Deflationary Policy under Digital and Fiat Currency Competition

Adib J. Rahman[†]

February 26, 2018

Abstract

I examine the implications of digital and fiat currency competition on optimal monetary policy according to the Friedman rule (a standard deflationary policy) in a Fernández-Villaverde and Sanches (2016) framework, with no search friction. Consistent with the existing literature, first, I find that monetary equilibrium under a purely private arrangement of digital currencies will not deliver a socially efficient allocation. Second, I place restrictions on the available supply of digital currencies and find that a socially efficient allocation is possible only if the upper bound on digital currency circulation is equal to the rate of time-preference, albeit some degree of government intervention is required to curb the profit-maximizing incentive of the miners. Third, I find that optimal monetary policy at the Friedman rule will be socially inefficient when digital currencies compete with government-issued fiat money. Finally, I show that the Friedman rule is a socially desirable policy only in a purely fiat monetary regime.

JEL Classification: E42, E52.

Keywords: digital currency, monetary policy, Friedman rule, deflation.

[†]Department of Economics, Simon Fraser University, 8888 University Drive, Burnaby, BC V5A 1S6, Canada. E-mail: adib_rahman@sfu.ca. Thanks to David Andolfatto, Kenneth Kasa, Cory Langlais, and Lucas Herrenbrueck for helpful comments and suggestions. In particular, the paper has benefited greatly from the comments of Michele Boldrin, and two anonymous referees.

1. INTRODUCTION

As of January 30, 2018, besides Bitcoin, there are approximately 1500 privately-issued digital currencies in operation with an aggregate market capitalization of roughly $575 billion. Bitcoin dominates the market for digital currencies, as it currently accounts for 33.5 % of the aggregate digital currency market capitalization.[1] Bitcoin or any other privately-issued digital currency (cryptocurrency) for that matter is a money and payment system that uses cryptographic rules in a decentralized manner (has no central authority). It works differently than a conventional (government-issued) money and payment system. Specifically, it is a virtual currency with zero intrinsic value and no legal backing. A Bitcoin blockchain is a distributed public ledger that records the entire history of all the bitcoin transactions. The blockchain is updated, maintained, and kept secure by profit-seeking accountants (miners) who are incentivized through a *proof-of-work* (or *proof-of-stake* in other private digital currencies) mechanism to act in the interests of Bitcoin community (their actions are also publicly observable). All other privately-issued digital currencies work in a similar manner with different instructions from their respective protocols. From the government's standpoint, a private digital currency can be regarded as a foreign currency as the central bank cannot control its supply unlike conventional (government-issued) fiat money.

The seemingly unexpected and rapid circulation of private digital currencies, such as Bitcoin and its competitors (other privately-issued digital currencies such as Etherium, Litecoin, and Ripple) has created a great deal of concern for the government. Some of these concerns are violation of capital controls, ease of certain crimes such as kidnapping and extortion that involve the payment of a ransom, tax evasion, and the sale of illicit drugs (Narayan et al., 2016).[2] In general, the anonymous identity of digital currency account holders and the distance in which transfer of funds can happen made these crimes easier.

Despite the rising public interest in privately-issued digital currencies, the economic literature on digital currencies has remained very thin. Much research on digital currencies in economics has been from a qualitative perspective (see for example, Yermack (2013), Böhme et al. (2015), Chuen (2015)) and only very recently economists have started to formalize the design features of digital currencies in their economic models. Hendrickson et al. (2016) use a monetary model with endogenous search and consumption preferences to show that bitcoin can co-exist with conventional fiat money at multiple equilibria. However, their model

[1] In contrast, at the end of August 2016, Bitcoin accounted for 79.6 % of all digital currency market capitalization when 698 privately-issued digital currencies were in operation. See http://http://coinmarketcap.com/ for the latest statistics and recent trends.

[2] In the case of Silk Road - an online platform for illicit drugs - payments in bitcoins made it difficult for law enforcement to trace the money and identify the participants.

does not include any essential feature of bitcoin that makes it distinct from government fiat money. In a DSGE framework, Barrdear and Kumhof (2016) show that the central bank issuing its own brand of digital currency could stabilize business cycles and potentially raise real GDP.

Other areas of research are concerned with the valuation of digital currencies and their optimal design. Gandal and Halaburda (2014) look at network effects associated with digital currencies and takes on an empirical approach to investigate how such effects are reflected in their relative prices. Huberman et al. (2017) explore the Bitcoin platform from a market design perspective and argue that the elimination of dead-weight loss from monopoly comes at the expense of inefficiencies and congestion in raising revenue and funding the infrastructure. Finally, Chiu and Koeppl (2017) model the "double-spending" incentives of blockchain technology to find negative welfare effects based largely on the inefficient design of Bitcoin in its current form.[3]

This paper mainly contributes to the literature about how privately-issued digital currencies can influence the way monetary policy is conducted. Fernández-Villaverde and Sanches (2016) extend the model of Lagos and Wright (2005) to explore the conditions under which competition among digital and government currencies can achieve price stability. They show that a uniquely determined socially efficient allocation requires government fiat money to drive digital currencies out of the economy. This socially efficient allocation is robust to the introduction of automaton issuers and productive capital. I build on their work and integrate their framework with that of Andolfatto (2013) in which no search frictions are present but renders clear the essential properties of the Lagos and Wright model.

The paper is motivated by Friedman (1969) who famously argued that money should earn a real rate of return equal to the rate of time-preference. When the nominal interest rate is set equal to zero, the "Friedman rule" implies that the optimal monetary policy is contractionary; thereby the standard measure is to engineer a deflation (Andolfatto, 2013). It would be interesting to see how optimal monetary policy at the Friedman rule would be affected in light of the sudden appearance of digital currencies that have the potential to compete with government-issued fiat money.[4] To an extent, the way in which the paper differs from Fernández-Villaverde and Sanches is in its emphasis on whether optimal monetary policy corresponds to an efficient allocation by highlighting the social desirability of the Friedman rule at different monetary regimes. As a result, I abstract away from the search friction

[3] They argue that replacing the consensus protocol of *proof-of-work* with *proof-of-stake* mechanism can significantly improve efficiency of the Bitcoin system.

[4] I say potentially because digital currencies are not established bona fide currencies yet, mainly because of the lack of stability in their valuation rendering them unreliable to serve as a store of value and as a unit of account. Yermack (2013) argues that digital currencies behave like speculative assets rather than actual currencies.

mechanism presented in their model. The quasilinear preferences of individuals in the setup greatly aids in the analytical tractability for the point I wish to make.

Similar to the main findings of Fernández-Villaverde and Sanches, first, I find that a purely private arrangement of digital currencies will not deliver a socially efficient allocation in a competitive environment. Second, the existence of an upper bound on digital currency circulation will deliver a socially efficient allocation if the upper bound is equal to the rate of time-preference. However, the profit-maximizing incentive of the miners will create barriers to meet this condition in practice, unless there is some degree of government regulation enforced on the upper bound within a purely private arrangement. Third, I find that the competitive monetary equilibrium does not implement the efficient allocation when digital currencies and government-issued fiat money co-exist in the economy under a hybrid monetary system. Finally, I show that a competitive monetary equilibrium corresponds to the efficient allocation at the Friedman rule only in a purely fiat monetary regime (with no digital currencies), and in addition, I trace out the locus of allocations one of which constitutes the equilibrium.

The remainder of the paper is structured as follows. Section 2 presents the environment and characterizes the socially efficient allocation. Section 3 characterizes the properties of a purely private arrangement and also studies the consequences of an exogenous upper bound on the supply of privately-issued digital currencies. Section 4 studies the interaction between digital currencies and government-issued fiat money, and describes the implication of monetary policy in a competitive environment. Section 5 shows that only a purely fiat monetary regime can guarantee the social desirability of the Friedman rule. Section 6 concludes.

2. THE ENVIRONMENT

The economy is populated by a continuum of infinitely-lived consumers and producers, distributed uniformly on the unit interval $[0, 1]$, and a finite number of miners. The agents are identical *ex ante*, but may differ *ex post*. Time is discrete; $t = 0, 1, 2, ..., \infty$ and each time period is divided into two subperiods; labelled *day* and *night*. Agents meet in a central location at each subperiod. A perishable good is produced and consumed in each subperiod.

The miners are endowed with a technology and have the ability to issue tokens in electronic form. These tokens are differentiated in the form of branding by many different miners and have no intrinsic value. Nonetheless, these tokens are circulated as a medium of exchange because their authenticity can be verified costlessly as a result of blockchain technology. In addition, these tokens, are not a liability of the issuer, which is one of the most important differences from fiat money. Furthermore, each miner issues its own brand of currency in a central location.

Let $\Delta^j \in \mathbb{R}_+$ denote the production of type-j tokens, with $j \in \{1, ..., N\}$ for an individual miner. Let $i \in [0, 1]$ denote an individual consumer or producer, and let $x_t(i) \in \mathbb{R}$ denote the consumption (production, if negative) of the perishable good in the day at date t. Let $x_t(j) \in \mathbb{R}_+$ denote miner j's consumption (production, if negative) of the day good. All agents want to consume the day good. Following Andolfatto (2013), agents have preferences that are linear in $x_t(i) \in \mathbb{R}$ and in $x_t(j) \in \mathbb{R}_+$. This is the key simplifying assumption in the model. Because this day good is perishable, there are two aggregate resource constraints given by

$$\int x_t(i)di \leqslant 0 \tag{1}$$

for all $t \geqslant 0$, and

$$\sum_{j=1}^{N} x_t(j) \leqslant 0 \tag{2}$$

for all $t \geqslant 0$.

Let $\{c_t(i), y_t(i)\} \in \mathbb{R}^2_+$ denote consumption and production of the night good at date t by individual i. Because this night good is also perishable, there is another aggregate resource constraint given by

$$\int c_t(i)di \leqslant \int y_t(i)di \tag{3}$$

for all $t \geqslant 0$.

In the day subperiod, all agents are in a position to produce or consume the perishable good, however, in the night subperiod, agents discover either a desire to consume, or an ability to produce, or remain idle. This desire/ability (agents type) to consume/produce is determined randomly by an exogenous stochastic process (*i.i.d.* across people and time). These agent types are classified as *consumers*, *producers*, and *nonparticipants*. A miner is a nonparticipant in the night subperiod. The utility associated for being a consumer is given by $u(c)$, where $u'' < 0 < u'$, $u'(0) = \infty$ and $u(0) = 0$. The utility associated for being a producer is given by $h(y)$, where $h' > 0$, $h'' > 0$, $h'(0) < \infty$ and $h(0) = 0$. The utility of nonparticipants is normalized to zero, as they neither have a desire to consume nor an ability to produce.

Let $\pi \in (0, 0.5]$ denote the measure of agents who become either a consumer or a producer, so that $(1-2\pi)$ denotes the measure of nonparticipants. Note that at the individual level, these measures represent probabilities. Hence, the *ex ante* preferences of the agents can be represented as

$$E_0 \sum_{t=0}^{\infty} \beta^t \left\{ x_t(i) + x_t(j) + \pi \left[u(c_{t(i)}) - h(y_{t(i)}) \right] \right\}, \tag{4}$$

where $\beta \in (0,1)$ and there is no discounting across subperiods. The social planner weights all agents equally and maximizes (4) subject to the resource constraints (1), (2), and (3). Since u is strictly concave, all consumers will be allocated the same level of consumption $c \geqslant 0$. Also, since h is strictly convex, all producers will be required to produce the same level of output $y \geqslant 0$. As there is an equal number of consumers and producers, the resource constraint (3) implies $c = y$. Conditional on a given level of output y and given the linearity of utility (for all agents) in x, the *ex ante* welfare is represented by

$$W = \frac{\pi}{(1-\beta)} \left[u(y) - h(y) \right], \tag{5}$$

with $W(0) = W(\bar{y}) = 0$ for some unique $0 < \bar{y} < \infty$. There exists a unique maximum $y^* \in (0, \bar{y})$ from the social planner's first-order condition

$$u'(y^*) = h'(y^*), \tag{6}$$

which yields a socially efficient allocation (x^*, y^*), with x^* satisfying any lottery such that $E_0 x_t(i) = 0$ and $E_0 x_t(j) = 0$ will hold. I refer to y^* as the *first-best* allocation. One can interpret the planner's solution as a type of social credit arrangement in which agents borrow from society when they have a desire to consume and fulfill their debt obligation to society when they have an ability to produce (Andolfatto, 2013).

I impose informational financial frictions that will render money essential. First, I assume that consumers and producers lack commitment, so that all exchanges must be sequentially rational. This assumption particularly rules out the use of coercive lump-sum tax instruments.[5] The miners are assumed to have quasi-commitment because pending transactions

[5] However, the use of distortionary taxes is not ruled out and is therefore abstracted away. See Andolfatto (2010) for an explanation.

requires sufficient consensus in the network. Second, I assume that consumers and producers are anonymous (rules out private debt of individuals), however, a miner's trading history is publicly observable via a costlessly endowed record-keeping technology. This public knowledge of a miner's trading history will allow the circulation of privately-issued digital currencies. Third, I assume that the government can also issue its own brand of fiat currency. Lastly, I restrict trade among individuals and miners to occur in competitive spot markets following Andolfatto (2010).[6]

3. COMPETITIVE MONETARY EQUILIBRIUM UNDER PURELY PRIVATE ARRANGEMENT

In standard monetary models, trade is facilitated in the form of a government-issued fiat currency, with the government following a money-growth rule. Following Fernández-Villaverde and Sanches (2016), I characterize the competitive monetary equilibrium under a purely private monetary arrangement. The money supply in the economy will be determined by the profit-maximizing incentive of the miners. Next, I describe the miner's optimization problem to determine the money supply in the economy.

3.1. *Miners*

To reiterate the issued digital currency is not a liability of the issuer unlike fiat money, and each miner issues its own currency. Let $M_j \in \mathbb{R}_+$ denote the current per-capita supply of currency j, and let $M^b \in \mathbb{R}_+$ denote the total supply of digital currencies in the economy. Let $(\omega_d^i, \omega_n^i) \in \mathbb{R}_+$ denote the value of digital currency j in the day and night, respectively. The digital currency circulation of the tokens issued by miner j is given by

$$\Delta_j = \frac{M_j}{M_j^-},$$

where M_j^- denotes initial money supply of type-j tokens. I assume that miners do not make any explicit promises to exchange their tokens for other interest-bearing assets and redeemable instruments at some future date. Also, I assume that the miners will only hold

[6] Buyers and sellers do not have the ability or the incentive to misrepresent themselves when they meet together for exchange on the spot.

their respective currencies, that is, $M_{jk} = 0$ for all $j \neq k$. Thus, the miner's budget constraint is given by

$$x_j = \omega_j \Delta_j.$$

This means that the miner's consumption is equal to the real value of digital currency circulation, assuming that there is no cost of minting tokens. This costless assumption on minting is clearly unrealistic, but is intended to simplify the analysis. Under perfect competition the miners will take prices as given, and will choose the optimal digital currency circulation, $\Delta_j^* \in \mathbb{R}_+$ by solving the following optimization problem:

$$\Delta_j^* = \arg\max_{\Delta \in \mathbb{R}_+} \omega_j \Delta_j.$$

This optimization problem captures the profit seeking incentive of the miners and draws a relation between digital currency circulation and its real price (inverse of ω_j).

3.2. *The day market*

I assume that individuals do not prefer any digital currency over another, so that there is perfect competition among digital currencies. Let m^{b-} denote an individual's initial portfolio of privately-issued digital currencies at the beginning of the day market; and let $m^b \geqslant 0$ denote the digital or bitcoin money an individual carries forward in the night market. Since all individuals (sans miners) are able to buy or sell output x, the day-market budget constraint is the following:

$$x = \omega_d \left(m^{b-} - m^b \right). \tag{7}$$

Let $D(m^{b-})$ denote the value of beginning the day with m^{b-} units; and let $N(m^b)$ denote the value of entering the night-market with m^b units. Then the two value functions must satisfy the following recursion:

$$D(m^{b-}) \equiv \max_{m^b \geqslant 0} \left\{ \omega_d \left(m^{b-} - m^b \right) + N(m^b) \right\}. \tag{8}$$

Assuming that $N'' < 0 < N'$, the demand for bitcoin money is determined by

$$\omega_d = N'(m^b). \tag{9}$$

Invoking the envelope condition gives us $D'(m^{b-}) = \omega_d$. Furthermore, this implies that the demand for bitcoin money is independent of an individual's initial portfolio holdings m^{b-}, as pointed out in Lagos and Wright (2005) and Andolfatto (2013).

3.3. *The night market*

Suppose an individual carries forward m^b units of bitcoin money in the night market. Because of the stochastic shock induced, an individual will realize whether he is a consumer, a producer, or neither (remain idle). Let $C(m^b)$, $P(m^b)$, and $I(m^b)$ denote the utility value of being a consumer, a producer, or being idle, respectively. It follows that the *ex ante* values of entering the night market satisfies

$$N(m^b) \equiv \pi C(m^b) + \pi P(m^b) + (1 - 2\pi) I(m^b). \tag{10}$$

3.3.1. *Consumers*

In the night market, a consumer holding m^b units of bitcoin money faces the following budget constraint:

$$m^{b+} = m^b - \omega_n^{-1} y,$$

where m^{b+} denotes bitcoin money holdings carried forward into the next period's day market and y denotes the output purchased at night. Assuming that this constraint binds, that is, they spend all their bitcoin money gives us $y = \omega_n m^b$; this yields the following result:

$$C'(m^b) \equiv \omega_n u'(y). \tag{11}$$

3.3.2. *Producers*

In the night market, a producer holding m^b units of bitcoin money faces the following budget constraint:

$$m^{b+} = m^b + \omega_n^{-1} y.$$

Unlike the consumer's constraint, the producer's constraint $m^{b+} \geqslant 0$ will not bind, as there is an incentive to accumulate money holdings. Thus, the producer's choice problem can be stated as

$$P(m^b) \equiv \max_y \left\{-h(y) + \beta D(m^b + \omega_n^{-1} y)\right\}. \tag{12}$$

The supply of output at night is therefore characterized by

$$\omega_n h'(y) = \beta \omega_d^+. \tag{13}$$

Moreover, by the envelope theorem,

$$P'(m^b) = \beta \omega_d^+. \tag{14}$$

An idle agent simple carries his portfolio of bitcoin holdings to the next day. As a result, we have

$$I'(m^b) = \beta\omega_d^+. \tag{15}$$

3.4. *Equilibrium*

First, differentiate (10), and then combine (11), (14), and (15) to obtain

$$N'(m^b) = \omega_n \left[\pi u'(y) + (1-\pi)\, h'(y)\right].$$

Second, substitute away $N'(m^b)$, which when combined with (9) from the day market yields

$$\omega_d = \omega_n \left[\pi u'(y) + (1-\pi)\, h'(y)\right].$$

Third, iterate the above expression by one period and combining with (13) results in

$$\omega_n h'(y) = \beta\omega_n^+ \left[\pi u'(y^+) + (1-\pi)\, h'(y^+)\right].$$

We know that for the consumer, $y = \omega_n m^b$, and the market clearing condition is $m^b = M^b$. Substitute these conditions into the above expression to obtain

$$h'(y) = \left(\frac{\beta}{\Delta_j}\right)\left(\frac{y^+}{y}\right)\left[\pi u'(y^+) + (1-\pi)\, h'(y^+)\right].$$

Finally, by restricting attention to the nondegenerate steady-state $y = y^+ > 0$, the above expression is simplified to

$$u'(y^e) = \pi^{-1}\left[\frac{\Delta_j}{\beta} - 1 + \pi\right] h'(y^e). \tag{16}$$

The monetary equilibrium level of output y^e is characterized by (16) and is expressed as a function of Δ_j and β. Clearly, this does not provide the socially optimum quantity of money.

In particular, we have the following result:

PROPOSITION 1. *Under a purely private monetary arrangement, there is no socially efficient allocation.*

The intuition for this result is as follows. If the economy consists of only digital currencies and no government-issued fiat money, then the profit-maximizing incentive of the miners will lead to an unbounded issuance of tokens (assuming costless production). As the flow of the circulation of tokens increases at an exponential rate, the monetary equilibrium will be farther and farther away from the socially efficient allocation. Since the government cannot control the supply of privately-issued digital currencies, there is no mechanism to achieve a socially desirable equilibrium under perfect competition among digital currencies.

3.5. *Limited Supply of Digital Currency*

Following Fernández-Villaverde and Sanches (2016), I impose restrictions on the supply of each currency issued by miners and once again characterize the monetary equilibrium. This is because, in reality, the protocol behind most digital currencies regulates the circulation of each currency by placing an upper bound on the supply. Also, miners will incur costs such as computer hardware, programming effort, and most importantly electricity for willing to solve a complicated mathematical problem specified by their respective protocols. In addition, computational costs may rise further because the problems become more difficult to keep the blockchain secure (Böhme et al., 2015). This fact suggests that miners may not be issuing tokens at an exponential rate when such production costs are considered. In particular, I assume that there is a cap on the amount of each digital currency that can be "mined".[7]

Let $\bar{\Delta}_j \in \mathbb{R}_+$ denote the cap on each digital currency $j \in \{1, ..., N\}$. Hence, the new optimization problem of the miner is the following:

$$\Delta_j^* = \arg\max_{0 \leqslant \Delta \leqslant \bar{\Delta}_j} \omega_j \Delta.$$

[7] For an explanation of technical terms related to digital currencies see Böhme et al. (2015).

Consequently, the monetary equilibrium is characterized the same way as before in (16), except now that there is an upper bound on the circulation of each digital currency, $\bar{\Delta}_j$.[8] This yields the following result:

PROPOSITION 2. *Under a purely private monetary arrangement, there exists a socially efficient allocation if* $\bar{\Delta}_j = \beta$.

This result tells us that the existence of an upper bound on each currency will provide a socially efficient allocation in a competitive monetary equilibrium, as long as the upper bound on the supply of each currency is equal to the rate of time-preference. Clearly, this condition favours sufficiently patient economies, however, I do not expect this result to hold in practice unless some government regulation of the upper bound on the available supply is put forth. This is because the upper bound on the available supply is expected to be quite large due to the profit-maximizing incentive of the miners. In other words, there is not enough incentive for the miners to deliver a socially efficient allocation even with cost-bearing restrictions on the circulation of digital currencies. To ensure that this result will hold in practice, it has to be the case that $\bar{\Delta}_j < 1$, which implies a contractionary supply of digital currency issued by miners. Therefore, government regulation must be implemented to reduce the growth rate of privately-issued digital currency in order to achieve a socially efficient allocation within a purely private arrangement. Next, I study the role of monetary policy in a hybrid monetary system consisting of digital and government-issued fiat currencies.

4. COMPETITIVE MONETARY EQUILIBRIUM UNDER HYBRID ARRANGEMENT

In this section, I introduce government-issued paper money in the presence of privately-issued digital currencies. I then proceed by describing the monetary policy available at the government's disposal.

[8] In other papers this bound comes from pairwise meetings and devices for monitoring, although imperfectly, money issuers.

4.1. *Monetary Policy*

Let $M^g \in \mathbb{R}_+$ denote the current stock of government-issued fiat money; with $M^{g^-} \in \mathbb{R}_+$ denoting initial stock of government money at the beginning of the day-market. Assume that the supply of government money follows a money-growth rule $M^g = \mu M^{g-}$, with μ denoting the gross rate of money creation. Unlike the total supply of bitcoin money, M^b, the government now has the authority to tax (τ) individuals in the economy at the beginning of each period.[9] Hence, the government budget constraint is given by

$$\tau = (\mu - 1)\, M^{g-}.$$

Following Andolfatto (2013), assume that this tax is paid voluntarily by individuals in the day-market. Also, assume that $\mu \geqslant \beta$ for the existence of equilibrium in the steady-state. Let $(\nu_d, \nu_n) \in \mathbb{R}_+$ denote the value of government money in the day and night, respectively. Define $\psi = \omega + \nu$ as an individual's portfolio of digital and government money holdings, and let $(\psi_d, \psi_n,) \in \mathbb{R}_+$ denote the value of total money in day and night, respectively. Most importantly, the total money supply in the economy is defined by the sum of the total supply of digital currencies and government money shown below

$$M = M^b + M^g. \tag{17}$$

In what follows, the monetary equilibrium will be characterized in a similar fashion to Section 3.

4.2. *The day market*

Let m^{g-} denote an individual's initial government money balances at the beginning of the day market; and let $m^g \geqslant 0$ denote the government money an individual carries forward in the night market. I assume that individuals do not value government money more than digital currencies. From an individual's standpoint, government money just serves as a medium of exchange and is not intrinsically valuable. The new day-market budget constraint is the

[9] Note that the government can only tax the fiat money holders and not the bitcoin money holders or the miners.

following:

$$x = \omega_d \left(m^{b-} - m^b\right) + \nu_d \left(m^{g-} + \tau - m^g\right). \tag{18}$$

Let $D\left(m^{b-}, m^{g-}\right)$ denote the value of beginning the day with m^{b-} and m^{g-} units of bitcoin and government money, respectively; and let $N\left(m^b, m^g\right)$ denote the value of entering the night-market with m^b and m^g units. These two value functions must satisfy the recursive relationship

$$D\left(m^{b-}, m^{g-}\right) \equiv \max_{m^b \geqslant 0, m^g \geqslant 0} \left\{\omega_d \left(m^{b-} - m^b\right) + \nu_d \left(m^{g-} + \tau - m^g\right) + N\left(m^b, m^g\right)\right\}. \tag{19}$$

Assuming for the moment that N is strictly concave in both its arguments, the demand for bitcoin money is given by

$$\omega_d = N_{m^b}, \tag{20}$$

and the demand for government money is given by

$$\nu_d = N_{m^g}. \tag{21}$$

Applying the envelope condition yields $D_{m^{b-}} = \omega_d$ and $D_{m^{g-}} = \nu_d$. This in turn tell us that the demand for total money is independent of an individual's initial bitcoin and government money holdings.

4.3. *The night market*

Suppose now an individual brings m^b units of bitcoin and m^g units of government monies into the night market. It follows that

$$N\left(m^b, m^g\right) \equiv \pi C\left(m^b, m^g\right) + \pi P\left(m^b, m^g\right) + (1-2\pi) I\left(m^b, m^g\right). \tag{22}$$

4.3.1. *Consumers*

In the night market, a consumer now faces the following budget constraint:

$$m^{+} = m - \psi_n^{-1} y,$$

where $m^{+} = m^{b+} + m^{g+}$ and $m = m^{b} + m^{g}$.

Assuming that this constraint binds, the solution to the consumer's choice problem simplifies to $y = \psi_n m$. This yields the following result

$$C_{m^b} = C_{m^g} \equiv \psi_n u'(y). \tag{23}$$

4.3.2. *Producers*

In the night market, a producer now faces the following budget constraint:

$$m^{+} = m + \psi_n^{-1} y.$$

As this constraint does not bind, the producer's choice problem is given by

$$P\left(m^b, m^g\right) \equiv \max_{y, m^{b+} \geqslant 0, m^{g+} \geqslant 0} \left\{-h(y) + D\left(m^b + m^g + \psi_n^{-1} y\right)\right\}. \tag{24}$$

The supply of output at night is therefore characterized by

$$\psi_n h'(y) = \beta \psi_d^{+}. \tag{25}$$

Furthermore, by the envelope theorem,

$$P_{m^b} = P_{m^g} = \beta\psi_d^+. \tag{26}$$

Also, for an idle agent we have

$$I_{m^b} = I_{m^g} = \beta\psi_d^+. \tag{27}$$

4.4. *Equilibrium*

I follow a similar procedure to Section 3 to derive the monetary equilibrium under a hybrid monetary system. First, start by differentiating (22) with respect to m^b and m^g, which gives the following equations:

$$N_{m^b} = \pi C_{m^b} + \pi P_{m^b} + (1 - 2\pi) I_{m^b}, \tag{28}$$

and

$$N_{m^g} = \pi C_{m^g} + \pi P_{m^g} + (1 - 2\pi) I_{m^g}. \tag{29}$$

Second, substitute away N_{m^b} in (28) by combining (20), (23), (26), and (27) to obtain

$$\omega_d = \pi\psi_n u'(y) + \pi\psi_n h'(y) + (1 - 2\pi) \beta\psi_d^+. \tag{30}$$

Also, substitute away N_{m^g} in (29) by combining (21), (23), (26), and (27) to obtain

$$\nu_d = \pi\psi_n u'(y) + \pi\psi_n h'(y) + (1 - 2\pi) \beta\psi_d^+. \tag{31}$$

Third, summing up (30) and (31) yields

$$\psi_d = 2\psi_n \left[\pi u'(y) + (1 - \pi) h'(y)\right].$$

Fourth, iterate the above expression by one period and combining with (25) results in

$$\psi_n h'(y) = 2\beta\psi_n^+ \left[\pi u'(y^+) + (1-\pi)\, h'(y^+)\right].$$

Substituting the solution to the consumer's problem $y = \psi_n m$, and imposing the new market clearing condition $m = M$ yields

$$h'(y) = \left(\frac{2\beta}{\Delta_j + \mu}\right)\left(\frac{y^+}{y}\right)\left[\pi u'(y^+) + (1-\pi)\, h'(y^+)\right].$$

Finally, focusing on the nondegenerate steady-state case, the above expression simplifies to

$$u'(y^e) = \left[\frac{\pi^{-1}}{2}\left(\frac{\Delta_j + \mu}{\beta}\right) + 1 - \pi\right] h'(y^e). \tag{32}$$

The monetary equilibrium level of output y^e is characterized by (32), and is expressed as a function of Δ_j and parameters β and μ. In particular, we have the following result.

PROPOSITION 3. *Under a hybrid monetary arrangement, the competitive monetary equilibrium does not correspond to the efficient allocation at the Friedman rule* ($\mu = \beta$).

This result tells us that a deflationary policy – that is, to operate monetary policy at the Friedman rule – does not implement the *first-best* allocation mentioned in Section 2. In other words, the Friedman rule is not a socially desirable policy in this case. The intuition for this result is as follows. A monetary equilibrium with a positive real return on money requires a contractionary monetary policy in the form of deflation. Because of the profit-maximizing incentive of the miners, the money supply from digital currency is not expected to diminish. The only option left for the government is to systematically shrink its own fiat money supply, so that the total money supply in the economy shrinks. However, as pointed out in Fernández-Villaverde and Sanches, this deflationary policy will soon become infeasible as the government will not be persistently able to deflate its own currency in every period. If we assume that digital currencies are bona fide currencies that are able to compete with government money, then there is no way of achieving a socially efficient allocation with a deflationary policy, unless government money drives digital currencies out of the economy.

PROPOSITION 4. *The effects of monetary policy on the circulation of digital currency and level of output are* $\partial\Delta_j/\partial\mu < 0$ *and* $\partial y/\partial\mu < 0$.

Higher inflation reduces the value of digital currency over time through competition with government money, and assuming a fixed number of goods in the economy; the miners will reduce their issuance of tokens because people's incentive for holding digital currency or even *any* type of money or currency is reduced. Higher inflation also reduces output because individuals will reduce their consumption (production) of the night good in the future. The predictions of Proposition 4 imply that digital currency circulation and output are negatively correlated with government transfer (or tax).

5. COMPETITIVE MONETARY EQUILIBRIUM UNDER PURELY FIAT ARRANGEMENT

In this section, I show that optimal monetary policy according to the Friedman rule is socially efficient only when government-issued fiat money exists in the economy. In a competitive monetary equilibrium, let $C(m)$ and $P(m)$ denote the value of being a consumer and a producer in the night market, respectively. The *ex ante* value of entering the night market with a 50-50 chance of producer/consumer is[10]

$$N(m) = \frac{1}{2}C(m) + \frac{1}{2}P(m). \tag{33}$$

The original setup of consumer and producer optimization problems remains the same as in Andolfatto (2013), and so is not repeated for brevity's sake. The only change from Section 4 is that m^b is equal to 0, and M is equal to M^g (and of course, their implications), that is, there are no bitcoin money holdings so that the total supply of money is now equal to the total supply of government money. Next, I use the following first-order conditions to characterize the competitive monetary equilibrium:

[10] The reader should notice that I have let π from Section 2 equal to 0.5, so that no agents remain idle in this case.

$$C'(m) = v_n u'(y), \tag{34}$$

$$P'(m) = \beta v_d^+, \tag{35}$$

$$v_d = N'(m), \tag{36}$$

$$v_n g'(y) = \beta v_d^+, \tag{37}$$

Differentiate (33) and combine (34) and (35) to obtain

$$N'(m) = \frac{1}{2}\left[v_n u'(y) + \beta v_d^+\right]. \tag{38}$$

Next, substitute away $N'(m)$ with (36) and combine (37) to obtain

$$v_d = \frac{1}{2} v_n \left[u'(y) + g'(y)\right]. \tag{39}$$

Then iterate the above expression by one period and combine (37) to get

$$v_n g'(y) = \frac{\beta}{2} v_n^+ \left[u'(y^+) + g'(y^+)\right]. \tag{40}$$

Since for the consumer, $y = v_n m$, and the market clearing condition is $m = M$, we substitute these conditions into the above expression to obtain

$$g'(y) = \frac{\beta}{2\mu}\left[u'(y^+) + g'(y^+)\right]. \tag{41}$$

This expression is further simplified by imposing the steady-state condition $y = y^+ > 0$ and we obtain

$$u'(y^e) = \left[2\left(\frac{\mu}{\beta}\right) - 1\right] g'(y^e). \tag{42}$$

The market equilibrium level of output y^e is characterized by (42) and is expressed as a function of parameters μ and β. At the Friedman rule ($\mu = \beta$), the competitive monetary equilibrium here corresponds to the *first-best* allocation. In other words, we obtain the following result.

PROPOSITION 5. *Under a purely fiat monetary arrangement, the competitive monetary equilibrium corresponds to the efficient allocation at the Friedman rule.*

This result will hold regardless of whether individuals are sufficiently patient, that is, for all rates of time-preference. In contrast, *Proposition 2* appears to hold for sufficiently patient individuals. Next, I solve for the equilibrium quantity x^e (an often underappreciated exercise for this class of models).

Suppose (x^e, y^e) is the allocation achieved by a competitive monetary equilibrium under the purely fiat monetary regime. I then solve for x^e with the following additional set of equations[11]:

$$x = v_d(z + \tau - m), \tag{43}$$

$$\tau = (\mu - 1)M^-, \tag{44}$$

$$z = \frac{y}{v_n^-} + M^-. \tag{45}$$

First, applying the market clearing condition $m = M$ and substituting away $y = v_n^- M$ from the consumer's problem and combining with (45) gives

$$z = 2M^-. \tag{46}$$

This implies that consumers sell all of their money to producers. Second, at steady-state, $z = z^+$ and $M^+ = M$. This implies that $x = v_d M$. Third, from the market clearing condition we know that $v_n = y/M$ and combining this condition with (37) yields

[11] Equation (43) is of course the new day-market budget with only fiat money in which z denotes an agent's initial money holdings at the beginning of the day market.

$$v_d M = \frac{1}{\beta} y g'(y). \tag{47}$$

Since $x = v_d M$, we obtain

$$x^e = \frac{1}{\beta} y^e g'(y^e). \tag{48}$$

This condition traces out a locus of allocations (x^e, y^e), and one such allocation constitutes the (nondegenerate) competitive equilibrium that depends on the monetary parameter μ in this purely fiat monetary regime.

6. CONCLUSION

In this paper, I build on Fernández-Villaverde and Sanches (2016) and use the methodology in Andolfatto (2013) to explore the consequences of digital and fiat currency competition on optimal monetary policy according to the Friedman rule. First, I find that monetary equilibrium under a purely private arrangement of digital currencies will not deliver a socially efficient allocation. Second, I place restrictions on the available supply of digital currencies and find that a socially efficient allocation is possible only if the upper bound on the available supply of digital currency circulation is equal to the rate of time-preference. However, the profit-maximizing incentive of the miners is unlikely to meet this condition in practice, and for that some form of government regulation needs to be enforced on the upper bound of digital currency circulation within a purely private arrangement. Third, I find that privately-issued currencies will create problems with the implementation of monetary policy under a money-growth rule. This is because the profit-maximizing incentive of the miners will lead to an unabated increase in money supply from the minting of private tokens, and therefore it would be infeasible for the government to run a persistent deflationary policy to shrink the total money supply in the economy. Finally, I show that a competitive monetary equilibrium corresponds to the efficient allocation at the Friedman rule only in a purely fiat regime with no digital currencies.

The baseline model of the paper corroborates some of the key findings in Fernández-Villaverde and Sanches (2016) and provides further insights into the social desirability of the Friedman rule at different monetary regimes that were discussed. Several extensions are possible with the inclusion of interest-bearing assets and redeemable instruments in this

Lagos and Wright framework with no search frictions present. In addition, it can be examined whether the socially efficient and monetary allocations are incentive-feasible in different monetary regimes for patient and impatient economies. Furthermore, heterogeneity of miners with different degrees of market power can be introduced.

References

[1] Andolfatto, D., 2010. Essential interest-bearing money. Journal of Economic Theory. 145, 1495-1507.

[2] Andolfatto, D., 2013. Incentive-feasible deflation. Journal of Monetary Economics. 60, 383-390.

[3] Barrdear, J., Kumhof, M., 2016. The macroeconomics of central bank issued digital currencies. Bank of England Staff Working Paper 605.

[4] Böhme, R., Christin, N., Edelman, B., Moore, T., 2015. Bitcoin: economics, technology, and governance. Journal of Economic Perspectives. 29, 213-238.

[5] Chiu, J., Koeppl, T. V., 2017. The economics of cryptocurrencies - Bitcoin and beyond. Queen's Economics Department Working Paper 1389.

[6] Chuen, D., 2015. Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data. Elsevier.

[7] Fernández-Villaverde, J., Sanches, D., 2016. Can currency competition work? National Bureau of Economic Research Working Paper 22157.

[8] Friedman, M., 1969. The Optimum Quantity of Money and Other Essays. Aldine, Chicago.

[9] Gandal, N., Halaburda, H., 2014. Some economics of private digital currency. Bank of Canada Working Paper 2014-33.

[10] Hendrickson, J. R., Hogan, T. L., Luther, W. J., 2016. The political economy of Bitcoin. Economic Inquiry. 54, 925-939.

[11] Huberman, G., Leshno, J., Moallemi, C., 2017. Monopoly without a monopolist: an economic analysis of the Bitcoin payment system. Columbia Business School Working Paper 17-92.

[12] Lagos, R., Wright, R., 2005. A unified framework for monetary theory and policy analysis. Journal of Political Economy. 113, 463-484.

[13] Narayan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S., 2016. Bitcoin and Cryptocurrency Technologies. Princeton University Press.

[14] Yermack, D., 2013. Is Bitcoin a real currency? an economic appraisal. National Bureau of Economic Research Working Paper 19747.