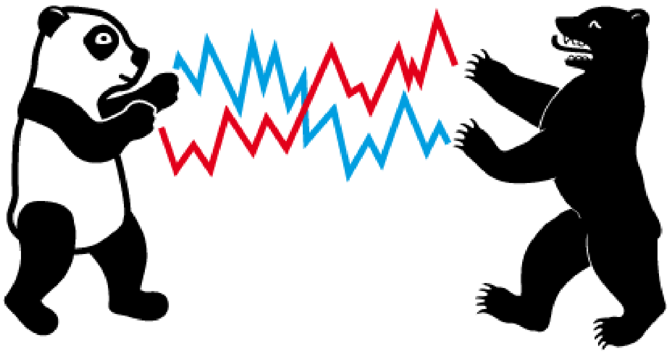
IRTG 1792 Discussion Paper 2018-006

A Note on Cryptocurrencies and Currency Competition

Anna Almosova *



* Humboldt-Universität zu Berlin, Germany

This research was supported by the Deutsche Forschungsgemeinschaft through the International Research Training Group 1792 "High Dimensional Nonstationary Time Series".

http://irtg1792.hu-berlin.de
ISSN 2568-5619

International Research Training Group 1792

A Note on Cryptocurrencies and Currency Competition

Anna Almosova *

December 2017

The recent development of private cryptocurrencies has created a need to extend existing models of private currency provision and currency competition. The outcome of cryptocurrency competition should be analyzed in a model which incorporates important features of the modern cryptocurrencies. In this paper I focus on two such features. First, cryptocurrencies operate according to a protocol - a blockchain - and are, therefore, free from the time-inconsistency problem. Second, the operation of the blockchain costs real resources. I use the Lagos-Wright search theoretic monetary model augmented with privately issued currencies as in Fernandez-Villaverde and Sanches (2016) and extend it by linear costs of private currency circulation. I show that in contrast to Fernandez-Villaverde and Sanches (2016) cryptocurrency competition 1) does not deliver price stability and 2) puts downward pressure on the inflation in the public currency only when the costs private currency circulation (mining costs) are sufficiently low.

Keywords: Currency competition, Cryptocurrency, Inflation, Blockchain
JEL classification: E40, E42, E50, E58

* Humboldt University of Berlin, School of Business and Economics. Spandauer Str.1, 100178, Berlin, Germany. Email: anna.almosova.hu.berlin@gmail.com.
This paper has benefited from the useful comments of Michael Burda, Michael Kumhof, Hermann Elendner, Lutz Weinke, Grzegorz Dlugoszek, Niek Andresen and the participants of the Brown Bag Seminar at HU Berlin. The support of the Collaborative Research Center 649 is generally acknowledged.

1 Introduction

In December 2017 there were more than 1300 different cryptocurrencies in operation with the total market capitalization of about \$600B (coinmarketcap.com). A rapid development of private cryptocurrencies revived a theoretical research on private currency provision. Since at least Hayek (1976) monetary economics tries to answer whether a competitive money supply is more efficient than a monopoly of the central bank on the money market. This paper contributes to the discussion about the outcome of cryptocurrency competition.

I argue that cryptocurrencies have two important features that distinguish them from the other forms of privately supplied money[1]. First, cryptocurrencies are circulating according to a protocol, a blockchain, which eliminates the time-inconsistency problem for a currency issuer. Second, in a blockchain-based monetary system financial operations are conduced in a decentralized manner by nodes of a network as opposed to a banking sector. The private activity of clearing financial transactions - called mining - is costly [2] and the costs are compensated by newly created coins. It follows that the money supply growth is a by-product of maintaining a blockchain. Mining costs are necessary for the operation of a blockchain algorithm due to a distributed trust problem. They will not disappear with an advancement of technology.

Fernandez-Villaverde and Sanches (2016)[3] - FVS henceforth - augment a Lagos-Write type of model[4] with privately supplied currencies. Currency issuers follow a commitment rule. This assumption represents a fact that the supply of cryptocurrencies is determined by a computer algorithm and cannot be changed discretionary. FVS show that an equilibrium with currency competition is efficient (in a sense that it delivers a price

[1] An example form the history is a free banking era in the US in 1837-1863 or Scotland until 1865 (see Gordon, 1985).

[2] For example, an operation of blockchains with a proof-of-work is associated with significant energy costs (See, O'Dwyer and Malone, 2014).

[3] This paper cites Fernandez-Villaverde and Sanches (2016) and was written independently from the later revision in October, 2017. The results of both papers are on par.

[4] One of the advantages of the Lagos-Write (2005) framework is an endogenous money demand. Alternative frameworks are transaction costs, money-in-the-utility, cash-in-advance constraint or an OLG model.

stability) but unstable.

I extend the FVS analysis by assuming that circulation of the private currencies is associated with liner operational costs (similar approach can be found in Marimon et al., 2003). I show that in this case the outcome of currency competition is inefficient. A monetary equilibrium with privately supplied currencies does not deliver a price stability. Instead, a positive inflation rate is required to compensate currency suppliers.

I further analyze a competition between private and public currencies. I assume that a government supplies public money at no costs under commitment to maximize its seigniorage. Monetary economics literature argues that a currency competition works as a disciplinary device and imposes an upper bound on the equilibrium inflation rate that the government can sustain. I show that this is true only if the costs of private currency circulation do not exceed a certain threshold level. For the chosen specification of preferences and production there exists a maximum level of cost parameter above which the inflation rate in the equilibrium with purely competitive currency provision is higher than the seigniorage maximizing inflation rate. Consequently, currency competition plays no role for the government policy.

Many ideas of this paper are in accordance with the literature on currency competition and the time inconsistency of monetary policy - Klein (1974) and Taub (1985) among others. These papers, however, do not model costs of money circulation. Marimon et al. (2012) do discuss the costs of currency provision and show that the equilibrium inflation level is increasing in the cost parameter. However, they assume that private currency issuers are subject to the lack of commitment in the same manner as the monetary authority. Marimon et al. (2003) is closely related to the analysis of this paper. They analyze a costly provision of currency substitutes by banks in a model with a cash-in-advance constraint. Similar to their paper I show that currency competition forces the government to set a lower inflation rate than it would prefer (for small enough cost parameter). However, this paper differs from Marimon er al. (2003) in that I treat currency units solely as means of payment in anonymous trade deals. No real asset and no form of credit can be used as a payment in such an environment. On contrary, Marimon et al. (2003) consider bank deposits as currency substitutes. Currency issuers - banks - have an access to interest bearing government bonds which means that the return on money and the return on the real bonds must be equalized. As a result in their model currency competition drives the inflation upper bound to a negative level dictated by the Friedman rule.

Other papers that analyse currency competition in a search-theoretic framework include Berentsen (2005), Cavalcanti et al. (1999) and Cavalcanti and Wallace (1999) among others.

The rest of the paper is organized as follows. Section 2 describes the money demand function in the Lagos-Wright model. Section 3 addresses private money supply and analyses the purely private currency equilibrium with currency competition. Section 4 introduces a seigniorage maximizing government and shows an effect of currency competition on the government policy. Section 5 concludes.

2 Money Demand

Money demand is identical to Fernandez-Villaverde and Sanches (2016) which is a replication of Lagos and Wright (2005) search theoretic approach. I only briefly sketch the structure of the economy and redirect a reader to the above mentioned papers for the detailed derivations.

Economy is populated by a continuum of buyers of measure 1, a continuum of sellers of measure 1 and infinitely many miners. Every period t consists of two sub periods - a centralized market on which every agent can produce and exchange a centralized good x and a decentralized market on which only sellers produce and only buyers buy and consume a decentralized good q. Production function of the sellers is linear and takes labor as the only input. During a centralized market phase buyers and sellers are endowed with a fixed amount of labor.

The utility function of the buyers is quasi-linear $x_t^b + u(q_t)$. As a result, on the centralized market buyers simply exchange self-produced goods for money to adjust their money holdings and consume the rest. Consequently, an individual money demand is independent from the trade history. Seller do not hold any money.

On the decentralized market buyers meet sellers with a probability σ. Every pair negotiates on a deal according to which a seller produces and sells a particular amount q of goods to the buyer. Negotiation is achieved by a "take-it-or-leave-it" offer. This type of bargaining eliminates additional inefficiencies arising from the bargaining process itself. More precisely, a buyer is fully compensated for holding money between periods.

A buyer and a seller in a pair meet once and never again. This means that it is not possible to use a credit in the trading process. Instead, the agents need to use a storable generally accepted medium of exchange - money [5]. The need for money arises endogenously from the fundamental structure of the economy. No other real assets can be used as a mean of payment.

Infinitely many private agents, called miners, provide private ctyprocurrencies which are perfect substitutes for each other. Each miner maintains a blockchain of a particular crytocurrency i. Let us assume that N cryptocurrency blockchains are in operation.

Given a vector of money holdings $m_t^b = (m_t^{b1}, ...m_t^{bN})'$ a buyer solves a utility maximization problem by deciding how much money to spend on consumption x_t^b and how much to save for a decentralized market phase $\hat{m}_t^b = (\hat{m}_t^{b1}, ...m_t^{bN})'$. A real value of a unit of the ith currency is ϕ_t^i and the total real value of money holdings is $\sum_{i=1}^N \phi_t^i m_t^{bi} = \phi_t m_t^b$ where $\phi_t = (\phi_t^1, ..\phi_t^N)$.

Let us denote the return to money $\gamma_{t+1} \equiv \frac{\phi_{t+1}}{\phi_t}$. Lagos and Write show that money demand is specified by two functions (see Appendix 7.1 for more details): the production on the decentralized market as a function of a return on money $q(\gamma_{t+1})$ (1) and the total real value of money holdings as a function of the level of production q (2). Note that since (1) holds for any currency i, the return on money must be equalized among currencies that are held in equilibrium (see FVS). From the equation (1) we also see that the trade

[5] In the Lagos and Wright (2005) paper every agent is assumed to produce a unique good and to have preferences over the goods of others. Money is required to overcome the double coincidence problem - that each party in a pair wants the good of the counter-party and the barter is possible. An exogenous distinction between buyers and sellers that I borrowed from Fernandez-Villaverde and Sanches (2016) does not affect the main results.

on the decentralized market q depends on the return on money γ_{t+1}.

$$\sigma \frac{u'(q_t)}{w'(q_t)} + 1 - \sigma = \frac{\phi_t}{\beta \phi_{t+1}} = \frac{1}{\beta \gamma_{t+1}} \tag{1}$$

$$\phi_{t+1} \hat{m}_t = \beta^{-1} w(q_t) \tag{2}$$

Real money demand can be expressed as $z(\gamma_{t+1}) \equiv \phi_t \hat{m}_t = \sum_{i=0}^{N} \frac{\phi^i_{t+1}}{\phi^i_{t+1}} \phi^i_t \hat{m}^i_t = \phi_{t+1} \hat{m}_t \frac{1}{\gamma_{t+1}}$.

$$z(\gamma_{t+1}) = \frac{\beta^{-1} w(q(\gamma_{t+1}))}{\gamma_{t+1}} \tag{3}$$

3 Equilibrium with Private Money

Private cryptocurrencies are provided by rational private agents - called miners - who maximize the utility from the stream of consumption x^M[6] subject to linear operational costs with a parameter ψ.

A behaviour of miners is determined by an algorithm of a blockchain protocol which is a public knowledge. All agents, therefore, know the future evolution of the money supply as in a perfect foresight set up.

$$\max_{\{M^i_t\}} \sum_{t=0}^{\infty} \beta^t x^{Mi}_t \tag{4}$$

$$\text{s.t. } x^{Mi}_t = \phi_t (M^i_t - M^i_{t-1}) - \psi \phi^i_t M^i_t \tag{5}$$

Here $0 < \psi < 1$ represents the costs that are associated with the operation of the cryptocurrency platform (blockchain) as a fraction of the real money stock. Linear opeational costs are similar to financial intermediation costs in Marimon et al. (2003). In case of a Bitcoin blockchain, for example, these costs correspond to electricity consumed for a verification of transactions (proof-of-work). The assumption about linear costs delivers a simple representation of the inefficiency of the private money provision technology.

[6] In the real world miners indirectly affect the money supply by optimally choosing the intensity of mining activity for a particular level of mining costs.

Is it plausible to assume that the total number of verified transactions and, therefore, the energy costs are increasing with the total real money stock? Or in other word should we multiply ψ with money stock and not with an increase in money stock $M_t^i - M_{t-1}^i$. The key feature of the blockchain that lies behind this assumption is that mining does not correspond to money issuance directly. Mining is an activity of verifying transaction. When already existing coins are transferred back and forth from one account to another every transaction has to be verified. Even if the money supply stays constant so $M_t^i - M_{t-1}^i = 0$ a circulation of the existing money units still consumes energy. Additionally, it is logical to assume that a higher purchasing power of a currency unit leads to a higher number of transactions with this currency and, hence, higher total costs of verifying theses transactions.

The market for cryptocurrencies features a free entry which implies a zero profit of miners in equilibrium.

$$\sum_{t=0}^{\infty} \beta^t [(1-\psi)\phi_t^i M_t^i - \phi_t^i M_{t-1}^i] = 0 \tag{6}$$

A consumption level is non-negative every period $(1-\psi)\phi_t^i M_t^i - \phi_t^i M_{t-1}^i \geq 0 \; \forall t$. Consequently,

$$(1-\psi)M_t^i - M_{t-1}^i = 0 \; \forall t \text{ if } \phi_t^i > 0 \tag{7}$$

Linear costs of mining require a money supply growth with a rate $\frac{\psi}{1-\psi}$. Miners are compensated for the costs by a positive seigniorage[7]. Note that the money growth rate can not be negative.

In equilibrium the total real money supply $\sum_i^N \phi_t^i M_t^i$ must be equal to the real money demand $z(\gamma_{t+1})$. The share of every currency in a buyer's portfolio is indetermined but since for all valued currencies the supply growth rate is the same and the return on

[7] If the cost parameter were different for different currencies than the growth rates of money supply would also differ.

money is equalized

$$M_t^i = \frac{1}{1-\psi} M_{t-1}^i = \left(\frac{1}{1-\psi}\right)^t M_0^i$$
$$\phi_{t+1}^i = \phi_t^i \gamma_{t+1} = \phi_0^i \prod_{\tau=0}^{t} \gamma_{\tau+1}$$

Let us assume that $M_0^i = M_0^j$ and $\phi_0^i = \phi_0^j \; \forall i, j$. Then every valued currency has an equal weight in a buyer's portfolio in every period. Combining (7) and (3) the equilibrium path is described by

$$(1-\psi) z(\gamma_{t+1}) - \gamma_t z(\gamma_t) = 0 \tag{8}$$

which defines $\gamma_{t+1}(\gamma_t)$. This equation has two stationary points: $\gamma = 0$ and $\gamma = 1 - \psi$. A monetary equilibrium with $\gamma = 1 - \psi$ implies a decreasing real price of money or in other words a positive inflation.

Proposition 1: In a monetary equilibrium $\gamma = 1 - \psi < 1$ which means that the real price of money is declining and the inflation level is strictly positive.

A currency competition can not deliver a price stability. As long the costs associated with an operation of private currency protocols are nonzero a positive seigniorage is required to compensate miners for their costs. This result is different from FVS who show that a competitive currency supply brings about a constant price equilibrium.

FVS, moreover, show that the monetary equilibrium is unstable. This result also holds in the current set up.

Proposition 2: A monetary equilibrium with a positive return on money is unstable. Non-monetary equilibrium with a zero return on money is stable.

Proof: is identical to FVS. As long as money demand function satisfies $z'(\gamma) > 0$ the equilibrium with a positive value of money is unstable. If initial conditions are such that $\gamma_0 < 1 - \psi$ then from equation (8) γ_t declines for $t \geq 1$. When $\gamma_0 > 1 - \psi$ the equilibrium path is explosive. Formally, using the implicit function theorem and the assumption that $z'(\gamma) > 0$:

$$\frac{d\gamma_{t+1}}{d\gamma_t} = \frac{z(\gamma_t) + \gamma_t z'(\gamma_t)}{(1-\psi)z'(\gamma_{t+1})}$$
$$\left.\frac{d\gamma_{t+1}}{d\gamma_t}\right|_{\gamma_t=\gamma_{t+1}=1-\psi} = \frac{z(1-\psi) + (1-\psi)z'(1-\psi)}{(1-\psi)z'(1-\psi)} > 1$$

thus, $\gamma_t \to 0$ if $\gamma_0 < 1-\psi$ and $\gamma_t \to \infty$ if $\gamma_0 > 1-\psi$. As γ converges to zero, the real money demand converges to zero and the economy converges to a non-monetary equilibrium. Since γ_t is the same for all valued currencies, money demand goes to zero for every currency i. Figure in Appendix 7.4 plots the function $\gamma_{t+1}(\gamma_t)$.

To sum up, the equilibrium with a private currency provision is neither efficient (in a sense that it does not deliver a price stability) nor stable. Clearly, the costs of currency circulation is harmful for a welfare. Inefficient (smaller than 1) return on money leads to an inefficiently low money demand and a low amount trade on the decentralized market.

Proposition 3: In a monetary equilibrium with $\gamma = 1-\psi < 1$ the level trade on the decentralized market q is decreasing in ψ.

Proof: compare a level of trade in a non-zero costs equilibrium (q) and in a zero costs equilibrium (q^0). (1) must hold for any equilibrium.

$$\sigma\frac{u'(q)}{w'(q)} + 1 - \sigma = \frac{1}{\beta(1-\psi)} \text{ and } \sigma\frac{u'(q^0)}{w'(q^0)} + 1 - \sigma = \frac{1}{\beta}$$

substarct the second equation from the first

$$\sigma\left(\frac{u'(q)}{w'(q)} - \frac{u'(q^0)}{w'(q^0)}\right) = \frac{1}{\beta(1-\psi)} - \frac{1}{\beta} > 0$$

The last condition means that either $u'(q) > u'(q^0)$ or $w'(q) < w'(q^0)$ or both. Since $u'(q)$ is decreasing and $w'(q)$ is increasing it implies that $q < q^0$. The larger the parameter ψ the larger is the difference between q and q^0. Costs of private currency circulation are, thus, welfare detrimental.

The first-best level of production q^* which is defined from $u'(q^*) = w'(q^*)$ is achieved when $\gamma = \beta^{-1}$. Which from the Fisher equation $1 + i_t = (1+r)(1+\pi_t)$ and the fact that $\gamma_t = \frac{1}{1+\pi_t}$ means that i=0. To see that formally rewrite (1) as

$$\begin{aligned}
&\sigma\frac{u'(q_t)}{w'(q_t)} + 1 - \sigma = \frac{1+\pi}{\beta} \\
&\sigma\frac{u'(q_t)}{w'(q_t)} = 1 + i_t - 1 + \sigma \\
&\frac{u'(q_t)}{w'(q_t)} = 1 + \frac{i_t}{\sigma} \qquad (9)
\end{aligned}$$

$q = q^*$ if $i_t = 0$.

The fist-best solution for the return on money corresponds to the Friedman (1969) rule. Friedman argued that the price of money - the nominal interest rate - should be equal to zero and the economy should be saturated with money. In this case the there will be no inefficiency in the real sector arising from monetary scarcity. Private currency competition in the current set up never achieves the Friedman rule because it requires a negative seigniorage. In the current model the seigniorage from a currency creation equals to the consumption of a miner which cannot be negative.

4 Equilibrium with Public Money

In this section I introduce a government that provides public money taking potential private currency issuers into account. The goal of this section is to show that 1) currency competition imposes an upper limit on the level of inflation for a seigniorage maximizing government if the costs of private currency circulation are small enough and that 2) this upper bound is positive.

I assume that a government finances a sequence of transfers G_t from its seigniorage. A path for the public money supply M^G is determined by a no-Ponzi games condition together with an intertemporal budget constraint

$$G_t = \phi_t^G (M_t^G - M_{t-1}^G) \qquad (10)$$

If additionally the government has an ability to impose lump-sum taxes and $G_t =$

$\phi_t(M_t^G - M_{t-1}^G) + \tau_t$ then the government can constantly shrink a money supply and achieve an efficient allocation on the decentralized market. Indeed if the benevolent government follows the Friedman rule by setting a return on public money γ^G to be β^{-1} the production on the decentralized market is equal to q^*.

Following a monetary economics literature I assume that the government follows a constant money growth rule, e.i. $M_t^G = (1+\omega)M_{t-1}^G$ and wants to maximize the stream of transfers $\sum_{t=0}^{\infty} \beta^t G_t$ by choosing ω rather than to rely on taxation. I denote a real value of public money as $m_t^G = \phi_t^G M_t^G$ and return on public money as γ^G. As for private currencies $\gamma_t^G = \frac{1}{1+\pi_t^G} = \frac{1}{1+\omega}$. The government takes the money demand $z(\gamma_t)$ as given.

The budget constraint (10) can be rewritten as

$$\sum_{t=0}^{\infty} \beta^t G_t = -\gamma_0^G m_{-1}^G + \sum_{t=0}^{\infty} \beta^{t+1} \left(\frac{1}{\beta} - \gamma_{t+1}^G \right) m(\gamma_{t+1}^G) \tag{11}$$

Since the government maintains a monopoly over the supply of the public money it faces a time-inconsistency problem. Namely, $-\gamma_t^G m_{t-1}^G$ equals to zero only in the period $t = 0$ and is positive afterwards. The government, thus, has an incentive to relaunch the public currency every period. Under a commitment the government decides on constant γ^G (see Marimon et al., 2003) to maximize a period by period seigniorage $f(\gamma_{t+1}) = \left(\frac{1}{\beta} - \gamma_{t+1} \right) z(\gamma_{t+1})$.

The inflationary tax $\left(\frac{1}{\beta} - \gamma_{t+1}^G \right)$ in decreasing in γ^G (increasing in the inflation rate) whereas the money demand is increasing in the return on money (decreasing in the inflation rate). For the standard utility and production functions the seigniorage $f(\gamma_{t+1})$ has a unique maximum γ^{G*}. Competition from the private sector, however, forces the government to set the return on currency to at least $\gamma = 1 - \psi$. Thus, the solution is restricted by $1 + \omega \leq \frac{1}{1-\psi}$.

If $f'(\gamma)$ is negative at $\gamma = 1 - \psi$ then the government would like to set γ^G lower than

than it is forced by currency competition. This happens if

$$f'(\gamma) = -z(\gamma) + (\frac{1}{\beta} - \gamma)z'(\gamma)] < 0 \text{ or}$$
$$f'(\gamma) = z(\gamma)\left[-1 + \left(\frac{1}{\beta} - \gamma\right)\frac{z'(\gamma)}{z(\gamma)})\right] < 0$$

We can concentrate on the expression in the brackets since $z(\gamma) \geq 0\ \forall\gamma$. I assume the same functional forms as in FVS: $u(q) = \frac{q^{1-\eta}}{1-\eta}$, $0 < \eta < 1$ and $w(q) = \frac{q^{1+\alpha}}{1+\alpha}$, $\alpha \geq 0$. Given these specifications $f'(\gamma)$ is negative if

$$\left(\frac{1}{\beta} - \gamma\right)\left[\frac{1-\eta}{\eta+\alpha}\frac{1}{\gamma} + \frac{1+\alpha}{\eta+\alpha}\frac{(1-\sigma)\beta}{1-(1-\sigma)\beta\gamma}\right] - 1 < 0$$

substituting 1-ψ for γ

$$\left(\frac{1}{\beta} - 1 + \psi\right)\left[\frac{1-\eta}{\eta+\alpha}\frac{1}{1-\psi} + \frac{1+\alpha}{\eta+\alpha}\frac{(1-\sigma)\beta}{1-(1-\sigma)\beta(1-\psi)}\right] - 1 < 0 \tag{12}$$

In general the sign of (12) depends on the parametrization. For example, Lagos and Write (2005) set $\beta = 0.997$ which corresponds to a 3% annual real interest rate, $\alpha = 0$ which corresponds to a linear disutility from labour, $\eta = 0.16$ and $\sigma = 0.5$. With these parameters a threshold level for ψ is 0.12. If a private currency provision is associated with costs that are higher than 0.12 then currency competition plays no role. If the costs of private money maintenance are lower than 12% per money unit then currency competition imposes a lower bound for the return on currency (an upper bound on the inflation level) that the government can sustain. The government can not set a return on public money lower than $1 - \psi = 0.88$ (or inflation higher than 13%). Appendix 7.5 presents threshold vales of ψ for different calibrations.

Proposition 4: With $u(q) = \frac{q^{1-\eta}}{1-\eta}$, $0 < \eta < 1$ and $w(q) = \frac{q^{1+\alpha}}{1+\alpha}$, $\alpha \geq 0$ a currency competition sets an upper bound for a sustainable inflation level only if ψ is below a threshold level defined by (12).

If ψ goes to zero the outcome converges to a zero inflation equilibrium. However, as long as operational costs of private currencies are positive, the upper bound on the inflation is also positive. The government can collect a positive seigniorage even under a threat of competing private currencies.

To gauge a realistic value for the ψ parameter one can look at statistics for cryptocurrencies. For example, blockchain.info indicates for Bitcoin that the average mining costs per money unit is below 2%[8]. It means that if a gross inflation level $1 + \pi$ in some hypothetical country goes above $1/(1 - \psi) \approx 1,02$ currency holders would prefer Bitcoin (abstracting from risk and trust concerns). From bitinfocharts one can compute the same number for other currencies. For eutherum the cost parameter would be less than 0,5%[9].

Finally, we need to discuss the situation when the government cannot commit to its policy. Imagine that the government follows a commitment rule until some period τ and discretionary decides on γ_t every period for $t > \tau$. Marimon et al. (2003) show that the government continues to follow the path of the commitment rule if there is a positive value attached to such a policy - a positive seigniorage. In the model of Marimon et al. (2003) private currency competition can drive an inflation rate to a negative region. Private currency providers would bear a negative inflation because they have an access to other forms of income. With a negative inflation the government deviates from the commitment path and over-issues the public currency. As a result the government money becomes valueless and is driven out of circulation. In contrast, in the current framework the inflation on private currencies is always positive due to the presence of costs. Even with a lack of commitment a private currency never drives a public currency out of circulation.

The model predicts that a high inflation in public currency incentives households to substitute private digital currencies for the public fiat money.

This process indeed can be observed in some countries with hyper inflation or low trust in the national authorities. For example, Jack and Suri (2011) showed that by the end of 2009 about 65% of households in Kenya was using cell phone currency M-

[8]https://blockchain.info/charts/cost-per-transaction-percent

[9]Computed as reward in the last 24 hours over the amount of coins sent in the last 24 hours. See https://bitinfocharts.com/ethereum/

Pesa for money transfers. M-Pesa was introduced in Kenya in 2007 by mobile provider Safaricom[10] and was represented by mobile phone minutes that could be send for large distances at extremely low costs with a help of a cell phone technology.

Another example would be Ecuador which introduced a government digital cash controlled by a central bank. The willingness to accept the digital cash might stem from the hyperinflation episodes in Ecuador fiat currency until 2000[11].

One must admit that a decision to use private money as a mean of exchange instead of a legal tender crucially depends on official inflation level as well as on trust in a local government. Moreover, it matters whether a private currency is widely accepted as a mean of payment and whether it has a stable exchange rate. All these issues are not addressed in this paper.

5 Conclusion

Monetary economics has been studying currency competition since at least free banking era episodes in the USA and Scotland. Recent development of cryptocurrencies attracted an interest in academia and revived the discussion on the outcome of currency competition.

Cryptocurrencies are "controlled" by (a network of) private rational agents in accordance with a specific protocol - a blockchain. Due to distributed trust concerns the functioning of a blockchain requires a significant input of a computational time and, thus, energy.

This paper studies how an outcome of currency competition is affected by the costs associated with a private currency circulation. I extend the model of Fernandez-Villaverde and Sanches (2016) with linear operational costs. I analyze an equilibrium with a purely private money provision and a competition between private and public currencies.

The equilibrium with private currency provision does not feature a price stability. A positive growth rate for private money supply and a positive seigniorage is needed to

[10] Safaricom was redesigned to a public-private partnership with 50% owned by Vodafon and 25% by Kenya Treasury department.

[11] https://www.economist.com/blogs/americasview/2014/09/electronic-money-ecuador

compensate private currency providers. The costs of private money circulation lead to an inefficient level of production and trade on a decentralized market. The magnitude of the welfare losses is proportional to the cost parameter.

Even if a currency competition does not deliver a price stability it might impose a discipline on a monopolist who provides public money. I show that currency competition plays a disciplinary role for the return on public money (and, thus, the inflation) only if operational costs of private cryptocurrencies are below a certain level. The role of currency competition, therefore, depends on the technology that underlies a circulation of private currencies.

Many assumption of this paper are simplifications of the reality that might matter for the equilibrium outcome. In reality miners do not directly decide on the money supply but on the mining intensity instead. In fact, for many cryptocurrencies the evolution of the money supply is specified directly in a blockchanin protocol. Costs of private money operation depend on the mining intensity and not directly on the coins in circulation or the number of transactions. These and many other features of cyptocurrencies provide exciting topics for future research.

6 References

1. Berentsen, A., 2006. On the private provision of fiat currency. European Economic Review, 50(7), pp.1683-1698.

2. Cavalcanti, R.D.O., Erosa, A. and Temzelides, T., 1999. Private money and reserve management in a random-matching model. Journal of Political Economy, 107(5), pp.929-945.

3. Cavalcanti, R.D.O. and Wallace, N., 1999. A model of private bank-note issue. Review of Economic Dynamics, 2(1), pp.104-136.

4. O'Dwyer, K.J. and Malone, D., 2014. Bitcoin mining and its energy footprint.

5. Gordon, G., 1985. Banking Theory and Free Banking History. Journal of Monetary

Economics, 16, pp.267-276.

6. Fernandez-Villaverde, J., and Sanches, D., 2016. Can Currency Competition Work? Upenn Working Paper.

7. Friedman, M., 2005. The optimum quantity of money. Transaction Publishers.

8. Hayek, F.A., 1976. Denationalism of Money: An Analysis of the Theory and Practice of Concurrent Currencies. Institute of Economic Affairs (Great Britain).

9. Jack, William, and Tavneet Suri. Mobile money: The economics of M-PESA. No. w16721. National Bureau of Economic Research, 2011.

10. Klein, Benjamin. "The competitive supply of money." Journal of Money, Credit and Banking 6.4 (1974): 423-453.

11. Lagos, R. and Wright, R., 2005. A unified framework for monetary theory and policy analysis. Journal of political Economy, 113(3), pp.463-484.

12. Marimon, R., Nicolini, J.P. and Teles, P., 2003. Insideoutside money competition. Journal of Monetary Economics, 50(8), pp.1701-1718.

13. Marimon, R., Nicolini, J.P. and Teles, P., 2012. Money is an experience good: Competition and trust in the private provision of money. Journal of Monetary Economics, 59(8), pp.815-825.

14. Taub, B., 1985. Private fiat money with many suppliers. Journal of Monetary Economics, 16(2), pp.195-208.

7 Appendix

7.1 Lagos-Wright Search Theoretic Model

$$W_t^b(m_t^b) = \max_{x_t^b, \hat{m}_t^b} [x_t^b + \sigma \left(u(q_t(\hat{m}_t^b, \hat{m}_t^s)) + \beta W_{t+1}^b(\hat{m}_t^b - p_t(\hat{m}_t^b, \hat{m}_t^s)) \right) + (1-\sigma)\beta W_{t+1}^b(\hat{m}_t^b)]$$

$$\text{s.t. } \phi_t \hat{m}_t^b + x_t^b = \phi_t m_t^b$$

or

$$W_t^b(m_t^b) = \phi_t m_t^b + \max_{\hat{m}_t^b} [-\phi_t \hat{m}_t^b + \sigma \left(u(q_t(\hat{m}_t^b, \hat{m}_t^s)) + \beta W_{t+1}^b(\hat{m}_t^b - p_t(\hat{m}_t^b, \hat{m}_t^s)) \right)$$

$$+ (1-\sigma)\beta W_{t+1}^b(\hat{m}_t^b)] \tag{13}$$

The utility function has standard properties: $u(0) = 0, u'(0) = \infty$, $u'(\cdot) > 0$, $u''(\cdot) < 0$.

With a probability σ a buyer meets a seller and negotiates on an amount q and on a payment $p_t(\hat{m}_t^b, \hat{m}_t^s)$. In general, the payment and the amount of trade depend on the buyer's and the seller's currency holdings on a decentralized market.

A seller solves an analogous problem

$$W_t^s(m_t^s) = \max_{x_t^s, \hat{m}_t^s} [x_t^s + \sigma \left[-w(q_t(\hat{m}_t^b, \hat{m}_t^s)) + \beta W_{t+1}^s(\hat{m}_t^s + p_t(\hat{m}_t^b, \hat{m}_t^s)) \right] + (1-\sigma)\beta W_{t+1}^s(\hat{m}_t^s)]$$

$$\text{s.t. } \phi_t \hat{m}_t^s + x_t^s = \phi_t m_t^s$$

where $w(n_t^s)$ is a disutility from labor and the production function is linear $q_t = n_t^s$. Standard assumptions on the disutility function hold: $w(0) = 0, w'(\cdot) > 0, w''(\cdot) > 0$.

Bargaining takes a form of a "take-it-or-leave-it" offer from a buyer to a seller in a pair. The buyer maximizes his utility subject to a participation constraint for the seller (PC) that ensures that the seller does not make losses and to a liability constraint (LC) that guarantees that the buyer cannot pay more money than he has. Under such a framework money holdings of the seller play no role for the bargaining outcome. The bargaining can be characterized in terms of q and p which are both functions of $\hat{m}_t^b$.

$$\max_{q_t,d_t}[u(q_t) - \beta\phi_{t+1}p_t] \tag{14}$$

$$\text{s.t. } -w(q_t) + \beta\phi_{t+1}p_t \geq 0 \qquad \text{PC} \tag{15}$$

$$p_t \leq \hat{m}_t^b \qquad \text{LC} \tag{16}$$

A standard result in the contract theory is that the PC is always binding. The objective function (14) can be written as $u(q_t) - w(q_t)$. Optimal q^* is then defined from $u'(q^*) = w'(q^*)$. If the buyer has enough money to compensate the seller for a production of q^* then q^* is produced. The optimal payment can be derived from the PC. If the buyer's money holdings are insufficient he simply pays everything he has and receives an amount q that the seller is willing to produce for the compensation $\hat{m}_t^b$.

$$q_t = \begin{cases} q^* \text{ if } \phi_{t+1}\hat{m}_t^b \geq \beta^{-1}w(q^*) \\ w^{-1}(\beta\phi_{t+1}\hat{m}_t^b) \text{ if } \phi_{t+1}\hat{m}_t^b < \beta^{-1}w(q^*) \end{cases}$$

$$\phi_{t+1}p_t = \begin{cases} \beta^{-1}w(q^*) \text{ if } \phi_{t+1}\hat{m}_t^b \geq \beta^{-1}w(q^*) \\ \phi_{t+1}\hat{m}_t^b \text{ if } \phi_{t+1}\hat{m}_t^b < \beta^{-1}w(q^*) \end{cases}$$

As FVS note, the problem can only be characterized in terms of aggregate payment $\phi_{t+1}p_t$. As long as the cryptocurrencies are perfect substitutes the composition of the buyers's portfolios is indeterminate. Nevertheless, we can still characterize some equilibrium properties.

FOC of the buyer's problem is: $\frac{dW^b(\hat{m}_t^b)}{d\hat{m}_t^b} \leq 0$ and $= 0$ if $\hat{m}_t^b > 0$. Thus, for any currency i that is held in equilibrium

$$\begin{cases} -\phi_t^i + \beta\phi_{t+1}^i = 0 \text{ if } \phi_{t+1}\hat{m}_t^b \geq \beta^{-1}w(q^*) \\ \sigma u'(q_t)q'_{m_t^i} + \beta(1-\sigma)\phi_{t+1}^i - \phi_t^i = 0 \text{ if } \phi_{t+1}\hat{m}_t^b < \beta^{-1}w(q^*) \end{cases}$$

Where q is a function of the total real money holdings $q(\hat{m}_t^b) = w^{-1}(\beta\phi_{t+1}\hat{m}_t^b)$.

Taking a derivative of the inverse function $q'_{\hat{m}^i_t} = \beta\phi^i_{t+1}\frac{1}{w'(q)}$. The second equation can be written as $\frac{\phi^i_t}{\beta\phi^i_{t+1}} = 1 + \sigma\frac{u'(q)}{w'(q)} - \sigma$ (see Appendix 7.2).

A solution exists only with $\frac{\phi_{t+1}}{\phi_t} \leq \beta^{-1}$. Indeed, if the return to money $\gamma_{t+1} \equiv \frac{\phi_{t+1}}{\phi_t}$ is larger than the inverse of the time preference parameter than agents would want to hold an infinite amount of money units. When $\frac{\phi_{t+1}}{\phi_t} \leq \beta^{-1}$ holding money is costly. Since the bargaining and the trade on the decentralized market depend solely on buyers' money holdings only buyers decide to hold currencies and $m^s_t = 0$. From now on I will use $\hat{m}_t = \hat{m}^b_t$ which denotes the total money demand in the economy.

One can show that the objective function of a buyer (13) is concave and is strictly decreasing at $\beta^{-1}w(q^*)$ if $\frac{\phi_{t+1}}{\phi_t} \leq \beta^{-1}$ (see Appendix 7.3). It means that the buyer's problem has a unique solution when $\phi_{t+1}\hat{m}_t < \beta^{-1}w(q^*)$. In a limiting case when $\phi_t = \beta\phi_{t+1}$ the derivative of the objective function is zero at $\beta^{-1}w(q^*)$. In this situation I assume a limiting solution $\hat{m}_t = \beta^{-1}w(q^*)$ as in Lagos and Wright (2005).

7.2 Money Demand

$$\frac{\phi^i_t}{\beta\phi^i_{t+1}} = 1 + \frac{\sigma}{\beta\phi^i_{t+1}}[u'(q) - w'(q)]q'_{m^i_t} \tag{17}$$
$$\frac{\phi^i_t}{\beta\phi^i_{t+1}} = 1 + \frac{\sigma}{\beta\phi^i_{t+1}}[u'(q) - w'(q)]\beta\phi^i_{t+1}\frac{1}{w'(q)} \tag{18}$$
$$\frac{\phi^i_t}{\beta\phi^i_{t+1}} = 1 + \sigma\frac{u'(q)}{w'(q)} - \sigma \tag{19}$$

7.3 Buyer Objective Function

The first derivative of the buyer objective function (for any currency i) can be written as

$$-\phi_t + \beta\phi_{t+1} + \sigma[u'(q) - w'(q)]\frac{1}{w'(q)}$$

As m approaches $\beta^{-1}w(q^*)$ from below, $q(m_t)$ goes to q^* and the second term goes to zero. The first term is negative for $\frac{\phi_{t+1}}{\phi_t} < \beta^{-1}$. Therefore, the derivative is negative and the objective function is decreasing at $\beta^{-1}w(q^*)$.

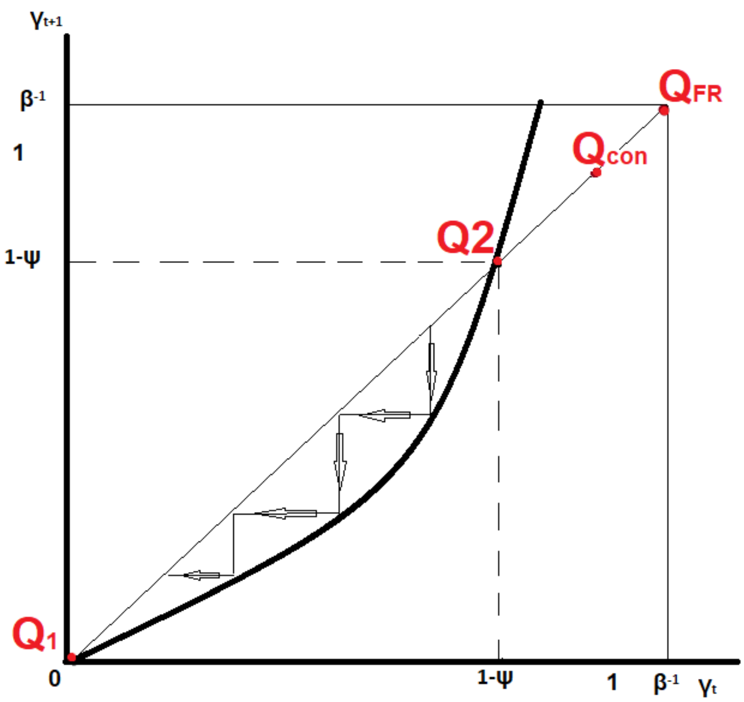
The second derivative of the objective function can be written as

$$\sigma u''[q(m_t)](q'(m_t))^2 + \sigma u'[q(m_t)]q''(m_t)$$

Using an implicit function theorem one can show that the second derivative is negative and the objective function is concave since $u''(q) < 0$, $u'(q) > 0$, $q'(m_t) = \frac{1}{w'(q)} > 0$ and $q''(m_t) = -\frac{w''(q)}{w'(q)^3} < 0$.

The buyer problem has a unique solution at $m_t < \beta^{-1}w(q^*)$.

7.4 Plot of the Equilibrium Dynamics



Q_1 denotes a non monetary equilibrium, Q_2 a monetary equilibrium with non-zero financial intermediation cots, Q_con an equilibrium with constant prices and Q_FR an equilibrium which corresponds to the Friedman rule.

7.5 Threshold Values for Cost Parameter

Table 1: Parameter Values

η	0.1	0.1	0.1	0.1	0.1	0.1	0.3	0.3	0.3	0.5	0.5
α	0.1	0.1	0.1	0.3	0.3	0.3	0.1	0.1	0.3	0.5	0.3
σ	0.1	0.3	0.5	0.1	0.3	0.5	0.1	0.3	0.1	0.1	0.1
γ^{G*}	0.97	0.92	0.86	0.95	0.85	0.8	0.94	0.8	0.91	0.88	0.84
ψ^{max}	0.03	0.08	0.14	0.05	0.15	0.2	0.06	0.2	0.09	0.12	0.16

IRTG 1792 Discussion Paper Series 2018

For a complete list of Discussion Papers published, please visit irtg1792.hu-berlin.de.

001 "Data Driven Value-at-Risk Forecasting using a SVR-GARCH-KDE Hybrid" by Marius Lux, Wolfgang Karl Härdle and Stefan Lessmann, January 2018.
002 "Nonparametric Variable Selection and Its Application to Additive Models" by Zheng-Hui Feng, Lu Lin, Ruo-Qing Zhu asnd Li-Xing Zhu, January 2018.
003 "Systemic Risk in Global Volatility Spillover Networks: Evidence from Option-implied Volatility Indices " by Zihui Yang and Yinggang Zhou, January 2018.
004 "Pricing Cryptocurrency options: the case of CRIX and Bitcoin" by Cathy YH Chen, Wolfgang Karl Härdle, Ai Jun Hou and Weining Wang, January 2018.
005 "Testing for bubbles in cryptocurrencies with time-varying volatility" by Christian M. Hafner, January 2018.
006 "A Note on Cryptocurrencies and Currency Competition" by Anna Almosova, January 2018.

IRTG 1792, Spandauer Straße 1, D-10178 Berlin
http://irtg1792.hu-berlin.de

This research was supported by the Deutsche Forschungsgemeinschaft through the IRTG 1792.