Almosova, Anna

Working Paper

A Monetary Model of Blockchain

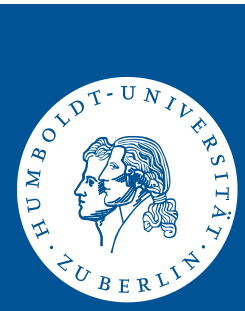
IRTG 1792 Discussion Paper, No. 2018-008

Provided in Cooperation with:
Humboldt University Berlin, International Research Training Group 1792 "High Dimensional Nonstationary Time Series"

Suggested Citation: Almosova, Anna (2018) : A Monetary Model of Blockchain, IRTG 1792 Discussion Paper, No. 2018-008, Humboldt-Universität zu Berlin, International Research Training Group 1792 "High Dimensional Nonstationary Time Series", Berlin

This Version is available at:
https://hdl.handle.net/10419/230719

IRTG 1792 Discussion Paper 2018-008



International Research Training Group 1792

A Monetary Model of Blockchain

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

A Monetary Model of Blockchain

Anna Almosova *

January 2018

The recent emergence of blockchain-based cryptocurrencies has received a considerable attention. The growing acceptance of cryptocurrencies has led many to speculate that the blockchain technology can surpass a traditional centralized monetary system. However, no monetary model has yet been developed to study the economics of the blockchain. This paper builds a model of the economy with a single generally acepted blockchain-based currency. In the spirit of the search and matching literature I use a matching function to model the operation of the blockchain. The formulation of the money demand is taken from a workhorse of monetary economics - Lagos and Wright (2005). I show that in a blockchain-based monetary system money demand features a precautionary motive which is absent in the standard Lagos-Wright model. Due to this precautionary money demand the monetary equilibrium can be stable for some calibrations. I also used the developed model to study how the equilibrium return on money is dependent on the blockchain parameters such as mining costs and rewards.

Keywords: Blockchain, Miners, Cryptocurrency, Matching function
JEL classification: E40, E41, E42

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

1 Introduction

More than 1400 different blockchain-based cryptocurrencies with a total market capitalization of about $700 billion were in circulation in January, 2018[1]. Over 300,000 transactions are conducted with cryptocurrencies every day and at least 1,000 off-line locations accept cryptocurrency as means of payment[2].

As Fernandez-Villaverde and Sanches (2017) write, the appearance of blockchain-based currencies has stated many normative and positive questions for monetary economics. These questions require a theoretical model that takes into account the most important characteristics of the blockchain operation. According to my knowledge, no such monetary model has yet been developed.

A growing amount of literature addresses the economic nature and the novelty of blockchains[3]. Most of the papers, however, focus on case studies or a general discussion of the blockchain protocol. Theoretical literature on private currency provision and currency competition is extensive[4]. However, the existing models lack many of the fundamental features of the blockchain operation and therefore can only partially be applied to study blockchain-based monetary systems.

Blockchain is a protocol which defines a decentralized monetary arrangement. Financial transactions in this arrangements can be verified and executed by every participant as opposed to banks in a traditional monetary system. Money supply evolves according to a pre-specified rule as opposed to the policy decisions of a central bank. Blockchain-based currencies are also different from other forms of privately supplied money known from history[5].

[1] www.coinmarketcap.com.

[2] The numbers is given for Bitcoin, the largest cryptocurrency. See https://www.coindesk.com/surge-in-real-locations-accepting-bitcoin/ and https://www.coindesk.com/surge-in-real-locations-accepting-bitcoin/.

[3] Berentsen and Schaer (2018), Swan (2015), Peter et al. (2016) to name just a few.

[4] For example, Cavalcanti, Erosa, and Temzelides (1999, 2005), Cavalcanti and Wallace (1999), Williamson (1999), Berentsen (2006), Monnet (2006), Marimon et al. (2003, 2012) and more recently, Fernandez-Villaverde and Sanches (2017).

[5] For example, during the free banking era. See Gordon (1985).

One of the basic features of the blockchain system is the absence of currency issuers (except for the very first units). Newly created currency units are injected into the network as a reward for the execution of financial transactions. The processing of financial transactions is called mining and the agents who conduct this activity are called miners[6]. Mining requires computational time as an input and consequently costs energy. Mining costs together with rewards determine the equilibrium supply of the mining service and as a byproduct affect the evolution of the money supply. Another important feature of the blockchain is that the processing of financial transactions takes time[7]. Hence, not all the transaction that were requested are processed within a period (or ever). Money market participants take a probabilistic nature of the transaction execution into account when signing trade contracts. Moreover, they can add a fee to a transaction request to facilitate the execution. Finally, the circulation of the blockchain-based currency features externalities. Miners compete with each other to be the first who process a particular transaction since only the first miner receives a reward for this transaction. Hence every miner is successful only with a particular probability. An increase in the total number of miners negatively affects the probability of miner's success. On the other hand, an increase in the number of the transaction requests positively affects miners' revenue through an increase in transaction fees. In a similarly way a probability that a particular transaction will be processed increases with the number of miners but decreases in the transaction demand.

In this paper I attempt to develop a monetary model that incorporates these key features of the blockchain and that can be used for the formal analysis of the blockchain-based monetary system. I study the economy with a single generally accepted blockchain-based currency. The money demand is based on the Lagos and Write (2005) and Fernandez-Villaverde and Sanches (2017). In the Lagos-Wright approach money de-

[6] I want to stress that mining is conceptually different from currency issuance.

[7] This is a necessary requirement for the operation of a blockchain which results from the double-spending problem and is not an artefact of technological constraints.

mand is endogenous rather than introduced in an ad hoc manner. Moreover, the model already includes the (exogenous) probability of trade on the decentralized market. The framework of this paper provides a new interpretation of this probability and makes it dependent on the parameters of the blockchain.

The processing of the financial transactions via a blockchain is modelled by a matching function in the spirit of the search and matching literature. The idea of a matching function is stemming from labor economics[8]. It is widely used in macro models to describe market imperfections: for example, labor market frictions[9] or the credit market mismatch[10]. I use the matching function to determine the probability of a miner success as well as the probability of a transaction confirmation. Both probabilities become functions of the number of transaction requests relative to the number of active miners. The (endogenous) probability of transaction confirmation corresponds the probability of trade in the Lagos-Wright model. Moreover, the matching function naturally reproduces externalities associated with mining.

I derive a monetary equilibrium of the model in terms of the return on money. Since the model explicitly includes some of the blockchain characteristics - such as mining costs and rewards - I am able to analyse their effects on the equilibrium money return in a comparative statics exercise. A higher reward to miners accelerates the money growth and reduces the equilibrium return on money. Higher costs of mining on the contrary put an upward pressure on the equilibrium return on money.

I also show that the agents in the economy hold an excess amount of currency units and submit an excess amount of transactions. Since agents know that every transaction request is processed only with a particular probability they submit more transaction requests than necessary out of a precautionary motive. As a consequence, the money demand function is hump-shaped: it increases for small values of the return on money

[8] Mortensen and Pissarides (1994) and (1999).
[9] See Gali (2010) for a review.
[10] For example, as den Haan et al., 2003, or Wasmer and Weil (2004).

and starts to decrease after some point. If the monetary equilibrium corresponds to the declining part of the money demand then the equilibrium is stable. These results are not present in the model of a traditional centralized monetary system.

The rest of the paper is organized as follows. Section 2 introduces a matching function for the money market. Section 3 describes the money demand. Section 4 presents the miners' problem and the evolution of the money supply. The equilibrium dynamics are discussed in section 5. Section 6 concludes.

2 Matching on the Money Market

The economy is populated by an infinity of miners who can decide to mine financial transactions or stay inactive. Active miners randomly choose transaction requests, verify them and execute (which technically means add them to the blockchain). The total number of processed transactions T_t is specified as a matching function

$$T(d_t, CPU_t) = \bar{T} d_t^{\eta} CPU_t^{1-\eta} \tag{1}$$

where transaction demand d_t is the number of submitted transaction requests, CPU_t is the number of computer processing units that were employed for mining. $0 < \eta < 1$ determines the elasticity of substitution between computational units and pending transaction requests. $\bar{T}$ is a scale parameter.

According to the matching function both miners and transaction requests are needed to "create" new processed transactions on the blockchain. For example, if $d_t = CPU_t$ then each miner "meets" a transaction request and $T_t = d_t = CPU_t$. If $CPU_t < d_t$ then $CPU_t < T_t < d_t$. The framework accounts for the fact that some transactions remain pending when the transaction demand is too high. The other way around, if $CPU_t > d_t$ then we have $d_t < T_t < CPU_t$. Some miners only spend electricity on mining but do not receive a reward. No transactions are processed when the demand for transactions

is zero or when there is no miners in operation.

Several clarifications are in order. First, real miners process blocks of transactions. For simplicity I assume that one block contains only one transactions with only one currency unit. I also assume that one miner posses one computer processing unit so CPU_t is equal to the number of miners on the money market.

Second, from the technical point of view miners can mine empty blocks and still receive a reward. The matching function rules this out. I argue that mining of empty blocks is not sustainable in equilibrium. If no transactions are verified and added to the blockchain the currency can not be effectively used as a mean of exchange. The value of such currency is zero in the long run and the reward is valueless for miners.

Third, the matching function states that an increase in CPU_t raises T_t. Many of the real blockchains periodically adjust the level of mining difficulty (and hence the mining costs) depending on the number of miners. These adjustments stabilize the number of transactions processed per unit of time. If, for example, CPU_t increases and, as a result, T_t rises then after a while the difficulty is increased and the number of verified transaction goes down again[11]. For such cryptoscurrencies this model can be applied to characterize a short run equilibrium.

Forth, my specification implies that a higher transaction demand makes it easier for miners to "meet" transaction requests. This is not true for real blockchains. Miners can always find a pending transaction at no costs. However, a higher transaction demand raises the fees that agents attach to their transaction requests and thus positively affects the profit of miners. I do not introduce fees explicitly. Instead, I assume that a positive effect of higher d_t comes from an increase in the probability of a miner's success.

Following the standard approach in the search and matching literature I characterize the money market in terms of market tightness $\theta = \frac{d_t}{CPU_t}$ which is the number of transaction requests per miner.

[11] In case of the Bitcoin blockchain the difficulty is adjusted approximately once in 2 weeks.

The matching function naturally introduces the externalities into the model. The probability of transaction confirmation $\sigma(\theta_t)$ increases with the number of miners and decreases with the total transaction demand on the market. The probability of success for miners $\lambda(\theta_t)$ increases with the transaction demand and decreases with the number of miners on the market.

$$\sigma(\theta_t) = \frac{T(d_t, CPU_t)}{d_t} = T\left(1, \frac{1}{\theta_t}\right) = \bar{T}\theta_t^{\eta-1},\ \sigma'(\theta_t) < 0 \tag{2}$$

$$\lambda(\theta_t) = \frac{T(d_t, CPU_t)}{CPU_t} = T\left(\theta_t, 1\right) = \bar{T}\theta^{\eta},\ \lambda'(\theta_t) > 0 \tag{3}$$

To sum up, too many transaction requests per miner implies an inefficiently small transaction confirmation probability in the model. In the real world we observe it through an increase in transaction fees. Too many miners relative to the transaction demand implies an inefficiently low probability of a miner's success. In reality a higher competition on the mining market results in higher energy consumption.

3 Demand for Money and Transactions

Money demand arises from a double coincidence problem as in the Lagos and Wright (2005) search theoretic approach. I only briefly sketch the framework and refer the reader to the original paper or to Fernandez-Villaverde and Sanches (2017) for the detailed derivations.

A continuum of buyers and a continuum of sellers, both of measure 1, live in the economy. Every period buyers are randomly assigned to sellers. Every buyer-seller pair negotiates on a deal according to which a seller produces and sells a particular amount of goods q_t to the buyer against a payment p_t. The buyer and the seller in every pair might never see each other again. Consequently they cannot rely on a credit and have to use money as a means of payment to be able to trade[12].

[12]In the Lagos and Wright (2005) every agent produces a unique good. Money is required to overcome

The negotiation of trade deals is achieved by "take-it-or-leave-it" offers from buyers to sellers. Denote the utility function of the buyer as $u(q_t)$ and the disutility from work of the seller as $w(n_t)$ where n_t is an amount of labor input[13]. The production function of the seller is linear and takes labor as the only input, $q_t = n_t$. Hence $w(n_t) = w(q_t)$. The first best amount of production and trade q^* is determined by $u'(q^*) = w'(q^*)$. If β is a discount factor, ϕ_t is a value of a currency units in terms of real goods and m_t is money holdings of the buyer then the bargaining problem can be written as

$$\max_{q_t, d_t} [u(q_t) - \beta \phi_{t+1} p_t] \tag{4}$$

$$\text{s.t. } -w(q_t) + \beta \phi_{t+1} p_t \geq 0 \tag{5}$$

$$p_t \leq m_t \tag{6}$$

The buyer wants to maximize his utility minus the real value of the payment. The participation constraint (5) ensures that a seller wants to participate in the trade deal. It always holds with equality. The liquidity constraint (6) states that the payment cannot excess the buyer's money holdings. Depending on whether the liquidity constraint is binding or not we might have an interior or a corner solution:

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

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

the double coincidence problem - that each party in the pair wants the good of the counter-party and the barter is possible. Exogenous distinction between buyers and sellers does not affect the results.

[13] $u(0) = 0, u'(0) = \infty, u'(\cdot) > 0, u''(\cdot) < 0$ and $w(0) = 0, w'(\cdot) > 0, w''(\cdot) > 0$.

Whenever the buyer has an amount of real balances $m^* = \beta^{-1}w(q^*)$ at hand he transfers this amount to the seller and consumes the optimal amount $q*$. If the buyer has less real money balances at hand he simply spends all his money and gets whatever the seller is willing to produce for this payment.

In the standard Lagos-Wright model buyers and sellers are able to trade with an exogenous probability σ. In the current model trade also occurs only with the probability $\sigma(\theta_t)$. However, the interpretation is different. In the current set-up the buyer-seller pair needs to transfer p_t currency units through a blockchain (one transaction is assumed to contain one currency unit). Each transaction is processed with the probability $\sigma(\theta_t)$. The pair thus submits d_t transaction requests such that $p_t = \sigma(\theta_t)d_t$. Since the buyer can only transfer currency units that he possesses, money demand equals the transaction demand, $m_t = d_t$.

Denote as $\gamma_t = \frac{\phi_{t+1}}{\phi_t}$ the return on money. Money demand stays finite only when $\gamma_t \leq \beta^{-1}$. Apart from the endogenous probability of trade money demand function is identical to Lagos, Wright (2005) and Fernandes-Villaverde and Sanches (2017).

$$\sigma(\theta_t)\frac{u'(q_t)}{w'(q_t)} + 1 - \sigma(\theta_t) = \frac{1}{\beta\gamma_{t+1}} \tag{7}$$

$$\phi_{t+1}m_t = \beta^{-1}w(q_t) \tag{8}$$

Condition (8) comes from the bargaining solution. Condition (7) is defined by the utility maximization of a buyer. It determines the amount of trade as a function of the return on money given the trade probability. If $\gamma_{t+1} = \beta^{-1}$ then $q_t = q^*$. This result corresponds to the Friedman (1969) rule.

One important feature of the Lagos-Wright model is a centralized market phase at the beginning of every period. On the centralized market buyers can freely adjust their money holdings and sellers can spend the earnings from the period before. This makes the distribution of money holdings degenerate.

Again, the detailed derivation of (7) and the discussion about the centralized market can be found in Lagos and Wright (2005).

4 Miners and Money Supply

The money market features a free entry for miners. Every miner uses one computer processing unit CPU to process a transaction request and pays real costs $P_t^e c\phi_t$. Here P_t^e is the price of electricity in currency units and c is a fixed amount of electricity that one CPU consumes.

With probability $\lambda(\theta_t)$ the miner "meets" a transaction request, processes it and receives r currency units as a reward. The reward can be spend in the next period and thus has a real value $\phi_{t+1}r$.

Free entry drives miners' profits to zero, therefore [14]

$$P_t^e c\phi_t = \beta\lambda(\theta_t)r\phi_{t+1} \tag{9}$$

If we were able to specify the electricity price in terms of consumer goods then we would be able to determine a real price of money. For example, if electricity is a consumer good itself then its price equals the price level in the economy $\frac{1}{\phi_t}$. Then the (expected) future real price of money is driven by the electricity consumption of miners and their reward $\phi_{t+1} = \frac{c}{\beta.\lambda(\theta_t)r}$.

Alternatively, the model needs to include an electricity market to describe the dynamics of P_t^e. I start with a simple version of the model by assuming that only a part of the total electricity demand comes from miners. Hence mining cannot significantly affect the electricity price. In other words I assume that the price is exogenous and constant: $P_t^e = P^e \ \forall t$ and $\psi \equiv P^e c$. Note that nominal costs ψ and the nominal reward r are per transferred currency unit and $0 < \psi < 1$ and $0 < r < 1$.

[14] Miners are owned by buyers and sellers in equal proportions. Consequently, outside of the equilibrium path all profits and losses are equally redistributed among buyers and sellers.

The free entry condition becomes:

$$\psi\phi_t = \beta\lambda(\theta_t)r\phi_{t+1} \tag{10}$$

Suppose that ϕ_{t+1} increases and the profit of miners becomes positive. New miners enter the money market. Consequently, the market tightness declines and so does $\lambda(\theta_t)$. This drives the profits back to zero such that the condition (10) holds again.

Miners can not directly decide on the money supply. Money stock is increased when the processing of new transactions T_t is rewarded.

$$M_t = M_{t-1} + rT_t \tag{11}$$

Equation (11) can be written as $M_t = M_{t-1} + r\sigma(\theta_t)d_t = M_{t-1} + r\sigma(\theta_t)m_t$. On the equilibrium path money demand m_t and money supply M_t are equal.

$$M_t = M_{t-1} + r\sigma(\theta_t)M_t \tag{12}$$

$$M_t = \frac{1}{1 - r\sigma(\theta_t)}M_{t-1} \tag{13}$$

The model predicts a constant money growth in equilibrium. The growth rate is higher, all the other things stay equal, when 1) the reward per block r is higher or 2) the probability of a transaction confirmation $\sigma(\theta_t)$ is higher. Since $\sigma'(\theta_t) < 0$ the second condition means that the money growth rate is higher when the market tightness is lower.

Proposition 1: On the equilibrium trajectory money supply is growing with a positive rate. Constant money supply (and constant price) equilibrium is achieved only with a zero reward per block.

5 Equilibrium Dynamics

Real money demand can be expressed as a function of the trade on the decentralized market q_t which is in turn a function of γ_{t+1} and θ_t. From (8) one can express

$$z(\gamma_{t+1}, \theta_t) = m_t \phi_t = \frac{w\left(q_t(\gamma_{t+1}, \theta_t)\right) \phi_t}{\beta \phi_{t+1}} = \frac{w\left(q_t(\gamma_{t+1}, \theta_t)\right)}{\beta \gamma_{t+1}} \tag{14}$$

where q_t is defined as (7). In equilibrium real money supply $M_t \phi_t$ which is driven by (13) must be equal to the real money demand $z(\gamma_{t+1}, \theta_t)$. The dynamics of θ_t follow (10). The equilibrium path is described by

$$z(\gamma_{t+1}, \theta_t) = \gamma_t z(\gamma_t, \theta_{t-1}) \frac{1}{1 - \sigma(\theta_t) r} \tag{15}$$

$$\psi = \beta r \gamma_{t+1} \lambda(\theta_t) \tag{16}$$

$$\psi = \beta r \gamma_t \lambda(\theta_{t-1}) \tag{17}$$

which defines $\gamma_{t+1}(\gamma_t)$. In contrast to Lagos and Wright (2005) demand for real money balances depends not only on the return on money but additionally on the money market tightness.

In the standard model money demand goes to 0 as γ_t converges to 0. In the current set-up this is not necessarily true. A decline in γ_t reduces the miners' profit and miners leave the money market. Market tightness rises and $\sigma(\theta_t)$ falls. Buyers adjust their money holdings based on two considerations. On the one hand, since currency units have lower return, holding them is more costly and money demand declines. This purchasing power channel is the same as in the standard Lagos-Wright framework. On the other hand, the probability of transaction confirmations is lower. Buyers, therefore, have to submit more transaction requests to be able to trade. Due to this precautionary motive buyers increase their money demand. The total result depends on the specification of functional forms and calibration.

To analyse the equilibrium explicitly I impose functional forms for the utility function and the function of the disutility from efforts. Following Fernandez-Villaverde and Sanches, (2017)

$$u(q) = \frac{q^{1-g}}{1-g}, \text{ and } w(q) = \frac{q^{1+\alpha}}{1+\alpha}, \text{where } 0 < g < 1, \ \alpha \geq 0. \tag{18}$$

The money demand function (19) resembles the one in Fernandez-Villaverde, Sanches (2017). However, the probability of trade $\sigma(\theta_t)$ is endogenous and determined by (2). θ_t can be expresses as a function of γ_{t+1} from (16)

$$z(\gamma_{t+1}, \theta_t) = \frac{(\beta\gamma_{t+1})^{\frac{1+\alpha}{g+\alpha}-1}}{1+\alpha} \left[\frac{\sigma(\theta_t)}{1-(1-\sigma(\theta_t))\beta\gamma_{t+1}}\right]^{\frac{1+\alpha}{g+\alpha}} \tag{19}$$

Figure (1) plots money demand (19). I took the standard parameter values: β =0.997, α =0.5, η=0.5, g =0.5 I chose the level of reward based on the statistics for the BTC blockchain. According to blockchain.info[15] a miner's revenue lies between 0.6% and 1.8% of a transaction volume. I set r=1.5%. Mining costs per block are 20% which means $\psi = 0.2$. While it is difficult to estimate the electricity costs of miners the resulting money demand function is pretty insensitive to the value of ψ.

The dashed line presents the demand function for a constant probability of transaction confirmation. $\sigma = 0.3$. It corresponds to the money demand function in the baseline model of Fernandez-Villaverde and Sanches (2017). In this case money demand uniformly increases with γ_{t+1}. This result comes from the purchasing power channel. The solid line plots the money demand in the current model. From the plot we see that after γ_{t+1} reaches a particular level the money demand starts to decrease. The reason for that is the presence of mining. When deciding on the money holdings and the transaction demand buyers take into account that only $\sigma_t d_t$ of currency units will be transferred. Because $\sigma(\theta_t)$ is less that one, buyers hold an excessive amount of currency and submit

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

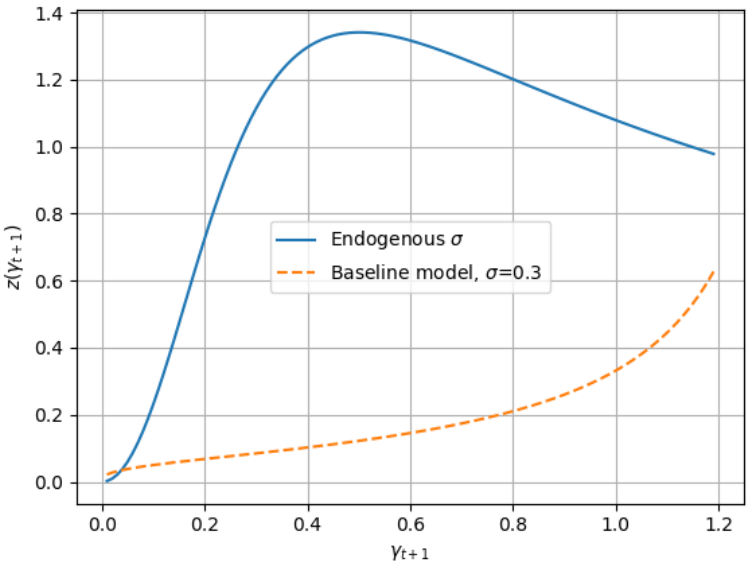


Figure 1: Money demand as a function of the return on money.

an excessive amount of transactions. This is a precautionary money demand channel.

When return on money increases new miners enter the money market and $\sigma(\theta_t)$ rises. Thus, the excessive demand for transactions goes down and the total money demand declines. Figure (1) indicates that after some value of the return on money the precautionary channel prevails and the demand for money decreases with γ_{t+1}.

The gap between the two functions quantitatively depends on the chosen parameter values. However, qualitatively the result is robust to different calibrations. The elasticity of substitution in the matching function most strongly affects the form of $z(\gamma_{t+1})$. The humped shape is preserved for non-extreme values, $\eta \in [0.3, 0.8]$.

The additional precautionary channel in the money demand changes the stability properties of the monetary equilibrium if the equilibrium γ^* corresponds to the declining part of $z(\gamma_{t+1})$. To see that, substitute the specifications (18) into the equilibrium

conditions (15) - (17) to obtain the equilibrium trajectory $\gamma_{t+1}(\gamma_t)$:

$$\frac{\gamma_{t+1}^{\frac{1+\alpha}{g+\alpha}\frac{1}{\eta}-1}\left[1-r\bar{T}(\frac{\psi}{\bar{T}r\beta\gamma_{t+1}})^{\frac{\eta-1}{\eta}}\right]}{\left[1-(1-T(\frac{\psi}{T\beta\gamma_{t+1}})^{\frac{\eta-1}{\eta}})\beta\gamma_{t+1}\right]^{\frac{1+\alpha}{g+\alpha}}}=\frac{\gamma_t^{\frac{1+\alpha}{g+\alpha}\frac{1}{\eta}}}{\left[1-(1-T(\frac{\psi}{T\beta\gamma_t})^{\frac{\eta-1}{\eta}})\beta\gamma_t\right]^{\frac{1+\alpha}{g+\alpha}}} \tag{20}$$

This expression describes the dynamics of the return on money γ_{t+1} as a function of γ_t. First, note that γ=0 is a solution of this equation. There exists a non-monetary equilibrium with zero return on money, zero money demand and no trade on the decentralized market.

Additionally, the economy can be in a monetary equilibrium with $\gamma > 0$ such that

$$A\gamma^{\frac{1-\eta}{\eta}}+\gamma-1=0 \tag{21}$$

$$\text{where } A=(Tr)^{\frac{1}{\eta}}\beta^{\frac{1-\eta}{\eta}}\psi^{\frac{\eta-1}{\eta}}>0 \tag{22}$$

Let us consider a special case with η=0.5. In this case the model can be solved analytically and

$$\gamma^*=\frac{1}{1+\frac{\beta T^2r^2}{\psi}}=\frac{\psi}{\psi+\beta T^2r^2} \tag{23}$$

The value of the γ^* depends on the ratio $\frac{r^2}{\psi}$.

Proposition 2 (comparative statics): The return on money in a monetary equilibrium 1) is increasing with the cost parameter ψ, 2) is decreasing with the reward r.

Higher mining costs discourage miners from processing transactions and hence a higher return on money γ^* is required to compensate the miners. In the extreme case if ψ goes to zero and $r > 0$ the miners receive a positive reward at zero costs. Infinitely many miners enter the money market and the probability of success of a single miner goes to zero. The number of mined blocks goes to zero and the currency becomes valueless,

$\gamma^* = 0$.

Higher reward r incentivizes more miners to enter the market. More currency units are injected into the network which leads to a lower return on money. If the reward to miners goes to zero then there is no injections of newly created currency units and return on money stays constant. It means that the price level stays constant.

Proposition 3: In a monetary equilibrium with finite mining costs $\gamma^* \leq 1$ which means that inflation is positive as long as the reward to miners is positive.

This is a pretty intuitive yet important feature of blockchain cryptocurrencies that the model is able to correctly describe.

A blockchain-based monetary system is unable to achieve a price stability. The presence of electricity costs requires a reward to miners in a form of newly created currency units. Consequently, the money supply is rising by construction. Moreover, if the blockchain protocol specifies that reward will go to zero at some point of time and miners will be compensated solely by transaction fees, then γ^* will converge to one and a positive money growth rate will no longer be necessary.

Let us consider the equation (20) again. Figure (2) plots the function $\gamma_{t+1}(\gamma_t)$ for the same calibration as described above together with a 45-degreee line. The equilibrium return on money is defined as an interception of two lines. For the used calibration $\gamma^* = 0.997$ which corresponds to approximately 3% inflation.

The slope of the function at γ^* is smaller than 1. It means that the equilibrium trajectories that start from $\gamma_0 > 0$ converge to a monetary equilibrium with a positive value of currency. Because γ^* corresponds to the declining part of the money demand function the precautionary channel plays a major role. The return on money declines when the initial value is too high and rises when the initial value is too low. As before this result holds for $\eta \in [0.3, 0.8]$.

Proposition 4: Monetary equilibrium is stable due to the presence of a precaution-

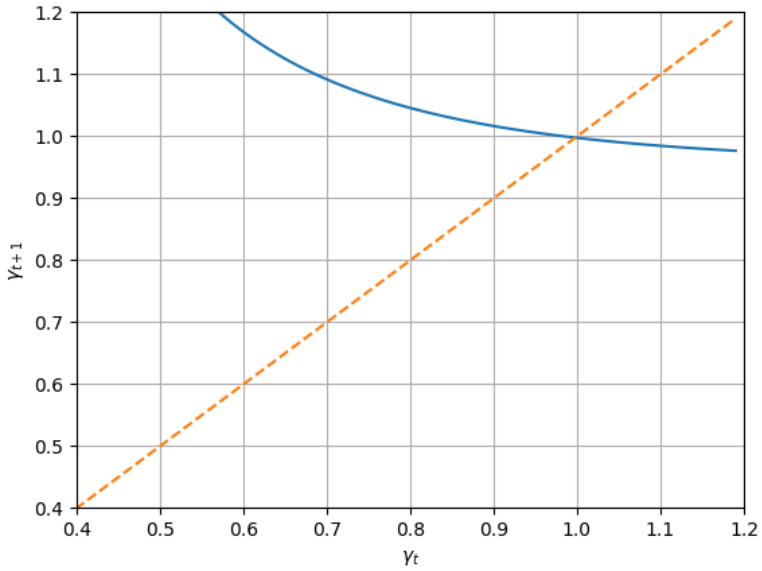


Figure 2: Monetary steady state

ary money demand channel.

6 Conclusion

This paper proposes a monetary model of a private digital currency circulating according to a blockchain protocol. The analysis is motivated by the recent development of cryptocurrencies. However, the main goal of the paper is to develop a general framework that would be able to describe a blockchian-based monetary system rather than to explain empirical findings about a particular cryptocurrency. This is the first attempt to my knowledge to build a monetary model that incorporates the basic features of the blockchain monetary system.

I propose to use a matching function to model how miners "meet" pending transaction requests and "create" new processed transactions on the blockchain. The matching function natural captures the externalities of the blockchain monetary system: the prob-

ability of a miner's success increases with the transaction demand and decreases with the total number of miners on the market; the transaction confirmation probability increases with the number of miners and declines with the number of pending transaction requests.

The demand side of the money market is based on the Lagos and Wright (2005). The standard framework is altered by the fact that agents have to submit transaction requests before they are able to transfer currency units. Every transaction request is processed only with a particular probability and hence the trade also happens only with a particular probability. In contrast to the Lagos-Wright approach in the current set-up the probability of trade is endogenous. It depends on the number of miners and the transaction demand.

I use the model to analyse the effects of mining costs and rewards on the equilibrium outcome. The return on money in equilibrium increases with the mining costs and decreases with the reward for miners. Higher mining costs require a higher return on currency to compensate miners for their work and a higher reward means that a lower return on money is sufficient.

Endogenous probability of the transaction verification and, hence, of trade changes the properties of the money demand function. More specifically, agents hold an excessive amount of money units due to a precautionary motive. The reason for the precautionary money demand is the fact that every transaction is processed only with a particular probability. With an increase in the return on money more miners start to operate and the probability of transaction confirmation rises. Agents reduce their excessive money holdings and the money demand goes down. In contrast to the standard model in which the money demand uniformly increases with the return on money, in the current set up the money demand is hump-shaped: it increases for low values of the return on money and starts to decline after a particular level when the precautionary motive prevails.

The hump-shaped money demand function changes the stability properties of the

system. If in the monetary equilibrium return on money corresponds to the declining part of the money demand function then this equilibrium becomes stable. In other words, money cannot become valueless if its initial value is positive. If, for example, a shock forces the return on money to go below the equilibrium level then some miners leave the market. Individuals then have to increase their precautionary money demand which puts an upward pressure on the money return. Similarly, the return on money cannot explode.

The proposed model abstracts away many important and interesting ingredients of actual blockchains-based currencies. For example, the decision to attach transaction fees to a transaction request, miners' decisions about the composition of the block, costs of entering the mining market, adjustments in the difficulty or a necessity to possess a particular amount of currency units to be allowed to mine. From the economic point of view the paper abstracts from the social costs of the excessive electricity consumption, the capital overinvestment and the environmental pollution. Additional features can be introduced into the current framework at the costs of reducing the model tractability. Many of these aspects are novel to the literature and their accurate formulation represents an independent research topic on its own.

7 References

1. Berentsen, A. and Schaer, F., 2018. A Short Introduction to the World of Cryptocurrencies. Federal Reserve Bank of St. Louis Review, First Quarter 2018, 100(1), pp. 1-16. https://doi.org/10.20955/r.2018.1-16.
2. Berentsen, A., 2006. On the private provision of fiat currency. European Economic Review, 50(7), pp.1683-1698.
3. 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.
4. Cavalcanti, R.D.O. and Wallace, N., 1999. A model of private bank-note issue. Review of Economic Dynamics, 2(1), pp.104-136.
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., 2017. Can Currency Competition Work? Upenn Working Paper.

7. Friedman, M., 1969. The Optimum Quality of Money, and Other Essays. Macmillan.

8. Gal, J., 2010. Monetary policy and unemployment (No. w15871). National Bureau of Economic Research.

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

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. Mortensen, D.T. and Pissarides, C.A., 1994. Job creation and job destruction in the theory of unemployment. The review of economic studies, 61(3), pp.397-415.

15. Mortensen, D.T. and Pissarides, C.A., 1999. Job reallocation, employment fluctuations and unemployment. Handbook of macroeconomics, 1, pp.1171-1228.

16. Peters, G.W. and Panayi, E., 2016. Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. In Banking Beyond Banks and Money (pp. 239-278). Springer International Publishing.

17. Swan, M., 2015. Blockchain: Blueprint for a new economy. " O'Reilly Media, Inc.".

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.

007 "Knowing me, knowing you: inventor mobility and the formation of technology-oriented alliances" by Stefan Wagner and Martin C. Goossen, February 2018.

008 "A Monetary Model of Blockchain" by Anna Almosova, February 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.