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

Antzelos Kyriazis*

July 2026

Abstract

What is the role of Bitcoin? This paper argues 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 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 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 making the case for the fiat currency regime. Over the transition, the absence of transaction blocking, the higher value of money, and the mining rewards lead to higher welfare for each agent in the Bitcoin regime. In addition, if fixed costs are introduced each type of miner needs less effort to deter the other type from entering. 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.

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. The most common answer is that Bitcoin is a hedge against global currency debasement due to being a hard asset. This paper focuses on the security aspect of Bitcoin and argues that the Bitcoin network can play the role of a defense mechanism against trtansaction blocking, 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 due to lack of trust caused by transaction blocking, the Bitcoin network naturally arises as an alternative global settlement layer due to being a decentralized, trustless, 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

[1]The 2026 Crypto Crime Trends report by Chainalysis (2026) suggests that less than 1% of total crypto transactions were associated with illicit activities in 2025, while the role of Bitcoin in those transactions has been declining over the years.

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 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. 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 the security friction disappears. 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 greater than 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 is higher for every agent along the transition in the Bitcoin regime, for all issuance speed parameters considered, because in the Bitcoin regime there is no transaction blocking, the value of money is higher, and agents receive mining rewards. Also the model produces qualitatively two features of the data: the logarithm of the value of holding money has a concave shape as the logarithm of the Bitcoin price, and individual mining effort initially increases fast mirroring the initial fast increase in the hash rate. However, the similarities are only about the shapes and not about the exact matching of variables: the dollar price level of Bitcoin and the efficiency of mining hardware are not part of the model.

Finally, I show that in the absence of any policy instruments, 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 a function of 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 transaction fees can work as the policy instruments that resolve the inefficiency. Specifically, 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, can implement the socially optimal quantities of the goods. The transaction fees work as Pigouvian taxes for the buyers. Nonetheless, implementing this fee policy would require singificant consensus in the network.

In the model considered the fiat currency friction is driven by exogenous probabilities while Bitcoin resolves the security issues through the optimizing behavior of miners. This is a deliberate choice that resembles the asymmetry in the real world: agents in fiat currency regimes do not control the probability of transaction blocking but they can participate in the Bitcoin network as honest miners and resolve the security issue. However, the model is not focusing only on the positive aspects of Bitcoin. Specifically, mining comes with the cost of operating the miner and transacting over the Bitcoin network requires the payment of fees. In addition, as argued later, Bitcoin is not a secure network when the marginal benefit per unit of marginal cost for the dishonest miners exceeds the corresponding ratio for the honest miners, and if the transaction blocking probabilities are close to zero, then the Bitcoin solution is not really improving welfare. The chosen values of the transaction blocking probabilities in the fiat regime at $\lambda = \gamma = 0.3$ might seem large, but are favorable for the fiat regime because what matters is the overall probability of a successful attack $\lambda\gamma$ and this increases from 0.09 to 0.3 if the attack is profitable, as assumed in the model, and if the attacker is able to choose $\lambda = 1$, reducing social welfare substantially.

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 initiated by Kiyotaki and Wright (1989) and Trejos and Wright (1995). Those papers 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 on the tradition of the previous two, but also allows for the confiscation of the money stock is the paper of He et al. (2005). This security friction is resolved by the endogenous emergence of banks that custody individual assets safely. In this paper I build on He et al. (2005). The fiat currency regime is kept similar to He et al. (2005), but now the security friction is the blocking of transaction flows and is resolved differently, through the decentralized Bitcoin mining network. As a result, the welfare comparison across the two regimes highlights the role of the defense mechanism and not differences in the environment between the two papers.

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. In Pagnotta (2022) the attacker has an exogenous hash-rate budget A, while in this paper the dishonest miners are choosing optimally their mining effort, which determines the success probability and as a result the attack probability by backwards induction. Hence, the security level is a sub-game perfect Nash equilibrium and the decision not to attack is derived, not imposed by exogenous parameters. In addition, in this paper the success probability is determined by an indicator function that assigns a probability of one if dishonest miners control the absolute majority of the mining effort and zero otherwise. The absence of the price-security feedback loop, because security is the result of a Nash equilibrium on mining efforts driven by different mining costs, eliminates the multiplicity found in Pagnotta (2022) and allow for a clean welfare comparison between the fiat currency and the Bitcoin regimes. The security function adopted by Pagnotta (2022) is considered in Appendix A.1 replacing the attacker's exogenous hash rate budget with the mining effort of the dishonest miners.

This paper is also related to papers that introduce an endogenous mechanism for the determination of money supply such as Lagos and Rocheteau (2008), Rocheteau and Rodriguez-Lopez (2014), and Geromichalos and Herrenbrueck (2016) because of the mining decisions in the Bitcoin network. Choi and Rocheteau (2021) have agents optimally deciding whether to become miners and determine the money supply, but in their model there is no game between honest and dishonest miners and the model focuses on price dynamics that resemble the boom-bust cycles observed in cryptocurrency prices. In this paper, the miners do not determine only the increase in the money supply, but also decide if money can be censored.

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). 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 by assumption more secure, and studied the conditions under which the two can coexist. The latter three papers abstract from the security friction of the private currency analyzed here or resolve it exogenously, while this paper uses an endogenous mechanism to resolve it.

Overall, this paper's combined main contributions are i) to model money censorship and the security of money as a game between honest and dishonest miners providing an endogenous resolution mechanism, ii) to provide a welfare comparison across monetary regimes and welfare decomposition for each agent both at the steady state and over the transition, and iii) to provide a way to implement the first best solution at the steady state by optimally setting transaction fees. The papers from the literature mentioned above contribute at most to one of these areas.

It should also be noted that the paper does not focus on the double spending problem because this would require the money holders to be miners and have the majority of the mining effort to be able to double spend. This would violate the assumption about money holders holding one unit of currency. Moreover, the model does not try to match the USD price of Bitcoin and the hardware efficiency of miners in the real world. The model focuses on mining incentives, not total hash-rate output.

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 indivisibility. 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 both regimes, and I provide a welfare comparison across the two regimes. 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 and section 6 recognizes the help of generative AI in this work.

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.

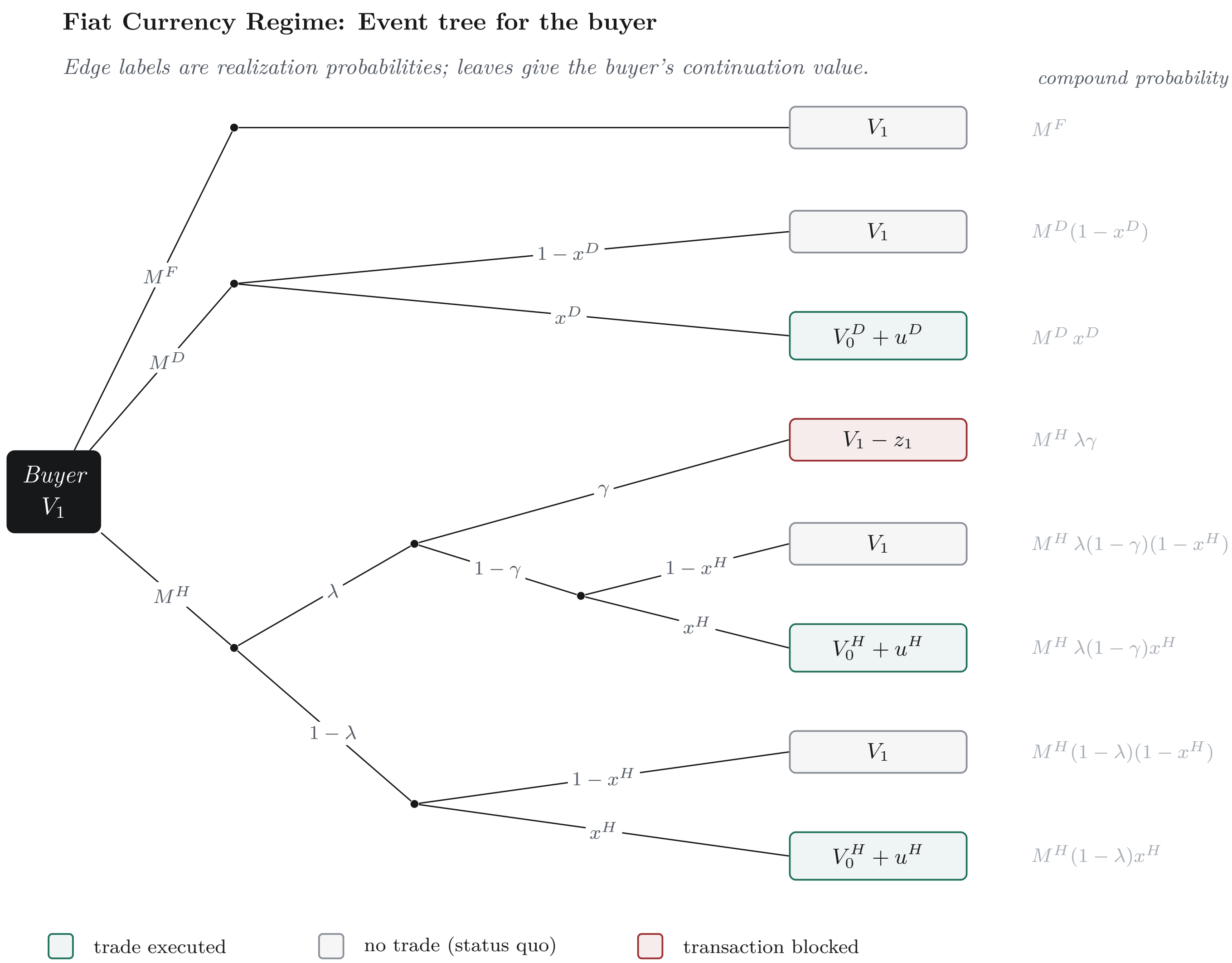
2.1 Fiat Currency

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

Figure 1: Event Tree for Buyers



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 the buyer likes the good produced by the seller with probability x^H the transaction takes place with total probability $M^H\lambda\left(1-\gamma\right)x^H$ 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 probability $M^H\lambda\left(1-\gamma\right)\left(1-x^H\right)$ 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 which depicts the matching expectations without the drift terms $\dot{V}_1$. 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 $r > 0$, the value function of a buyer can be written as

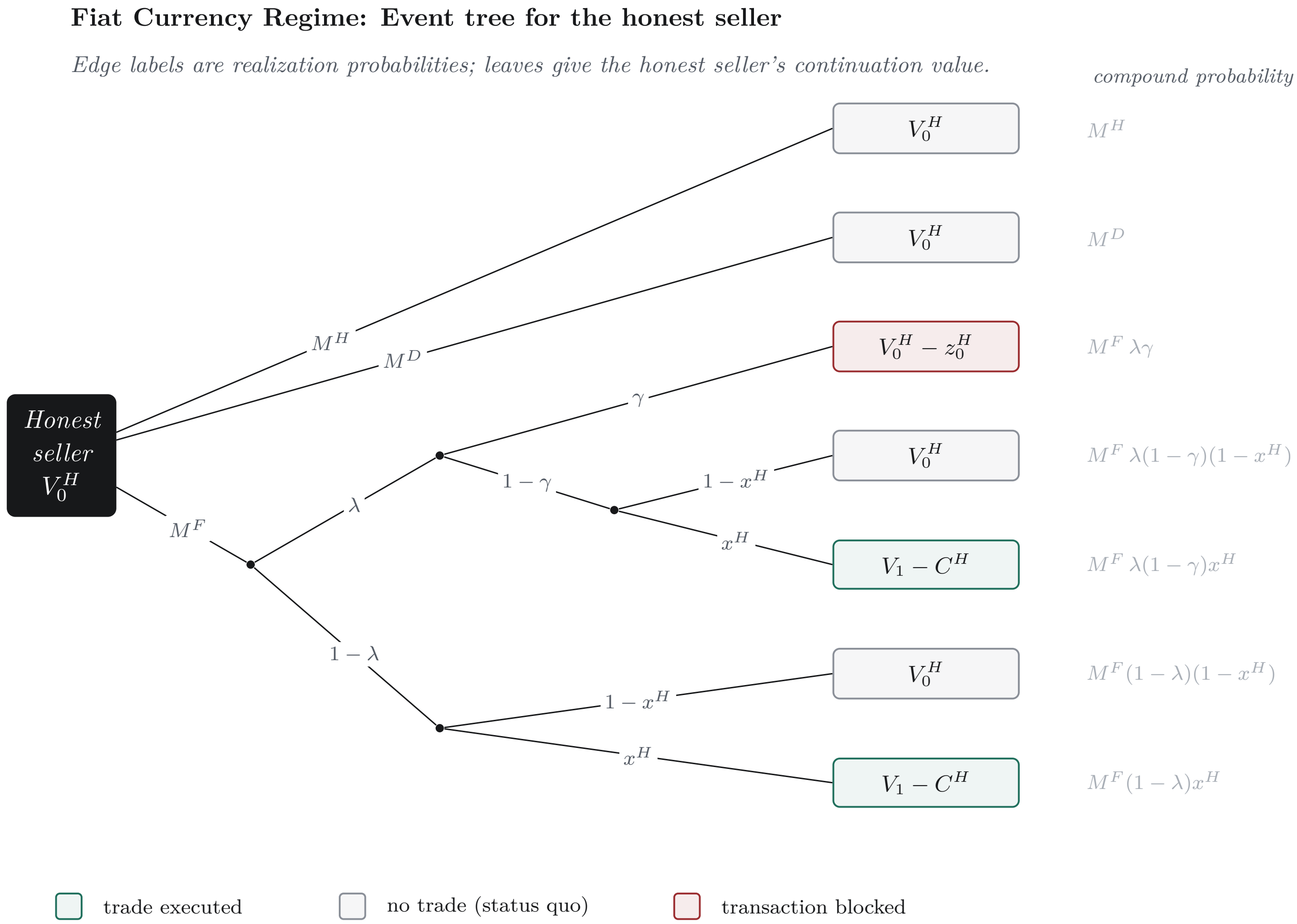
$$
\begin{aligned}
V_1 = & \frac{1}{1+r} \Big[M^F V_1 + M^D \left(1 - x^D\right) V_1 + M^D x^D \left(V_0^D + u^D\right) + M^H \lambda \gamma \left(V_1 - z_1\right) + M^H \lambda (1-\gamma) \left(1 - x^H\right) V_1 \\
& + M^H \lambda (1-\gamma) x^H \left(V_0^H + u^H\right) + M^H (1-\lambda) \left(1 -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

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 probability $M^F \lambda (1-\gamma) x^H$ 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 probability $M^F \lambda (1-\gamma) \left(1 - x^H\right)$ 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 $M^F (1-\lambda) x^H$ 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 $M^F (1-\lambda) \left(1 - x^H\right)$ and the value of the honest seller becomes $V_0^H + \dot{V}_0^H$.

Figure 2: Event Tree for Honest Sellers

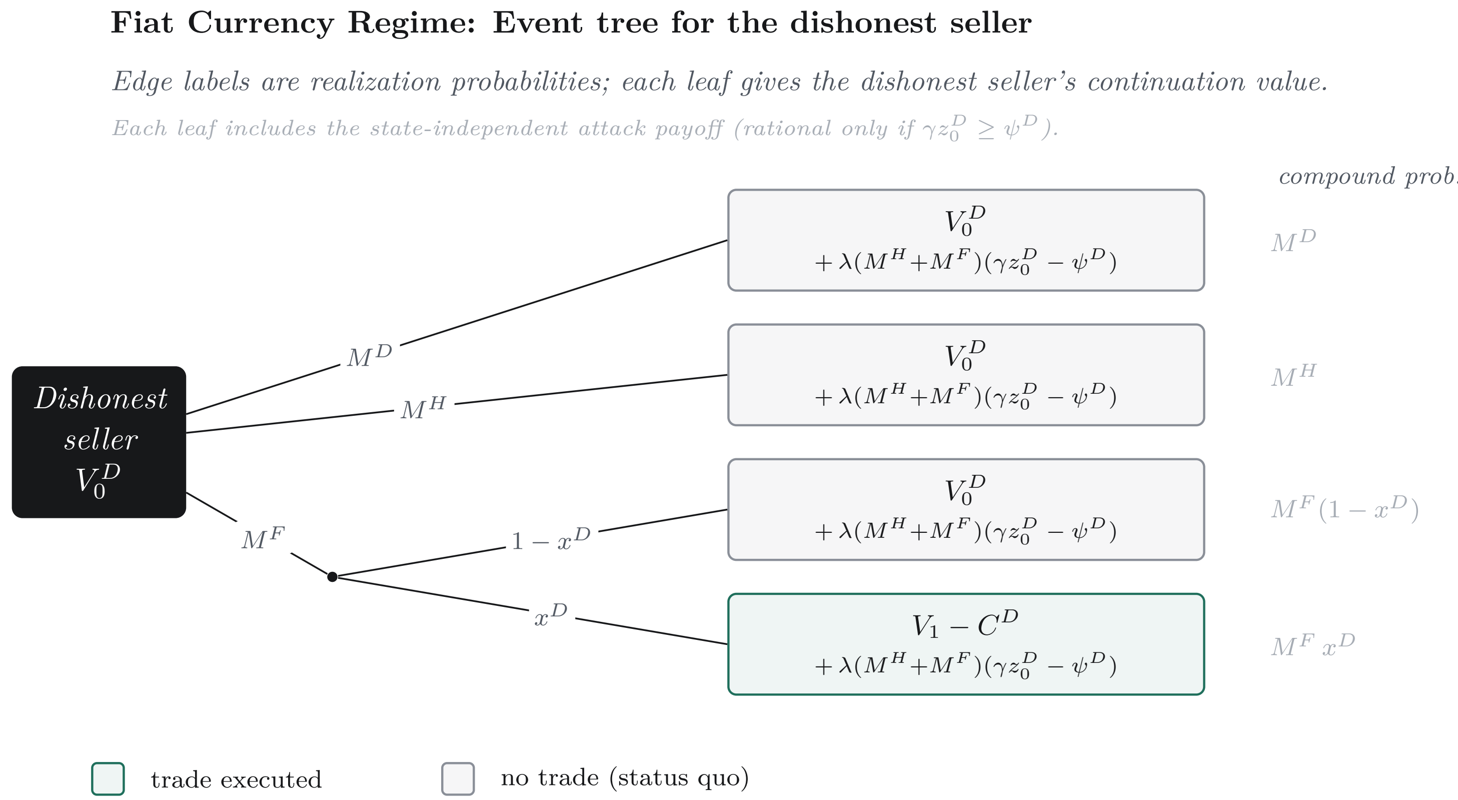


All the previous events are summarized in Figure 2 which depicts the matching expectations without the drift terms $\dot{V}_0^H$. The honest seller also equates in equilibrium his current value with the expected present discounted value he can get from all the previous outcomes so that

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

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

Figure 3: Event Tree for Dishonest Sellers



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 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 which depicts the matching expectations without the drift terms $\dot{V}_0^D$. 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

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

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 constraints $V_0^H > 0$ 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

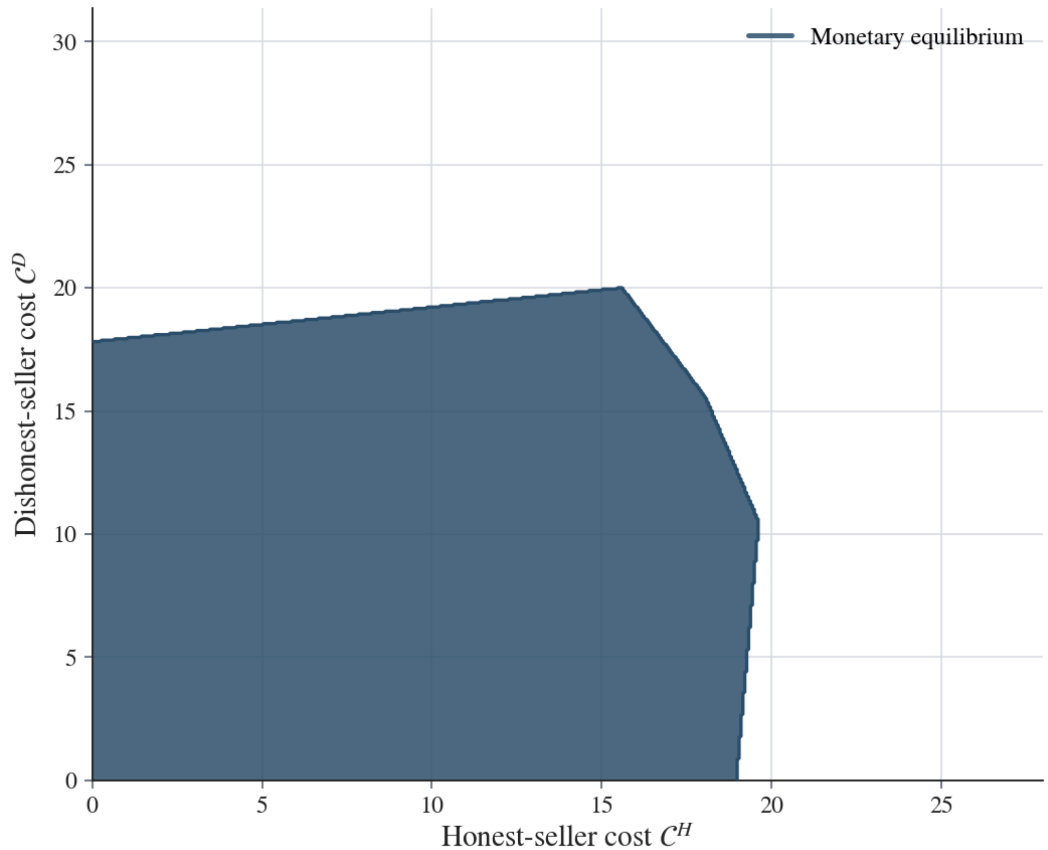
In this part I focus at the steady state of the model with fiat currency. The steady state is the state in which all the endogenous variables of the model do not evolve anymore. Starting from the value function of money holders we have that

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

For the honest sellers we also have that

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

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.

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

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

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

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

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

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

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 than or equal to 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 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

[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 simplifies the analysis. A more general probability function for a successful attack is considered in Appendix A.1.

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.

[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 for fees expressed in terms of the generic good.

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

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

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

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

Proposition 1: *The Bitcoin network remains secure if and only if the marginal benefit from mining per unit of marginal cost for the honest sellers is greater than or equal to the same ratio for the dishonest sellers.*

Proof: Divide equation (2.16) by (2.19) and get

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

For the Bitcoin network to be secure we need

$$\frac{M^H e_H}{M^D e_D} \geq 1 \Leftrightarrow \frac{c_D}{c_H}\frac{MB_H}{MB_D} \geq 1 \Leftrightarrow \frac{MB_H}{MC_H} \geq \frac{MB_D}{MC_D}. \ \blacksquare \tag{2.22}$$

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.

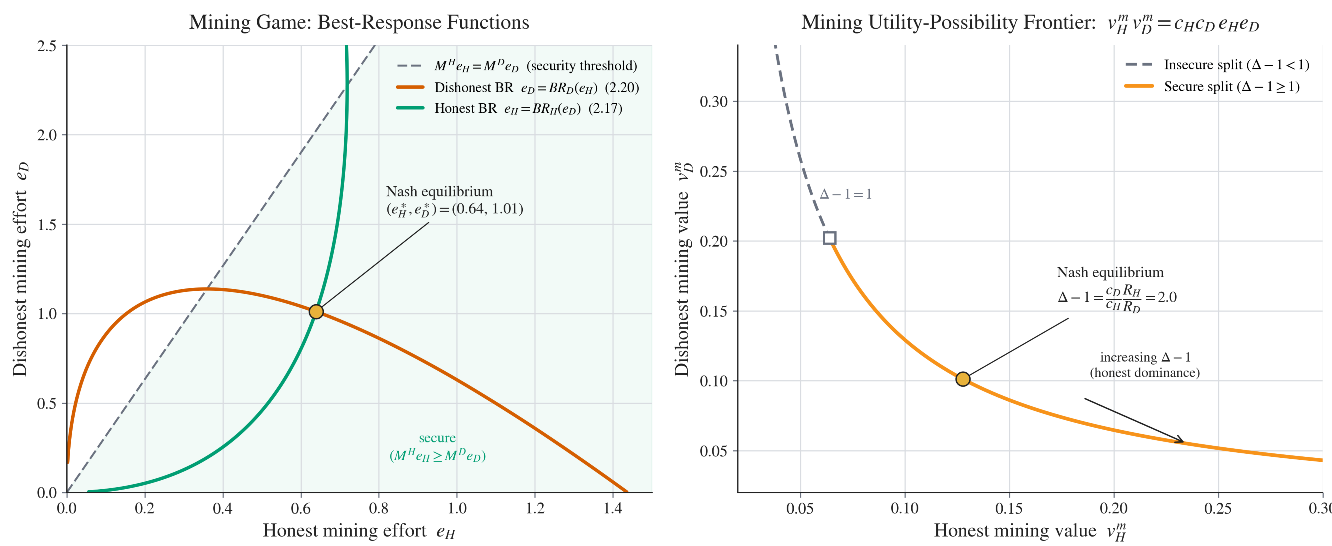
Corollary 1: *At the steady state, the Bitcoin network remains secure if and only if the cost of mining of the dishonest miners is greater than or equal to the cost of mining of the honest sellers.*

Proof: At the steady state $M^B = \bar{M}^B \overset{(2.21)}{\Longrightarrow} MB_H = MB_D$. Then the corollary follows from (2.22). $\blacksquare$

If we use equation (2.21) we can also determine the aggregate mining effort as follows

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

Figure 5: Mining Game: Best Response Functions and Utility Possibility Frontier



Notes: The left panel shows the best response functions for the effort levels of each type of miners for a given level of effort of the other type of miners along with the region in which the security condition (2.22) is satisfied and the Nash equilibrium in a mid-adoption state of the transition path. The right panel shows the utility-possibility frontier between the mining values of the two types of miners together with the region in which the security condition is satisfied and the corresponding Nash equilibrium.

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

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

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

Observe that $v_H^m(e_H^*, e_D^*) > 0$ and $v_D^m(e_D^*, e_H^*) > 0$ 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. Equations (2.26) and (2.27) define a utility possibility frontier that implies a negative relation between the value of mining for the two miner types. Figure 5 depicts the best response functions together with the utility possibility frontier and the corresponding Nash equilibrium.

2.2.2 Trading Decisions

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

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

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

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

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

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

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

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

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

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

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 $M^B = \bar{M}^B$, $M^H = \bar{M}^H$ and $M^D = \bar{M}^D$, 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

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

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

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

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

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

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

$$rV_1 = \bar{M}^H x^H \left(V_0^H - V_1 + u^H - f^H\right) + \bar{M}^D x^D \left(V_0^D - V_1 + u^D - f^D\right). \tag{2.37}$$

For the honest sellers we have that

$$rV_0^H = \bar{M}^B x^H \left(V_1 - V_0^H - \mathcal{C}^H\right) + \bar{v}_H^m \left(\bar{e}_H^*, \bar{e}_D^*\right). \tag{2.38}$$

For the dishonest sellers we also have that

$$rV_0^D = \bar{M}^B x^D \left(V_1 - V_0^D - \mathcal{C}^D\right) + \bar{v}_D^m \left(\bar{e}_D^*, \bar{e}_H^*\right). \tag{2.39}$$

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

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

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

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

The steady state social welfare under the Bitcoin regime is defined by $\bar{W}^B = \bar{M}^B V_1 + \bar{M}^H V_0^H + \bar{M}^D V_0^D$.

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

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

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

Proposition 2: *The steady state social welfare under the Bitcoin regime exceeds the steady state social welfare under the fiat currency regime if and only if the total gains from trade in the Bitcoin network minus the total cost of mining are higher than the total gains from trade in the fiat currency regime minus the net total cost of transaction halt.*

Proof: Assume different steady state cohort sizes across the two regimes. Subtract (2.11) from (2.42) term by term and impose $\bar{W}^B > \bar{W}^F$ to get

$$\begin{aligned}&\bar{W}^B > \bar{W}^F \Leftrightarrow \bar{M}^B \bar{M}^H x^H \left(u^H - \mathcal{C}^H - \frac{2c_H c_D}{(c_H + c_D)^2} f^H\right) + \bar{M}^B \bar{M}^D x^D \left(u^D - \mathcal{C}^D - \frac{2c_H c_D}{(c_H + c_D)^2} f^D\right) > \\ &\bar{M}^F \bar{M}^H (1 - \lambda\gamma) x^H \left(u^H - \mathcal{C}^H\right) + \bar{M}^F \bar{M}^D x^D \left(u^D - \mathcal{C}^D\right) - \bar{M}^F \bar{M}^H \lambda\gamma \left(z_1 + z_0^H\right) + \bar{M}^D \lambda \left(\bar{M}^H + \bar{M}^F\right) \left(\gamma z_0^D - \psi^D\right) \blacksquare\end{aligned} \tag{2.44}$$

Corollary 2: *If the steady state cohort sizes are equal across the two regimes, steady state social welfare under the Bitcoin regime exceeds steady state social welfare under 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.*

Proof: Let the cohort sizes be equal across the two regimes. Cancel out the common terms arising on both sides of (2.44) and get

$$\begin{aligned}\bar{W}^B > \bar{W}^F \Leftrightarrow \bar{M}^B &\left(\bar{M}^H x^H f^H + \bar{M}^D x^D f^D\right) \frac{2c_H c_D}{(c_H + c_D)^2} < \\ &\lambda\gamma \bar{M}^F \bar{M}^H x^H \left(u^H - \mathcal{C}^H\right) + \bar{M}^F \bar{M}^H \lambda\gamma \left(z_1 + z_0^H\right) - \bar{M}^D \lambda \left(\bar{M}^H + \bar{M}^F\right) \left(\gamma z_0^D - \psi^D\right). \blacksquare\end{aligned} \tag{2.45}$$

Observe that the terms in the left hand side of (2.44) 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. An argument against the usage of Bitcoin would be that transaction blocking probabilities are not high in the real world. However, individuals in authoritarian regimes and autocracies and sanctioned populations face probabilities $0 << \lambda$ and $0 << \gamma$. The sizes of these cohorts in the global population are substantial as discussed later in the calibration part. 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 (2.44) 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 (2.44) 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 than 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 of the dishonest miners that would make the honest ones unwilling to exert any effort and modify the best response function as follows

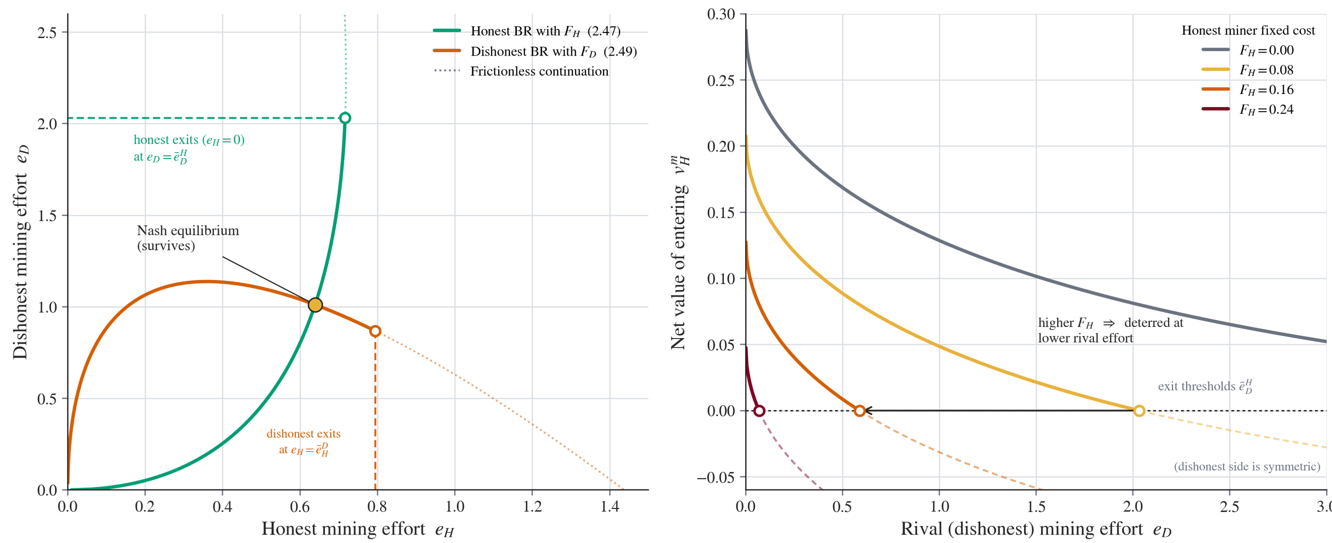
$$BR_H\left(e_D\right) = \begin{cases} \dfrac{1}{M^H} \left[M^D e_D \dfrac{M^B \left(M^H x^H \left(1 - \lambda^B \gamma^B\right) f^H + M^D x^D f^D \right) + \delta \left(\bar{M}^B - M^B \right) \left(V_1 - V_0^H \right)}{c_H} \right]^{\frac{1}{2}} - \dfrac{M^D}{M^H} e_D, \\ \text{if } e_D \leq \dfrac{M^H}{M^D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

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, the results are symmetric

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

Figure 6: Mining Game: Best Response Functions with Fixed Costs



Notes: The left panel shows the best response functions for the mining efforts under the existence of fixed costs. The right panel shows the net value of entering of an honest miner and the exit threshold as a function of the mining effort of a dishonest miner for different levels of the fixed cost faced by the honest miner.

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

Figure 6 depicts the new best response functions under fixed costs, together with the exit points and the property that higher fixed costs for one miner type lead to lower effort for the other type. Nuzzi et al. (2024) report that the fixed cost of a dishonest miner trying to take over the network is estimated to be in the billions of dollars. Large fixed costs combined with large hash rates make it substantially more difficult for attackers to take over the network, making 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 $u'(q) > 0 \geq u''(q)$, while the producers incur a cost $\mathcal{C}^i\left(q^i\right)$ when producing q^i units with $d\mathcal{C}(q)/dq > 0$ and $d^2\mathcal{C}(q)/dq^2 \geq 0$, 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 subject to the incentive constraints. In what follows I present the problem and describe the equilibria under the two regimes.

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. It is assumed that $\theta_F^i = \theta_F = \left(M^F\right)^2$ and $\theta^H = \theta^D = \left(1 - M^F\right)/2$. The previous modeling choices imply that there is a Metcalfe's network externality running on the side of the buyers which see their bargaining power increasing in a convex/squared way as more money enters the economy and their size increases, leading to a rising value of holding money over the transition and a rising value of the network. At the same time, there is no externality on the side of the sellers, and their size is chosen so that it is symmetric across the two types of sellers and equal to $\left(M^H + M^D\right)/2$ by information consistency because their type is private information at the match and the weight cannot condition on their individual size. The first order condition to the previous problem for any type i is

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

The value function for buyers under the fiat currency regime now is given by

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

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

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

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

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

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

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

To facilitate the analysis and make comparisons I also assume that the size of the money supply grows in a similar way as in the Bitcoin network. For the other two types of agents I assume that their sizes shrink by constant rates κ and $1-\kappa$ times the increase in the amount of money holders.

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

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

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

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. These equations define a system of eight equations in eight unknown paths.

3.1.1 Calibration

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 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. The next paragraphs provide an explanation for the parameter values.

Money Holders: The monthly discount rate is set to 0.004 which gives an annual rate of around 5%. The parameter σ that controls the curvature of the utility function is set at 0.5. This parameter is important for the efficiency part as we will see in the next section so a larger value of σ leaves more buyer surplus that can then fund the optimal transaction fees. The psychological cost for the buyer from transaction blocking is normalized at $z_1 = 1$. The speed of the money supply increase is set at $\delta^F = 0.03$, equal to the speed of money supply increase in the Bitcoin network.

Honest Sellers: The monthly discount rate is set at 0.004. The marginal cost of production η^H is set equal to 0.1. This level fixes the efficient quantity at $q^* = \eta^{-1/\sigma} = 100$. The probability of trading with buyers x^H is set at 0.2 implying mid-range matching efficiency of one out of five meetings. The individual cost of not being able to transact is set at $z_0^H = 0.75$ which is slightly lower than the buyer. The seller even if the transaction does not go through keeps the good in the end and this lowers his cost from transaction blocking. Finally, the speed of the cohort size κ is set at 0.646 which is pinned down by the initial split $\left[M^F(0), M^H(0), M^D(0)\right] = [0.02, 0.654, 0.326]$ and terminal split $\left[\bar{M}^F, \bar{M}^H, \bar{M}^D\right] = [0.8, 0.15, 0.05]$ which are chosen also in the Bitcoin regime. The parameter is given by $\kappa = \frac{M^H(0)-\bar{M}^H}{\bar{M}^F - M^F(0)}$.

Table 1: Fiat Currency Regime Parameter Values

Parameter	Description	Value
Money Holders		
σ	Utility Curvature	0.5
r	Monthly Discount Rate	0.004
z_1	Individual Cost from Transaction Blocking	1
δ^F	Speed of Money Supply / Cohort Size Increase	0.03
$M^F(0)$	Initial Cohort Size	0.02
$\bar{M}^F$	Terminal Cohort Size	0.8
Honest Sellers		
r	Monthly Discount Rate	0.004
η^H	Marginal Cost of Production of Specialized Good	0.1
x^H	Probability of Trading with Buyers	0.2
z_0^H	Individual Cost from Transaction Blocking	0.75
κ	Speed of Cohort Size Decrease	0.646
$M^H(0)$	Initial Cohort Size	0.654
$\bar{M}^H$	Terminal Cohort Size	0.15
Dishonest Sellers		
r	Monthly Discount Rate	0.004
η^D	Marginal Cost of Production of Specialized Good	0.1
x^D	Probability of Trading with Buyers	0.2
λ	Probability of Attempting Transaction Blocking	0.3
γ	Probability of Succeeding in Transaction Blocking	0.3
z_0^D	Individual Benefit from Transaction Blocking	0.4
ψ^D	Individual Cost from Transaction Blocking	0.08
$M^D(0)$	Initial Cohort Size	0.326
$\bar{M}^D$	Terminal Cohort Size	0.05

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.

Dishonest Sellers: The monthly discount rate is set at 0.004. The marginal cost of production and the probability of trading with buyers are symmetric with the honest sellers so $\eta^D = 0.1$ and $x^D = 0.2$. The probability of attacking is set at $\lambda = 0.3$ and the probability that the attack succeeds is set also at $\gamma = 0.3$. Only the probability of a successful attack $\lambda\gamma = 0.09$ matters for welfare. Under this specification one in eleven transactions are blocked. The friction is significant enough to matter for welfare but not too large to make the fiat equilibrium unsustainable. Moreover the justification of $\lambda = \gamma = 0.3$ is based on two facts about the global population: i) a large part of the global population is unbanked, estimated at around 1.3 billion[4] individuals, an access friction that complements transaction blocking and ii) around 5.8 billion[5] people live under autocratic regimes, and can potentially face significant hurdles in transactions, which means $0 << \lambda$ and $0 << \gamma$. The individual gain from a successful attack is set at $z_0^D = 0.4$ and the cost of attacking is set at $\psi^D = 0.08$. These two, together with γ imply that the benefit from attacking is positive $\gamma z_0^D - \psi^D = 0.04$. Moreover, $z_0^D = 0.4$ ensures a private gain from transaction blocking lower than the social costs $z_1 = 1$ and $z_0^H = 0.75$. Hence, attacks might be privately optimal, but they are socially costly.

3.1.2 Transitional Dynamics

The transitional dynamics are presented in Figure 7 under two different scenarios. In the first case the fiat monetary system is a new technology that allows trading of goods to take place creating dynamics between buyers and sellers. In the second case, the fiat currency system is an incumbent system that has reached maturity and operates at its steady state values. The split between those two cases will be helpful later when the fiat currency system is compared to Bitcoin.

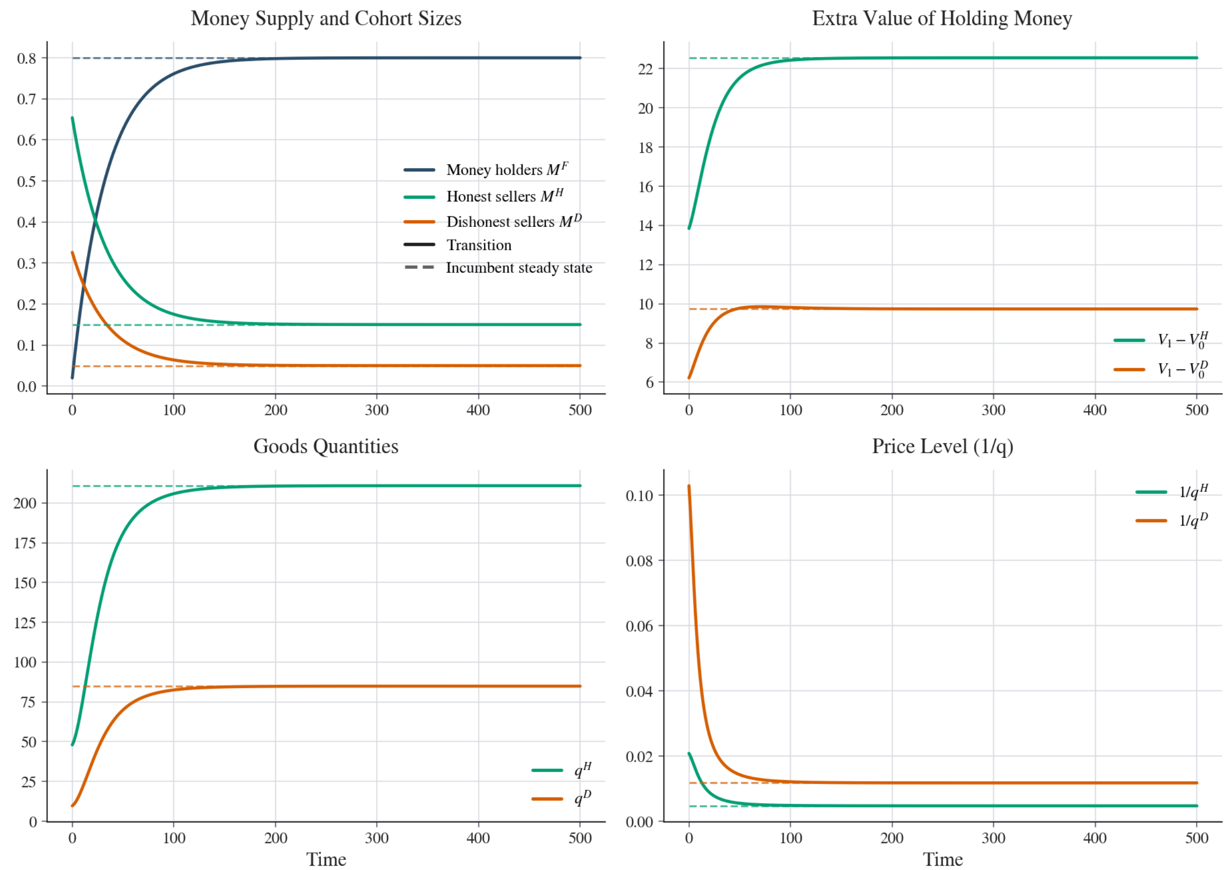
Starting from the case in which fiat currency is a new technology that allows trading of goods between buyers and sellers, we see that the money supply grows over time according to equation (3.7). At the same time the sizes of the cohorts of the sellers decline according to equations (3.8) and (3.9). The extra values of holding money relative to the honest and dishonest sellers increase initially fast and then slow down over time until they converge to their steady state value. These extra values are driven by the externality on the bargaining power of buyers and increase fast because initially money is scarce so being a participant in an economy that will soon be monetized carries a premium. 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 while the prices of goods naturally move to the opposite direction. In the second case in which fiat currency is an incumbent system that has reached maturity, all relevant variables remain at their steady state values.

For individual and social welfare we see that for all types of agents under the transition case welfare is hump-shaped. Initially welfare jumps and increases for some time and then declines towards the steady state value. For the buyers initially there is strong value in matching due to their increase in population size that leads to more bargaining power, but as the number of sellers declines over time the value of the buyers falls. For the sellers the hump-shaped values are driven by the dynamics of the extra value from holding money which initially rises fast, but then slows down. For all agents individual welfare overshoots the steady state

[4]See Klapper et al. (2025) for more details.

[5]See V-Dem Institute (2025) for more details.

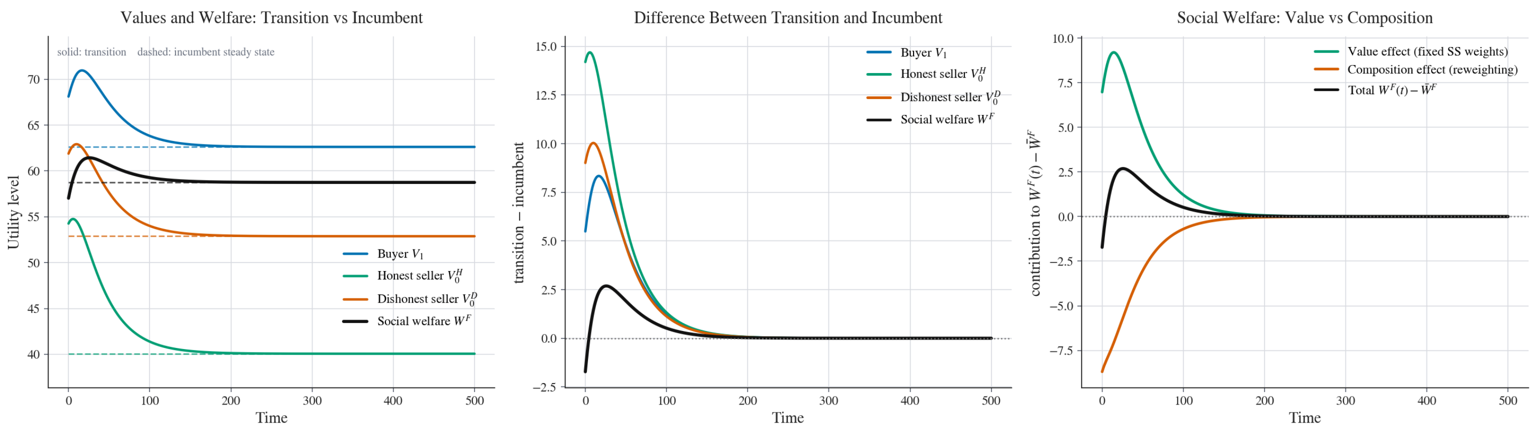
Figure 7: Transitional Dynamics in the Fiat Currency Regime



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^D that solve the Nash bargaining problem in (3.1). The lower right panel shows the path for the price level of the two goods $1/q^H$ and $1/q^D$. All panels include the case of fiat currency as an incumbent system that operates already at the steady state from the beginning.

value initially and then slowly declines towards steady state. However, social welfare still undershoots its steady state value initially, creating a Simpson's paradox in which while all individual values initially exceed their steady state values, their weighted average is still lower than its steady state value as shown clearly in the second panel of Figure 8. The explanation is given by the third panel where the movement in social welfare is decomposed into a value effect, where the sizes of cohorts are held constant and values change, and a composition effect where the values are held constant and the sizes of cohorts change. Initially the negative composition effect dominates the positive value effect because of the very small size of the buyers at 2% of total population, despite the strong positive value effect for every agent.

Figure 8: Welfare in the Fiat Currency Regime



Notes: The left panel 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 against the case in which the fiat currency regime starts and remains at its steady state. The center panel shows the difference in individual and social welfare under the two cases. The right panel decomposes the social welfare movement into a value effect, and a composition effect.

3.2 Bitcoin

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

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

Again $\theta_B^i = \theta_B = \left(M^B\right)^2$ and $\theta_H = \theta_D = \left(1 - M^B\right)/2$. The first order condition to the previous problem is

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

Recall that the value for the buyers is

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

The value for the honest sellers is

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

The value for the dishonest sellers is

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

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

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

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 $\{M^B, M^H, M^D, q^H, q^D, V_1, V_0^H, V_0^D\}$ 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. These equations define a system of eight equations in eight unknown paths.

3.2.1 Calibration

In this part I provide details about the calibration under the Bitcoin regime. Table 2 contains the parameter values. The next paragraphs provide an explanation for the values of the parameters not existing or not discussed in the fiat currency regime calibration.

Money Holders: The speed of the money supply increase is set at $\delta^B = 0.03$. At this value the model produces the concavity in the logarithm of the value of holding money and generates a hump-shaped individual mining effort for the miners which initially increase fast their mining effort, and later, as the economy approaches its steady state, mining rewards fade and tend to their very low steady state values that depend on the transaction fees. The parameter δ^B is not estimated by matching some data moment. The size of the initial cohort of money holders is set at $M^B(0) = 0.02$ in accord with the initial low adoption of the Bitcoin network. The steady state size of the buyers is set at $\bar{M}^B = 0.8$ which is a value corresponding to a mature network. The transaction fees are set equal to $f^H = f^D = 0.025$ which is 0.25% of the production cost at the efficient quantity $\eta^i q^* = 10$. These fees are small so they do not lead to a stop of trading, but are positive, to keep the network operating at the steady state. At the same time, small fees make the net welfare cost of mining at the steady state small, which allows the welfare comparison later to focus on the transaction blocking friction rather than fee effects.

Honest Sellers: The mining cost is set at $c_H = 0.1$. The mining cost sets the scale in which mining rewards are measured against and the chosen level ensures interior and strictly positive effort for the honest sellers. The initial size of the cohort is set at $M^H(0) = 0.654$ which makes the honest sellers around 2/3 of the total sellers. At the steady state, the size of the cohort is set at $\bar{M}^H = 0.15$ or 15% of the total population making the honest sellers 3/4 of the total sellers.

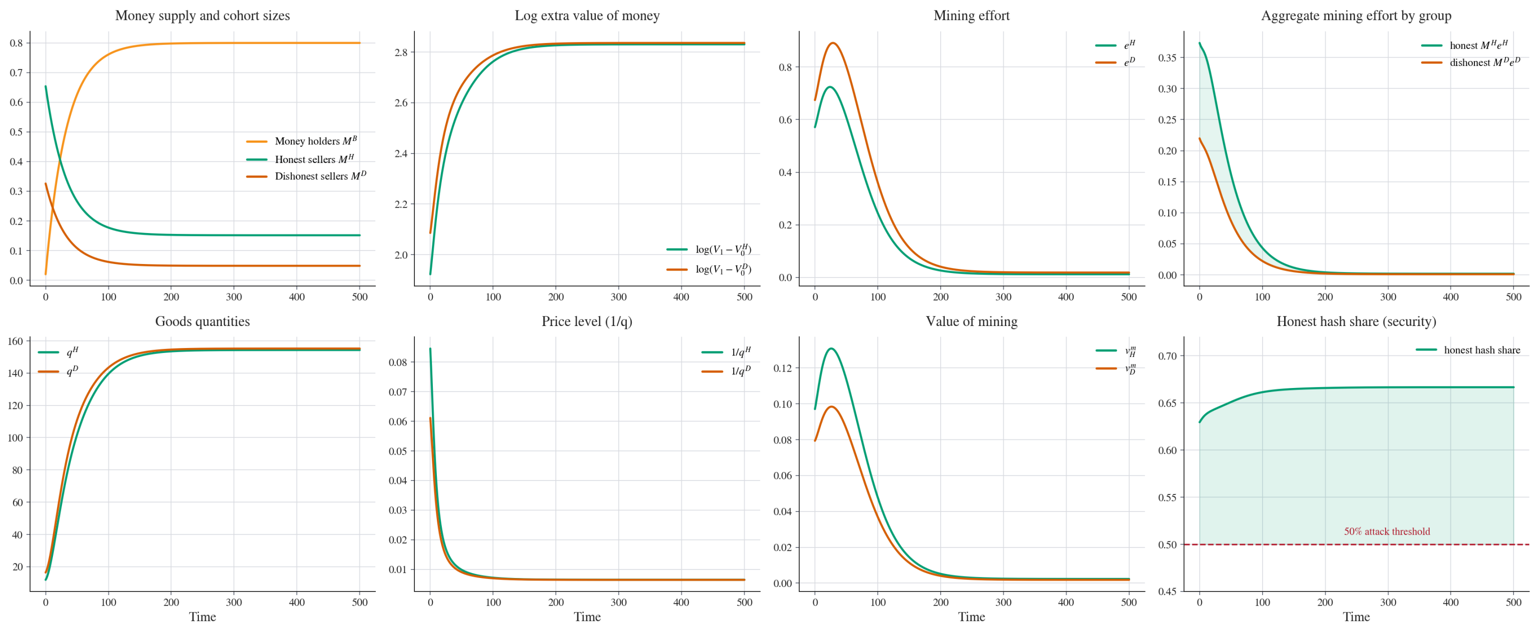
Table 2: Bitcoin Regime Parameter Values

Parameter	Description	Value
Money Holders		
σ	Utility Curvature	0.5
r	Monthly Discount Rate	0.004
z_1	Individual Cost from Transaction Blocking	1
δ^B	Speed of Cohort Size Increase	0.03
$M^B(0)$	Initial Cohort Size	0.02
$\bar{M}^B$	Terminal Cohort Size	0.8
f^H	Transaction Fee Paid to Honest Seller	0.025
f^D	Transaction Fee Paid to Dishonest Seller	0.025
Honest Sellers		
r	Monthly Discount Rate	0.004
η^H	Marginal Cost of Production of Specialized Good	0.1
x^H	Probability of Trading with Buyers	0.2
z_0^H	Individual Cost from Transaction Blocking	0.75
c_H	Marginal utility cost of mining	0.1
$M^H(0)$	Initial Cohort Size	0.654
$\bar{M}^H$	Terminal Cohort Size	0.15
Dishonest Sellers		
r	Monthly Discount Rate	0.004
η^D	Marginal Cost of Production of Specialized Good	0.1
x^D	Probability of Trading with Buyers	0.2
z_0^D	Individual Benefit from Transaction Blocking	0.4
ψ^D	Individual Cost from Transaction Blocking	0.08
c_D	Marginal utility cost of mining	0.2
$M^D(0)$	Initial Cohort Size	0.326
$\bar{M}^D$	Steady State Cohort Size	0.05

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.

Dishonest Sellers: The mining cost is set at $c_D = 0.2$. At this value, the ratio of mining costs is $c_D/c_H = 2$. At this level, the security condition for the Bitcoin network is more likely to hold. Indeed, as shown in the transitional dynamics, the Bitcoin network remains secure across the whole path, consistent with the fact that the Bitcoin network has never been hacked. The initial size of the cohort is set at $M^D(0) = 0.326$ which makes the dishonest sellers around 1/3 of the total sellers. At the steady state, the size of the cohort is

Figure 9: Transitional Dynamics in the Bitcoin Regime



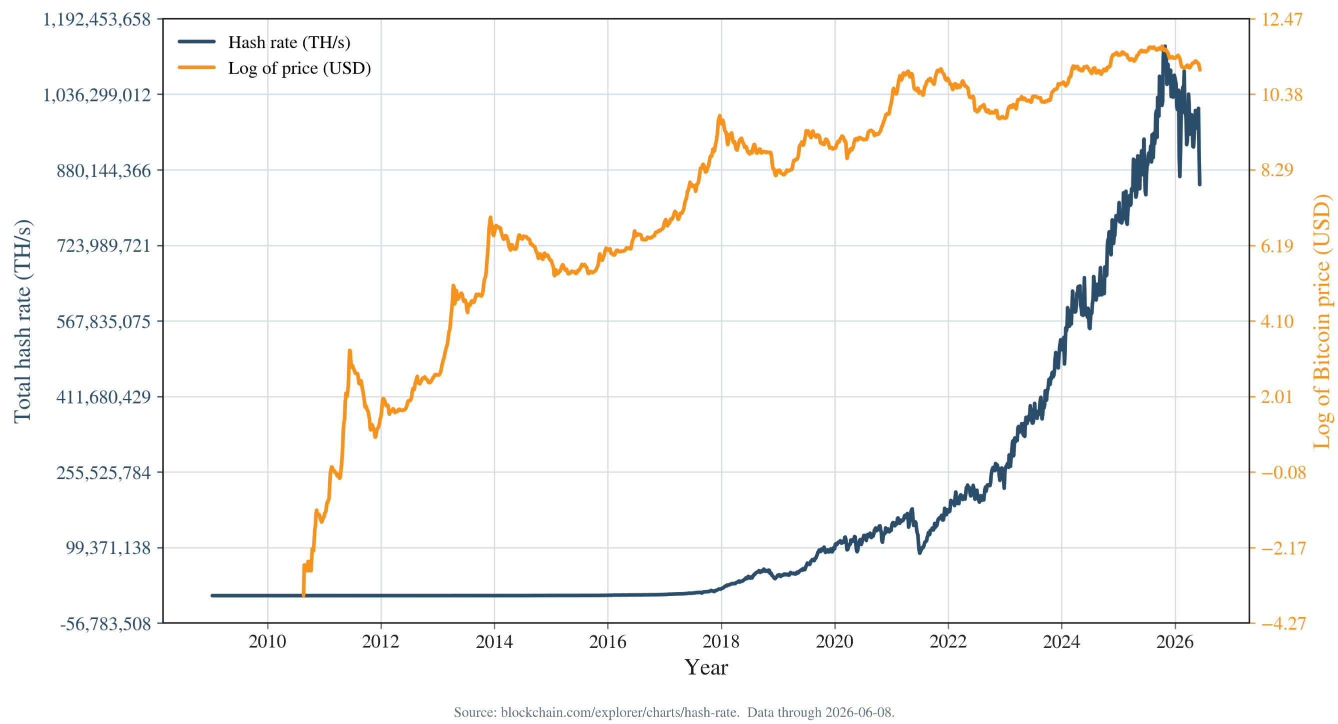
Notes: The upper left panel shows the transitional dynamics of the money supply and the sizes of various cohorts M^B, M^H and M^D. The upper second panel shows the transitional dynamics for the extra value of holding BTC relative to non-money holders $V_1 - V_0^H$ and $V_1 - V_0^D$. The upper third panel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

set at $\bar{M}^D = 0.05$ or 5% of the total population making the dishonest sellers 1/4 of the total sellers. The lower steady state level of this cohort reflects also the security of the Bitcoin network, which progressively discourages dishonest behavior.

3.2.2 Transitional Dynamics

The transitional dynamics under the Bitcoin regime are shown in Figure 9. The log of extra values of holding money again initially increase fast and then slow down over time and similarly for the quantities of the goods produced. The same intuition applies here as in the fiat currency case: being an early participant in an economy that soon will be monetized increases the value of money initially and then as the size of the sellers declines the increase is slower over time. This is qualitatively in line with the log of the Bitcoin price

Figure 10: 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.

behavior seen over the years as shown in Figure 10, which is a qualitative benchmark for the model, and contains data from Blockchain.com (2026) on the price behavior and the hash rate behavior since the early days of the Bitcoin network. But the model's value of holding money is measured in utility units, not in dollar terms so the comparison is about the shape and not about the levels.

As regards the mining efforts of the two types of miners, initially the mining efforts increase fast, but then reach a peak and start declining substantially, approaching a steady state value close to zero due to the low calibrated value of the transaction fees. Thus, the model qualitatively produces a response for the individual mining efforts that is in line with the initial substantial increase of the hash rate. During the transition, the mining effort is driven by the money rewards and the extra value of holding money, which also depends on the money supply. Once the money supply growth slows down significantly, the mining effort follows. The aggregate mining effort declines from the start of the transition since it is driven by the issuance of money which declines over time. In reality the increase in hash rate is now due to the improvements in hardware efficiency, which is not modeled here. Thus, the model speaks to the individual incentives to mine, and not to total hash output.

As seen in Figure 9, although individually the dishonest miners put more effort across the transition path, on aggregate the mining effort of the honest miners is always higher, keeping the Bitcoin network secure. Honest miners are a larger cohort across the transition path, so individually they do not need to put as much effort to outhash the dishonest miners. As regards the value of mining, this remains higher across the transition path for honest miners due to their assumed lower mining cost.

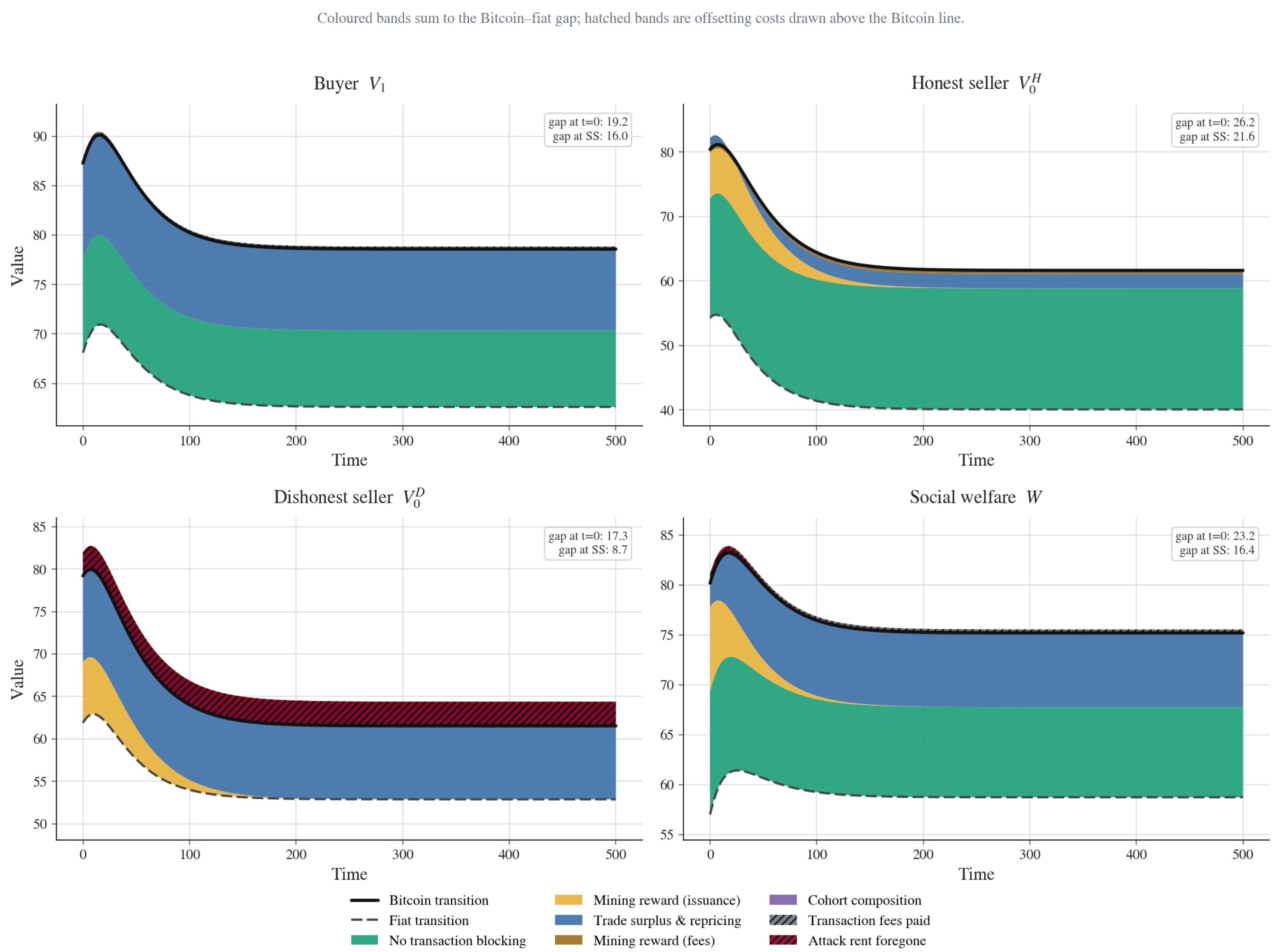
3.2.3 Welfare Comparison: Bitcoin vs. Fiat Currency

The previous subsections focused on the dynamics under different regimes, including fiat currency as an innovation that creates dynamics, fiat currency as an incumbent steady state system and Bitcoin as an innovation that creates dynamics. A question that arises naturally is what are the welfare differences for the various types of agents when using fiat currency or Bitcoin. Figure 11 provides the answer. Each panel contains the value of an agent, or the aggregate value in the fiat currency regime (dashed line) and in Bitcoin (solid line) under the assumption that both currencies are innovations and create dynamics.

The upper left panel shows that for the buyer the individual value is higher in the Bitcoin regime because transactions are not blocked anymore and because money is worth more in the Bitcoin regime, as expressed by the extra value of holding money, leading to higher quantities. The upper right panel shows that the value of an honest seller also increases in the Bitcoin regime. Again the main driver is the absence of transaction blocking. But the honest seller now earns also the mining reward from issuance and the mining reward from fees which also increase his welfare. The repricing effect is also positive in general, except for the very beginning, which seems to be a small negative general equilibrium effect. The lower left panel shows the same decomposition for the dishonest seller. The dishonest seller gains significantly from the higher value of money as well as the mining rewards and those gains would lead to an even higher value if there was not a loss associated with the loss of ability to block transactions. Then, the lower right panel of Figure 11 shows the decomposition for aggregate social welfare, which is just an aggregation of the previous three cases. The absence of transaction blocking, the higher value of Bitcoin and the mining rewards lead to higher social welfare under the Bitcoin regime. Moreover, the fact that every agent is better off across the whole transition path implies that the introduction of Bitcoin is a strict Pareto improvement, at least under the current calibration.

The Pareto improvement claim could be disproved by the welfare gap of the dishonest seller which could potentially become negative due to the loss of the attacking gain under Bitcoin. The welfare gap of the dishonest seller takes its lowest value at the steady state, therefore, as long as this gap is positive at the steady state the Pareto claim holds. This strengthens the ranking of Proposition 2 from a statement about social welfare to a statement about each agent individually.

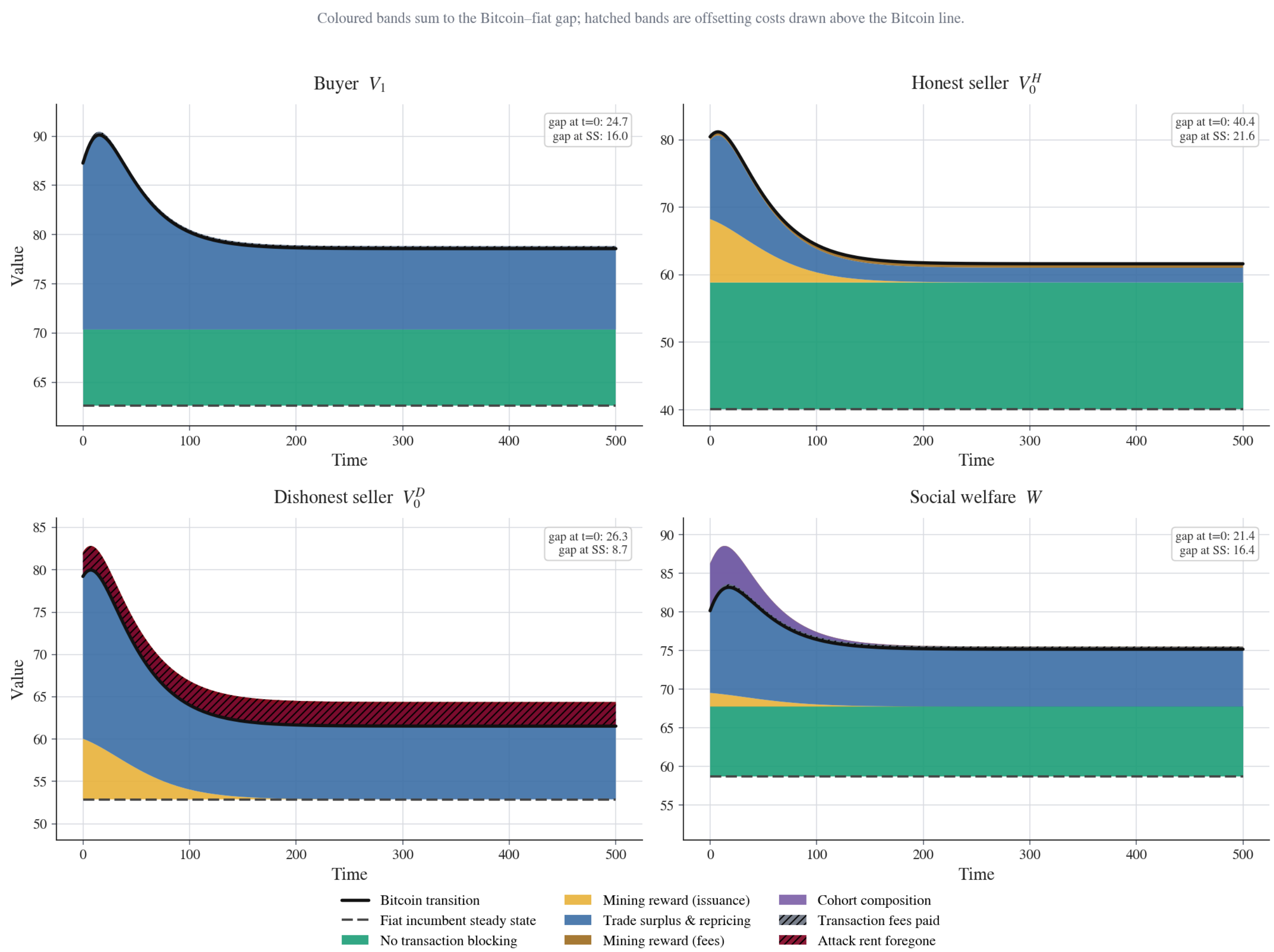
Figure 11: Welfare Dynamics and Welfare Gaps: Bitcoin vs. Fiat Currency (Transition Case)



Notes: The upper left panel shows the decomposition of the difference between the individual value of a buyer in the fiat currency regime and Bitcoin when both work as innovations and create dynamics. The upper right panel similarly shows the decomposition for the honest seller. The lower left panel shows the decomposition for the dishonest seller and the lower right panel shows the decomposition for aggregate welfare.

Figure 12 shows the same decomposition under the case in which fiat currency is steady state incumbent system without dynamics and Bitcoin enters as an innovation. Qualitatively, Figure 12 does not differ much from Figure 11. However, quantitatively, there are important differences between welfare in the initial periods exactly because now fiat currency is an incumbent system that has reached maturity so the initial jump in welfare from holding fiat currency does not exist anymore, leading to an even higher welfare gain from holding Bitcoin in the initial periods. Other than that, the absence of transaction blocking, the higher Bitcoin value and the gains from mining are again the main drivers of welfare differences. However, for social welfare

Figure 12: Welfare Dynamics and Welfare Gaps: Bitcoin vs. Fiat Currency (Incumbent Case)

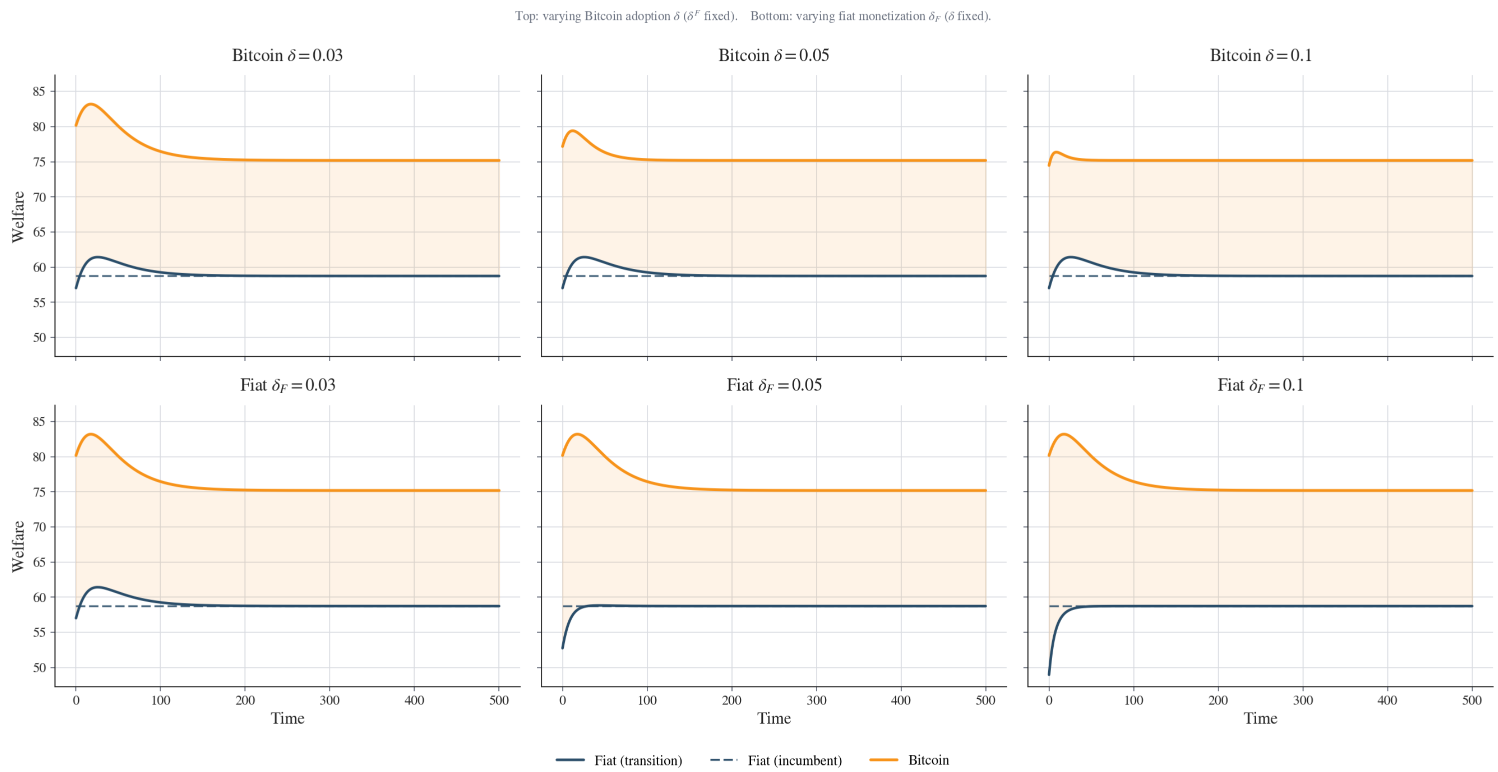


Notes: The upper left panel shows the decomposition of the difference between the individual value of a buyer in the fiat currency regime and Bitcoin when fiat currency works as an incumbent steady state system and Bitcoin works as an innovation and creates dynamics. The upper right panel similarly shows the decomposition for the honest seller. The lower left panel shows the decomposition for the dishonest seller and the lower right panel shows the decomposition for aggregate welfare.

we see that the composition of the cohorts also plays a role now. This is natural since the fiat currency regime is at its steady state and the sizes of cohorts do not change anymore with the buyers having the majority, while in the Bitcoin network there are fewer buyers in the beginning, so fewer agents with the highest values. However, this effect is not high enough to reverse the positive effect of Bitcoin on social welfare.

Figure 13 shows the social welfare gap between Bitcoin and fiat currency during the transition, under different money issuance speeds for the two regimes. It should be noted that in the Bitcoin regime parameter δ is not controlling only the issuance speed of the money supply but also the mining reward so it has a more

Figure 13: Social Welfare Gaps and Adoption Speeds



Notes: The upper line of panels compare social welfare over time in the fiat currency regime and in the Bitcoin regime for different values of the Bitcoin issuance speed δ and the lower line of panels do the same for different values of the fiat issuance speed δ^F.

complicated role, while in the fiat currency regime δ^F controls the degree of monetization only. In any case, it is evident from the panels that changing the issuance speed parameters does not lead to a case in which social welfare is higher under the fiat currency regime. In Bitcoin, higher δ increases adoption speed and shrinks the welfare overshoot. However, δ does not affect the steady state and in all cases social welfare ends up at the same level. In the fiat currency regime speeding up monetization brings the economy almost immediately at the steady state and leads to a strong undershooting of welfare initially. So, the money supply dynamics are not enough to overturn the improvement in social welfare from Bitcoin due to absence of transaction blocking, higher value of money and mining rewards.

Finally, it should be noted that a more definitive and complete answer about the two regimes would require the use of a richer model that 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.[6] 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.[7]

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

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

The first order conditions for the social planner are

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

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

[6]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.

[7]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.

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 quantities produced under the fiat currency regime q_F^i are determined by the steady state versions of (3.1). For these quantities to be equal to the quantities chosen by the social planner the ratios of bargaining power would have to be equal to

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

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

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. 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.[8] 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

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

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

[8] 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.

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

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

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

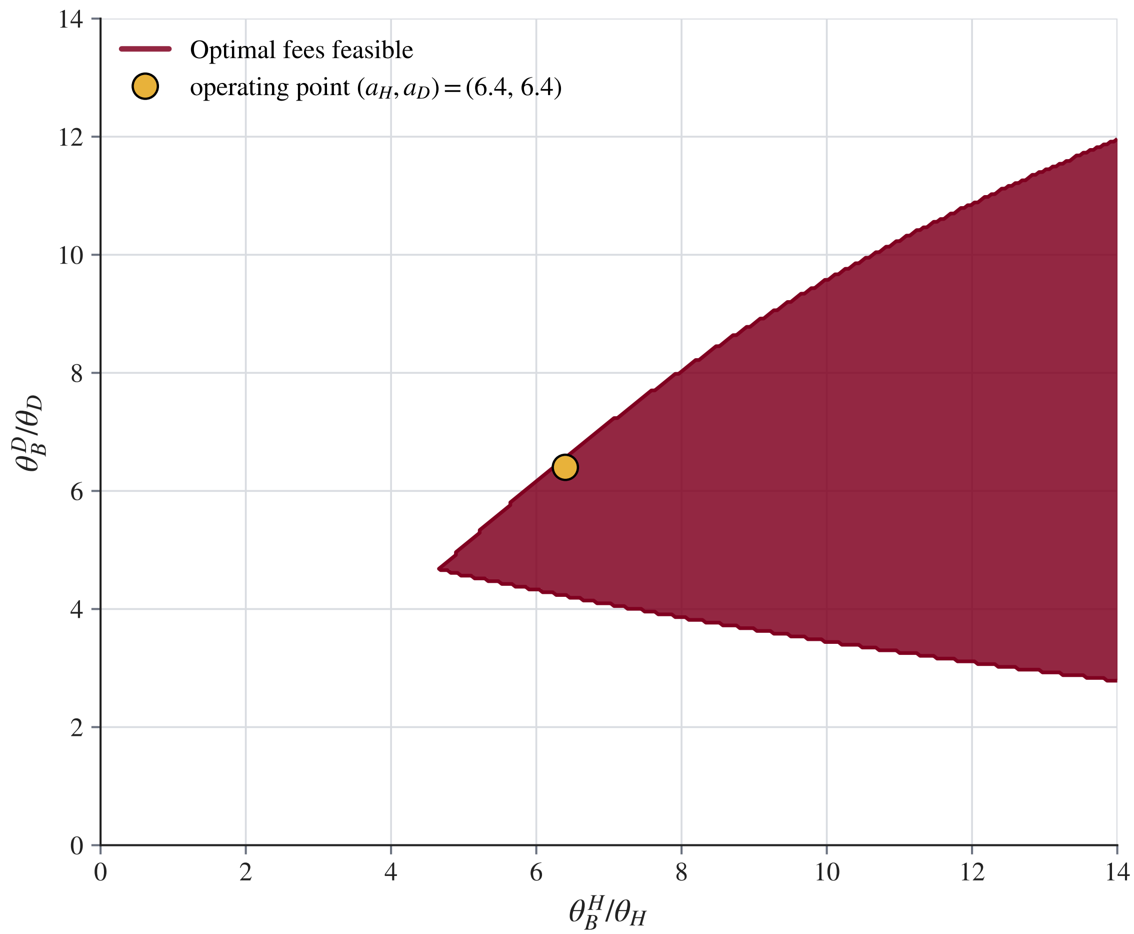
Equations (4.11)-(4.12) are evaluated at the socially optimal quantities chosen by the social planner. However, we need to ensure that the transaction fees satisfy the incentive constraints of the buyers and at the same time are positive in order to incentivize mining at the steady state. Starting from 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 helpful to build intuition, and for that reason the four equations are solved numerically and then the four unknown variables are

Figure 14: 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.

evaluated for different values of the two ratios of bargaining power. From Figure 14, 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. Moreover, the current calibration produces an equilibrium that belongs to the set of efficient equilibria.

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 schedule 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 log of the value of money and individual mining efforts that have a qualitatively similar shape to the log price of Bitcoin and the hash rate in the initial periods. As for social welfare, this is higher in the Bitcoin regime for each agent in the economy mainly due to the absence of transaction blocking costs and repricing for buyers and honest sellers and mainly due to repricing and mining rewards for dishonest sellers. Finally, the first best can be achieved in the Bitcoin network by optimally setting the transaction fees.

6 Declaration of Generative AI and AI-assisted Technologies

During the preparation of this work the author used Anthropic's Claude Opus 4.8 and Fable 5 in order to assist with developing and debugging the numerical code, producing and refining the figures, cross-checking the model's equations against the manuscript, and checking the manuscript for spelling mistakes. After using this tool, the author reviewed and edited the content as needed and takes full responsibility for the content of the published article.

References

Blockchain.com, 2026. URL https://Blockchain.com. 38

Chainalysis. The 2026 crypto crime report. Industry report, Chainalysis Inc., 2026. URL https://www.chainalysis.com/reports/crypto-crime-2026/. Accessed July 2026. 2

M. Choi and G. Rocheteau. Money mining and price dynamics. *American Economic Journal: Macroeconomics*, 13(4):246–294, 2021. 5

J. Cochrane. The fiscal theory of the price level. 2022. 43

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. 5

P. He, L. Huang, and R. Wright. Money and banking in search equilibrium. *International Economic Review*, 46 (2):637–670, 2005. 5

N. Kiyotaki and R. Wright. On money as a medium of exchange. *Journal of political Economy*, 97(4):927–954, 1989. 5

L. Klapper, D. Singer, L. Starita, and A. Norris. The global findex database 2025: Connectivity and financial inclusion in the digital economy. Technical report, World Bank, Washington, DC, 2025. URL http://hdl.handle.net/10986/43438. 31

A. Kyriazis. Quantitative easing and fiscal policy effectiveness. *Available at SSRN 4371287*, 2022. 43

R. Lagos and G. Rocheteau. Money and capital as competing media of exchange. *Journal of Economic theory*, 142(1):247–258, 2008. 5

E. M. Leeper. Equilibria under active and passive monetary and fiscal policies. *Journal of monetary Economics*, 27(1):129–147, 1991. 43

S. Lotz and F. Vasselin. A new monetarist model of fiat and e-money. *Economic Inquiry*, 57(1):498–514, 2019. 6

S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008. 5

L. Nuzzi, K. Waters, and M. Andrade. Breaking bft: Quantifying the cost to attack bitcoin and ethereum. *Available at SSRN*, 2024. 26

E. S. Pagnotta. Decentralizing money: Bitcoin prices and blockchain security. *The Review of Financial Studies*, 35(2):866–907, 2022. 5, 50

G. Rocheteau and A. Rodriguez-Lopez. Liquidity provision, interest rates, and unemployment. *Journal of Monetary Economics*, 65:80–101, 2014. 5

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. 5

V-Dem Institute. Democracy report 2025: 25 years of autocratization – democracy trumped? Technical report, University of Gothenburg, V-Dem Institute, 2025. 31

Appendix A: Robustness

This Appendix is about the robustness of the results presented in the main part of the paper. Several robustness checks are examined including a more general function for the successful transaction blocking attack or comparative statics with respect to different key parameters of the model.

A.1 Generalizing the Successful Attack Probability Function

In the main text, the probability of a successful transaction blocking attack is given by an indicator function such that the attack succeeds with probability 1 if the dishonest miners control the absolute majority of the total hash rate and fails if the honest miners control the absolute majority of total hash rate so that

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

In this part now I generalize the probability function for successful attacks following Pagnotta (2022) who models the security probability as

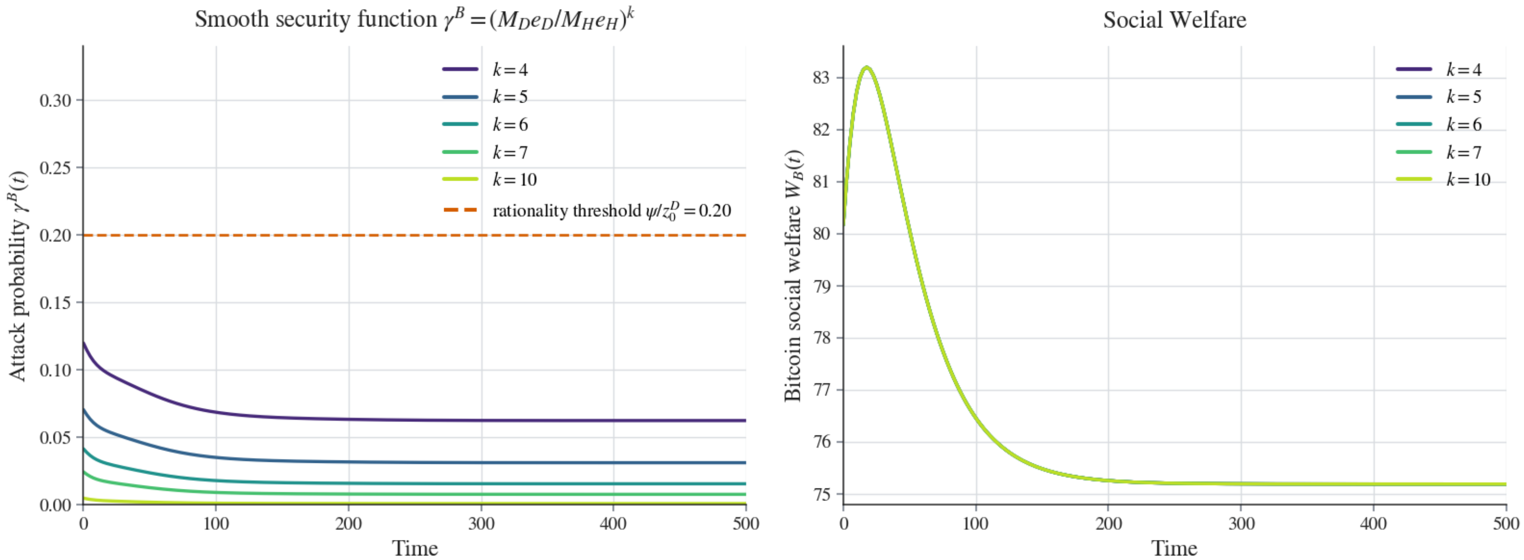
$$S\left(H_t, A\right) = \begin{cases} 1 - \left(\dfrac{A}{H_t}\right)^k & H_t \geq A \\ \\ 0 & \text{else.} \end{cases}$$

In the previous equation A is the exogenous hash rate budget of the attacker and H_t is the hash rate of honest actors, while k is the minimum fork length for collapse. Under this specification the Bitcoin network is not safe when honest miners control less than 50% of the mining effort. The successful attack probability is then given by $1 - S\left(H_t, A\right)$. There is a direct mapping to a successful transaction blocking probability given as

$$\gamma^B = \begin{cases} \left(\dfrac{M^D e_D}{M^H e_H}\right)^k & M^H e_H \geq M^D e_D \\ \\ 1 & \text{else.} \end{cases} \tag{A.1}$$

When compared to the security function used by Pagnotta (2022), we see now that the dishonest miners' hash rate is no longer exogenous and the security of the network is evaluated at equilibrium hash rate values, not exogenous ones. In addition, the assumption that individual miners do not internalize the effect of their actions on the probability of successful attack remains.

Figure A.1: Welfare in the Bitcoin Regime and Probability of Successful Attack



Notes: The left panel shows the probability of successful attack γ^B against the rationality threshold for different values of the parameter $k \geq 4$. The right panel shows the social welfare in the Bitcoin regime under the same values of k.

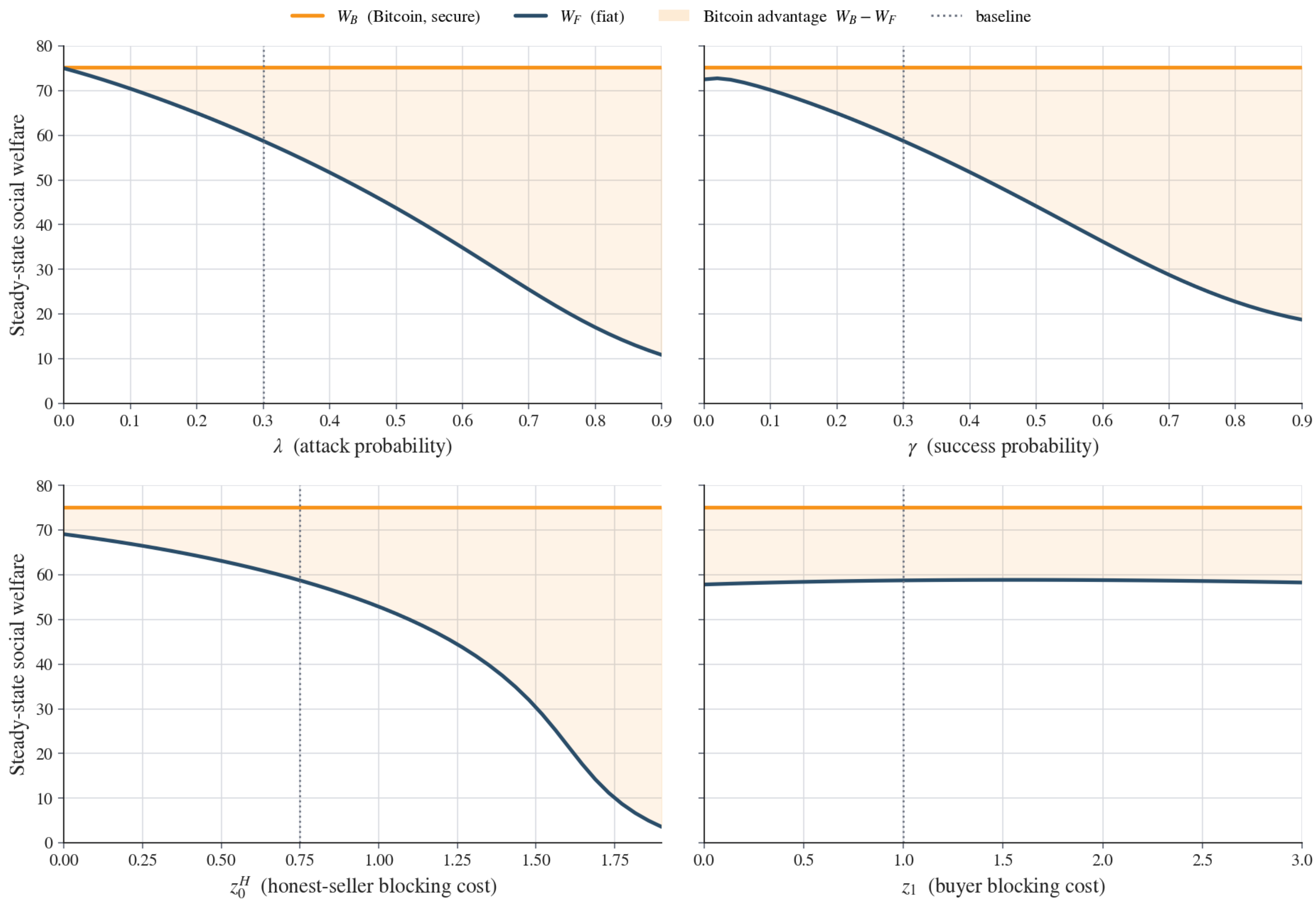
In equation (A.1) the role of k is crucial. Based on the lowest equilibrium split of $M^H e_H = 1.7 M^D e_D$ during the initial periods when the cohort of honest miners is the thinnest, the previous function gives $\gamma^B = \left(\frac{1}{1.7}\right)^k$. Attacks are not rational if $\gamma^B z_0^D < \psi^D$ implying that $\left(\frac{1}{1.7}\right)^k < \frac{\psi^D}{z_0^D} = 0.2$. The previous inequality implies that the Bitcoin network remains secure if $k \geq 4$. I will adopt this assumption for the rest of this subsection given that the Bitcoin network has remained safe over the years. For $k \geq 4$ we also have that $\lambda^B = 0$ because the attack is never profitable. Figure A.1 confirms the previous numerical analysis and shows that social welfare is invariant in k for $k \geq 4$.

Given that for $k \geq 4$ the network remains always secure, and given the assumed behavior of the miners to not internalize the effect of their individual decisions on the aggregate probability of successful transaction blocking, the model dynamics remain identical with the case of the indicator function for the probability of successful attack used in the main part. Hence, there is no need to reproduce the same graphs here.

A.2 Comparative Statics

In this section the focus is on comparative statics with respect to parameters of interest both at the steady state and outside of the steady state in the transition.

Figure A.2: Transaction Blocking Comparative Statics

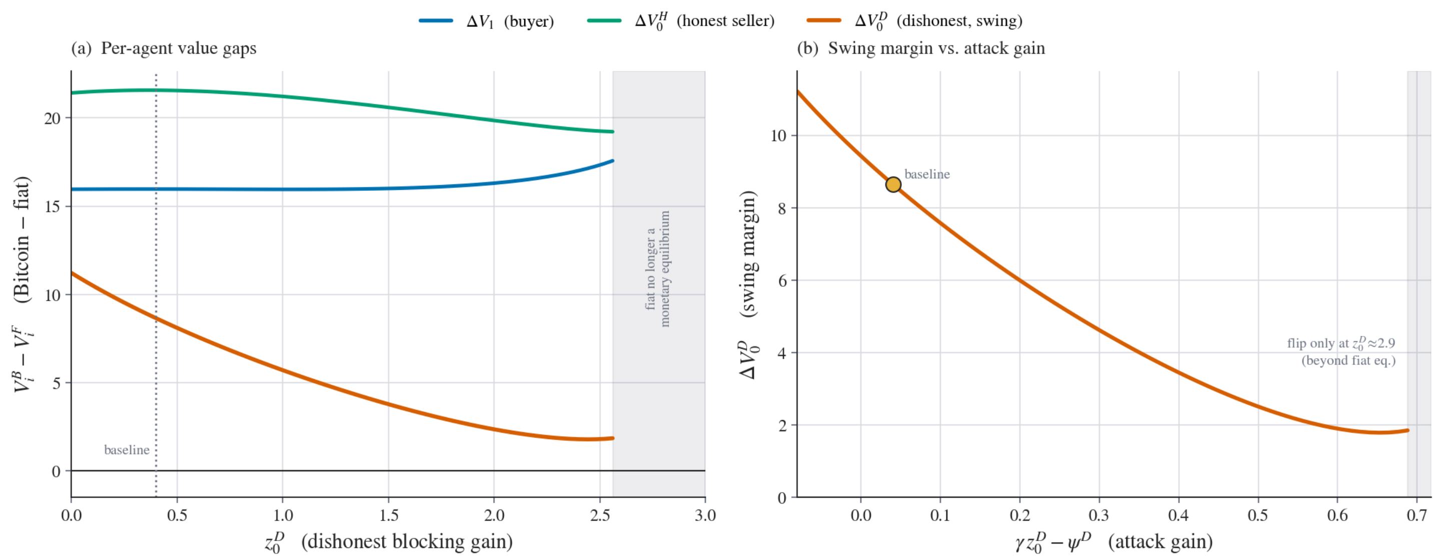


Notes: The upper left panel shows the steady state social welfare in the fiat currency regime and the Bitcoin regime for different values of the attack probability λ. The upper right panel makes the same comparison for the success probability γ. The lower left and lower right panels make the same comparison for the honest seller's transaction blocking cost z_0^H and the buyer's transaction blocking cost z_1.

A.2.1 Steady State

Transaction Blocking: We start the analysis at the steady state and focus on the parameters related to transaction blocking. The four parameters of interest are the attack probability λ and the success probability γ, the honest seller's cost from transaction blocking z_0^H and the buyer's cost from transaction blocking z_1. Figure A.2 shows how steady state social welfare changes as those parameters change in the two regimes. In the Bitcoin regime, social welfare is not affected by the change in the blocking parameters because Bitcoin remains secure by assumption at the steady state.

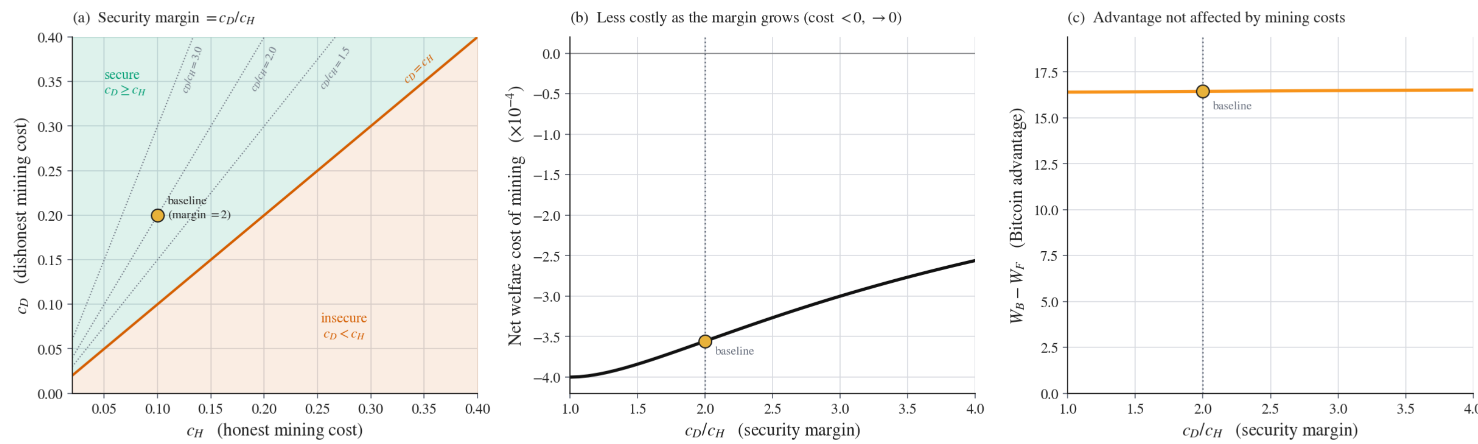
Figure A.3: Attack Gain Comparative Statics



Notes: The left panel shows the individual welfare gap for different agents across the two regimes for different values of the transaction blocking gross gain z_0^D while the right panel shows only the individual welfare gap for the dishonest sellers for different values of the net gain $\gamma z_0^D - \psi^D$.

For the fiat currency regime, social welfare decreases and falls more steeply as the probabilities related to transaction blocking increase and as the cost of the seller from transaction blocking increases. Higher values for these parameters imply more transaction blocking and more damage from transaction blocking respectively. As a result the gains from trade are lower and social welfare falls. Interestingly, the social welfare level in the fiat currency regime does not move lower as the transaction blocking cost for the buyer increases but it barely moves higher for intermediate values of z_1. Of course, the cost has a negative effect, but this negative effect is offset by other positive general equilibrium effects. Specifically, because of the Metcalfe-style bargaining power of the buyers $\theta_F = \left(M^F\right)^2 = 0.8^2 = 0.64$, the trades are oversized relative to the surplus maximizing quantity q^*, with $q^H \approx 200$ versus $q^* = 100$. So, a higher cost of blocking for the buyer tends to decrease the bargained quantity which tends to increase the value of the seller. This increase in the value of the honest seller offsets the decrease in the value of the buyer. In the case of an increasing z_0^H the value of the seller falls further and the extra value of the money holder increases leading to an even higher quantity produced by the seller but at a substantially lower surplus for him. The mechanism is clear by inspection of equation (3.6) in the main text. From the same equation z_0^H is multiplied by M^F which has a large value at the steady state, amplifying the already negative effect, while z_1 is multiplied by M^H that has a low value at the steady state keeping the overall effect from this parameter muted.

Figure A.4: Mining Costs Comparative Statics



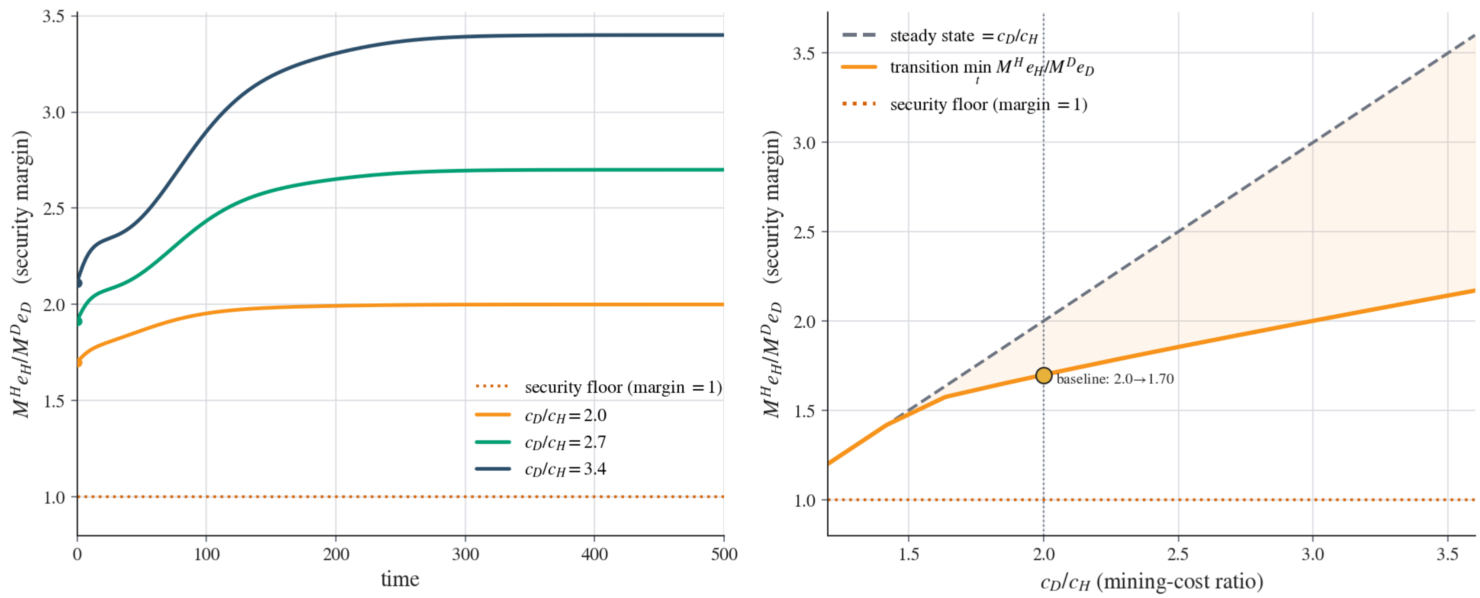
Notes: The left panel shows the security and the insecurity regions for different values of the mining costs. The panel in the middle shows the net welfare cost from mining at the steady state for different values of the mining marginal cost ratio c_D/c_H. The right panel shows the steady state social welfare gap between the two regimes for different values of the mining marginal cost ratio c_D/c_H.

Attack Gain: The left panel of Figure A.3 plots the difference between steady state individual welfare in the fiat currency regime versus the Bitcoin regime across different agents for different values of the blocking gain of the dishonest sellers z_0^D. The buyer and the honest seller prefer the Bitcoin regime as the gap sits comfortably above zero. For the dishonest sellers the gap still stays above zero for different values of z_0^D but the gap declines as z_0^D increases, which is expected. The right panel depicts again the welfare gap for the dishonest seller for different values of the net attack gain this time and this also remains positive. Overall, the fact that the Bitcoin welfare gap remains positive for all agents across all values of z_0^D for which the fiat currency regime reaches a monetary equilibrium implies that all agents become strictly better at the steady state by holding Bitcoin, even the dishonest sellers. So there is a Pareto improvement by holding Bitcoin at the steady state and this is quantitatively robust with respect to the gain of the dishonest seller in the fiat currency regime.

Mining Costs: Figure A.4 focuses on the comparative statics related to mining costs c_H and c_D. As mentioned in the main text, the Bitcoin network remains secure at the steady state if $c_D \geq c_H$. The left panel of Figure A.4 depicts the region in which this condition is satisfied as well the region in which this condition is not satisfied together with the steady state equilibrium from the baseline calibration.

The panel in the middle shows the net welfare cost of mining, as described in equation (2.43). This is negative and tiny at the steady state and tends to zero as the marginal cost ratio c_D/c_H increases. This happens because as c_D increases, the honest miners need to devote lower effort to secure the network because

Figure A.5: Mining Costs Comparative Statics



Notes: The left panel shows the security margin $M^H e_h / M^D e_D$ over the transition for different values of the mining marginal cost ratio c_D/c_H while the right panel shows the minimum security margin for each value of the mining marginal cost ratio across the transition path.

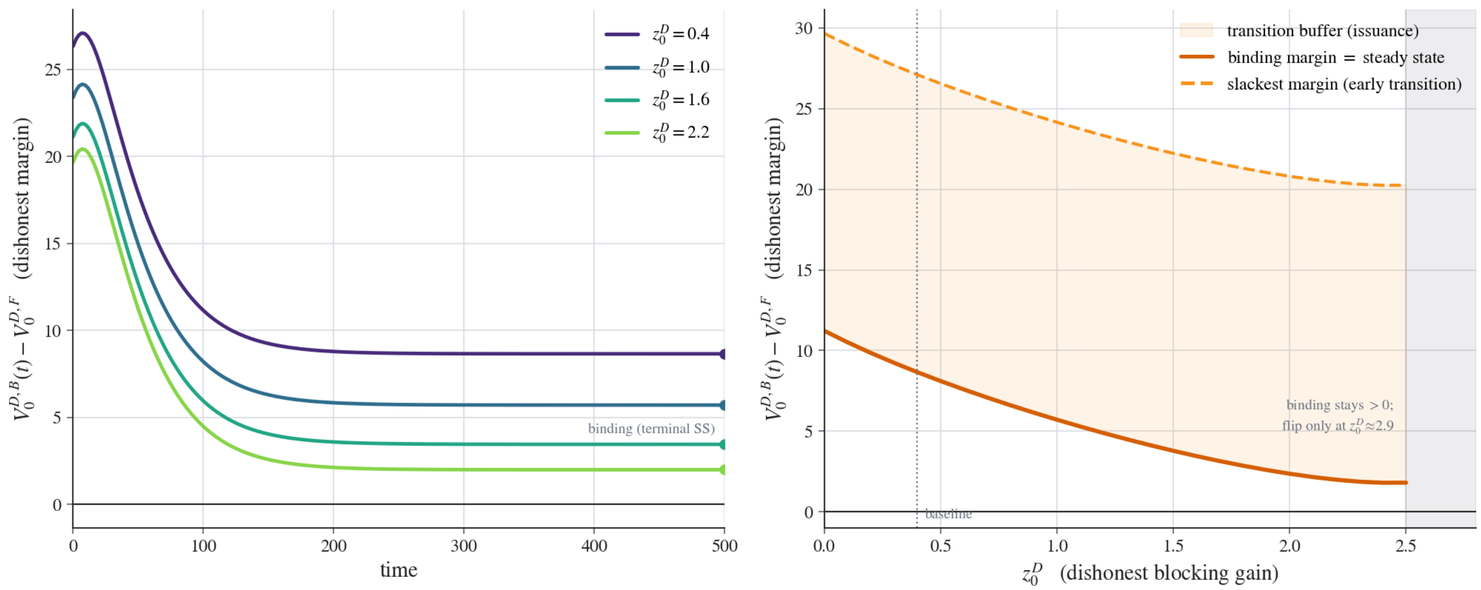
the higher cost for the dishonest miners disincentivizes higher effort levels for the dishonest miners. Lower total mining effort leads to lower waste of resources because of mining at the steady state. Recall that at the steady state mining is a costly redistribution scheme because no new money is produced. Steady state mining creates the most cost when $c_D = c_H$ exactly because at this point the competition between the two types of miners is very intense. Dishonest miners put more effort at this point since c_D is lower when it equals c_H, and honest miners have to put more mining effort as well to contest for the mining reward and keep the network secure.

Lastly, the panel on the right depicts the steady state social welfare gap for different values of the marginal cost ratio c_D/c_H and shows that this gap is not affected much by this ratio. The gap is driven mainly by transaction blocking and not by mining costs.

A.2.2 Transition

Mining Costs: We now turn to the comparative statics during the transition. Initially we focus on the mining costs. The left panel of Figure A.5 shows the security margin over the transition given by $M^H e_H / M^D e_D$ for different values of the mining cost ratio c_D/c_H. As the mining cost ratio increases, the security margin is

Figure A.6: Attack Gain Comparative Statics



Notes: The left panel shows the welfare gap for the dishonest seller under the two regimes over the transition path for different values of the gross attack gain z_0^D. The right panel shows the welfare gap range for the dishonest sellers, where the upper part of the range is the early large value of the margin from the left panel, while the lower part is the welfare margin evaluated at the steady state.

also higher across the whole transition. Each security margin curve has its lowest value in the initial period and then the curves tend over time to their steady state values c_D/c_H. The low value in the first period is the result of the lower relative majority of honest sellers versus dishonest sellers M^H/M^D. As the economy tends to the steady state, both M^H and M^D decline since the size of money holders increases, but the ratio M^H/M^D increases.

The right panel of Figure A.5 shows the minimum value of the security margin $M^H e_H / M^D e_D$ over the transition against the steady state margin c_D/c_H for different values of the mining cost ratio. Essentially, the panel shows the first point of each potential curve from the left panel versus the steady state mining cost ratio. This minimum value remains above one for every $c_D \geq c_H$. Hence, security is most at risk in the beginning of the adoption, which is also intuitive, but is never really compromised during the transition.

Attack Gains: As in the case of the steady state, we focus on the comparative statics related to the attack gain of the dishonest seller z_0^D but over the transition now. The left panel of Figure A.6 shows that the Bitcoin gap for the dishonest seller welfare is higher in the beginning of the transition because at this point the value of mining is very high, making the value of money high as well, and then the welfare gap falls towards its steady state value which is also the lowest value of the gap. But for every z_0^D considered such that there is still a monetary equilibrium in the fiat currency regime, the welfare gap remains positive across the whole transition path. So Bitcoin is making even the dishonest seller better off at all times, supporting the case of a Pareto improvement at least under the baseline calibration.

The right panel of Figure A.6 shows the range of the welfare margin. The lower part of the range is the welfare margin evaluated at the steady state lowest value for different values of z_0^D and the higher part of the range is the early large value of the margin. The margin remains positive across all values of z_0^D considered. This implies that the Pareto improvement for the dishonest seller is satisfied as long as there is improvement at the steady state which is the binding constraint. The transition adds slack to this condition.