A MONETARY THEORY OF BLOCKCHAINS*

Dean Corbae
University of Wisconsin

Ted Temzelides
Rice University

Randall Wright
University of Wisconsin

January 31, 2019

Abstract

We develop a monetary theory of blockchains.

*Preliminary and incomplete

1 Introduction

Government issued paper money has been the medium of exchange of choice for well over a century. As technology and record-keeping improve, new possibilities emerge involving (possibly private) monetary systems that can compete with and eventually replace fiat money. Some underlying conditions are necessary for the viability of such e-cash systems. These include the need for intertemporal trade when simple barter does not suffice, and the existence of frictions that make credit non-viable, at least in some transactions. Paper money has some other disadvantages. It can be stolen or counterfeited, it may be hard to transport across space, unhygienic, etc.

In this paper we build a model of blockchains. Our environment combines decentralized markets (DM) with endogenous matching, as in CTW, and centralized markets (CM) with quasi-linear utility, as in LW.

2 The Economic Environment

Time is discrete: $t = 0, 1, ...$ Let $I = \{1, ..., N\}$ be a finite set of agents, where $N > 2$ is an even number. Agents discount the future at the common discount factor $\beta \in (0, 1)$. Each period consists of two subperiods. In the first, agents interact in a DM, while in the second they participate in a CM. Agents consume and work in both subperiods., and their overall period-utility is given by

$$\mathcal{U}(x, h, X, H) = u(x) - c(h) + U(x) - H \tag{1}$$

where x, h (X, H) are consumption and labor during the DM (CM). The DM involves trade of perfectly divisible, non-storable goods. As is standard, we will assume an extreme specialization of tastes and production possibilities that makes trade necessary for consumption. Agent i likes good i only and produces good $i+1$ only (mod k). The CM involves trade of a general good that is liked by everyone and can be produced by everyone using a linear production function. As is standard, we assume u, c, U are C^2, u', c', $U' > 0$, u'', $U'' < 0$, $c'' > 0$, $u(0) = c(0) = 0$, $\exists q^* \in (0, \infty)$ s.t. $u'(q^*) = c'(q^*)$. The quantity q^* is *efficient,* in the sense that it equates the marginal utility of the consumer to the marginal cost of the producer in each transaction. We will pay exclusive attention to setting up incentives in a way that q^* is the resulting quantity exchanged in each transaction. Abusing notation, we will henceforth use u to denote $u(q^*)$, and c to denote $c(q^*)$. We will assume that $c < \beta u$. We also assume that in the CM $\exists X^* \in (0, \infty)$ s.t. $U'(X^*) = 1$, with $U(X^*) > X^*$.

The details of trade are described next. We begin with the DM. Agents are matched bilaterally in each period. This is described by an *assignment rule* $\Psi = \{\psi_t\}$, where at every date t, $\psi_t : I \to I$ is a bijection that assigns to every individual a partner. As a convention, $\psi_t[\psi_t(i)] = i$. At every date t, ψ_t induces a *partition* θ_t of A into subsets, or *coalitions*, of size 1 or 2. Let Θ be the set of partitions consisting of all such coalitions.

Next, we define an equilibrium. Our equilibrium concept uses both coalitional stability (DM) and competitive equilibrium (CM) elements.

Let z_t^i be the individual state. The aggregate state, Z_t, specifies z_t^i for every i. Let σ_t^i be an individual decision variable, constrained to lie in a set which generally depends on the state, $\Sigma^i(Z_t)$. Let σ_t specify σ_t^i for every i. Let $Y_t = (\theta_t, Z_t, \sigma_t)$, and denote instantaneous payoffs by $w_t^i(Y_t)$ and the law of motion for the state by $Z_{t+1} = f(Y_t)$. A history at t is given by $h_t = (Y_0, Y_1, ..., Y_{t-1}, Z_t)$, and H_t is the set of possible histories. Matching is described by $\Phi = \{\Phi_t\}$ where $\Phi_t : H_t \to \Theta$. For each agent i we also have a decision rule $\Gamma^i = \{\Gamma_t^i\}$ where $\Gamma_t^i : H_t \times \Theta \to \Sigma^i$. Let Γ specify the profile of individual decision rules.

For any Φ and Γ, lifetime utility of agent i at t in history h_t is given by

$$v_t^i(h_t) = w_t^i\left[\Phi_t(h_t), Z_t, \sigma_t\right] + \beta v_{t+1}^i(h_{t+1}) \tag{2}$$

where σ_t is determined from the decision rules $\Gamma_t^i(h_t, \theta_t)$ and h_{t+1} is constructed in the obvious way. An equilibrium In the DM is a pair (Φ, Γ) such that for every t and h_t, no coalition C consisting of 1 or 2 agents can do better by deviating either by matching differently than as prescribed by Φ or by taking a decision different than that prescribed by Γ. When we say that C does better we require two things. First, agents take as given that at date t, every $j \notin C$ matches according to Φ, as above. Second, from date $t+1$ on, matches and decisions are determined by (Φ, Γ) from the history h_{t+1} induced by the deviation. In a *history-independent* equilibrium, (Φ, Γ) does not depend on h_t except through the current state Z_t.

As the CM is "frictionless," we will model it as a Walrasian market and employ competitive equilibrium as the solution concept. An overall equilibrium requires equilibrium in both the DM and the CM.

3 The First-Best

Since meetings in the DM are bilateral, the best possible symmetric allocation has every agent consuming and producing in every other period. This allocation is efficient, provided that $u > c$. For example, at $t = 0$, agent 1 produces for agent 2, agent 3 produces for agent 4, and so on, while at $t = 1$, agent 2 produces for agent 3, agent 4 produces for agent 5, and so on, and this periodic pattern repeats every two periods. The lifetime utilities in this efficient allocation are as follows:

$$\text{Agents } 2,4,...,N\text{: } W^e = \sum_{t=0}^{\infty}(u - \beta c) = \frac{u - \beta c}{1 - \beta^2}$$

$$\text{Agents } 1,3,...,N-1\text{: } W^e = \sum_{t=0}^{\infty}(-c + \beta u) = \frac{-c + \beta u}{1 - \beta^2} \tag{3}$$

Of course, a symmetric efficient arrangement exists in which we start with agents $2, 4, ..., N$ producing and agents $1, 3, ..., N-1$ consuming at $t = 0$ and so on. The efficient allocation satisfies two conditions. First, no production/consumption opportunities are lost. Second, the efficient quantity, q^*, is produced and consumed in every exchange. The first-best allocation in the CM is indeterminate and involves any combination across agents that leads to consumption and production of X^*, where $U'(X^*) = 1$.

In what follows, we will concentrate on efficient allocations; i.e., those in which no trade opportunities are lost, and where the socially efficient quantity is exchanged in all trades.

4 Blockchains

We model a technology that decentralizes both information and record-keeping. While there is a large literature on blockchains, it tends to concentrate on investigating its cryptography and computer implementation aspects.[1] Here we will largely abstract from these aspects in order to concentrate on economic incentives related to the monetary/transactions aspect of the problem. More precisely, we will demonstrate how this technology can decentralize information and support an analog of the first best allocation of the previous section. Our analysis is mainly normative, in the sense that we study the implementation of efficient transaction patterns under blockchain technologies, rather than trying to replicate properties of existing blockchains systems.

Abstracting from details, a blockchain is effectively a technology allowing for money transfers, say, from buyers to sellers, to take place instantly and in the absence of a third "trusted" intermediating party. These transactions are then recorded in a "decentralized" fashion. This is accomplished through the concept of an "open distributed ledger." Every time a transaction occurs, this is added as part of a new "block;" thus, updating the chain of the existing blocks in the ledger. Importantly, the updated ledger, including every participant's balance,

[1] Exceptions include...

is "distributed," that is, it is available to every "node;" i.e., every participating agent in the network. This removes the dependence on third parties. Of course, it is essential that the distributed ledgers are "synchronized," in the sense that they are showing the same balances, summarizing the same histories of transactions, at each point in time. In addition, it is necessary to ensure that every update of the ledger is credible and no illegitimate changes are made. In current practice, a common way to accomplish this involves "proof of work" schemes which, in turn, impose certain (mining) costs. Thus, actual blockchain systems consist of a set of "users" who wish to perform transactions, together with a set of "miners," who encode them and add them to the ledger. Other aspects are present, some due to technology constraints, others due to choice of design.

Miners are compensated only when they are selected to mine a block. The reward is in an electronic currency, say, bitcoin. There can also be transaction fees paid by the users whose transactions are to be processed. The protocol specifies how many bitcoins are awarded for each block. Interestingly (from a monetary theory point of view), this number is set to decline over time (halved every four years). Transaction fees are chosen by the users, who might try to gain priority in the case where the system is congested and there are delays. In that case, miners will prioritize the recording of transactions for users who are willing to pay higher fees.

It is important to point out that mining costs can be substantial (for example, in implied electricity consumption), and there is concern about the social waste associated with such activities. For example, when multiple miners are working on a problem, they all use a substantial amount of computer power, although only one will eventually solve the underlying problem and earn the reward associated with the ability to record a transaction.

Our model will abstract from many of the ad hoc aspects of actual blockchain structures. For example, we assume that each block contains one transaction, and we currently do not distinguish between fixed (bitcoin) and transaction fee compensation for miners.

5 Decentralization through a Blockchain

Here we introduce blockchains as a way to induce trade in the DM. Our goal will be to support the efficient allocation in the absence of public memory. We can think of all agents simultaneously making reports to the blockchain in every period. If the reports "match" in the obvious sense; i.e.,

$$
\begin{aligned}
i &: \text{"sending } m \text{ bitcoins to } j \text{ in exchange for } q \text{ units of good"} \\
j &: \text{"sending } q \text{ units of the good to } i \text{ in exchange for } m \text{ bitcoins"}
\end{aligned}
$$

then we would like to assign them to a new block and add them to the blockchain. Otherwise, they are ignored. A **blockchain** is a sequence of vectors of nonnegative balances $\{(B_t^i)_{i=1}^N\}_{t=0}^\infty$ with $(B_0^i)_{i=1}^N \in \mathbb{R}_+^{\mathbb{N}}$ given, and a rule f for updating these balances, where $(B_{t+1}^i)_{i=1}^N = f[(B_t^i)_{i=1}^N,$agents' reports at $t]$. Recording requires the use of a "miner." In principle, each of the N agents can be a miner. For now, we assume that there are $\mu = n$ additional agents, whom we will call miners. A miner can verify and record at most one transaction per period, at cost C_B. He is compensated for his effort in the centralized market. We assume that this compensation, Y, will be paid by the consumers in the DM transactions and that the payment comes through transferable utility in the next CM. Since the CM will re-initialize agents' balances, we will concentrate on balance adjustments that do not depend on t; i.e., $(B_{t+1}^i)_{i=1}^N = f[$agents' reports at $t]$.

5.1 Rationing

One important feature of actual blockchains is the possibility that the volume of transactions needing to be recorded in a given period exceeds the recording ability of the system. In that case, some ”rationing” will need to take place. Given the decentralized nature of the ledger, it is important that the rationing is implemented in a way that all participants update their ledgers in the same way. We will consider the case where technical constraints result in $\lambda \leq n = \frac{N}{2}$ transactions being recorded in every period. We will consider the following rationing rule for the case where $\lambda < n$: each of the n transaction pairs chooses and publicly submits a number in the interval $[0, 1]$. Subsequently, a real number in $[0, 1]$ is randomly chosen and announced publicly. The λ transactions that are associated with the announcements that are the closest to the chosen number are assigned to miners for implementation (ties are probability zero events). For now, we assume that remaining $n - \lambda$ transactions are dissolved and do not materialize (we can change this later, to introduce a queue).

Two features of the above scheme are worth noting. First, it relies on a random choice of number that becomes common knowledge. Thus, each agent can update their ledger in the same way, since there is no ambiguity as to which transactions were the closest to the number. Second, from a modeling point of view, this scheme effectively introduces random matching in the DM, although agents have no problem locating each other. The randomness is the result of the rationing.

Returning to the realized transactions, the system will transfer m bitcoins from the buyer to the seller in the transaction. How is the miner compensated for his cost? The total static surplus created in a transaction is $u - c - C_B$.[2] To compensate the miner, we assume that a fraction of the surplus, Y, will be paid as transferable utility in the CM to the miner by the buyer.

Let $W(M)$ be the value function of an agent with M bitcoins at the beginning of period t's CM. Recall that we concentrate on supporting the efficient quantity

[2] In actual blockchains, miners' compensation comes from two sources: (1) newly-minted bitcoins paid by the blockchain, and (2) fees paid by the transaction participants. The first source is designed to vanish over time. Here we assume that only the second source is present.

in every transaction. How is m determined? We can use Nash bargaining assuming the "efficient" bargaining weights in order to accommodate the Hosios inefficiency:

$$\begin{aligned} &\max_{q,m} \left[u(q) + W\left(M - m\right) - W_t(m)\right] \\ &\qquad\text{s.t. } m \leq M,\ q \geq 0 \end{aligned} \tag{4}$$

Let ϕ be the price of bitcoin in the CM. The ex ante value function of a buyer, a seller, and a miner with M bitcoins at the beginning of period t's DM are respectively given by:

$$\begin{aligned} V^B(M) &= \min\{1, \frac{\lambda}{n}\} \left[u + W(M - m - \frac{Y}{\phi})\right] + \left[1 - \min\{1, \frac{\lambda}{n}\}\right] W(M) \\ V^S(M) &= \min\{1, \frac{\lambda}{n}\} \left[-c + W(M + m)\right] + \left[1 - \min\{1, \frac{\lambda}{n}\}\right] \left[W(M)\right] \\ V^{Mi}(M) &= \min\{1, \frac{\lambda}{n}\} \left[-c_B + W(M + \frac{Y}{\phi})\right] + \left[1 - \min\{1, \frac{\lambda}{n}\}\right] \left[W(M)\right] \end{aligned} \tag{5}$$

Certain incentive conditions must hold:

$$\begin{aligned} &\text{buyer: } u + W(M - m - \frac{Y}{\phi}) \geq W(M) \\ &\text{seller: } -c + W(M + m) \geq W(M) \\ &\text{miner: } C_B + W(M + \frac{Y}{\phi}) \geq W(M) \end{aligned} \tag{6}$$

Finally, $W(M)$, the value function of an agent with M bitcoins at the beginning of period t's CM is:

$$\begin{aligned} W(M) &= \max_{X,H,M'} \left\{U(X) - H + \beta V^i(M')\right\} \\ \text{s.t. } X &= H + \phi M - \phi M' \\ i &\in \{B, S, Mi\},\ X \geq 0,\ M' \geq 0,\ 0 \leq H \leq \overline{H} \end{aligned} \tag{7}$$

Note that the above value functions are written guessing that all agents will exist the CM with the same amount of money holdings in each period.

6 Blockchain Equilibrium

We can define a **Dynamic Blockchain Equilibrium** as an array $\left\{V_t^B, V_t^S, V_t^{Mi}, W_t, X_t, H_t, m_t', q_t, \phi_t\right\}$ s.t. *(i)* given prices, the decision rules satisfy the respective FE; *(ii)* given value functions, terms of trade in the DM solve the bargaining problem; *(iii)* $\phi_t > 0$; *(iv)* the CM clears, *(v)* meetings in the DM are consistent with stable matching.

We can then think of monetary policy as lump-sum bitcoin transfers in the CM and conjecture that the Friedman rule will be optimal.

7 Questions to be Addressed

1. This is written as if all agents exit the CM with equal money balances. However, agents will start the next DM as heterogeneous (buyers, sellers, miners).

2. Miners can only be compensated in the CM. Should miners also trade in the DM?

3. If a transaction is rationed, we assume that it ”disappears.” We can have it enter a queue instead and be executed with some probability in the next period. Multiple DM rounds before each CM?

4. Other than optimal monetary policy, other issues can be addressed.

8 References

Athey, S., Parashkevov, I., Sarukkai, V., and J. Xia (2016): ”Bitcoin pricing, adoption, and usage: Theory and evidence”

Chiu J., and T. Koeppl (2017): ”The Economics of Cryptocurrencies: Bitcoin and Beyond”

Chiu J., and T. Koeppl (2018): ”Blockchain-based Settlement for Asset Trading”

Easley, D., O’Hara, M., and S. Basu (2017): ”From mining to markets: The evolution of bitcoin transaction fees,” Working paper

Huberman, G., Jacob D. Leshno, J.D., and C. Moallemi (2017): ”Monopoly without a Monopolist: An Economic Analysis of the Bitcoin Payment System,” Columbia Business School Working Paper