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

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

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

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

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

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

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

and the boundary condition $\beta\gamma_{t}z\left(\gamma_{t};\delta\right)\leq w\left(q^{*}\right)$.

Suppose $u\left(q\right)=\left(1-\eta\right)^{-1}q^{1-\eta}$ and $w\left(q\right)=\left(1+\alpha\right)^{-1}q^{1+\alpha}$, with $0<\eta<1$ and $\alpha\geq0$. Then, the dynamic system describing the equilibrium evolution of γ_t is given by

$$\frac{\gamma_{t+1}^{\frac{1+\alpha}{\eta+\alpha}-1}}{\left[1-\left(1-\delta\right)\beta\gamma_{t+1}\right]^{\frac{1+\alpha}{\eta+\alpha}}}=\frac{\gamma_{t}^{\frac{1+\alpha}{\eta+\alpha}}}{\left[1-\left(1-\delta\right)\beta\gamma_{t}\right]^{\frac{1+\alpha}{\eta+\alpha}}}. \tag{16}$$

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

Proposition 7 *Suppose $u\left(q\right)=\left(1-\eta\right)^{-1}q^{1-\eta}$ and $w\left(q\right)=\left(1+\alpha\right)^{-1}q^{1+\alpha}$, with $0<\eta<1$ and $\alpha\geq0$. There exists a stationary equilibrium with the property that the quantity traded in the DM is given by $\hat{q}\left(\delta\right)\in\left(0,q^{*}\right)$ satisfying*

$$\delta\frac{u'\left(\hat{q}\left(\delta\right)\right)}{w'\left(\hat{q}\left(\delta\right)\right)}+1-\delta=\beta^{-1}. \tag{17}$$

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

Proof. It is straightforward to show that the sequence $\gamma_t=1$ for all $t\geq0$ satisfies (16). Then, the solution to the optimal portfolio problem implies that the DM output must satisfy (17). Because the term $u'\left(q\right)/w'\left(q\right)$ is strictly decreasing in q, it follows that the solution $\hat{q}\left(\delta\right)$ to (17) must be strictly increasing in δ. ■

The previously described stationary allocation is associated with price stability across all locations, but production in the DM occurs only in a fraction $\delta\in\left(0,1\right)$ 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 build 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

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

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

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

Because the market-clearing condition implies

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

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

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

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

Suppose $u\left(q\right)=\left(1-\eta\right)^{-1}q^{1-\eta}$ and $w\left(q\right)=\left(1+\alpha\right)^{-1}q^{1+\alpha}$, with $0<\eta<1$ and $\alpha\geq 0$. Then, the dynamic system describing the equilibrium evolution of γ_t is

$$\gamma_{t+1}^{\frac{1+\alpha}{\eta+\alpha}-1}=\gamma_t^{\frac{1+\alpha}{\eta+\alpha}}. \tag{18}$$

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

Proposition 8 *Suppose $u\left(q\right)=\left(1-\eta\right)^{-1}q^{1-\eta}$ and $w\left(q\right)=\left(1+\alpha\right)^{-1}q^{1+\alpha}$, 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*

$$\frac{u'(\hat{q}(1))}{w'(\hat{q}(1))} = \beta^{-1}. \tag{19}$$

Proof. It is straightforward to show that the sequence $\gamma_t = 1$ for all $t \geq 0$ satisfies (18). Then, the solution to the optimal portfolio problem implies that the DM output must satisfy (19). 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. Our analysis in this section shows that the presence of network effects can be relevant for the welfare properties of equilibrium allocations in the presence of competing monies.

7 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 showing 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. Furthermore, at this stage of the research, we do not have any argument to forecast the empirical likelihood of each of these equilibria.

An important finding in this paper is that the main features of cryptocurrencies, such as the existence of an upper bound on the available supply, promote price stability in a competitive environment. Hence, the private system envisaged by Hayek 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 determining the available supply of each currency.

Our analysis has also shown that the presence of privately issued currencies can create problems for monetary policy implementation under a money-growth rule. In view of these difficulties, we have characterized an alternative monetary policy rule that uniquely implements an efficient allocation, even though it requires driving private monies out of the

economy.

We have, nevertheless, just scratched the surface of the study of private currency competition. Many topics, including 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, or the consequences of the lack of enforceability of contracts are some of the avenues for future research that we hope to tackle shortly.

References

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 hovernance," *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. (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.

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*, forthcoming.

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.

Selgin, G. A., and L. H. White (1994): "How would the invisible hand handle money?," *Journal of Economic Literature*, 32(4), 1718–1749.

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.