The Bitcoin Network as a Defense Mechanism: A Search and Matching Approach

Antzelos Kyriazis*

May 2025†

Abstract

What is the role of Bitcoin? This paper tries to argue that one of the roles of the Bitcoin network is to be a defense mechanism against transaction blocking by introducing a search and matching model with indivisible money. The model is enriched with security frictions due to a positive probability of transaction blocking. I study the optimal trading decisions between buyers and sellers under a fiat currency regime and under the assumption that trading happens with BTC tokens over the Bitcoin network. I show that if the honest miners in the Bitcoin network have higher marginal revenues from mining per unit of marginal cost than dishonest miners, the network remains secure. In this case, if the welfare cost of mining is lower than the welfare cost of not being able to transact in the fiat regime or if the total transaction volume is higher in the Bitcoin regime, then social welfare is more likely to be higher under the Bitcoin regime. If dishonest miners are in control, transactions between honest sellers and buyers are blocked. In this case the fiat currency regime can be better. Over the transition, social welfare depends on the parameter that controls for the speed of the money supply increase and it is not clear which of the two regimes is better. In addition, I show that if fixed costs are introduced then honest miners need a lower amount of total effort to secure the network. Finally, the first-best outcome can be achieved in the Bitcoin regime, even if the solution comes from a Nash bargaining, by optimally setting the transaction fees.

*Email: antzelos.kyriazis@aya.yale.edu

Disclaimer: This publication is made available for informational purposes only. Nothing herein shall be construed as investment advice and this is not a recommendation or advice to buy or sell bitcoin or any other commodity or security or investment. The reader is urged to seek professional assistance before investing. As of the date of this publication, the author does hold BTC and may, in the future, engage in additional purchase or sale transactions involving BTC. The views, analyses and conclusions contained in this article are solely those of the author and do not represent the views of the organization he works for.

†This is a project that I started as a graduate student in the Department of Economics at Yale University, but I was unable to finish by the time of graduation. The project was independently completed after graduating.

1 Introduction

A question that has been posed multiple times since 2009 is what is the role of Bitcoin. There are several reasons behind this question including the limited, but growing over the years, Bitcoin transactions, together with a not well-defined regulatory framework for digital assets. In this paper I follow a different approach and argue that the Bitcoin network can play the role of a defense mechanism against economic exclusion, by using a search and matching model of money augmented with security frictions due to a positive probability of transaction blocking. Interpreting Bitcoin as a network that allows its users to "communicate", that is to transact, in a censorship resistant way without transaction blocking risks due to the high costs of blocking transactions, can lead to different conclusions about the role of Bitcoin.

Specifically, according to Bitcoin proponents, agents who can benefit from censorship resistance in halting transactions include individuals and human right organizations in authoritarian regimes, unbanked or underbanked populations in poorer countries who may face significant hurdles in transacting etc. Also Bitcoin proponents argue that in a world dominated by a few payment systems controlled by superpowers in which these superpowers transact with the smaller countries aligned with them, but not necessarily with the other countries, the Bitcoin network naturally arises as an alternative global settlement layer due to being a decentrallized, permissionless, and censorship resistant network. In other words, the Bitcoin network can be the cooperative solution against a Nash equilibrium with multiple settlement layers subject to restrictions, interoperability issues etc. On the other hand, Bitcoin skeptics argue that censorship resistance in transactions can create incentives for agents to proceed with transactions related to illegal activities[1]. This paper does not focus on and is completely against using the network for illicit activities. Instead, the paper assumes that the agents facing transaction blocking are agents such as the individuals in authoritarian regimes.

In the model, I first analyze the decisions of buyers and sellers under the assumption that they can meet and trade in decentralized markets with some probability using an intrinsically worthless object that cannot be produced or consumed: fiat currency. I assume that some of the sellers are benevolent while others are not. The latter decide if they will allow the honest sellers to transact with the buyers. On the other hand, the buyers value the specialized goods sold by the sellers and would like to trade with them, but they are subject to transaction blocking risks. Transaction blocking is defined as a situation in which a buyer and an honest seller meet and are ready to trade, but their transaction does not go through due to a successful blocking attack from dishonest sellers. As a result, the status of buyers and honest sellers remains unchanged after their meeting in the market since the trade did not take place. Transaction halt happens with some exogenous probability in the fiat currency regime, and succeeds with some different exogenous probability. If buyers

[1]Recent reports such as the 2025 Crypto Crime Trends report by Chainalysis suggest that only 0.14% of total crypto transactions were associated with illicit activities in 2024 while the role of Bitcoin in those transactions has been declining over the years.

are not able to transact they incur a utility cost. Similarly, honest sellers also face a utility cost from not being able to transact. In the long run the value of money is positive because it allows agents to transact, but it is negatively affected by the probabilities related to transaction blocking and the associated utility costs. Social welfare, as a result, is lower in the fiat currency regime when security frictions are stronger, that is when the probabilities related to transaction blocking are higher, and when the resulting utility costs are higher.

Second, I repeat the analysis under the Bitcoin regime. The difference between transacting with fiat currency and transacting over the Bitcoin network is that the probability of transaction halt is now determined by the rules of the Bitcoin network. According to those rules, transaction blocking can happen only if somebody controls the absolute majority of the mining effort, that is $50\% + \varepsilon$. If there is no agent or entity controlling the majority of the mining effort then security frictions disappear. Based on the rules of the Bitcoin network I build a game between honest and dishonest miners, representing honest sellers and dishonest sellers respectively, and I derive the condition under which the probabilities related to a successful transaction halt become zero making the Bitcoin network secure. The condition says that as long as the marginal benefit of the benevolent miners per unit of marginal cost exceeds the marginal benefit of dishonest miners per unit of marginal cost, the honest miners will put more mining effort, and the network will be secure. I also show that in this case it is optimal for the dishonest miners to set the probability of attempting to block transactions equal to zero as well. The logic is very simple: since the attackers know that any form of attack has a zero probability of success, then it is optimal not to attack in the first place. At the steady state I show that the condition that guarantees the security of the network simplifies to requiring the dishonest miners to have a marginal cost of mining which is higher or equal to the marginal cost of mining of the honest ones.

I also compute the steady state social welfare under the Bitcoin regime and I compare it to that in the fiat currency regime. I find that if the distribution of buyers and sellers in the overall population is the same under the two regimes, then social welfare under the Bitcoin regime is higher if the social cost of mining at the steady state is lower than the net social cost of transaction blocking in the fiat currency regime. If, on the other hand, the distribution of buyers and sellers differs across the two regimes, then steady state social welfare can be higher in the Bitcoin regime also if the transaction activity under the Bitcoin network is higher than the transaction activity under fiat currency. In this case more trades happen between buyers and sellers in the Bitcoin network and utility benefits are higher.

Third, I introduce fixed costs for both types of miners. Fixed costs do not change the optimality conditions, but change the miners' decisions to enter the market. I derive analytically the conditions under which each type of miners enters the market and exerts effort. Higher fixed costs for any type of miners imply that the other type of miners needs to exert less effort to disincentivize the first type from entering the market.

Fourth, I introduce divisibility of goods and allow agents to decide how much of each good will be produced. The decision is made by following a generalized Nash bargaining which is subject to the incentive

constraints of the buyers and the sellers. I solve for the transitional dynamics under the two regimes and find that social welfare can be higher or lower along the transition in the Bitcoin regime, depending on how fast the money supply increases in each of the two regimes. Also the dynamics produced by the model under the Bitcoin regime resemble the dynamics for the price of BTC and hash rate seen in reality.

Finally, I show that in general, the Nash bargaining approach can lead only by chance to the socially optimal quantity that a social planner would choose, both under the fiat currency and under the Bitcoin regime. In both cases, the relative bargaining power of the buyers over the bargaining power of each type of sellers has to be determined by the relative surplus of buyers over the net gain from trade. In more realistic settings in which the bargaining power is determined by the size of each cohort in the population, the socially optimal quantities need not necessarily be produced. However, in the Bitcoin regime, I show that if there is significant consensus to implement a policy that sets the transaction fees equal to a weighted average of the utility of buyers and the cost of sellers for each good minus the extra value from holding money relative to being a seller of the corresponding good, then the socially optimal quantities of the goods can still be produced. The transaction fees work as a Pigouvian taxes for the buyers.

Related Literature: This paper is related mainly to the literature that uses search and matching type of models and analyzes money as a medium of exchange. Some prominent papers from this literature are the early and foundational first and second generation models of Kiyotaki and Wright (1989) and Trejos and Wright (1995). Those models analyze the properties of monetary equilibria under the assumptions of money indivisibility, but Kiyotaki and Wright (1989) also assume goods indivisibility, an assumption that was later relaxed by Trejos and Wright (1995). Another paper that builds in the tradition of the previous two, but also allows for asset confiscation is the paper of He et al. (2005). This paper introduces a security friction in the model that allows to analyze the role of defense mechanisms. In this paper I follow the three previous papers. I start with a model similar to He et al. (2005) under the fiat currency regime, but now the security friction is transaction halt. Then I introduce the Bitcoin network as a possible defense mechanism. I analyze the properties of monetary equilibria both under goods indivisibility and goods divisibility, for both regimes.

Under the Bitcoin regime the supply of assets is determined endogenously by the mining decisions. This distinguishes the paper from other papers in which there is an endogenous determination of asset supply such as Lagos and Rocheteau (2008), Rocheteau and Rodriguez-Lopez (2014), and Geromichalos and Herrenbrueck (2016). Moreover, Choi and Rocheteau (2021) also have miners deciding optimally about mining efforts and determining the money supply, but there is no game between honest and dishonest miners, since only sellers choose mining intensity.

Another strand of the literature that this paper relates to is the growing literature on Bitcoin and also on the relation between Bitcoin and money. The idea of the Bitcoin network was introduced by Nakamoto (2008). Since then, the Bitcoin network was also introduced in practice and has grown to be one of the

most important networks of our time, given the value that is being exchanged per year. Schilling and Uhlig (2019) studied a model with Bitcoin and government money and showed that the BTC price follows a martingale process in equilibrium. Fernández-Villaverde and Sanches (2019) studied a model of competition between private currencies and showed that the cost function is critical for the stability of prices in monetary equilibria. Lotz and Vasselin (2019) developed a model in which agents can hold both fiat currency and e-money, with e-money being more secure than fiat, and studied the conditions under which the two can coexist. I also introduce security frictions in this study, but I focus specifically on how those frictions can be overcome under the Bitcoin network by introducing a game about mining efforts between honest and dishonest miners. Finally, Pagnotta (2022) studied the determination of the BTC price together with the level of security of the network and found that there can be multiple equilibria. This paper is complimentary to Pagnotta (2022). I also study the determination of price and security level of the Bitcoin network, under a different and simpler model, I discuss the important role of transaction fees and fixed costs, and I show that socially optimal solutions can be achieved in the Bitcoin regime even under a Nash bargaining solution.

Paper Organization: Section 2 introduces the economic environment and the model under the assumption of goods indivisibility. I discuss the value of money under the two regimes, I derive the social welfare functions and I compare social welfare outcomes. Section 3 relaxes the assumption of goods invdivisibility. I allow the optimal quantity of produced goods to be chosen under a generalized Nash bargaining process and then I solve for the transitional dynamics. In section 4 I derive steady state conditions that could make the outcome of the Nash bargaining the same as the outcome that a social planner would choose including the transaction fees schedule in the Bitcoin network that leads to the social planner's solution. Section 5 concludes.

2 Economic Environment

There is a continuum of agents in the interval $[0,1]$. These agents trade in two different subperiods within a single period. There is a day market, which is frictionless, and a night market which is decentralized and characterized by matching between agents. The centralized market is simple: agents produce a general good Q, which requires no specialization. This good is divisible but non-storable. The utility from consuming this good is $U(Q) = Q$ and the cost of production of this good is $C(Q) = Q$.

In the decentralized market, the matching is random, anonymous and bilateral. In order for trade to happen, an agent who is willing to buy, needs to meet another agent who specializes in the production of the good the buyer prefers. Such a meeting happens with probability x^i with $i \in \mathcal{I} = \{H, D\}$. A good that is traded is assumed to be non-storable, and offers utility u^i to the buyer, while it costs $\mathcal{C}^i$ to the seller. The utility from consuming the specialized good exceeds the cost of production so that $u^H > \mathcal{C}^H$ and $u^D > \mathcal{C}^D$.

In addition, in the decentralized market trade can happen only by using a medium of exchange. It is assumed that a portion $M^j \in (0,1)$ of the population is initially endowed with the medium of exchange, where $j \in \mathcal{J} = \{F, B\}$ denotes the two regimes: fiat and bitcoin. This medium of exchange, or money, is assumed to be indivisible taking values in the set $\mathcal{M} = \{0,1\}$. In both regimes transactions can be blocked. The agents who can block transactions are agents that do not hold money and their size is equal to $M^D \in (0, 1 - M^j)$, where D stands for dishonest. I also assume that there are honest sellers who can trade with the buyers. The honest sellers do not block transactions by assumption and their size is equal to M^H where $M^j + M^H + M^D = 1$. The key difference between fiat money and BTC is that in the fiat money regime transactions can be blocked with some exogenous probability $\lambda\gamma \in [0,1]$ where $\lambda \in [0,1]$ is the exogenous probability that dishonest sellers make an attack, and $\gamma \in [0,1]$ is the exogenous probability that the attack succeeds and transactions are blocked. Transactions in the Bitcoin network, on the other hand, can be blocked only if the dishonest miners control the network by putting more mining effort than honest miners.

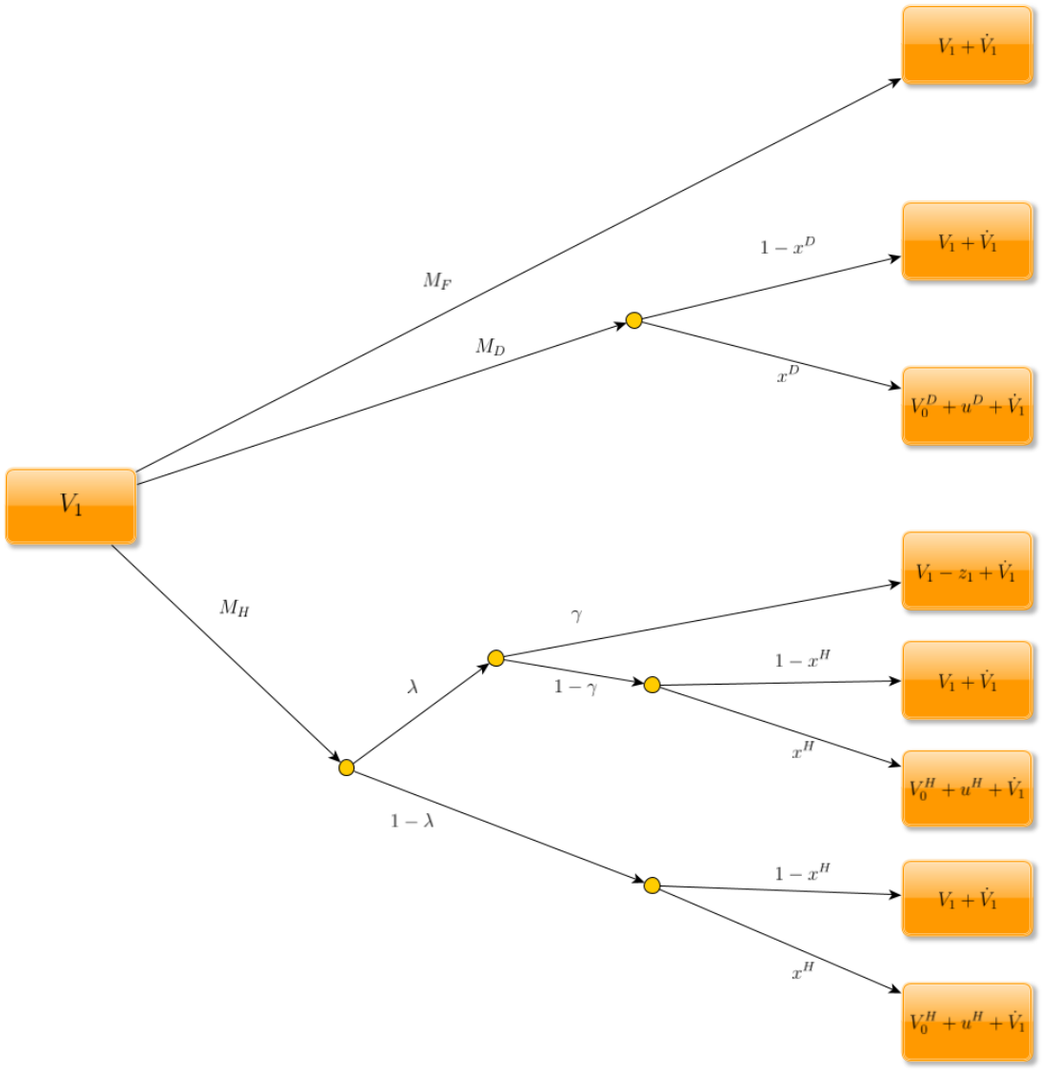
2.1 Fiat Currency

I start with the case of fiat currency. I first describe the dynamic programming problem for each type of agent in the economy.

Money Holders/Buyers: For an agent who holds money and wants to use this money to buy a specialized good, which we will call buyer from now on, we have the following possible outcomes: with probability M^F he meets another buyer and there is no trade taking place. In this case his value would change only as time changes, but his value would still remain the value of a money holder $V_1 + \dot{V}_1$. With probability M^D he meets a dishonest seller. The transactions between buyers and dishonest sellers are not blocked, since dishonest sellers would not have an incentive to block their own transactions. Trade happens between the two with probability x^D, the probability that the buyer likes the good sold by the dishonest seller. In this case the buyer gives the one unit of money to the seller and his value changes to the value of a dishonest seller, plus the change in his value due to time plus the utility from consuming the good $V_0^D + \dot{V}_1 + u^D$. With probability $M^D\left(1 - x^D\right)$ trade does not happen and the value of the buyer becomes $V_1 + \dot{V}_1$.

On the other hand, the buyer meets an honest seller with probability M^H. The dishonest sellers with probability λ attack and try to block the transaction between the buyer and the honest seller. With probability γ they succeed in blocking the transaction. So, with probability $M^H\lambda\gamma$ the buyer does not trade, so his value remains the value of a buyer plus the change in value due to time. Also when the attack succeeds, the buyer incurs a utility cost z_1 which is interpreted as a psychological cost for not being able to transact after matching with a seller who produces a good preferred by the buyer. The value of the buyer if the attack succeeds is $V_1 + \dot{V}_1 - z_1$. On the other hand, with probability $1 - \gamma$ transaction halt does not succeed. If

Figure 1: Fiat Currency Regime: Event Tree for Buyers



the buyer likes the good produced by the seller with probability x^H the transaction takes place with total probabillity $M^H \lambda (1-\gamma) x^H$ and the value of the buyer becomes $V_0^H + \dot{V}_1 + u^H$. With probability $1 - x^H$ the buyer does not like the good sold by the honest seller. The transaction does not take place with total probabillity $M^H \lambda (1-\gamma) \left(1 - x^H\right)$ and the value of the buyer becomes $V_1 + \dot{V}_1$.

Going one step back, the dishonest sellers do not try to block the transaction with probability $1 - \lambda$. Again, if the buyers likes the good with probability x^H the transaction takes place with total probability $M^H (1-\lambda) x^H$ and the value of the buyer becomes $V_0^H + \dot{V}_1 + u^H$. Otherwise with probability $1 - x^H$ the buyer does not like the good, so the transaction does not take place with total probability $M^H (1-\lambda) \left(1 - x^H\right)$ and the value of the buyer becomes $V_1 + \dot{V}_1$.

All the previous events are summarized in Figure 1. The buyer in equilibrium equates his current value with the expected present discounted value he can get from all the previous outcomes. Denoting the rate of time preference by $r > 0$ we have that

$$V_1 = \frac{1}{1+r}\Big[M^F V_1 + M^D\left(1-x^D\right)V_1 + M^D x^D\left(V_0^D + u^D\right) + M^H\lambda\gamma\left(V_1 - z_1\right) + M^H\lambda\left(1-\gamma\right)\left(1-x^H\right)V_1$$
$$+ M^H\lambda\left(1-\gamma\right)x^H\left(V_0^H + u^H\right) + M^H\left(1-\lambda\right)\left(1-x^H\right)V_1 + M^H\left(1-\lambda\right)x^H\left(V_0^H + u^H\right) + \dot{V}_1\Big] \quad (2.1)$$

Honest Non-Money Holders/Sellers: An honest seller faces the following outcomes: with probability M^H meets another honest seller and trade does not happen. In this case, his value would change only as time changes, but his value would still remain the value of an honest seller $V_0^H + \dot{V}_0^H$. With probability M^D he meets a dishonest seller, and again trade does not happen. His value in the end is again $V_0^H + \dot{V}_0^H$.

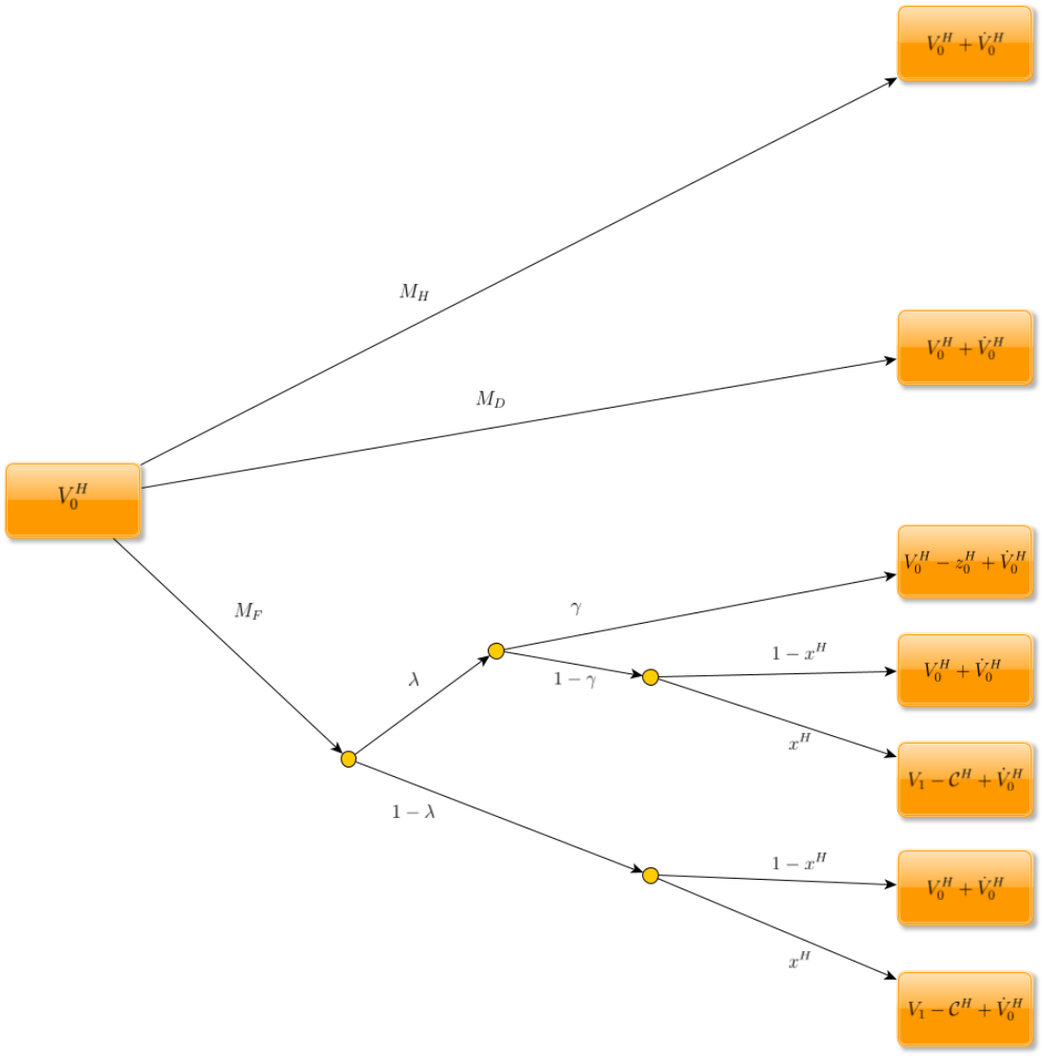
On the other hand, with probability M^F he meets a buyer. The dishonest sellers with probability λ attack and try to block the transaction between the buyer and the honest seller. With probability γ they succeed in blocking the transaction. So, with probability $M^F\lambda\gamma$ the seller does not trade, so his value remains the value of an honest seller plus the change in value due to time. Also when the attack succeeds, the honest seller incurs a utility cost z_0^H which is interpreted as a psychological cost for not being able to transact after matching with a buyer who likes the good produced by the seller. The value of the honest seller if the attack succeeds is $V_0^H + \dot{V}_0^H - z_0^H$. On the other hand, with probability $1-\gamma$ transaction halt does not succeed. If the buyer likes the good produced by the seller with probability x^H the transaction takes place with total probabillity $M^F\lambda\left(1-\gamma\right)x^H$ and the value of the honest seller becomes $V_1 + \dot{V}_0^H - \mathcal{C}^H$. With probability $1-x^H$ the buyer does not like the good sold by the honest seller. The transaction does not take place with total probabillity $M^F\lambda\left(1-\gamma\right)\left(1-x^H\right)$ and the value of the honest seller becomes $V_0^H + \dot{V}_0^H$.

Going one step back, the dishonest sellers do not try to block the transaction with probability $1-\lambda$. Again, if the buyers likes the good with probability x^H the transaction takes place with total probability $M^F\left(1-\lambda\right)x^H$ and the value of the honest seller becomes $V_1 + \dot{V}_0^H - \mathcal{C}^H$. Otherwise with probability $1-x^H$ the buyer does not like the good, so the transaction does not take place with total probability $M^F\left(1-\lambda\right)\left(1-x^H\right)$ and the value of the honest seller becomes $V_0^H + \dot{V}_0^H$.

All the previous events are summarized in Figure 2. The honest seller also equates in equilibrium his current value with the expected present discounted value he can get from all the previous outcomes so that

$$V_0^H = \frac{1}{1+r}\Big[M^H V_0^H + M^D V_0^H + M^F\lambda\gamma\left(V_0^H - z_0^H\right) + M^F\lambda\left(1-\gamma\right)\left(1-x^H\right)V_0^H + M^F\lambda\left(1-\gamma\right)x^H\left(V_1 - \mathcal{C}^H\right)$$
$$+ M^F\left(1-\lambda\right)\left(1-x^H\right)V_0^H + M^F\left(1-\lambda\right)x^H\left(V_1 - \mathcal{C}^H\right) + \dot{V}_0^H\Big]. \quad (2.2)$$

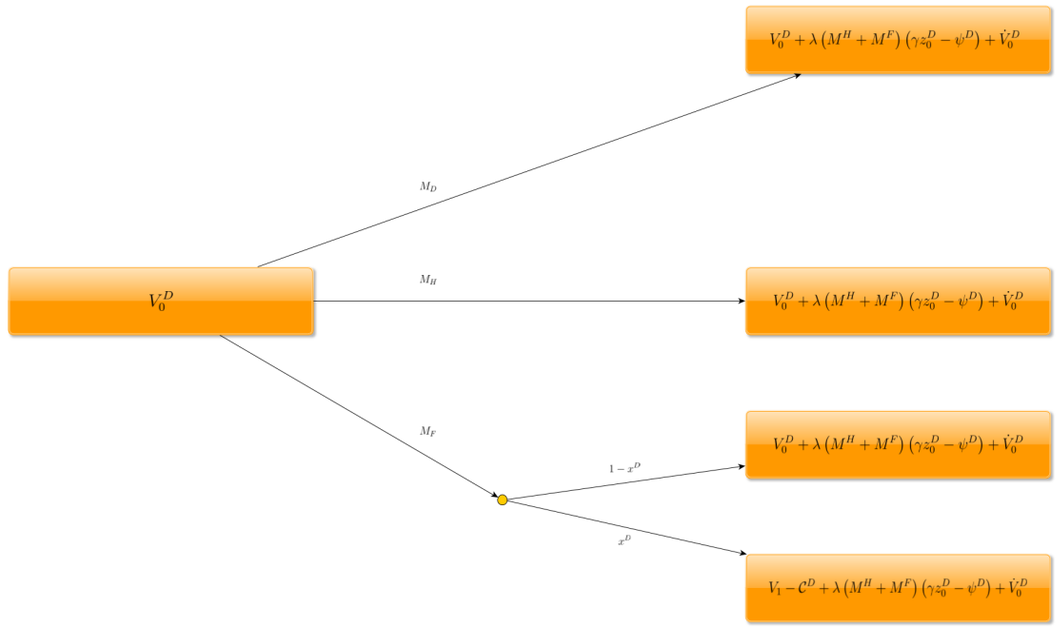
Figure 2: Fiat Currency Regime: Event Tree for Honest Sellers



Dishonest Non-Money Holders/Sellers: A dishonest seller faces the following outcomes: with probability M^D he meets another dishonest seller and there is no trade taking place. In this case his value would change only as time changes, but his value would still remain the value of a non-money holder $V_0^D + \dot{V}_0^D$. The same happens with probability M^H, when he meets an honest seller. With probability M^F he meets a buyer. With probability $1 - x^D$ the buyer does not like the good produced by the seller so there is no trading and the dishonest seller's value is $V_0^D + \dot{V}_0^D$. On the other hand, with probability x^D the buyer likes the good of the seller and trade happens, so in this case the value of the dishonest seller becomes $V_1 + \dot{V}_0^D - \mathcal{C}^D$.

Moreover, the dishonest seller in each period gets an exogenous utility benefit from blocking transactions equal to $\lambda\gamma z_0^D \left(M^H + M^F\right)$, which takes into account the probability that the attack happens and is successful

Figure 3: Fiat Currency Regime: Event Tree for Dishonest Sellers



times the total probability of meetings between buyers and sellers. When the dishonest seller attacks, he also pays an exogenous cost $\lambda\psi^D\left(M^H + M^F\right)$ which is independent of the outcome of the attack since it does not depend on γ. In other words, as long as the dishonest sellers attack to block transactions the cost is paid, even if the attack fails. For the attack to be a rational choice we need $\gamma z_0^D \geq \psi^D$. Of course, when $\gamma = 0$ attacking is not a rational choice. The benefit and the cost from the attack are independent of the meetings of the dishonest seller since they are related to meetings of the other two types of agents. So both of them affect the value of the dishonest seller in all possible states.

All the previous events are summarized in Figure 3. The dishonest seller also equates in equilibrium his current value with the expected present discounted value he can get from all the previous outcomes

$$V_0^D = \frac{1}{1+r}\left[M^D V_0^D + M^H V_0^D + M^F\left(1 - x^D\right)V_0^D + M^F x^D\left(V_1 - \mathcal{C}^D\right) + \lambda\left(M^H + M^F\right)\left(\gamma z_0^D - \psi^D\right) + \dot{V}_0^D\right] \tag{2.3}$$

The extra value of holding money relative to being an honest seller is

$$V_1 - V_0^H = \frac{1}{r + \left(M^H + M^F\right)\left(1 - \lambda\gamma\right)x^H}\Big[M^H\left(1 - \lambda\gamma\right)x^H u^H + M^D x^D u^D + M^F\left(1 - \lambda\gamma\right)x^H\mathcal{C}^H + M^F\lambda\gamma z_0^H - M^H\lambda\gamma z_1 - M^D x^D\left(V_1 - V_0^D\right) + \dot{V}_1 - \dot{V}_0^H\Big]. \tag{2.4}$$

The extra value of holding money relative to being a dishonest seller is

$$V_1 - V_0^D = \frac{1}{r + (M^D + M^F) x^D} \Big[M^H (1 - \lambda\gamma) x^H u^H + M^D x^D u^D + M^F x^D \mathcal{C}^D - \lambda \left(M^H + M^F \right) \left(\gamma z_0^D - \psi^D \right) - M^H \lambda\gamma z_1 - M^H (1 - \lambda\gamma) x^H \left(V_1 - V_0^H \right) + \dot{V}_1 - \dot{V}_0^D \Big]. \tag{2.5}$$

In a monetary equilibrium we need the incentive compatibility constraints to hold: $u^H \geq V_1 - V_0^H \geq \mathcal{C}^H$ and $u^D \geq V_1 - V_0^D \geq \mathcal{C}^D$. Given that $\mathcal{C}^H > 0$ and $\mathcal{C}^D > 0$, then $V_1 > 0$. So we need to impose only the extra participation contraints $V_0^H > 0$ and $V_0^D > 0$ since agents are free to choose to not go to the decentralized market to trade.

2.1.1 Steady State

In this part I focus at the steady state of the model with fiat currency. The steady state is the state in which all the endogenous variables of the model do not evolve anymore. Starting from the value function of money holders we have that

$$rV_1 = \bar{M}^D x^D \left(V_0^D - V_1 + u^D \right) + \bar{M}^H (1 - \lambda\gamma) x^H \left(V_0^H - V_1 + u^H \right) - \bar{M}^H \lambda\gamma z_1. \tag{2.6}$$

For the honest sellers we also have that

$$rV_0^H = \bar{M}^F (1 - \lambda\gamma) x^H \left(V_1 - V_0^H - \mathcal{C}^H \right) - \bar{M}^F \lambda\gamma z_0^H \tag{2.7}$$

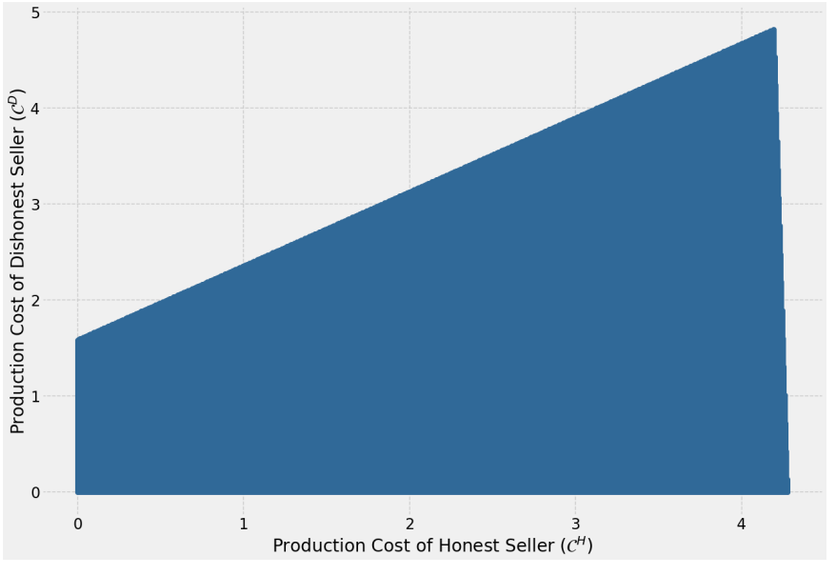
Similarly, for the dishonest sellers we have

$$rV_0^D = \bar{M}^F x^D \left(V_1 - V_0^D - \mathcal{C}^D \right) + \lambda \left(\bar{M}^H + \bar{M}^F \right) \left(\gamma z_0^D - \psi^D \right). \tag{2.8}$$

The extra value of holding money relative to being an honest seller at the steady state is

$$V_1 - V_0^H = \frac{1}{r + (M^H + M^F)(1 - \lambda\gamma) x^H} \Big[M^H (1 - \lambda\gamma) x^H u^H + M^D x^D u^D + M^F (1 - \lambda\gamma) x^H \mathcal{C}^H + M^F \lambda\gamma z_0^H - M^H \lambda\gamma z_1 - M^D x^D \left(V_1 - V_0^D \right) \Big]. \tag{2.9}$$

Figure 4: Monetary Equilibrium: Production Costs Combinations



Notes: The graph shows the values of the cost $\mathcal{C}^D$ for a range of values of the cost $\mathcal{C}^H$ that satisfy the participation and the incentive constraints of the buyers and the sellers at the steady state of the fiat currency regime for the parameter values in Table 1.

The extra value of holding money relative to being a dishonest seller at the steady state is

$$V_1 - V_0^D = \frac{1}{r + \left(M^D + M^F\right) x^D} \Big[M^H \left(1 - \lambda\gamma\right) x^H u^H + M^D x^D u^D + M^F x^D \mathcal{C}^D - \lambda \left(M^H + M^F\right) \left(\gamma z_0^D - \psi^D\right) - M^H \lambda\gamma z_1 - M^H \left(1 - \lambda\gamma\right) x^H \left(V_1 - V_0^H\right) \Big]. \tag{2.10}$$

Figure 4 shows combinations of the cost parameters $\mathcal{C}^H$ and $\mathcal{C}^D$ for which the incentive constraints and the participation constraints are satisfied, so that $u^H \geq V_1 - V_0^H \geq \mathcal{C}^H$ and $u^D \geq V_1 - V_0^D \geq \mathcal{C}^D$, and $V_0^H \geq 0$ and $V_0^D \geq 0$ for given parameter values, including the utility of each good.

The steady state social welfare in the fiat currency regime is defined by $\bar{W}^F = \bar{M}^F V_1 + \bar{M}^H V_0^H + \bar{M}^D V_0^D$ and is equal to

$$\bar{W}^F = \frac{1}{r} \Big[\underbrace{\bar{M}^F \bar{M}^H x^H \left(1 - \lambda\gamma\right) \left(u^H - \mathcal{C}^H\right) + \bar{M}^F \bar{M}^D x^D \left(u^D - \mathcal{C}^D\right)}_{\text{total gains from trade}} - \underbrace{M^F M^H x^H \lambda\gamma \left(z_1 + z_0^H\right) + \bar{M}^D \lambda \left(\bar{M}^H + \bar{M}^F\right) \left(\gamma z_0^D - \psi^D\right)}_{\text{total net welfare cost of blocking transactions}} \Big]. \tag{2.11}$$

2.2 Bitcoin

I now consider the regime in which buyers and sellers participate in the Bitcoin network and transact using BTC tokens. The element of the Bitcoin network that I focus on is security. The security of the Bitcoin network depends on the distribution of the total effort level exerted by the miners which are an integral part of the Proof-of-Work consensus mechanism. In reality the miners decide how much effort they will devote, in order to solve mathematical puzzles that will allow them to verify the latest transactions and be rewarded with newly mined BTC tokens and transactions fees. As we will see in this part, transaction fees are very important for the Bitcoin network, because without transaction fees in the steady state, when money supply stops growing, there would be no new rewards to incentivize the miners to continue their mining operations. This would make the network unsafe and prone to attacks.

Probability of Successful Transaction Blocking: In reality, if there is no dishonest miner controlling 50%+ε of the total hash rate, the Bitcoin network remains secure and no dishonest actor can block transactions of other agents. Since I consider three types of agents, money holders, honest sellers and dishonest sellers, and since money holders already hold the maximum possible value of money of one unit, I will assume that the two types of non-money holders are the ones who devote effort to mine and become money holders. The probability that transaction blocking succeeds is now determined by the rules of the Bitcoin network and can be summarized as follows

$$\gamma^B = \begin{cases} 0, & \text{if } M^H e_H \geq M^D e_D \\ 1, & \text{if } M^H e_H < M^D e_D, \end{cases}$$

where e_i is the effort level of miner type i. What the previous function says is that if the total effort level of honest non-money holders is greater or equal than the effort level of the dishonest non-money holders, the probability of a successful transaction halt becomes zero, otherwise it becomes one.[2]

Probability of Attack: I allow λ^B to be decided by dishonest sellers in this part. The way to understand this is to interpret the different final nodes in the decision trees that give the values of the two types of agents as outcomes of sub-games, and then solve by backwards induction. Specifically, the two types of miners play a game in each period of choosing mining effort in their last node. Assuming without loss of generality that in

[2]In reality the probabilities might be somewhat different from the zero/one extremes in the following way: when nobody controls the absolute majority of the hash rate an individual miner can still not include a transaction in a specific block. However, other miners are likely to include the same transactions. On the other hand, even if an entity controls the absolute majority of the mining effort, this does not automatically mean that they can block transactions, since more actions are needed. The indicator function used here simplifies the analysis. A sigmoid function could be more appropriate for a realistic description.

the last node $M^H e_H^* \geq M^D e_D^*$ after the players optimize, then by construction of the Bitcoin network $\gamma^B = 0$. A dishonest seller in this case, knowing that trying to block transactions of other agents is not working anymore, will choose not to attack in the first place since the expected benefit from attacking and succeeding $\lambda^B \gamma^B z_0^D \left(\bar{M}^H + \bar{M}^B\right)$ is zero when $\gamma^B = 0$ while the expected cost $\lambda^B \psi^D \left(\bar{M}^H + \bar{M}^B\right)$ is not zero. Thus, by choosing $\lambda^B = 0$ the dishonest seller can increase his welfare by not undertaking the cost. If $M^H e_H^* < M^D e_D^*$, then $\gamma^B = 1$ and a dishonest seller can increase his value by choosing $\lambda^B = 1$ since $\gamma^B z_0^D \geq \psi^D$.

Money Supply: The newly mint money supply in the Bitcoin network in reality is roughly constant for 210.000 blocks, and then it gets halved once the previous number of blocks has been added. This keeps happening until the total money supply reaches its upper bound of around 21.000.000 BTC tokens. However, this behavior is described by a step function which is not continuous. To simplify the analysis I will assume a continuous time analog: the money supply grows at a constant rate times the remaining BTC tokens to be mined until the network reaches the steady state and maximum money supply

$$\dot{M}^B = \frac{M^H e_H + M^D e_D}{d} \delta \left(\bar{M}^B - M^B\right) = \delta \left(\bar{M}^B - M^B\right), \tag{2.12}$$

where $d = M^H e_H + M^D e_D$ is the mining difficulty and $\bar{M}^B$ the upper bound on the money supply. In reality the mining difficulty adjusts with a two-week lag to the aggregate mining effort in order to keep the quantity of new BTC tokens mined roughly constant. However, again in order to facilitate the analysis I assume that difficulty adjusts instantaneously to the total mining effort.

At the same time, the size of the honest and the dishonest non-money holders who are able to mine a unit of money and become money holders decrease based on their mining effort so that

$$\dot{M}^H = -\frac{M^H e_H}{M^H e_H + M^D e_D} \delta \left(\bar{M}^B - M^B\right) \tag{2.13}$$

$$\dot{M}^D = -\frac{M^D e_D}{M^H e_H + M^D e_D} \delta \left(\bar{M}^B - M^B\right). \tag{2.14}$$

By assumption the total population has a unit size so that $M^B + M^H + M^D = 1 \Rightarrow \dot{M}^B + \dot{M}^H + \dot{M}^D = 0$. Equations (2.12)-(2.14) satisfy the constraint.

2.2.1 Mining Decisions

Honest Sellers: I formalize now the effort choice problem for the miners. I start with the honest sellers, although the problem of the dishonest sellers is symmetric. The honest sellers choose their mining effort e_H to maximize their expected value from mining which consists of the monetary rewards produced by the

network as expressed in equation (2.12) plus the transaction fees, minus the cost of mining. For simplicity, given that money is indivisible, I will assume that the fees are paid in units of the generic good Q from the centralized market.[3] Their effort choice problem is the following

$$\max_{e_H} v_H^m = \frac{e_H}{M^H e_H + M^D e_D}\left[M^B\left(M^H x^H\left(1-\lambda^B\gamma^B\right)f^H + M^D x^D f^D\right) + \delta\left(\bar{M}^B - M^B\right)\left(V_1 - V_0^H\right)\right] - c_H e_H \tag{2.15}$$

where in the previous equation v_H^m refers to the value of an honest seller from mining. Observe that this value depends on three terms. The third one is just the cost of mining, which is assumed to be linear for simplicity. The other two terms in the brackets are the rewards from mining which can be earned according to the miner's effort relative to the total mining effort. This is why the probability $\frac{e_H}{M^H e_H + M^D e_D}$ multiplies the rewards. This probability creates an externality: as the mining effort of the other type of miners rises, the individual miner has to increase his effort in order to increase the probability to earn rewards. This is the main reason why there is so intense competition between Bitcoin miners in the real world.

The first reward term in the brackets is the expected gains from mining by earning transaction fees. In the Bitcoin network it is the buyer the one who pays the fee. For a buyer, a transaction with an honest miner happens with probability $M^H x^H\left[\lambda^B\left(1-\gamma^B\right)+\left(1-\lambda^B\right)\right] = M^H x^H\left(1-\lambda^B\gamma^B\right)$ with the fee being f^H, and a transaction with a dishonest miner happens with probability $M^D x^D$ with the fee being f^D. Both fees are assumed to be constant for simplicity. In addition, since the fees are expressed in terms of the generic good, the utility from any fee is equal to the fee. All the buyers pay $M^B\left(M^H x^H\left(1-\lambda^B\gamma^B\right)f^H + M^D x^D f^D\right)$ in total fees. Finally, the second term is the new tokens mined at Poisson rate δ, times the value of holding money $V_1 - V_0^H$. The first order condition for the problem in (2.15) is the following

$$\frac{M^D e_D}{\left[M^H e_H + M^D e_D\right]^2}\left[M^B\left(M^H x^H\left(1-\lambda^B\gamma^B\right)f^H + M^D x^D f^D\right) + \delta\left(\bar{M}^B - M^B\right)\left(V_1 - V_0^H\right)\right] = c_H \tag{2.16}$$

The honest sellers equate in equilibrium the expected marginal benefit from mining, the left-hand side, with the marginal cost, which is in the right-hand side. From the previous condition we can solve for the best response mining effort function of the honest sellers

$$e_H\left(e_D\right) \equiv BR_H\left(e_D\right) = \frac{1}{M^H}\left[M^D e_D \frac{M^B\left(M^H x^H\left(1-\lambda^B\gamma^B\right)f^H + M^D x^D f^D\right) + \delta\left(\bar{M}^B - M^B\right)\left(V_1 - V_0^H\right)}{c_H}\right]^{\frac{1}{2}} - \frac{M^D}{M^H}e_D \tag{2.17}$$

[3] In reality the fees paid in any Bitcoin transaction are measured in BTC. However, introducing money fees paid between agents in a setting with indivisible money can create problems, so I opt out for fees expressed in terms of the generic good.

Equation (2.17) is the honest miners' best response function with respect to the mining effort of the dishonest ones. As expected, the mining effort of the honest miners increases with the rewards and falls when the marginal cost of effort is higher. As regards the effort level of the dishonest sellers, the best response function is initially increasing, so that the honest miners initially increase their mining effort when the dishonest miners increase their mining effort, but after some point it becomes decreasing and it is optimal for the honest miners to decrease their mining effort as the dishonest ones increase theirs.

Dishonest Sellers: The effort-choice problem for the dishonest sellers is symmetric

$$\max_{e_D} v_D^m = \frac{e_D}{M^H e_H + M^D e_D} \left[M^B \left(M^H x^H \left(1 - \lambda^B \gamma^B \right) f^H + M^D x^D f^D \right) + \delta \left(\bar{M}^B - M^B \right) \left(V_1 - V_0^D \right) \right] - c_D e_D \tag{2.18}$$

The first order condition is

$$\frac{M^H e_H}{\left[M^H e_H + M^D e_D \right]^2} \left[M^B \left(M^H x^H \left(1 - \lambda^B \gamma^B \right) f^H + M^D x^D f^D \right) + \delta \left(\bar{M}^B - M^B \right) \left(V_1 - V_0^D \right) \right] = c_D \tag{2.19}$$

We can solve for the best response function of the dishonest sellers as follows

$$e_D\left(e_H\right) \equiv BR_D\left(e_H\right) = \frac{1}{M^D} \left[M^H e_H \frac{M^B \left(M^H x^H \left(1 - \lambda^B \gamma^B \right) f^H + M^D x^D f^D \right) + \delta \left(\bar{M}^B - M^B \right) \left(V_1 - V_0^D \right)}{c_D} \right]^{\frac{1}{2}} - \frac{M^H}{M^D} e_H \tag{2.20}$$

If we combine equations (2.16) and (2.19) we get

$$M^H e_H = \underbrace{\frac{c_D}{c_H}}_{\text{MC ratio}} \underbrace{\frac{M^B \left(M^H x^H \left(1 - \lambda^B \gamma^B \right) f^H + M^D x^D f^D \right) + \delta \left(\bar{M}^B - M^B \right) \left(V_1 - V_0^H \right)}{M^B \left(M^H x^H \left(1 - \lambda^B \gamma^B \right) f^H + M^D x^D f^D \right) + \delta \left(\bar{M}^B - M^B \right) \left(V_1 - V_0^D \right)}}_{\text{MB ratio}} M^D e_D, \tag{2.21}$$

so the aggregate mining effort of the honest miners will be proportional to the aggregate mining effort of the dishonest ones with the ratio between the two being the product of the relative marginal cost of the dishonest miners times the relative marginal benefit of honest ones. For the network to be secure we would need the proportionality number to be greater or equal to one, so that

$$\frac{c_D}{c_H} \geq \frac{MB_D}{MB_H} \Leftrightarrow \frac{MB_H}{MC_H} \geq \frac{MB_D}{MC_D} \tag{2.22}$$

Therefore, if the marginal benefit of the honest miners relative to their marginal cost is higher than the marginal benefit of the dishonest miners relative to their marginal cost, the honest ones will put more mining effort on aggregate, and the network will be secured. At the steady state where $\bar{M}^B = M^B$ the previous condition simplifies to $c_D \geq c_H$, because at the steady state all the BTC tokens are minted and the marginal benefit is the same for the two types of miners being equal to the marginal benefit from earning the transaction fees. If we use equation (2.21) we can also determine the aggregate mining effort as follows

$$\begin{aligned} M^H e_H + M^D e_D &= \left[1 + \frac{c_D}{c_H} \frac{M^B \left(M^H x^H \left(1 - \lambda^B \gamma^B\right) f^H + M^D x^D f^D\right) + \delta \left(\bar{M}^B - M^B\right) \left(V_1 - V_0^H\right)}{M^B \left(M^H x^H \left(1 - \lambda^B \gamma^B\right) f^H + M^D x^D f^D\right) + \delta \left(\bar{M}^B - M^B\right) \left(V_1 - V_0^D\right)}\right] M^D e_D \\ &\equiv \Delta M^D e_D. \end{aligned} \tag{2.23}$$

Next, we can determine the optimal mining efforts of dishonest miners by using equations (2.16) and (2.23)

$$e_D^* = \frac{1}{M^D c_H} \left[M^B \left(M^H x^H \left(1 - \lambda^B \gamma^B\right) f^H + M^D x^D f^D\right) + \delta \left(\bar{M}^B - M^B\right) \left(V_1 - V_0^H\right)\right] \frac{1}{\Delta^2} > 0, \tag{2.24}$$

which also implies that $e_H^* > 0$ from equation (2.21). We can determine the optimal mining efforts of honest miners by combining equations (2.21) and (2.24)

$$e_H^* = \frac{1}{M^H c_H} \left[M^B \left(M^H x^H \left(1 - \lambda^B \gamma^B\right) f^H + M^D x^D f^D\right) + \delta \left(\bar{M}^B - M^B\right) \left(V_1 - V_0^H\right)\right] \frac{\Delta - 1}{\Delta^2}. \tag{2.25}$$

The value from mining is

$$v_H^m \left(e_H^*, e_D^*\right) = e_H^* c_H \left(\Delta - 1\right) \tag{2.26}$$

$$v_D^m \left(e_D^*, e_S^*\right) = e_D^* c_D \frac{1}{\Delta - 1}. \tag{2.27}$$

Observe that $v_H^m \left(e_H^*, e_D^*\right) > 0$ and $v_D^m \left(e_D^*, e_H^*\right) > 0$ since $\Delta > 1$. This implies that in the Nash equilibrium, even though there is a negative externality arising from mining competition to ensure a higher expected reward, both types of miners have welfare benefits.

2.2.2 Trading Decisions

Money Holders/Buyers: There is one important change in the dynamic programming problem of the buyers. Their incentive compatibility constraints are slightly modified now to account for the transaction fees so that $u^i - f^i \geq V_1 - V_0^i$.

$$V_1 = \frac{1}{1+r}\Big[M^B V_1 + M^D\left(1-x^D\right)V_1 + M^D x^D\left(V_0^D + u^D - f^D\right) + M^H\lambda^B\gamma^B\left(V_1 - z_1\right)$$
$$+ M^H\lambda^B\left(1-\gamma^B\right)\left(1-x^H\right)V_1 + M^H\lambda^B\left(1-\gamma^B\right)x^H\left(V_0^H + u^H - f^H\right)$$
$$+ M^H\left(1-\lambda^B\right)\left(1-x^H\right)V_1 + M^H\left(1-\lambda^B\right)x^H\left(V_0^H + u^H - f^H\right) + \dot{V}_1\Big] \tag{2.28}$$

Honest Sellers: The value for the honest sellers is augmented with the utility from mining.

$$V_0^H = \frac{1}{1+r}\Big[M^H V_0^H + M^D V_0^H + M^B\lambda^B\gamma^B\left(V_0^H - z_0^H\right) + M^B\lambda^B\left(1-\gamma^B\right)\left(1-x^H\right)V_0^H$$
$$+ M^B\lambda^B\left(1-\gamma^B\right)x^H\left(V_1 - \mathcal{C}^H\right) + M^B\left(1-\lambda^B\right)\left(1-x^H\right)V_0^H + M^B\left(1-\lambda^B\right)x^H\left(V_1 - \mathcal{C}^H\right)$$
$$+ v_H^m\left(e_H^*, e_D^*\right) + \dot{V}_0^H\Big] \tag{2.29}$$

Dishonest Sellers: The value for the dishonest sellers is also augmented with the utility from mining.

$$V_0^D = \frac{1}{1+r}\Big[M^D V_0^D + M^H V_0^D + M^B\left(1-x^D\right)V_0^D + M^B x^D\left(V_1 - \mathcal{C}^D\right) + \lambda^B\left(M^H + M^B\right)\left(\gamma z_0^D - \psi^D\right)$$
$$+ v_D^m\left(e_D^*, e_H^*\right) + \dot{V}_0^D\Big] \tag{2.30}$$

The extra value of holding money relative to being a dishonest seller is

$$V_1 - V_0^D = \frac{1}{r + \left(M^D + M^B\right)x^D}\Big[M^H x^H\left(1-\lambda^B\gamma^B\right)\left(u^H - f^H\right) + M^D x^D\left(u^D - f^D\right)$$
$$+ M^B x^D\mathcal{C}^D - M^H\lambda^B\gamma^B z_1 - \lambda^B\left(M^B + M^H\right)\left(\gamma^B z_0^D - \psi^D\right) - v_D^m\left(e_H^*, e_D^*\right) + \dot{V}_1 - \dot{V}_0^D\Big]$$
$$- \frac{M^H x^H\left(1-\lambda^B\gamma^B\right)}{r + \left(M^D + M^B\right)x^D}\left(V_1 - V_0^H\right). \tag{2.31}$$

The extra value of holding money relative to being an honest seller is

$$V_1 - V_0^H = \frac{1}{r + \left(M^H + M^B\right)x^H\left(1-\lambda^B\gamma^B\right)}\Big[M^H x^H\left(1-\lambda^B\gamma^B\right)\left(u^H - f^H\right) + M^D x^D\left(u^D - f^D\right)$$
$$+ M^B x^H\left(1-\lambda^B\gamma^B\right)\mathcal{C}^H - M^H\lambda^B\gamma^B z_1 + M^B\lambda^B\gamma^B z_0^H - v_H^m\left(e_H^*, e_D^*\right) + \dot{V}_1 - \dot{V}_0^H\Big]$$
$$- \frac{M^D x^D}{r + \left(M^H + M^B\right)x^H\left(1-\lambda^B\gamma^B\right)}\left(V_1 - V_0^D\right). \tag{2.32}$$

2.2.3 Steady State

In this part I focus at the steady state of the model under the Bitcoin regime. At the steady state $\bar{M}^B = M^B$, $\bar{M}^H = M^H$ and $\bar{M}^D = M^D$, which simplify the analysis significantly. Specifically at the steady state we have from inequality (2.22) that the network will be secure if and only if $c_D \geq c_H$. I will adopt this assumption for the rest of this section. This implies that $\gamma^B = \lambda^B = 0$ at the steady state. Also, from the definition of Δ we have that $\bar{\Delta} = \frac{c_H + c_D}{c_H} > 1$ and $\bar{\Delta} - 1 = \frac{c_D}{c_H}$. The optimal mining efforts at the steady state are given as

$$\bar{e}_D^* = \frac{1}{\bar{M}^D c_H} \bar{M}^B \left(\bar{M}^H x^H f^H + \bar{M}^D x^D f^D \right) \frac{c_H^2}{(c_H + c_D)^2} \tag{2.33}$$

$$\bar{e}_H^* = \frac{1}{\bar{M}^H c_D} \bar{M}^B \left(\bar{M}^H x^H f^H + \bar{M}^D x^D f^D \right) \frac{c_D^2}{(c_D + c_H)^2}. \tag{2.34}$$

In addition, the value of mining at the steady state becomes

$$\bar{v}_D^m \left(e_D^*, e_H^* \right) = \bar{e}_D^* c_H = \frac{1}{\bar{M}^D} \bar{M}^B \left(\bar{M}^H x^H f^H + \bar{M}^D x^D f^D \right) \frac{c_H^2}{(c_H + c_D)^2} \tag{2.35}$$

$$\bar{v}_H^m \left(e_H^*, e_D^* \right) = \bar{e}_H^* c_D = \frac{1}{\bar{M}^H} \bar{M}^B \left(\bar{M}^H x^H f^H + \bar{M}^D x^D f^D \right) \frac{c_D^2}{(c_D + c_H)^2}. \tag{2.36}$$

Equations (2.33)-(2.36) show the importance of the transaction fees. At the steady state where the money supply has reached its maximum value, and there are no new BTC tokens to be mined, the only way to incentivize miners to continue mining is by having them earning transaction fees through their mining operations. If the transaction fees are zero, then the optimal mining efforts and the values from mining at the steady state are all zero.

I now turn to the trading decisions. At the steady state we have that $\gamma^B = \lambda^B = 0$ and $\dot{V}_1 = \dot{V}_0^H = \dot{V}_0^D = 0$. Then, the value of money holders becomes

$$r V_1 = \bar{M}^H x^H \left(V_0^H - V_1 + u^H - f^H \right) + \bar{M}^D x^D \left(V_0^D - V_1 + u^D - f^D \right). \tag{2.37}$$

For the honest sellers we have that

$$r V_0^H = \bar{M}^B x^H \left(V_1 - V_0^H - \mathcal{C}^H \right) + \bar{v}_H^m \left(\bar{e}_H^*, \bar{e}_D^* \right). \tag{2.38}$$

For the dishonest sellers we also have that

$$r V_0^D = \bar{M}^B x^D \left(V_1 - V_0^D - \mathcal{C}^D \right) + \bar{v}_D^m \left(\bar{e}_D^*, \bar{e}_H^* \right). \tag{2.39}$$

The extra value of holding money relative to being a dishonest seller is

$$V_1 - V_0^D = \frac{1}{r + (M^D + M^B)\, x^D} \left[M^H x^H \left(u^H - f^H \right) + M^D x^D \left(u^D - f^D \right) + M^B x^D \mathcal{C}^D - \bar{v}_D^m \left(e_H^*, e_D^* \right) \right] - \frac{M^H x^H}{r + (M^D + M^B)\, x^D} \left(V_1 - V_0^H \right). \tag{2.40}$$

The extra value of holding money relative to being an honest seller is

$$V_1 - V_0^H = \frac{1}{r + (M^H + M^B)\, x^H} \left[M^H x^H \left(u^H - f^H \right) + M^D x^D \left(u^D - f^D \right) + M^B x^H \mathcal{C}^H - \bar{v}_H^m \left(e_H^*, e_D^* \right) \right] - \frac{M^D x^D}{r + (M^H + M^B)\, x^H} \left(V_1 - V_0^D \right). \tag{2.41}$$

The steady state social welfare under the Bitcoin regime is defined by $\bar{W}^B = \bar{M}^B V_1 + \bar{M}^H V_H + \bar{M}^D V_D$.

$$\bar{W}^B = \frac{1}{r} \left[\underbrace{\bar{M}^B \bar{M}^H x^H \left(u^H - \mathcal{C}^H \right) + \bar{M}^B \bar{M}^D x^D \left(u^D - \mathcal{C}^D \right) - \bar{M}^B \left(\bar{M}^H x^H f^H + \bar{M}^D x^D f^D \right)}_{\text{total gains from trade}} + \underbrace{\bar{M}^H \bar{v}_H^m + \bar{M}^D \bar{v}_D^m}_{\text{total welfare from mining}} \right]. \tag{2.42}$$

The total welfare from mining is not high enough to compensate for the welfare cost of transaction fees at the steady state. The reason is that since there are no new BTC tokens to be mined, mining becomes a costly redistribution scheme, since it only leads to a redistribution of the fees between agents, without increasing their assets, while agents still undertake the cost of mining. In other words, the two types of miners earn together the total amount of fees paid by the buyers, but they still pay the cost of mining, so the net contribution of mining at the steady state is negative as shown below

$$\bar{M}^H \bar{v}_H^m + \bar{M}^D \bar{v}_D^m - \bar{M}^B \left(\bar{M}^H x^H f^H + \bar{M}^D x^D f^D \right) = -\left(c_H \bar{e}_H^* + c_D \bar{e}_D^* \right) = -\bar{M}^B \left(\bar{M}^H x^H f^H + \bar{M}^D x^D f^D \right) \frac{2 c_H c_D}{\left(c_H + c_D \right)^2}. \tag{2.43}$$

If we assume for a moment that the steady state portion of various agents is the same across the two regimes, then we have that social welfare under the Bitcoin regime will be higher than social welfare in the fiat currency regime if and only if the net cost of mining is lower than the net cost of transaction blocking in the fiat currency regime

$$\bar{W}^B > \bar{W}^F \Leftrightarrow \bar{M}^B \left(\bar{M}^H x^H f^H + \bar{M}^D x^D f^D \right) \frac{2c_H c_D}{(c_H + c_D)^2} < \lambda\gamma \bar{M}^F \bar{M}^H x^H \left(u^H - \mathcal{C}^H \right) + \bar{M}^F \bar{M}^H x^H \lambda\gamma \left(z_1 + z_0^H \right) - \bar{M}^D \lambda \left(\bar{M}^H + \bar{M}^F \right) \left(\gamma z_0^D - \psi^D \right). \tag{2.44}$$

If the number of various agents is not equal across the two regimes, the previous condition becomes

$$\bar{M}^B \bar{M}^H x^H \left(u^H - \mathcal{C}^H - \frac{2c_H c_D}{(c_H + c_D)^2} f^H \right) + \bar{M}^B \bar{M}^D x^D \left(u^D - \mathcal{C}^D - \frac{2c_H c_D}{(c_H + c_D)^2} f^D \right) > \bar{M}^F \bar{M}^H (1 - \lambda\gamma) x^H \left(u^H - \mathcal{C}^H \right) + \bar{M}^F \bar{M}^D x^D \left(u^D - \mathcal{C}^D \right) - \bar{M}^F \bar{M}^H x^H \lambda\gamma \left(z_1 + z_0^H \right) + \bar{M}^D \lambda \left(\bar{M}^H + \bar{M}^F \right) \left(\gamma z_0^D - \psi^D \right). \tag{2.45}$$

Condition (2.45) states that, in this specific model, steady state social welfare under the Bitcoin network will be higher relative to the fiat currency regime if the total gains from trade in the Bitcoin network minus the total cost of mining is higher than the total gains from trade in the fiat currency regime minus the net total cost of transaction halt. Observe that the terms in the left hand side of (2.45) are always positive since the incentive constraints of buyers and sellers imply that $u^i \geq \mathcal{C}^i + f^i$ and $2c_H c_D < (c_H + c_D)^2$. On the other hand, the sign of the right hand side depends on the value of $\lambda\gamma$. If $\lambda\gamma$ takes high values, then the expected gains from trade in the fiat currency regime are lower due to the costs of not transacting, making the whole term lower, or even negative. Thus, the Bitcoin network can be better for social welfare when the probability of a successful attack in the fiat currency regime is high. Moreover, the higher the terms related to the volume of transaction activity in the Bitcoin network, $\bar{M}^B \bar{M}^H$ and $\bar{M}^B \bar{M}^D$, the more likely it is that (2.45) holds, while a higher transaction activity in the fiat currency regime $\bar{M}^F \bar{M}^H$ and $\bar{M}^F \bar{M}^D$, makes (2.45) less likely to hold. This is also intuitive: a network with more transaction activity is a network in which more trading takes place, and this leads to more gains from trading, leading to higher welfare.

The Case of Network Collapse: As a last note, the steady state analysis so far was based on the assumption that the marginal cost of the dishonest sellers is greater or equal to the marginal cost of the honest ones. If, however, $c_D < c_H$, the Bitcoin network is not secure anymore, and the probability that transaction blocking attacks succeed becomes $\gamma^B = 1$. This would incentivize the sellers to choose $\lambda^B = 1$. In the real world, if the dishonest miners control the network they can also double spend BTC tokens, something that is not modeled here. Double spending together with transaction blocking leads to a loss of trust in the network and the network eventually collapses. In our setting, even if buyers are blocked from transacting with honest sellers, they can still transact with dishonest sellers, so the network would continue to operate. One way

to catch the collapse of the network, given the absence of double spending, would be to assume that z_1 is a large number that makes the expected loss of the buyers from transaction blocking exceed the expected benefit from transacting with dishonest sellers when $\lambda^B = \gamma^B = 1$, so that $z_1 > \frac{\bar{M}^D x^D u^D}{\bar{M}^H}$. In this case there would be no incentive for buyers to go to the market and the network would collapse as there would be no trading, making the fiat currency regime a better choice.

2.3 Fixed Costs

So far we have assumed that miners face a linear cost of production that depends only on their effort, so that $C_i = c_i e_i$. I will now assume that the cost function includes a fixed cost $\mathcal{F}_i$ that could play the role of a large investment cost needed in order to enter the market. Adding a fixed cost in functions (2.15) and (2.18) will not change the optimality conditions of the miners, but it will change their decision to enter the market and exert effort in the first place.

Honest Miners: Starting from the honest miners, if we substitute out the effort e_H in the objective function (2.15) using the best response function (2.17) we get that the value of mining becomes

$$v_H^m = \left[\left(\frac{M^B \left(M^H x^H \left(1 - \lambda^B \gamma^B \right) f^H + M^D x^D f^D \right) + \delta \left(\bar{M}^B - M^B \right) \left(V_1 - V_0^H \right)}{M^H} \right)^{\frac{1}{2}} - \left(\frac{M^D}{M^H} c_H e_D \right)^{\frac{1}{2}} \right]^2 - \mathcal{F}_H \tag{2.46}$$

If we use equation (2.46) we can solve for the effort level from the side of the dishonest miners that would make the honest ones unwilling to exert any effort and modify the best response function as follows

$$BR_H\left(e_D\right) = \begin{cases} \frac{1}{M^H} \left[M^D e_D \frac{M^B \left(M^H x^H \left(1 - \lambda^B \gamma^B \right) f^H + M^D x^D f^D \right) + \delta \left(\bar{M}^B - M^B \right) \left(V_1 - V_0^H \right)}{c_H} \right]^{\frac{1}{2}} - \frac{M^D}{M^H} e_D, \\ \text{if } \; e_D \leq \frac{M^H}{M^D c_H} \left[\left(\frac{M^B \left(M^H x^H \left(1 - \lambda^B \gamma^B \right) f^H + M^D x^D f^D \right) + \delta \left(\bar{M}^B - M^B \right) \left(V_1 - V_0^H \right)}{M^H} \right)^{\frac{1}{2}} - \mathcal{F}_H^{\frac{1}{2}} \right]^2 \\ \\ 0, \text{ if } \; e_D > \frac{M^H}{M^D c_H} \left[\left(\frac{M^B \left(M^H x^H \left(1 - \lambda^B \gamma^B \right) f^H + M^D x^D f^D \right) + \delta \left(\bar{M}^B - M^B \right) \left(V_1 - V_0^H \right)}{M^H} \right)^{\frac{1}{2}} - \mathcal{F}_H^{\frac{1}{2}} \right]^2 \end{cases} \tag{2.47}$$

According to (2.47) when the fixed cost for the honest miners $\mathcal{F}_H$ is large the dishonest miners need a lower level of effort to disincentivize the honest ones from mining. On the other hand, the opposite is true with respect to the expected reward: the higher the expected reward, the higher the profits for the honest miners, so the dishonest miners would need a higher level of effort to preclude the honest ones from exerting effort.

Dishonest Miners: Turning to the dishonest miners, we can follow a similar procedure and get

$$v_D^m = \left[\left(\frac{M^B \left(M^H x^H \left(1 - \lambda^B \gamma^B \right) f^H + M^D x^D f^D \right) + \delta \left(\bar{M}^B - M^B \right) \left(V_1 - V_0^D \right)}{M^D} \right)^{\frac{1}{2}} - \left(\frac{M^H}{M^D} c_D e_H \right)^{\frac{1}{2}} \right]^2 - \mathcal{F}_D. \tag{2.48}$$

$$BR_D\left(e_H\right) = \begin{cases} \frac{1}{M^D} \left[M^H e_H \frac{M^B \left(M^H x^H \left(1 - \lambda^B \gamma^B \right) f^H + M^D x^D f^D \right) + \delta \left(\bar{M}^B - M^B \right) \left(V_1 - V_0^D \right)}{c_D} \right]^{\frac{1}{2}} - \frac{M^H}{M^D} e_H, \\ \text{if } e_H \leq \frac{M^D}{M^H c_D} \left[\left(\frac{M^B \left(M^H x^H \left(1 - \lambda^B \gamma^B \right) f^H + M^D x^D f^D \right) + \delta \left(\bar{M}^B - M^B \right) \left(V_1 - V_0^D \right)}{M^D} \right)^{\frac{1}{2}} - \mathcal{F}_D^{\frac{1}{2}} \right]^2 \\ \\ 0, \text{ if } e_D > \frac{M^D}{M^H c_D} \left[\left(\frac{M^B \left(M^H x^H \left(1 - \lambda^B \gamma^B \right) f^H + M^D x^D f^D \right) + \delta \left(\bar{M}^B - M^B \right) \left(V_1 - V_0^D \right)}{M^D} \right)^{\frac{1}{2}} - \mathcal{F}_D^{\frac{1}{2}} \right]^2 \end{cases} \tag{2.49}$$

Similarly, according to (2.49), when the fixed cost for the dishonest miners $\mathcal{F}_D$ is large the honest miners need a lower level of effort to disincentivize the dishonest miners from mining. The opposite is true with respect to the benefits from newly mint tokens and aggregate fees. In the real world the investment/fixed cost of a dishonest miner who would try to take over the network is estimated to be in the billions of dollars according to Nuzzi et al. (2024). Given that the fixed cost is large, and the effort of the incumbents is large, with hash rates breaking records, then it is not profitable for attackers to undertake the large fixed cost and devote the effort needed to take over the network. This makes the Bitcoin network a very important defense mechanism in the digital era.

3 Divisible Goods and Transitional Dynamics

In this part I introduce divisible goods and I assume that buyers and sellers bargain over the quantity of goods q^i produced by seller of type i. I also assume that buyers derive utility $u\left(q^i\right)$ from consuming q^i units of the specialized good, with $u'\left(q\right) > 0 \geq u''\left(q\right)$, while the producers incur a cost $\mathcal{C}^i\left(q^i\right)$ when producing q^i units with $d\mathcal{C}\left(q\right)/dq > 0$ and $d^2\mathcal{C}\left(q\right)/dq^2 \geq 0$, which allow for a case with linear utility and linear costs of production. I assume that the price is determined by the solution to a generalized Nash bilateral bargaining problem. In what follows I present the problem and describe the equilibria under the fiat currency regime and the Bitcoin regime.

3.1 Fiat Currency: Bargaining and Trading Decisions

In the fiat currency regime, the generalized Nash bargaining leads to the quantity q_F^i that maximizes the weighted surplus of the buyers and the corresponding sellers so that

$$\begin{aligned} q_F^i = \arg\max & \left[V_0^i + u\left(q^i\right) - V_1\right]^{\theta_F^i} \left[V_1 - \mathcal{C}^i\left(q^i\right) - V_0^i\right]^{\theta_i} \\ \text{s.t.} \quad & V_0^i + u\left(q^i\right) \geq V_1 \\ & V_1 - \mathcal{C}^i\left(q^i\right) \geq V_0^i \end{aligned}$$

In the previous problem the parameter $\theta_F^i \in [0,1]$ is a measure of the relative bargaining power of the buyer when he meets a seller of type i and θ_i is the relative bargaining power of a seller of type i. The first order condition to the previous problem for any type i is

$$V_0^i + u\left(q^i\right) - V_1 = \frac{\theta_F^i}{\theta_i} \frac{\dfrac{du\left(q^i\right)}{dq^i}}{\dfrac{d\mathcal{C}^i\left(q^i\right)}{dq^i}} \left[V_1 - \mathcal{C}^i\left(q^i\right) - V_0^i\right] \tag{3.1}$$

Recall that the value function for buyers under the fiat currency regime is given by

$$\begin{aligned} V_1 = \frac{1}{1+r}\Big[& M^F V_1 + M^D\left(1-x^D\right)V_1 + M^D x^D\left(V_0^D + u\left(q^D\right)\right) + M^H\lambda\gamma\left(V_1 - z_1\right) + M^H\lambda\left(1-\gamma\right)\left(1-x^H\right)V_1 \\ & + M^H\lambda\left(1-\gamma\right)x^H\left(V_0^H + u\left(q^H\right)\right) + M^H\left(1-\lambda\right)\left(1-x^H\right)V_1 + M^H\left(1-\lambda\right)x^H\left(V_0^H + u\left(q^H\right)\right) + \dot{V}_1\Big] \end{aligned} \tag{3.2}$$

The value of honest sellers is

$$V_0^H = \frac{1}{1+r}\Big[M^H V_0^H + M^D V_0^H + M^F \lambda\gamma\left(V_0^H - z_0^H\right) + M^F \lambda\left(1-\gamma\right)\left(1-x^H\right)V_0^H + M^F\lambda\left(1-\gamma\right)x^H\left(V_1 - \mathcal{C}^H\left(q^H\right)\right) + M^F\left(1-\lambda\right)\left(1-x^H\right)V_0^H + M^F\left(1-\lambda\right)x^H\left(V_1 - \mathcal{C}^H\left(q^H\right)\right) + \dot{V}_0^H\Big]. \tag{3.3}$$

The value of dishonest sellers is

$$V_0^D = \frac{1}{1+r}\left[M^D V_0^D + M^H V_0^D + M^F\left(1-x^D\right)V_0^D + M^F x^D\left(V_1 - \mathcal{C}^D\left(q^D\right)\right) + \lambda\left(M^H + M^F\right)\left(\gamma z_0^D - \psi^D\right) + \dot{V}_0^D\right] \tag{3.4}$$

The extra value of holding money relative to being an dishonest seller is

$$V_1 - V_0^D = \frac{1}{r + \left(M^D + M^F\right)x^D}\Big[M^H\left(1-\lambda\gamma\right)x^H u\left(q^H\right) + M^D x^D u\left(q^D\right) + M^F x^D \mathcal{C}^D\left(q^D\right) - \lambda\left(M^H + M^F\right)\left(\gamma z_0^D - \psi^D\right) - M^H\lambda\gamma z_1 - M^H\left(1-\lambda\gamma\right)x^H\left(V_1 - V_0^H\right) + \dot{V}_1 - \dot{V}_0^D\Big]. \tag{3.5}$$

The extra value of holding money relative to being an honest seller is

$$V_1 - V_0^H = \frac{1}{r + \left(M^H + M^F\right)\left(1-\lambda\gamma\right)x^H}\Big[M^H\left(1-\lambda\gamma\right)x^H u\left(q^H\right) + M^D x^D u\left(q^D\right) + M^F\left(1-\lambda\gamma\right)x^H\mathcal{C}^H\left(q^H\right) + M^F\lambda\gamma z_0^H - M^H\lambda\gamma z_1 - M^D x^D\left(V_1 - V_0^D\right) + \dot{V}_1 - \dot{V}_0^H\Big]. \tag{3.6}$$

I will also assume that the size of the money supply grows in a similar way as in the Bitcoin network.[4] For the other two types of agents I will assume that their size in the population shrinks by constant rates κ and $1-\kappa$ times the increase in the amount of money holders.

$$\dot{M}^F = \delta^F\left(\bar{M}^F - M^F\right) \tag{3.7}$$

$$\dot{M}^H = -\kappa\delta^F\left(\bar{M}^F - M^F\right) \tag{3.8}$$

$$\dot{M}^D = -\left(1-\kappa\right)\delta^F\left(\bar{M}^F - M^F\right). \tag{3.9}$$

[4] In reality money supply in fiat currency regimes can grow without bound, but here to facilitate the analysis a steady state for the money supply is assumed to exist.

Table 1: Fiat Currency Regime Parameter Values

Parameter	Description	Value
Money Holders		
σ	Relative Risk Aversion Coefficient	0.28
r	Discount Factor	0.000001
z_1	Individual Cost from Transaction Blocking	5
δ^F	Speed of Money Supply / Cohort Size Increase	0.0015
Honest Sellers		
r	Discount Factor	0.000001
η^H	Marginal Cost of Production of Specialized Good	0.15
x^H	Probability of Trading with Buyers	0.05
z_0^H	Individual Cost from Transaction Blocking	1.5
κ	Speed of Cohort Size Decrease	0.5
Dishonest Sellers		
r	Discount Factor	0.000001
η^D	Marginal Cost of Production of Specialized Good	0.15
x^D	Probability of Trading with Buyers	0.05
z_0^D	Individual Benefit from Transaction Blocking	1
ψ	Individual Cost from Transaction Blocking	0.2
λ	Probability of Attempting Transaction Blocking	0.15
γ	Probability of Succeeding in Transaction Blocking	0.15

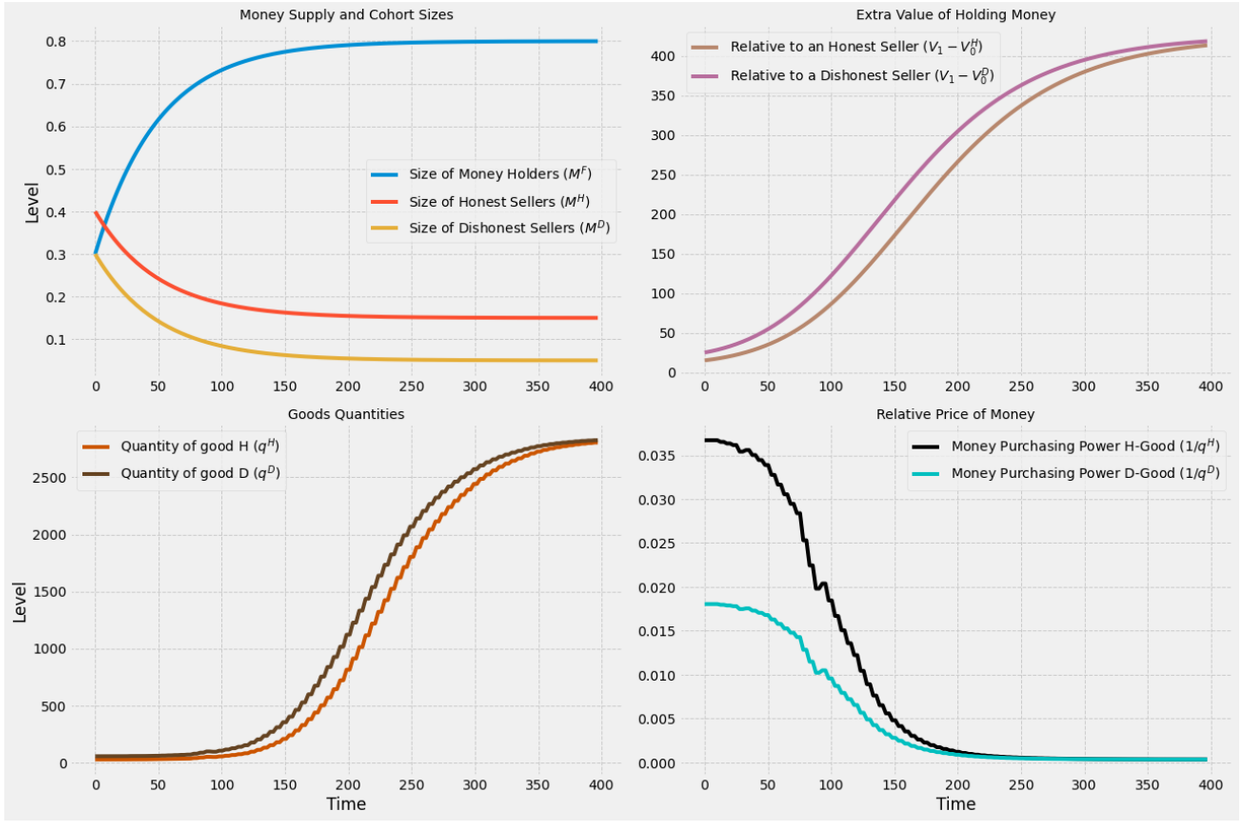
Notes: The table contains the parameter values used in the baseline scenario for the transitional dynamics in the fiat currency regime along with the description of the parameters.

Definition: An equilibrium is a list $\left\{M^F, M^H, M^D, q^H, q^D, V_1, V_0^H, V_0^D\right\}$ that satisfies the two conditions in (3.1) for the two types of sellers, and also equations (3.2)-(3.4) and (3.7)-(3.9), and the incentive constraints in the generalized Nash bargaining problem. The aforementioned equations define a system of eight equations in eight unknowns.

3.1.1 Transitional Dynamics

In this part I will assume that the utility function has the form $u\left(q^i\right) = \frac{\left(q^i\right)^{1-\sigma}}{1-\sigma}$, where σ is a constant that satisfies $\sigma > 0$ and $\sigma \neq 1$. The cost function is linear, so that $\mathcal{C}^i\left(q^i\right) = \eta^i q^i$ where $0 < \eta^i < \sigma$. Table 1 contains the parameter values in the fiat currency regime.

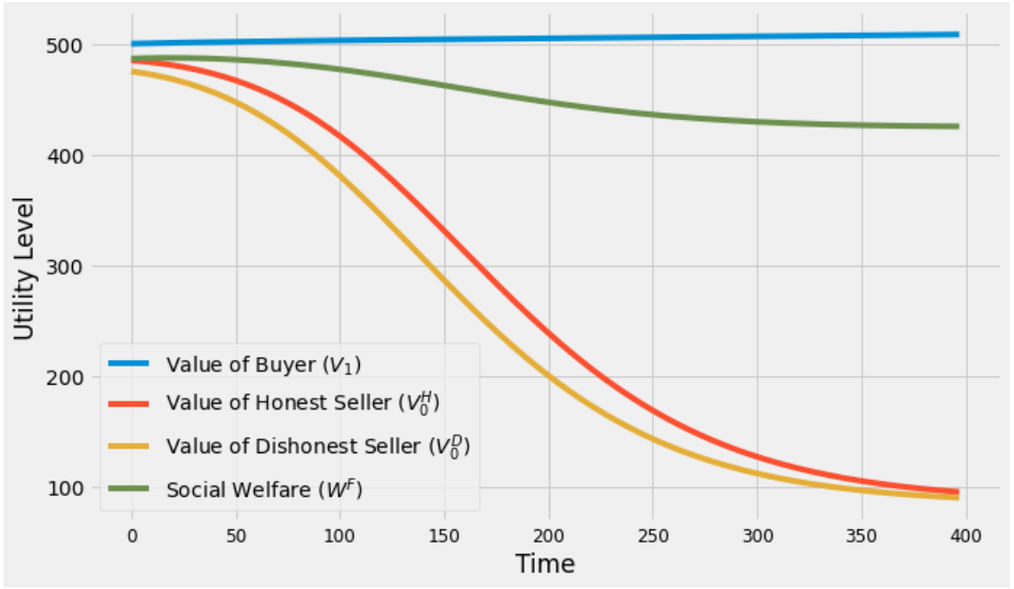
Figure 5: Transitional Dynamics in the Fiat Currency Regime



Notes: The upper left panel shows the transitional dynamics of the money supply and the sizes of various cohorts M^F, M^H and M^D. The upper right panel shows the path of the extra value of holding fiat currency relative to non-money holders $V_1 - V_0^H$ and $V_1 - V_0^D$. The lower left panel shows the path for the quantities of the goods q^H and q^L that solve the Nash bargaining problem in (3.1). The lower right panel shows the path for the purchasing power of money over the two goods $1/q^H$ and $1/q^L$.

The transitional dynamics are presented in Figure 5. The money supply grows over time according to equation (3.7). At the same time the sizes of the cohorts of the sellers decline according to equations (3.8) and (3.9). The extra value of holding money relative to the honest and dishonest sellers increases initially fast and then slows down over time until it converges to its steady state value. These extra values increase because they are driven by the sizes of the cohorts which drive in turn the individual values as shown also in Figure 6. As the money supply grows and the size of the sellers falls, the value of the buyers rises, while the values of the sellers fall. Thus, the extra values of holding money increase. At the same time, the quantities of the goods produced increase in a similar way since they depend on the extra values of holding money, which in turn, depend on the movements of cohort sizes. Then, the quantities affect the extra value of holding money creating this feedback between cohort sizes, extra value of holding money, and quantities.

Figure 6: Welfare in the Fiat Currency Regime



Notes: The figure shows the welfare of various agents V_1, V_0^H, and V_0^D along with social welfare W^F during the transition in the fiat currency regime.

Social welfare declines over time, as shown in Figure 6, since the decrease in the utility level of the sellers is faster than the increase in the utility level of the buyers, even though the buyers grow to be a majority.

3.2 Bitcoin

In the Bitcoin regime, the generalized Nash bargaining leads to the quantity q_B^i that solves

$$\begin{aligned} q_B^i = \arg\max \left[V_0^i + u\left(q^i\right) - V_1 - f^i\right]^{\theta_B^i} \left[V_1 - C^i\left(q^i\right) - V_0^i\right]^{\theta_i} \\ \text{s.t.} \quad V_0^i + u\left(q^i\right) \geq V_1 + f^i \\ V_1 - C^i\left(q^i\right) \geq V_0^i \end{aligned}$$

The first order condition to the previous problem is

$$V_0^i + u\left(q^i\right) - V_1 - f^i = \frac{\theta_B^i}{\theta_i} \frac{\frac{du\left(q^i\right)}{dq^i}}{\frac{dC^i\left(q^i\right)}{dq^i}} \left[V_1 - C^i\left(q^i\right) - V_0^i\right] \tag{3.10}$$

Recall that the value for the buyers is

$$V_1 = \frac{1}{1+r}\Big[M^B V_1 + M^D\left(1-x^D\right)V_1 + M^D x^D\left(V_0^D + u\left(q^D\right) - f^D\right) + M^H\lambda^B\gamma^B\left(V_1 - z_1\right) + M^H\lambda^B\left(1-\gamma^B\right)\left(1-x^H\right)V_1 + M^H\lambda^B\left(1-\gamma^B\right)x^H\left(V_0^H + u\left(q^H\right) - f^H\right) + M^H\left(1-\lambda^B\right)\left(1-x^H\right)V_1 + M^H\left(1-\lambda^B\right)x^H\left(V_0^H + u\left(q^H\right) - f^H\right) + \dot{V}_1\Big] \tag{3.11}$$

The value for the honest sellers is

$$V_0^H = \frac{1}{1+r}\Big[M^H V_0^H + M^D V_0^H + M^B\lambda^B\gamma^B\left(V_0^H - z_0^H\right) + M^B\lambda^B\left(1-\gamma^B\right)\left(1-x^H\right)V_0^H + M^B\lambda^B\left(1-\gamma^B\right)x^H\left(V_1 - \mathcal{C}^H\left(q^H\right)\right) + M^B\left(1-\lambda^B\right)\left(1-x^H\right)V_0^H + M^B\left(1-\lambda^B\right)x^H\left(V_1 - \mathcal{C}^H\left(q^H\right)\right) + v_H^m\left(e_H^*, e_D^*\right) + \dot{V}_0^H\Big] \tag{3.12}$$

The value for the dishonest sellers is

$$V_0^D = \frac{1}{1+r}\Big[M^D V_0^D + M^H V_0^D + M^B\left(1-x^D\right)V_0^D + M^B x^D\left(V_1 - \mathcal{C}^D\left(q^D\right)\right) + \lambda^B\left(M^H + M^B\right)\left(\gamma z_0^D - \psi^D\right) + v_D^m\left(e_D^*, e_H^*\right) + \dot{V}_0^D\Big] \tag{3.13}$$

The extra value of holding money relative to being a dishonest seller is

$$\begin{aligned} V_1 - V_0^D =& \frac{1}{r + \left(M^D + M^B\right)x^D}\Big[M^H x^H\left(1-\lambda^B\gamma^B\right)\left(u\left(q^H\right) - f^H\right) + M^D x^D\left(u\left(q^D\right) - f^D\right) \\ &+ M^B x^D\mathcal{C}^D\left(q^D\right) - M^H\lambda^B\gamma^B z_1 - \lambda^B\left(M^B + M^H\right)\left(\gamma^B z_0^D - \psi^D\right) - v_D^m\left(e_H^*, e_D^*\right) + \dot{V}_1 - \dot{V}_0^D\Big] \\ &- \frac{M^H x^H\left(1-\lambda^B\gamma^B\right)}{r + \left(M^D + M^B\right)x^D}\left(V_1 - V_0^H\right). \end{aligned} \tag{3.14}$$

The extra value of holding money relative to being an honest seller is

$$V_1 - V_0^H = \frac{1}{r + \left(M^H + M^B\right) x^H \left(1 - \lambda^B \gamma^B\right)} \Big[M^H x^H \left(1 - \lambda^B \gamma^B\right) \left(u\left(q^H\right) - f^H\right) + M^D x^D \left(u\left(q^D\right) - f^D\right)$$
$$+ M^B x^H \left(1 - \lambda^B \gamma^B\right) \mathcal{C}^H\left(q^H\right) - M^H \lambda^B \gamma^B z_1 + M^B \lambda^B \gamma^B z_0^H - v_H^m\left(e_H^*, e_D^*\right) + \dot{V}_1 - \dot{V}_0^H \Big]$$
$$- \frac{M^D x^D}{r + \left(M^H + M^B\right) x^H \left(1 - \lambda^B \gamma^B\right)} \left(V_1 - V_0^D\right). \tag{3.15}$$

The money supply evolves according to

$$\dot{M}^B = \delta\left(\bar{M}^B - M^B\right) \tag{3.16}$$
$$\dot{M}^H = -\frac{M^H e_H}{M^H e_H + M^D e_D} \delta\left(\bar{M}^B - M^B\right) \tag{3.17}$$
$$\dot{M}^D = -\frac{M^D e_D}{M^H e_H + M^D e_D} \delta\left(\bar{M}^B - M^B\right). \tag{3.18}$$

Definition: An equilibrium is a list $\left\{M^B, M^H, M^D, q^H, q^D, V_1, V_0^H, V_0^D\right\}$ that satisfies the two equations in (3.10), equations (3.11)-(3.13), and equations (3.16)-(3.18), and the constraints in the Nash bargaining problem. The aforementioned equations define a system of six first order differential equations in six unknowns, plus the two optimality conditions in the bargaining problem that determine the optimal quantities.

3.2.1 Transitional Dynamics

In this part I will continue to use the same utility function and the same cost function for the production of the specialized goods. Table 2 contains the parameter values in the Bitcoin regime. If we compare to Table 1, we can find some differences. First, there are transaction fees paid to the two types of sellers that are assumed to be small in size. Second, we also have the marginal utility cost from mining for both types of agents. The marginal utility cost of mining for dishonest sellers is assumed to be two times the marginal cost of mining for honest sellers. This ensures that condition (2.22) is satisfied along the whole transition path, which is in line with the fact that nobody has ever managed to attack succesfully the Bitcoin network.

The transitional dynamics under the Bitcoin regime are shown in Figure 7. Now the money supply, and the size of the non-money holders coverge over the years to their steady state values. The log of extra values of holding money again initially increase fast and then slow down over time. This is in line with the log of the Bitcoin price behavior seen over the years. Initially, as the size of the money holders increases fast, the value of holding money also increases fast. As the growth rate of money slows down, the extra value of holding money also slows down. The quantities of the two specialized goods follow a similar path to the

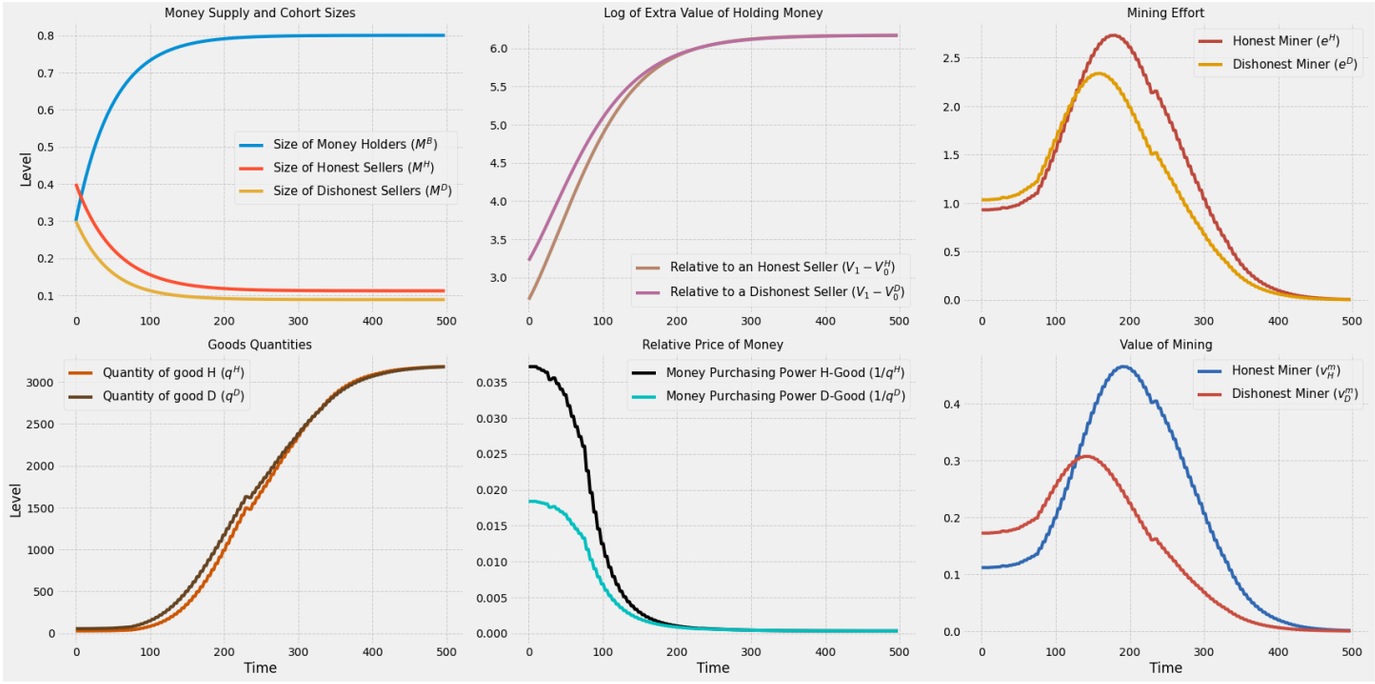
Table 2: Bitcoin Regime Parameter Values

Parameter	Description	Value
Money Holders		
σ	Relative Risk Aversion Coefficient	0.28
r	Discount Factor	0.000001
$\bar{M}^B$	Steady State Cohort Size	0.8
z_1	Individual Cost from Transaction Blocking	5
δ^B	Speed of Cohort Size Increase	0.0015
f^H	Transacttion Fee Paid to Honest Seller	0.01
f^D	Transacttion Fee Paid to Dishonest Seller	0.01
Honest Sellers		
r	Discount Factor	0.000001
$\bar{M}^H$	Steady State Cohort Size	0.15
η^H	Marginal Cost of Production of Specialized Good	0.15
x^H	Probability of Trading with Buyers	0.05
z_0^H	Individual Cost from Transaction Blocking	1.5
c_H	Marginal utility cost of mining	0.1
Dishonest Sellers		
r	Discount Factor	0.000001
$\bar{M}^D$	Steady State Cohort Size	0.05
η^D	Marginal Cost of Production of Specialized Good	0.15
x^D	Probability of Trading with Buyers	0.05
z_0^D	Individual Benefit from Transaction Blocking	1
c_D	Marginal utility cost of mining	0.2
ψ	Individual Cost from Transaction Blocking	0.2

Notes: The table contains the parameter values used in the baseline scenario for the transitional dynamics in the Bitcoin regime along with the description of the parameters.

extra values of holding money, since they depend positively and directly on them through conditions (3.10). As regards the mining efforts of the two types of miners, initially the mining effort increases fast, but then reaches a peak and then declines substantially and approaches zero. The mining effort is also driven by the money rewards and the extrta value of holding money, which also depends on the money supply. Once the money supply growth slows down significantly, the mining effort follows. The initial exponential increase in the mining effort of individual miners is in line with the exponential increase seen in the hash rate. Thus, the model produces a log of value of holding money that increases fast and then slows down over time, and

Figure 7: Transitional Dynamics in the Bitcoin Regime



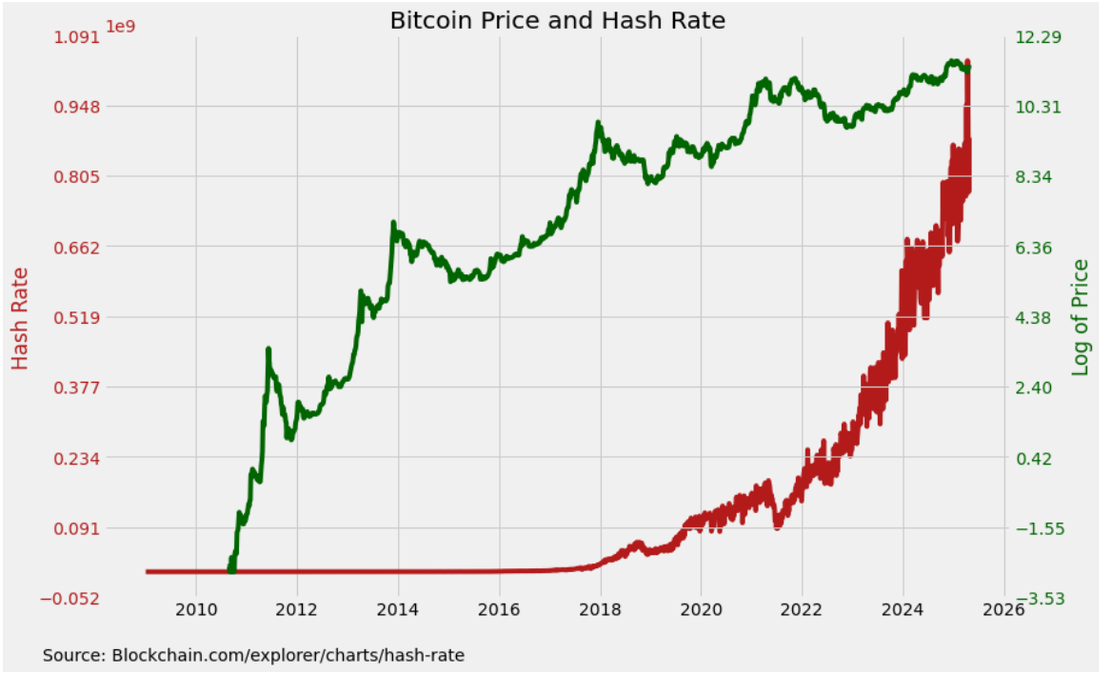
Notes: The upper left panel shows the transitional dynamics of the money supply and the sizes of various cohorts M^B, M^H and M^D. The upper middle panel shows the transitional dynamics for the extra value of holding BTC relative to non-money holders $V_1 - V_0^H$ and $V_1 - V_0^D$. The upper right panel shows the transitional dynamics of the effort levels for honest and dishonest miners e_H and e_D. The lower left panel shows the path for the quantities of the goods q^H and q^L that solve the Nash bargaining problem in (3.10). The lower middle panel shows the path for the purchasing power of money over the two goods $1/q^H$ and $1/q^L$. Finally the lower right panel shows the path for the value of mining for the two types of miners v_H^m and v_D^m.

an initially exponential increase in the mining efforts. Figure 8 contains data from Blockchain.com (2024) on the price behavior and the hash rate behavior since the early days of the Bitcoin network in 2011.

The upper right panel of Figure 9 contains the utility levels for each cohort over time as well as the social welfare. Here, again, social welfare falls over time, since the welfare of the sellers falls faster than the slow increase in the value of the buyers. However, now all utilities reach a steady state level over time.

The question that naturally arises at this point is which of the two regimes leads to higher social welfare over the transtion period. It turns out that there is no definitive answer based on the model used so far. Instead, parameter values such as the speed over which the money supply increases in each regime δ^F and δ are critical. This is not unexpected since in our model the money supply is the main driver of utility dynamics. In both regimes a faster increase of the money supply can lead to higher social welfare over the transition period. Figure 9 also contains the social welfare dynamics under different assumptions for δ^F.

Figure 8: Bitcoin Price and Hash Rate Over Time



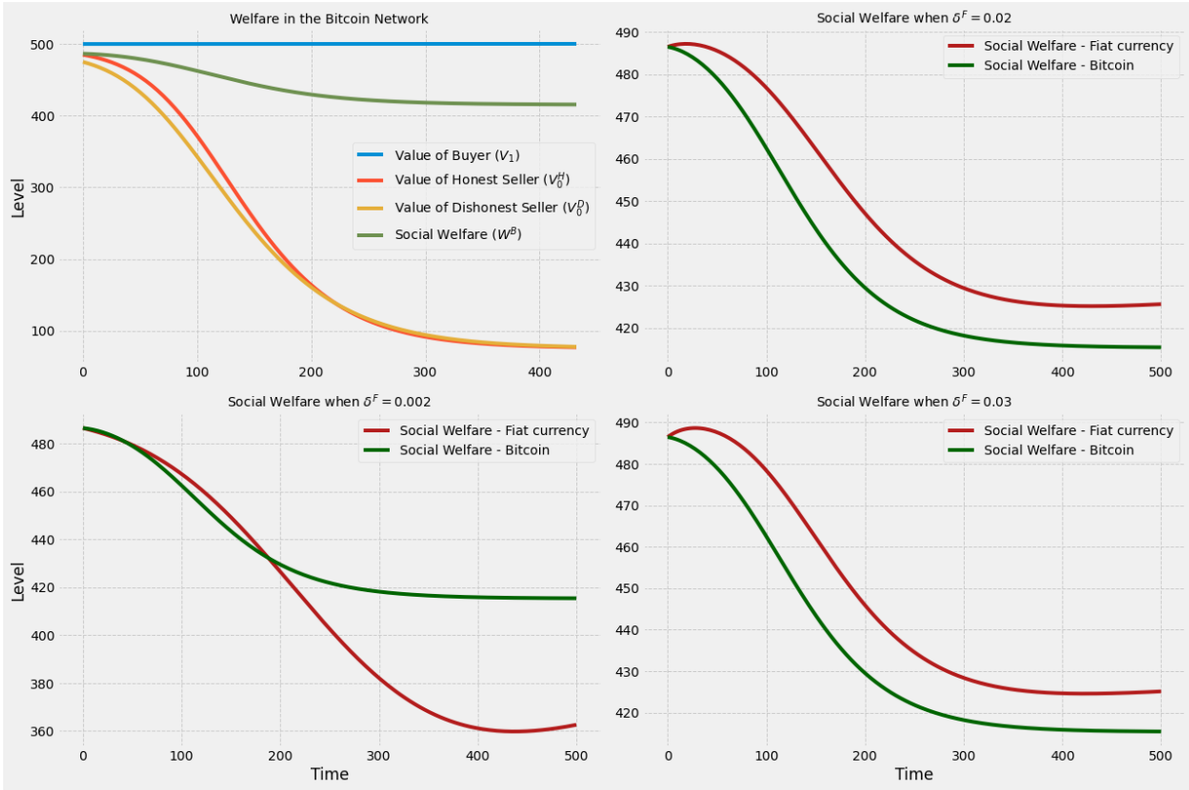
Notes: The above figure shows the log of the USD price of Bitcoin and the hash rate measured in TH/s. Source: https://www.blockchain.com/explorer/charts/hash-rate.

Thus, a more definitive answer would require the use of a richer model that considers the possibility of an unbounded money supply schedule and analyzes the positives and the negatives from a money supply schedule that can be altered through monetary policy and a fixed money supply path such as the one in the Bitcoin network. For instance, a small amount of money floating around that cannot be changed by anyone can protect from dilution, inflation, and currency debasement, but can be a problem during a time of crisis when the demand for money is strong and the supply is fixed, leading to high interest rates that exacerbate the crisis.[5] On the other hand, money supply that is always growing creates dilution and currency debasement, and depending on the fiscal policy stance, it can also create inflation.[6]

[5]As an example we could think of a group of countries that are using a single currency in which they have no control of monetary policy, since monetary policy is controlled by the central bank of the monetary union. If the central bank of the monetary union is not implementing monetary easing for a specific country, for instance through a country-specific QE program, then each country could face an exacerbation of the crisis, which could probably be alleviated if the country could implement a monetary expansion.

[6]See Leeper (1991) and Cochrane (2022), for the interaction of traditional monetary and fiscal policy and their effects on inflation, and Kyriazis (2022) for the interaction of traditional monetary policy, QE and fiscal policy, and their effects on inflation.

Figure 9: Welfare in the Bitcoin Regime



Notes: The figure shows the welfare of various agents V_1, V_0^H, and V_0^D along with social welfare W^B during the transition in the fiat currency regime.

4 Social Welfare and First Best Outcomes

In this section I focus on the problem of a hypothetical social planner that chooses the optimal quantities of the goods produced to maximize steady state social welfare. I first discuss the planning problem under the fiat currency regime and then under the Bitcoin regime. In both cases I also discuss the conditions under which the decentralized equilibrium can lead to the same outcome.

4.1 Fiat Currency

The question that arises at the steady state under the fiat currency regime is if the quantities of the goods q_F^H and q_F^D produced after the bargaining process is the same as the one that a social planner would choose in order to maximize social welfare. To answer this question I consider the social welfare function at the steady state of the fiat currency regime and maximize with respect to q^H and q^D

$$\max_{q^H,\, q^D} W^F = \frac{1}{r}\Big[\bar{M}^F\bar{M}^H x^H (1-\lambda\gamma)\left(u\left(q^H\right)-\mathcal{C}^H\left(q^H\right)\right)+\bar{M}^F\bar{M}^D x^D\left(u\left(q^D\right)-\mathcal{C}^D\left(q^D\right)\right)$$
$$-M^F M^H x^H\lambda\gamma\left(z_1+z_0^H\right)+\bar{M}^D\lambda\left(\bar{M}^H+\bar{M}^F\right)\left(\gamma z_0^D-\psi^D\right)\Big]. \tag{4.1}$$

The first order conditions for the social planner are

$$\frac{du\left(q^H\right)}{dq^H}=\frac{d\mathcal{C}^H\left(q^H\right)}{dq^H} \tag{4.2}$$
$$\frac{du\left(q^D\right)}{dq^D}=\frac{d\mathcal{C}^D\left(q^D\right)}{dq^D} \tag{4.3}$$

So the socially optimal quantities of the goods equate the marginal utility of the buyers with the marginal cost of the corresponding seller. On the other hand, the quantity produced under the fiat currency regime q_F^i is determined by the steady state version of (3.1). This quantity will be equal to the quantity chosen by the social planner if

$$\frac{\theta_F^H}{\theta_H}=\frac{V_0^H+u\left(q^H\right)-V_1}{V_1-\mathcal{C}^H\left(q^H\right)-V_0^H} \tag{4.4}$$
$$\frac{\theta_F^D}{\theta_D}=\frac{V_0^D+u\left(q^D\right)-V_1}{V_1-\mathcal{C}^D\left(q^D\right)-V_0^D} \tag{4.5}$$

However, the ratios θ_F^H/θ_H and θ_F^D/θ_D can be given by equations (4.4)-(4.5) only by chance. A more realistic scenario would be $\theta_F^i=\bar{M}^F$, $\theta_H=\bar{M}^H$ and $\theta_D=\bar{M}^D$ so that the bargaining power of each agent type is given by its relative size in the population. But the ratios between the size of cohorts need not necessarily be determined by equations (4.4)-(4.5). Hence, it is possible to achieve the socially optimal quantity under the fiat currency regime, but not likely.

4.2 Bitcoin

At the steady state I still assume that $c_D \geq c_H$, which implies that the Bitcoin network remains secure. The question that arose under the fiat currency regime arises also under the Bitcoin network: are the quantities determined after the bargaining process the socially optimal? Again we need to compare the optimality

conditions related to the bargaining problems to the solution corresponding to the social planner's problem.[7] The social planner under the Bitcoin network would maximize the following social welfare function

$$\max_{q^H,\, q^D} W^B = \frac{1}{r}\Big[\bar{M}^B\bar{M}^H x^H\left(u\left(q^H\right)-\mathcal{C}^H\left(q^H\right)\right)+\bar{M}^B\bar{M}^D x^D\left(u\left(q^D\right)-\mathcal{C}^D\left(q^D\right)\right) - \bar{M}^B\left(\bar{M}^H x^H f^H+\bar{M}^D x^D f^D\right)+\bar{M}^H\bar{v}_H^m+\bar{M}^D\bar{v}_D^m\Big] \tag{4.6}$$

The value of mining at the steady state is given by equation (2.43) and is independent of q^H and q^D. The solution to the above problem again leads to a socially optimal quantity such that

$$\frac{du\left(q^H\right)}{dq^H}=\frac{d\mathcal{C}^H\left(q^H\right)}{dq^H} \tag{4.7}$$

$$\frac{du\left(q^D\right)}{dq^D}=\frac{d\mathcal{C}^D\left(q^D\right)}{dq^D} \tag{4.8}$$

Obviously equations (4.7)-(4.8) are different conditions relative to (3.10). Again, we can solve for the ratios of bargaining power that could make the two conditions be the same

$$\frac{\theta_B^H}{\theta_H}=\frac{V_0^H+u\left(q^H\right)-V_1-f^H}{V_1-\mathcal{C}^H\left(q^H\right)-V_0^H} \tag{4.9}$$

$$\frac{\theta_B^D}{\theta_D}=\frac{V_0^D+u\left(q^D\right)-V_1-f^D}{V_1-\mathcal{C}^D\left(q^D\right)-V_0^D} \tag{4.10}$$

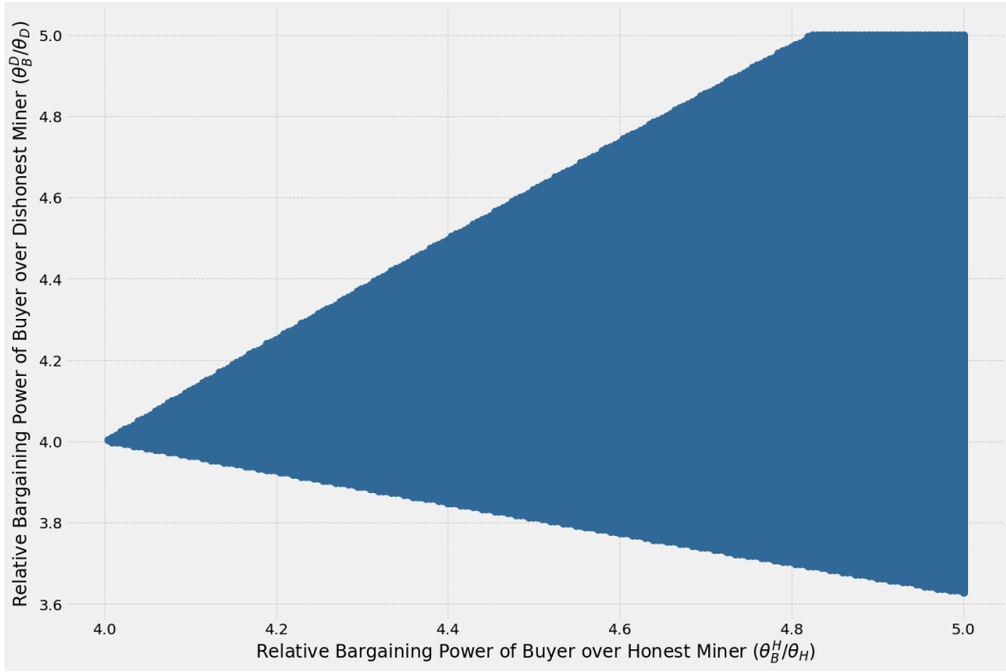
Again, the ratios can take the values described in (4.9)-(4.10) only by chance. However, under the Bitcoin network there is another way to achieve the socially optimal quantities, and this is by choosing the transaction fees so as to make the bargaining outcome the same as the efficient one. So far I have assumed that the fees are just exogenous constants. Now I will assume that the fees are still constants, but are determined at the steady state so as to make equations (3.10) the same as the efficiency conditions (4.7)-(4.8) so that

$$f^H=u\left(q^H\right)+\frac{\theta_B^H}{\theta_H}\mathcal{C}^H\left(q^H\right)-\frac{\theta_B^H+\theta_H}{\theta_H}\left(V_1-V_0^H\right) \tag{4.11}$$

$$f^D=u\left(q^D\right)+\frac{\theta_B^D}{\theta_D}\mathcal{C}^D\left(q^D\right)-\frac{\theta_B^D+\theta_D}{\theta_D}\left(V_1-V_0^D\right). \tag{4.12}$$

[7] Of course in the Bitcoin network there is no social planner and this is part of the value proposition of decentralized networks. However, it is still possible to implement a "policy" if there is significant consensus about this "policy", although implementation would probably require a change in the protocol.

Figure 10: Efficient Relative Bargaining Power Combinations



Notes: The graph shows the values of the ratio θ_B^D/θ_D for a range of values of the ratio θ_B^H/θ_H that satisfy equations (2.40)-(2.41) and equations (4.11)-(4.12) and lead to $f^H > 0$, $f^D > 0$, $V_0^H \geq 0$, $V_0^D \geq 0$, $V_1 - V_0^H \geq \mathcal{C}^H\left(q^H\right)$ and $V_1 - V_0^D \geq \mathcal{C}^D\left(q^D\right)$ when evaluated at the socially optimal quantities at the steady state.

Equations (4.11)-(4.12) are evaluated at the socially optimal quantities chosen by the social planner. However, we need to ensure that the transaction fees satisfy the incentive constraints of the buyers and at the same time are positive in order to incentivize mining at the steady state. Starting from the incentive constraints of the buyers, we can substitute out the terms f^H and f^D by using equations (4.11) and (4.12) and get

$$V_0^i + u\left(q^i\right) - V_1 - f^i \geq 0 \overset{(4.11)-(4.12)}{\Longrightarrow} \frac{\theta_B^i}{\theta_i}\left[V_1 - V_0^i - \mathcal{C}^i\left(q^i\right)\right] \geq 0. \tag{4.13}$$

The previous condition is true since those are the incentive constraints of the sellers, and I solve for equilibria that satisfy those constraints. Ideally, one can solve analytically the system of equations given by equations (2.40)-(2.41) and equations (4.11)-(4.12) and derive the solutions for f^H, f^D, $V_1 - V_0^H$ and $V_1 - V_0^D$. Then extra conditions for the values of the ratios θ_B^H/θ_H and θ_B^D/θ_D can be imposed so that the fees are positive $f^H > 0$, $f^D > 0$ and the incentive constraints of the sellers $V_1 - V_0^H \geq \mathcal{C}^H\left(q^H\right)$ and $V_1 - V_0^D \geq \mathcal{C}^D\left(q^D\right)$ are satisfied. When the incentive constraints of the sellers are satisfied, the incentive constraints of the buyers are also satisfied.

However, given the complexity of these equations, analytical solutions are not very helpful to build intuition, and for that reason the four equations are solved numerically and then the four unknown variables are evaluated for different values of the two ratios of bargaining power. From Figure 10, it is evident that when the relative bargaining power of the buyers over the honest sellers increases, the range of values for which the relative bargaining power of the buyers over the dishonest sellers leads to the desired results increases.

Therefore, in the Bitcoin network, if transaction fees at the steady state are given by equations (4.11)-(4.12), and the relative bargaining ratios take values consistent with a monetary equilibrium, then the quantities of the goods produced are socially optimal. However, implementing a new transaction fee shedule such as the one described by equations (4.11)-(4.12) would most likely require a fork of the Bitcoin blockchain.

5 Concluding Remarks

In this paper, I focused on the potential social welfare benefits from using the Bitcoin network over a fiat currency network. First, I derived the conditions under which the Bitcoin network remains secure. Then, I showed that when the Bitcoin network is secure, transacting over this network can lead to social welfare gains if the transaction volume is higher than the fiat currency regime and also when the cost of transaction blocking in the fiat currency regime is higher than the welfare cost of mining. I also showed that when fixed costs are introduced then miners need to exert less effort to disincentivize their competitors from entering the market. In the real world the fixed costs of investment in equipment are extremely high, and this makes dishonest miners less likely to enter the market. In terms of transitional dynamics, the model produces dynamics for the value of money and mining efforts that have similar shape to those observed in reality. As for social welfare, parameter values related to the speed of increase of the money supply are critical for comparing the two regimes. Finally, the first best can be achieved in the Bitcoin network by optimally setting the transaction fees.

References

Blockchain.com, 2024. URL https://Blockchain.com. 32

M. Choi and G. Rocheteau. Money mining and price dynamics. *American Economic Journal: Macroeconomics*, 13(4):246–294, 2021. 4

J. Cochrane. The fiscal theory of the price level. 2022. 33

J. Fernández-Villaverde and D. Sanches. Can currency competition work? *Journal of Monetary Economics*, 106: 1–15, 2019. 5

A. Geromichalos and L. Herrenbrueck. The strategic determination of the supply of liquid assets. Technical report, working paper, 2016. 4

P. He, L. Huang, and R. Wright. Money and banking in search equilibrium. *International Economic Review*, 46 (2):637–670, 2005. 4

N. Kiyotaki and R. Wright. On money as a medium of exchange. *Journal of political Economy*, 97(4):927–954, 1989. 4

A. Kyriazis. Quantitative easing and fiscal policy effectiveness. *Available at SSRN 4371287*, 2022. 33

R. Lagos and G. Rocheteau. Money and capital as competing media of exchange. *Journal of Economic theory*, 142(1):247–258, 2008. 4

E. M. Leeper. Equilibria under activeand passivemonetary and fiscal policies. *Journal of monetary Economics*, 27(1):129–147, 1991. 33

S. Lotz and F. Vasselin. A new monetarist model of fiat and e-money. *Economic Inquiry*, 57(1):498–514, 2019. 5

S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008. 4

L. Nuzzi, K. Waters, and M. Andrade. Breaking bft: Quantifying the cost to attack bitcoin and ethereum. *Available at SSRN*, 2024. 23

E. S. Pagnotta. Decentralizing money: Bitcoin prices and blockchain security. *The Review of Financial Studies*, 35(2):866–907, 2022. 5

G. Rocheteau and A. Rodriguez-Lopez. Liquidity provision, interest rates, and unemployment. *Journal of Monetary Economics*, 65:80–101, 2014. 4

L. Schilling and H. Uhlig. Some simple bitcoin economics. *Journal of Monetary Economics*, 106:16–26, 2019. 5

A. Trejos and R. Wright. Search, bargaining, money, and prices. *Journal of political Economy*, 103(1):118–141, 1995. 4